# ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

## ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ


**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

# Κρυπτογραφία και κρυπτανάλυση από την αρχαιότητα μέχρι σήμερα


**ΚΑΡΑΜΟΛΕΓΚΟΥ ΑΝΝΑ-ΝΕΦΕΛΗ**

**ΑΜ: 09102154**


# Ψηφιακές υπογραφές


**ΚΟΡΔΟΝΟΥΡΗ ΑΛΕΞΑΝΔΡΑ**

**ΑΜ: 09102198**


ΝΟΕΜΒΡΙΟΣ 2011


ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΠΑΠΑΙΩΑΝΝΟΥ ΑΛΕΞΑΝΔΡΟΣ
ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:
ΠΑΠΑΙΩΑΝΝΟΥ ΑΛΕΞΑΝΔΡΟΣ
ΚΟΥΚΟΥΒΙΝΟΣ ΧΡΗΣΤΟΣ
ΣΤΕΦΑΝΕΑΣ ΠΕΤΡΟΣ

# ΠΕΡΙΕΧΟΜΕΝΑ

# ΠΡΟΛΟΓΟΣ

Η παρακάτω εργασία αναφέρεται στη διαχρονική εξέλιξη μεθόδων κρυπτογραφίας και κρυπτανάλυσης στις παρακάτω περιόδους και την συμβολή της κρυπτογραφίας τόσο κατά την περίοδο των πολέμων όσο και κατά την περίοδο της ειρήνης.

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά κρυπτός + γράφω και είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης, με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας.

Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για 2 ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη. Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη κρυπτός και τη λέξη λόγος και χωρίζεται σε δύο κλάδους : Την Κρυπτογραφία και την Κρυπτανάλυση.

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων, δηλαδή μετατροπή της πληροφορίας από μια κατανοητή μορφή σε ένα γρίφο, που χωρίς τη γνώση του κρυφού μετασχηματισμού θα παρέμενε ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στη γλωσσική δομή. Στις νεότερες μορφές κρυπτογραφίας η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών, στατιστική και συνδυαστική ανάλυση.

Η κρυπτογραφία έχει 4 βασικές λειτουργίες :

- Εμπιστευτικότητα : Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη και είναι ακατανόητη σε κάποιον τρίτο.
- Ακεραιότητα : Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.
- Μη απάρνηση : Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.
- Πιστοποίηση : Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Η ιστορία της κρυπτογραφίας μπορεί κατά προσέγγιση να διαιρεθεί σε 3 στάδια.

Στο πρώτο στάδιο οι διαδικασίες κρυπτογράφησης αφορούσαν τον τρόπο της έντυπης απεικόνισης (μελάνι και χαρτί). Έλαβαν τη μορφή αντικατάστασης και αναδιάταξης των γραμμάτων της αλφαβήτου.

Σαν δεύτερο στάδιο αναφέρεται αυτό των κρυπτογραφικών μηχανών, ιδίως στην περίοδο του Β΄ παγκοσμίου πολέμου(η γερμανική μηχανή Enigma).

Τελευταίο στάδιο θεωρείται το σύγχρονο κρυπτογραφικό σύστημα, απόρροια της αμοιβαίας αλληλεπίδρασης των μαθηματικών και των υπολογιστών ( οι υπολογιστές επέτρεψαν τη χρήση περιπλοκότερων αλγορίθμων κρυπτογράφησης και τα μαθηματικά προσέφεραν τον σχεδιασμό).

Χρονολογικά οι 3 περίοδοι της κρυπτογραφίας είναι:

- 1900 π.Χ – 1900 μ. Χ
- 1900 μ. Χ – 1950 μ. Χ
- 1950 μ. Χ – Σήμερα

Αρχαιότητα: Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων και οι οποίες στηρίζονταν στην ευφυΐα και την ευρηματικότητα των δημιουργών τους. Η απαρχή αυτών των μεθόδων και κατά συνέπεια της χρήσης της κρυπτογραφίας τοποθετείται από τους ιστορικούς περίπου στα 1900 π.Χ. στην αιγυπτιακή πόλη Menet-Khufu. Χαρακτηριστικά μέσα κρυπτογραφίας τη συγκεκριμένη εποχή είναι η

σκυτάλη, μια εφεύρεση των Σπαρτιατών, η δημιουργία ενός πίνακα ο οποίος αντιστοιχεί σε αριθμούς από τον Πολύβιο το 170 π.Χ, αλλά και το κρυπτοσύστημα αντικατάστασης του Καίσαρα τα οποία θα περιγραφούν αναλυτικά παρακάτω.

Μεσαίωνας: Στην διάρκεια του Μεσαίωνα, η κρυπτολογία όπως και όλες οι επιστήμες ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. Η εξέλιξη, τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Χαρακτηριστικό επίσης αυτής της εποχής είναι η εμφάνιση της πρώτης μηχανικής κρυπτοσυσκευής καθώς και η αποκρυπτογράφηση των αιγυπτιακών ιερογλυφικών. Γνωστότερος εκπρόσωπος της αραβικής κρυπτολογίας είναι ο Αλ Κιντί.

Περίοδος των δύο παγκοσμίων πολέμων: Η επόμενη περίοδος της κρυπτογραφίας τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950.Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους καθώς και το χρονικό διάστημα μεταξύ αυτών στο οποίο εντάσσεται η Οκτωβριανή επανάσταση. Εξαιτίας των πολέμων (λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά την μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών) αναπτύχθηκε η κρυπτογραφία τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές». Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά την διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη.

Ψυχρός Πόλεμος-Σήμερα: Η περίοδος αυτή ξεκινάει με τους πολέμους στην Κορέα και στο Βιετνάμ, ακολουθεί η κρίση στην Κούβα και η περίοδος περεστρόικας και καταλήγει στη σημερινή εποχή η οποία χαρακτηρίζεται από την έξαρση της ανάπτυξης στους επιστημονικούς κλάδους των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων. Η εποχή της σύγχρονης κρυπτογραφίας αρχίζει ουσιαστικά με τον Claude Shannon, αναμφισβήτητα ο πατέρας των μαθηματικών συστημάτων κρυπτογραφίας.

# ΚΕΦΑΛΑΙΟ 1

## *1.1. Ιστορική αναδρομή*

Κατά τη διάρκεια της αρχαιότητας η κρυπτογραφία ήταν αρκετά απλή και βασιζόταν σε αντικαταστάσεις γραμμάτων οι οποίες δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές αλλά στηρίζονταν στην ευρηματική σκέψη των δημιουργών τους. Όλα αυτά τα συστήματα έχουν στις μέρες μας κρυπταναλυθεί και έχει αποδειχθεί ότι, εάν είναι γνωστό ένα μεγάλο κομμάτι του κρυπτογραφημένου μηνύματος, τότε το αρχικό κείμενο μπορεί σχετικά εύκολα να επανακτηθεί.

Όπως προκύπτει από τους ιστορικούς η απαρχή της κρυπτογραφίας τοποθετείται περίπου στα 1900 π.Χ. στην αιγυπτιακή πόλη Menet-Khufu στις όχθες του Νείλου. Ένας γραμματέας φέρεται να χρησιμοποίησε περίεργα ιερογλυφικά όταν ανέγραφε την ιστορία του κύρη του, του Khnumhotep II. Παρόμοια ίχνη πρώιμης μορφής κρυπτογραφίας βρέθηκαν και σε άλλους πολιτισμούς όπως στις Ινδίες, τη Μεσοποταμία και στους Ασσύριους. Τότε για παράδειγμα χάραζαν μηνύματα υψηλής μυστικότητας στα ξυρισμένα κεφάλια των σκλάβων με τη μορφή τατουάζ και περίμεναν φυσικά μέχρι να μεγαλώσουν πάλι τα μαλλιά ή έκρυβαν μηνύματα στις κοιλιές λαγών που μεταφέρονταν από κυνηγούς.

Στην αρχαία Κίνα συνήθιζαν να γράφουν μηνύματα σε λεπτό μετάξι, το οποίο στη συνέχεια τοποθετούσαν σε μικροσκοπική σφαίρα, που καλυπτόταν τελικά με κερί. Ο αγγελιοφόρος που επιφορτιζόταν με τη μεταφορά του μηνύματος κατάπινε την κέρινη σφαίρα. Ακόμη σε σημαντικά αρχαία λογοτεχνικά και θρησκευτικά κείμενα είναι εμφανής η χρήση της κρυπτογραφίας.

Στην Παλαιά Διαθήκη για παράδειγμα ο προφήτης Ηλίας αναφέρεται στη Βαβυλώνα με τη λέξη Seshach και στο Κασμίτ με τη λέξη Leb Kamai. Ο καθηγητής Elijahu Risp ανακάλυψε ότι τα αυθεντικά κείμενα της Παλαιάς Διαθήκης διέπονται από ένα κώδικα, το λεγόμενο Κώδικα της Βίβλου, η αποκρυπτογράφηση του οποίου αποκαλύπτει με προφητικό τρόπο σημαντικά γεγονότα στη διάρκεια της ανθρώπινης ιστορίας. Οι βιβλικές προφητείες προκύπτουν μετά από αναζήτηση ακολουθιών γραμμάτων που απέχουν ίσες αποστάσεις.

Ένα ακόμη στοιχείο χρήσης της κρυπτογραφίας και από άλλους πολιτισμούς είναι μία μικρή σφηνοειδής επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο (με βάση τον Kahn). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση την μέθοδο της αντικατάστασης. Όπως αναφέρει ο Πλούταρχος, η «Σπαρτιατική Σκυτάλη» ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Μια άλλη μορφή κρυπτογράφησης είναι η υποκατάσταση.

Μία από τις αρχαιότερες περιγραφές κρυπτογράφησης με υποκατάσταση εμφανίζεται στα Κάμα Σούτρα, ένα κείμενο που το έγραψε τον $4^{ο}$ μ.Χ. αιώνα ο λόγιος Βατσιαγιάννα, ο οποίος όμως βασίστηκε σε χειρόγραφα αναγόμενα στον $4^{ο}$ αιώνα π.Χ. Τα Κάμα Σούτρα συνιστούν στις γυναίκες να μελετούν 64 τέχνες όπως η μαγειρική, η ενδυματολογία, οι μαλάξεις και η αρωματοποιία. Ο κατάλογος περιλαμβάνει και κάποιες τέχνες λιγότερο εμφανείς όπως ο εξορκισμός και το σκάκι. Στην $45^{η}$ θέση του καταλόγου αυτού συναντάμε τη μιλεχίτα βικάλπα, την τέχνη της μυστικής γραφής που προτείνεται στις γυναίκες για να μπορούν να κρύβουν τις λεπτομέρειες των ερωτικών τους δεσμών. Μία από τις συνιστώμενες τεχνικές είναι να ζευγαρώνεις τυχαία τα γράμματα του αλφαβήτου και στη συνέχεια να αντικαθιστάς κάθε γράμμα του

αρχικού μηνύματος με το ταίρι του. Αυτή η μορφή μυστικής γραφής αποκαλείται κρυπτόγραμμα υποκατάστασης.

Η πρώτη τεκμηριωμένη χρήση κρυπτογράμματος υποκατάστασης για στρατιωτικούς σκοπούς εμφανίζεται στους Γαλατικούς πολέμους του Ιούλιου Καίσαρα. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται 3 θέσεις μετά, στο Λατινικό Αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα.

Είναι εμφανές ότι εκτός από τη μετάθεση 3 θέσεων, αν χρησιμοποιήσουμε οποιαδήποτε μετάθεση μεταξύ 1 και 23 θέσεων, μπορούμε να δημιουργήσουμε 23 ξεχωριστά κρυπτογράμματα. Στην πραγματικότητα αν δεν περιοριστούμε στη μετάθεση των γραμμάτων του αλφαβήτου αλλά επιτρέψουμε στο κρυπτογραφικό αλφάβητο να προκύψει από οποιαδήποτε αναδιάταξη του κανονικού, τότε μπορούμε να δημιουργήσουμε πολύ περισσότερα ξεχωριστά κρυπτογράμματα. Υπάρχουν πάνω από 400.000.000.000.000.000.000.000.000 τέτοιες αναδιατάξεις, και άρα ανάλογος αριθμός ξεχωριστών κρυπτογραμμάτων. Κάθε ξεχωριστό κρυπτόγραμμα μπορεί να θεωρηθεί ότι προκύπτει από μια γενική κρυπτογραφική μέθοδο, γνωστή ως αλγόριθμο, και από ένα κλειδί, το οποίο εξειδικεύει τις ακριβείς λεπτομέρειες της συγκεκριμένης κρυπτογράφησης. Το κλειδί καθορίζει το ακριβές κρυπτογραφικό αλφάβητο (το οποίο προκύπτει από οποιαδήποτε αναδιάταξη του κανονικού) που πρέπει να χρησιμοποιηθεί για μια συγκεκριμένη κρυπτογράφηση. Η σπουδαιότητα του κλειδιού σε αντιδιαστολή με τον αλγόριθμο, είναι μια σταθερή αρχή της κρυπτογραφίας.

Ο Καίσαρας χρησιμοποίησε και άλλα, πιο πολύπλοκα συστήματα κρυπτογράφησης, για τα οποία έγραψε ένα βιβλίο ο Valerius Probus, το οποίο δυστυχώς δεν διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες. Πολλοί αρχαίοι μελετητές θεωρούσαν το κρυπτόγραμμα υποκατάστασης απαραβίαστο, χάρη στον κολοσσιαίο αριθμό πιθανών κλειδιών, και επί αιώνες αυτό έμοιαζε να είναι αληθές. Ωστόσο οι κωδικοθραύστες θα έβρισκαν εντέλει μια σύντομη οδό για τη διαδικασία διεξοδικού ελέγχου όλων των κλειδιών. Αντί να χρειάζονται δισεκατομμύρια χρόνια για να σπάσει ένα κρυπτόγραμμα, η σύντομη οδός μπορούσε να αποκαλύψει το μήνυμα εντός λεπτών. Το επίτευγμα αυτό συνέβη στην Ανατολή και απαίτησε ένα λαμπρό συνδυασμό γλωσσολογίας, στατιστικής και θρησκευτικής αφοσίωσης.

Στην διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συντέλεσε στην καθυστέρηση της ανάπτυξης της. Η εξέλιξη, τόσο της κρυπτολογίας, όπως και των μαθηματικών, συνεχίζεται στον Αραβικό κόσμο.

Ο πλούτος του ισλαμικού πολιτισμού ήταν κατά ένα μεγάλο μέρος αποτέλεσμα μιας εύπορης και ειρηνικής κοινωνίας, η οποία στηριζόταν σε ένα αποτελεσματικό σύστημα διοίκησης, οι διοικούντες του οποίου με τη σειρά τους στηρίζονταν στην ασφαλή επικοινωνία που επιτυγχανόταν με τη χρήση της κρυπτογραφίας. Είναι τεκμηριωμένο ότι οι αξιωματούχοι κρυπτογραφούσαν τις ευαίσθητες κρατικές υποθέσεις, αλλά και προστάτευαν τα φορολογικά αρχεία επιδεικνύοντας ευρύτατη και καθημερινή χρήση της κρυπτογραφίας. Τα διοικητικά στελέχη εκτός από ένα κρυπτογραφικό αλφάβητο το οποίο ήταν μια αναδιάταξη του κανονικού, όπως περιγράφηκε πιο πάνω, χρησιμοποιούσαν και κρυπτογραφικά αλφάβητα που περιείχαν άλλους τύπους συμβόλων. Μονοαλφαβητικό κρυπτόγραμμα υποκατάστασης είναι η γενική ονομασία που δίνεται σε οποιοδήποτε κρυπτόγραμμα υποκατάστασης στο οποίο το κρυπτογραφικό αλφάβητο αποτελείται είτε από γράμματα είτε από σύμβολα ή από μείγμα και των δύο.

Οι Άραβες λόγιοι, εκτός από το να χρησιμοποιούν κρυπτογράμματα ήταν έμπειροι και στο να τα σπάζουν. Αυτοί επινόησαν την κρυπτανάλυση, την επιστήμη της αποκρυπτογράφησης ενός μηνύματος χωρίς γνώση του κλειδιού. Οι Άραβες κρυπταναλυτές κατόρθωσαν να βρουν μια μέθοδο για να σπάζουν το μονοαλφαβητικό κρυπτόγραμμα υποκατάστασης που επί αιώνες παρέμενε απαραβίαστο. Όπως όλοι οι Μουσουλμάνοι έτσι και οι Άραβες ήταν υποχρεωμένοι να αναζητούν τη γνώση σε όλες τις μορφές της. Έτσι στην προσπάθειά τους να αποκτήσουν τις γνώσεις των παλιότερων πολιτισμών, συγκέντρωναν αιγυπτιακά, βαβυλωνιακά , κινέζικα, περσικά, εβραικά και ρωμαικά κείμενα και τα μετέφραζαν στα αραβικά. Ταυτόχρονα με τη συλλογή της γνώσης, ο ισλαμικός πολιτισμός ήταν σε θέση να τη διδάξει χάρη στην τέχνη παρασκευής χαρτιού που είχαν διδαχθεί από τους Κινέζους η οποία γέννησε την εκδοτική παραγωγή.

Προυπόθεση για την επινόηση της κρυπτανάλυσης δεν ήταν μόνο η πληρέστερη κατανόηση των κοσμικών ζητημάτων, αλλά και η ανάπτυξη θρησκευτικών σπουδών. Λόγω του ενδιαφέροντος να καθορίσουν τη χρονολογική σειρά των αποκαλύψεων μετρούσαν τη συχνότητα εμφάνισης των λέξεων που

περιείχε κάθε αποκάλυψη. Η θεωρία ήταν ότι ορισμένες λέξεις είχαν εξελιχτεί σχετικά πρόσφατα και άρα αν μια αποκάλυψη περιείχε μεγάλο αριθμό τέτοιων λέξεων, αυτό θα μπορούσε να αποτελεί ένδειξη ότι είναι μεταγενέστερη χρονολογικά. Μελετούσαν επίσης την ετυμολογία των λέξεων και τη δομή των φράσεων για να ελέγξουν αν τα συγκεκριμένα κείμενα συμφωνούσαν με τα γλωσσικά σχήματα του Προφήτη. Η έρευνα όμως δεν σταματούσε στο επίπεδο των λέξεων, αλλά συνεχιζόταν και στην ανάλυση των επιμέρους γραμμάτων, με αποτέλεσμα να παρατηρήσουν ότι ορισμένα γράμματα ήταν πιο κοινά από άλλα. Αυτή η φαινομενικά ανώδυνη παρατήρηση οδήγησε τελικά στην πρώτη μεγάλη πρόοδο στην κρυπτανάλυση. Η παλαιότερη γνωστή περιγραφή της συγκεκριμένης τεχνικής ανήκει στον επιστήμονα Αλ-Κιντί η θεωρία του οποίου είναι πιο εύκολο να εξηγηθεί με βάση το ελληνικό αλφάβητο.

Είναι απαραίτητο να μελετήσουμε ένα εκτενές κανονικό κείμενο, ίσως και περισσότερα για να καθορίσουμε τη συχνότητα εμφάνισης κάθε γράμματος του αλφαβήτου. Στα ελληνικά το πιο κοινό γράμμα είναι το α, και ακολουθεί το ο, το τα κ.ο.κ όπως φαίνεται στον παρακάτω πίνακα 1. Στη συνέχεια εξετάζουμε το κρυπτογραφικό κείμενο που μας ενδιαφέρει και βρίσκουμε τη συχνότητα εμφάνισης κάθε γράμματος. Αν λοιπόν για παράδειγμα το πιο κοινό γράμμα στο κρυπτογραφικό αλφάβητο είναι το χ, τότε πιθανότατα αυτό να έχει αντικαταστήσει το α. Ομοίως, αν το δεύτερο σε συχνότητα γράμμα στο κρυπτογραφικό κείμενο είναι το ν, τότε πιθανότατα έχει αντικαταστήσει το ο κ.ο.κ. Η τεχνική αυτή είναι γνωστή ως ανάλυση συχνότητας και δείχνει ότι δεν είναι απαραίτητο να ελέγξουμε καθένα από τα δισεκατομμύρια πιθανά κλειδιά, αλλά μπορούμε να αποκαλύψουμε το περιεχόμενο ενός κρυπτογραφημένου μηνύματος αναλύοντας απλώς τη συχνότητα των χαρακτήρων στο κρυπτογραφικό κείμενο. Πρέπει ωστόσο να σημειωθεί ότι δεν είναι δυνατόν να εφαρμόσουμε αυτή τη τεχνική σε όλες τις περιπτώσεις, καθώς ο κατάλογος συχνοτήτων του παρακάτω πίνακα είναι απλώς ένας μέσος όρος και δεν ανταποκρίνεται επακριβώς στις συχνότητες κάθε κειμένου. Γενικά ισχύει ότι τα σύντομα κείμενα έχουν μεγάλες πιθανότητες να αποκλίνουν σημαντικά από τις μέσες συχνότητες και κυρίως αυτά που περιλαμβάνουν λιγότερα από 100 γράμματα. Αντίθετα, τα εκτενέστερα κείμενα είναι πιο πιθανό να ακολουθούν τις συνήθεις συχνότητες χωρίς αυτό να συμβαίνει πάντα.

Όπως είδαμε λοιπόν η τεχνική της ανάλυσης συχνοτήτων απαιτεί λογική σκέψη αλλά συγχρόνως προϋποθέτει πονηριά, ενόραση, προσαρμοστικότητα και μαντικές ικανότητες.

**ΠΙΝΑΚΑΣ 1**

| Γράμμα | Συχνότητα εμφάνισης (%) | Γράμμα | Συχνότητα εμφάνισης (%) |
|---|---|---|---|
| α | 12 | ν | 7.9 |
| β | 0.8 | ξ | 0.6 |
| γ | 2 | ο | 9.8 |
| δ | 1.7 | π | 5.024 |
| ε | 8 | ρ | 5.009 |
| ζ | 0.5 | σ | 4.9 |
| η | 2.9 | τα | 9.1 |
| θ | 1.3 | υ | 4.3 |
| ι | 7.8 | φ | 1.2 |
| κ | 4.2 | χ | 1.4 |
| λ | 3.3 | ψ | 0.2 |
| μ | 4.4 | ω | 1.6 |

Όσο οι Άραβες λόγιοι γνώριζαν μία περίοδο άνθησης και πνευματικών επιτευγμάτων, η Ευρώπη ήταν καθηλωμένη στο Μεσαίωνα. Ενώ ο Αλ-Κιντί περιέγραφε την επινόηση της κρυπτανάλυσης, οι Ευρωπαίοι ακόμη πάλευαν με τις βασικές αρχές της κρυπτογραφίας. Τα μόνα ευρωπαϊκά ιδρύματα που ενθάρρυναν τη μελέτη της μυστικής γραφής ήταν τα μοναστήρια, όπου οι μοναχοί μελετούσαν τη Βίβλο αναζητώντας κρυφά μηνύματα, ένα πάθος που συνεχίστηκε ως τη σύγχρονη εποχή. Οι μοναχοί του Μεσαίωνα προβληματίζονταν από το γεγονός ότι η Παλαιά Διαθήκη περιέχει παραδείγματα εμφανούς και ηθελημένης κρυπτογραφίας. Για παράδειγμα, περιλαμβάνει κείμενα κρυπτογραφημένα με ένα παραδοσιακό εβραϊκό κρυπτοσύστημα υποκατάστασης, το ατμπάς.

Το ατμπάς λειτουργεί ως εξής: για κάθε γράμμα υπολογίζουμε τις θέσεις που απέχει από την αρχή του αλφαβήτου και το αντικαθιστούμε με το γράμμα εκείνο που απέχει ίδια απόσταση από το τέλος του αλφαβήτου. Στα ελληνικά αυτό θα ισοδυναμούσε με αντικατάσταση του πρώτου γράμματος (α) με το τελευταίο, (ω), του δεύτερου (β), με το δεύτερο από το τέλος (ψ) κ.ο.κ. Το ατμπάς και άλλα παρόμοια κρυπτοσυστήματα είχαν κατά πάσα πιθανότητα σκοπό απλώς να προσθέσουν μυστήριο και όχι να αποκρύψουν το νόημα των γραφομένων, στάθηκαν όμως αρκετά για να πυροδοτήσουν το ενδιαφέρον για τη σοβαρή κρυπτογραφία. Οι ευρωπαίοι μοναχοί συνέβαλαν στην επανεισαγωγή της κρυπτογραφίας στο δυτικό πολιτισμό.

Το 14ο αιώνα η χρήση της κρυπτογραφίας είχε ήδη διαδοθεί ευρύτατα, με τους αλχημιστές και τους επιστήμονες να τη χρησιμοποιούν για να τηρούν μυστικές τις αποκαλύψεις τους. Ένα από τα πιο διάσημα παραδείγματα πρώιμης ευρωπαικής κρυπτογράφησης ανήκει στον λογοτέχνη αστρονόμο και κρυπτογράφο Τζόφρι Τσόσερ, η κρυπτογράφηση του οποίου αντικαθιστούσε τα γράμματα του κανονικού κειμένου με σύμβολα. Ένα κρυπτογραφημένο κείμενο που αποτελείται από παράξενα σύμβολα και όχι από γράμματα μπορεί εκ πρώτης όψεως να φαίνεται πιο περίπλοκο, αλλά ουσιαστικά ισοδυναμεί με την κλασική υποκατάσταση γράμματος από γράμμα. Η διαδικασία της κρυπτογράφησης και το επίπεδο ασφαλείας είναι ακριβώς τα ίδια.

Το 15ο αιώνα η ευρωπαική κρυπτογραφία ήταν ήδη μια ακμάζουσα βιοτεχνία. Η έκρηξη των πολιτικών δολοπλοκιών προσέφερε μεγάλα κίνητρα για μυστική επικοινωνία. Η Ιταλία ιδίως παρείχε ιδεώδες περιβάλλον για κρυπτογραφία καθώς αποτελείτο από ανεξάρτητες πόλεις-κράτη που η καθεμιά τους προσπαθούσε να υποσκελίσει τις άλλες. Η διπλωματία ανθούσε και κάθε κράτος έστελνε πρέσβεις στις αυλές των υπολοίπων. Ο κάθε πρεσβευτής λάμβανε από τον αρχηγό του κράτους του μηνύματα που περιλάμβαναν λεπτομέρειες για την εξωτερική πολιτική την οποία έπρεπε να εφαρμόσει. Αντίστοιχα ο πρεσβευτής είχε την υποχρέωση να απαντά στέλνοντας ότι πληροφορίες είχε συγκεντρώσει. Αυτό ήταν σαφώς ένα σοβαρό κίνητρο για την κρυπτογράφηση των επικοινωνιών και προς τις δύο κατευθύνσεις, και έτσι κάθε κράτος διατηρούσε γραφείο κρυπτογραφήσεων και κάθε πρεσβευτής διέθετε ειδικό γραμματέα για το σκοπό αυτό. Ταυτόχρονα άρχισε να αναδύεται στη Δύση η επιστήμη της κρυπτανάλυσης. Είναι πολύ πιθανό να ανακαλύφθηκε η κρυπτανάλυση ανεξάρτητα στην Ευρώπη, υπάρχει όμως και το ενδεχόμενο να εισήχθη από τον αραβικό κόσμο.

Ο πρώτος μεγάλος ευρωπαίος κρυπταναλυτής ήταν ο Τζιοβάνι Σόρο, ο οποίος διορίστηκε το 1506 γραμματέας κρυπτογράφησης στη Βενετία και του οποίου η φήμη είχε διαδοθεί σε όλη την Ιταλία, και τα φιλικά κράτη, ακόμα και το Βατικανό, έστελναν στη Βενετία μηνύματα που είχαν υποκλέψει για κρυπτανάλυση.

Γενικά η συγκεκριμένη περίοδος ήταν μεταβατική, με τους κρυπτογράφους να στηρίζονται ακόμη στο μονοαλφαβητικό κρυπτόγραμμα υποκατάστασης , ενώ οι κρυπταναλυτές άρχιζαν να χρησιμοποιούν την ανάλυση συχνοτήτων για να το σπάζουν. Εκείνοι που δεν είχαν ακόμη ανακαλύψει την ισχύ της ανάλυσης συχνοτήτων εξακολουθούσαν να εμπιστεύονται τη μονοαλφαβητική υποκατάσταση, αγνοώντας σε ποια έκταση κρυπταναλυτές σαν το Σορό μπορούσαν να διαβάσουν τα μηνύματά τους.

Μία από τις απλούστερες βελτιώσεις στην ασφάλεια κρυπτογράμματος μονοαλφαβητικής υποκατάστασης ήταν η εισαγωγή των λεγόμενων «ακύρων» δηλαδή συμβόλων ή γραμμάτων που δεν υποκαθιστούν πραγματικά γράμματα, στην ουσία δηλαδή δεν εκπροσωπούν τίποτα. Για παράδειγμα μπορούμε να αντικαταστήσουμε κάθε κανονικό γράμμα με έναν αριθμό από το 1 ως το 99, και έτσι μένουν 73 αριθμοί που δεν εκπροσωπούν τίποτα και οι οποίοι μπορούν να διασπαρθούν τυχαία στο κρυπτογραφημένο κείμενο με διάφορες συχνότητες. Τα άκυρα δεν δημιουργούν κανένα πρόβλημα στον παραλήπτη, που γνωρίζει ότι πρέπει να αγνοηθούν, αλλά προκαλεί μεγάλη σύγχυση στον υποκλοπέα εχθρό, επειδή μπερδεύουν την ανάλυση συχνοτήτων.

Μια άλλη, εξίσου απλή επινόηση είναι να γραφεί ο κρυπτογράφος τις λέξεις ανορθόγραφα πριν κρυπτογραφήσει το μήνυμα καθώς και η εισαγωγή κωδικών λέξεων. Όσο αφορά την τελευταία, αποτελεί ένα ανώτερο επίπεδο κρυπτογράφησης καθώς πλέον δεν αντικαθιστούμε γράμματα με γράμματα αλλά κάθε λέξη εκπροσωπείται από μια άλλη λέξη ή σύμβολο-αυτό είναι ένας κώδικας.

Παράδειγμα:

| | | |
|---|---|---|
| δολοφονώ = D | στρατηγός = Σ | αμέσως = 08 |
| εκβιάζω = P | βασιλιάς = Ω | σήμερα = 73 |

αιχμαλωτίζω = J  υπουργός = Ψ  απόψε = 28
προστατεύω = Z  πρίγκιπας = Θ  αύριο = 43

*Κανονικό μήνυμα = δολοφονείστε το βασιλιά απόψε*
*Κωδικοποιημένο μήνυμα = D-Ω-28*

Από τεχνική άποψη, ο κώδικας (code) ορίζεται ως υποκατάστατο στο επίπεδο των λέξεων ή των φράσεων, ενώ το κρυπτόγραμμα (cipher) ως υποκατάσταση στο επίπεδο των γραμμάτων. Επομένως ο όρος κρυπτογραφώ σημαίνει αναδιατάσσω ένα μήνυμα χρησιμοποιώντας κώδικα.

Οι κώδικες εκ πρώτης όψεως μοιάζουν να παρέχουν μεγαλύτερη ασφάλεια από τα κρυπτογράμματα καθώς οι λέξεις είναι πολύ λιγότερο ευάλωτες στην ανάλυση συχνοτήτων από ότι τα γράμματα. Για να αποκρυπτογραφήσεις ένα μονοαλφαβητικό κρυπτόγραμμα, αρκεί μόνο να προσδιορίσεις την πραγματική αξία του καθενός από τους 24 χαρακτήρες, ενώ για να αποκρυπτογραφήσεις έναν κώδικα πρέπει να προσδιορίσεις την πραγματική αξία εκατοντάδων ή και χιλιάδων κωδικών λέξεων.

Τέλος, οι κώδικες έχουν και δύο βασικά μειονεκτήματα. Πρώτον, από τη στιγμή που αποστολέας και παραλήπτης έχουν συμφωνήσει στα 24 γράμματα του κρυπτογραφικού αλφαβήτου (δηλαδή του κλειδιού) μπορούν να κρυπτογραφήσουν οποιοδήποτε μήνυμα, ενώ για να πετύχουν το ίδιο επίπεδο ευχέρειας χρησιμοποιώντας κώδικα θα πρέπει να φέρουν εις πέρας ένα επίπονο έργο, δηλαδή να ορίσουν μια κωδική λέξη για καθεμιά από τις χιλιάδες πιθανές λέξεις του κανονικού κειμένου. Δεύτερον, οι συνέπειες της υποκλοπής ενός κωδικού βιβλίου είναι ολέθριες καθώς όλες οι κωδικοποιημένες λέξεις γίνονται αυτομάτως γνωστές στον εχθρό. Έτσι αποστολείς και παραλήπτες είναι υποχρεωμένοι να υποστούν την επίπονη διαδικασία σύνταξης ενός εντελώς νέου κωδικού βιβλίου, το οποίο θα πρέπει να διανεμηθεί σε όλους όσους συμμετέχουν στο δίκτυο επικοινωνιών.

Όπως και στη μονοαλφαβητική μετάθεση κάθε γράμμα ή σύμβολο του αρχικού κειμένου αντικαθίσταται από ένα άλλο γράμμα ή σύμβολο με τη διαφορά ότι χρησιμοποιούνται για την κρυπτογράφηση περισσότερα του ενός κρυπτογραφικά αλφάβητα. Παραδείγματα αποτελούν ο κώδικας του Vigenere, ο κώδικας Vernam και το κρυπτογραφικό αλφάβητο που χρησιμοποιείται από τις μηχανές κρυπτογράφησης που λειτουργούσαν με τροχούς, όπως η Enigma.

Ο κώδικας του Vigenere αναπτύχθηκε για να καλύψει τις αδυναμίες του κώδικα του Καίσαρα, πάνω στον οποίο βασίστηκε. Δημιουργήθηκε από το διπλωμάτη Blaise de Vigenere (1523-1596) και χρησιμοποιεί αντί για ένα 26 αλφάβητα, καθένα από τα οποία σχηματίζεται από το προηγούμενο με κυκλική εναλλαγή ενός γράμματος. Όλα μαζί απεικονίζονται σε έναν πίνακα (ταμπλώ), το ταμπλώ του Vigenere, που παρατίθεται δίπλα. Ακόμη απαιτείται μια λέξη-κλειδί, η οποία καθορίζει με ποια σειρά του πίνακα θα γίνει η αντικατάσταση. Δηλαδή με βάση το πρώτο γράμμα της λέξεως κλειδί αντιστοιχούμε το γράμμα του αρχικού κειμένου με το γράμμα από το κρυπτογραφικό αλφάβητο που βρίσκεται στην ίδια σειρά με το πρώτο γράμμα της λέξεως κλειδί. Το ίδιο γίνεται και με τα επόμενα γράμματα των λέξεων, ενώ θεωρούμε ως βάση για τη μεταφορά του αρχικού μηνύματος σε κρυπτογραφημένη μορφή την διαδοχική επανάληψη της λέξεως-κλειδί

| **a** | **b** | **c** | **d** | **e** | **f** | **g** | **h** | **i** | **j** | **k** | **l** | **m** | **n** | **o** | **p** | **q** | **r** | **s** | **t** | **u** | **v** | **w** | **x** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| **B** | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |
| **C** | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| **D** | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| **E** | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| **F** | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| **G** | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| **H** | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| **I** | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| **J** | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| **K** | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| **L** | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| **M** | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| **N** | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| **O** | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| **P** | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| **Q** | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| **R** | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| **S** | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| **T** | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| **U** | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| **V** | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| **W** | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| **X** | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| **Y** | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| **Z** | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |

Ο κώδικας του Vigenere έσπασε αρκετά νωρίς με πρώτο διδάξαντα τον αξιωματικό Friedrich W. Kasiski (1805-1881) από την Πρωσία, ενώ ακολούθησε το 1925 ο Αμερικάνος William F. Friedman (1891-1969). Και οι δύο βάσισαν την κρυπταναλυτική τους έρευνα στο μέγεθος της λέξεως-κλειδί και ακολούθως στην εξέταση του κρυπτογραφικού κειμένου με τη μέθοδο ανάλυσης της πιθανότητας εμφάνισης του κάθε γράμματος

Η κρυπτογραφία, λόγω των στρατιωτικών εξελίξεων, σημείωσε σημαντική ανάπτυξη στους επόμενους αιώνες. Ο Ιταλός *Giovanni Batista Porta*, το 1563, δημοσίευσε το περίφημο για την κρυπτολογία βιβλίο «*De furtivis literarum notis*», με το οποίο έγιναν γνωστά τα πολυαλφαβητικά συστήματα κρυπτογράφησης και τα διγραφικά κρυπτογραφήματα, στα οποία, δύο γράμματα αντικαθίστανται από ένα.

Σημαντικός εκπρόσωπος εκείνης της εποχής είναι και ο Γάλλος *Vigenere*, του οποίου ο πίνακας πολυαλφαβητικής αντικατάστασης, χρησιμοποιείται ακόμη και σήμερα.

Αργότερα ο *C.Wheatstone*, γνωστός από τις μελέτες του στον ηλεκτρισμό, παρουσίασε την πρώτη μηχανική κρυπτοσυσκευή, η οποία απετέλεσε τη βάση για την ανάπτυξη των κρυπτομηχανών της δεύτερης ιστορικής περιόδου της κρυπτογραφίας. Η μεγαλύτερη αποκρυπτογράφηση ήταν αυτή των αιγυπτιακών ιερογλυφικών τα οποία, επί αιώνες, παρέμεναν μυστήριο και οι αρχαιολόγοι μόνο εικασίες μπορούσαν να διατυπώσουν για τη σημασία τους. Ωστόσο, χάρη σε μία κρυπταναλυτική εργασία, τα ιερογλυφικά εν τέλει αναλύθηκαν και έκτοτε οι αρχαιολόγοι είναι σε θέση να διαβάζουν ιστορικές επιγραφές. Τα αρχαιότερα ιερογλυφικά χρονολογούνται περίπου από το 3000 π.Χ. Τα σύμβολα των ιερογλυφικών ήταν υπερβολικά πολύπλοκα για την καταγραφή των συναλλαγών εκείνης της εποχής. Έτσι, παράλληλα με αυτά, αναπτύχθηκε για καθημερινή χρήση η ιερατική γραφή, που ήταν μία συλλογή συμβόλων, τα οποία ήταν εύκολα τόσο στο γράψιμο όσο και στην ανάγνωση. Τον 17ο αιώνα αναθερμάνθηκε το ενδιαφέρον για την αποκρυπτογράφηση των ιερογλυφικών, έτσι το 1652 ο Γερμανός Ιησουΐτης Athanasins Kircher εξέδωσε ένα λεξικό ερμηνείας τους, με τίτλο «*Oedipus Aegyptiacus*». Με βάση αυτό προσπάθησε να ερμηνεύσει τις αιγυπτιακές γραφές, αλλά η προσπάθεια του αυτή ήταν κατά γενική ομολογία αποτυχημένη. Για παράδειγμα, το όνομα του Φαραώ Απρίη, το ερμήνευσε σαν «τα ευεργετήματα του θεϊκού Όσιρι εξασφαλίζονται μέσω των ιερών τελετών της αλυσίδας των πνευμάτων, ώστε να επιδαψιλευθούν τα δώρα του Νείλου». Παρόλα αυτά, η προσπάθεια του άνοιξε τον δρόμο προς την σωστή ερμηνεία των ιερογλυφικών, που προχώρησε χάρη στην ανακάλυψη της «Στήλης της Ροζέτας». Ήταν μια πέτρινη στήλη που βρήκαν τα στρατεύματα του Ναπολέοντα στην Αίγυπτο και είχε χαραγμένο πάνω της το ίδιο κείμενο τρεις φορές. Μια με ιερογλυφικά, μια στα ελληνικά και μια σε ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους. Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ.

Η Κρητική εικονογραφική (ή ιερογλυφική) γραφή δεν μας έχει αποκαλύψει τον κώδικα της, γνωρίζουμε ωστόσο ότι δεν πρόκειται για γραφή που χρησιμοποιεί εικόνες ως σημεία, αλλά για φωνητική γραφή, η οποία εξαντλείται σε περίπου διακόσιους σφραγιδόλιθους και συνυπήρχε με την γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στον Δίσκο της Φαιστού, που ανακαλύφθηκε το 1908 στην νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με την μορφή δύο σπειρών. Τα σύμβολα δεν είναι χαραγμένα, αλλά έχουν σφραγισθεί με την βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας τον Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), τον μεγάλο Άγγλο αρχαιολόγο, που άνεσκαψε συστηματικά την Κνωσό το 1900. Ο ίδιος ονόμασε αυτή τη γραφή γραμμική, επειδή τα γράμματα της είναι γραμμές (ένα γραμμικό σχήμα) και όχι σφήνες, όπως στην σφηνοειδή γραφή ή εικόνες όντων, όπως στην αιγυπτιακή ιερατική. Η γραμμική γραφή Α είναι μάλλον η γραφή των Μινωιτών (από το μυθικό Μίνωα, βασιλιά της Κνωσού), των κατοίκων της αρχαίας Κρήτης και από αυτή ίσως να προήλθε το σημερινό ελληνικό αλφάβητο. Τα γράμματα της γραμμικής γραφής χαράζονταν με αιχμηρό αντικείμενο πάνω σε πήλινες πλάκες, οι οποίες κατόπιν ξεραίνονταν σε φούρνους. Οι περισσότερες από τις επιγραφές με Γραμμική γραφή Α (περίπου 1500) είναι λογιστικές και περιέχουν εικόνες ή συντομογραφίες των εμπορεύσιμων προϊόντων και αριθμούς για υπόδειξη της ποσότητας ή οφειλής.

Ο Έβανς κατέγραψε 135 σύμβολα της. Χρησιμοποιήθηκε κυρίως στην Κρήτη, αν και ορισμένα πρόσφατα ευρήματα καταδεικνύουν ότι μπορεί να αποτέλεσε μέσο γραφής και αλλού, αφού επιγραφές με Γραμμική Α έχουν βρεθεί στην Κνωσό και Φαιστό της Κρήτης, αλλά και στη Μήλο και τη Θήρα. Πλάκες με επιγραφές σε γραμμική Α, εκτίθενται στο Μουσείο Ηρακλείου. Παρά την πρόοδο που έχει σημειωθεί, η γραμμική γραφή Α δεν έχει αποκρυπτογραφηθεί ακόμη και αποτελεί ένα από τα μεγαλύτερα μυστήρια της σύγχρονης αρχαιολογίας. Η αποκρυπτογράφησή της θα αποκαλύψει τη γλώσσα και ενδεχομένως και την καταγωγή των Μινωιτών.

Ο Evans έδωσε και την ονομασία στην Γραμμική Γραφή Β, επειδή αναγνώρισε ότι πρόκειται για συγγενική γραφή με την γραμμική Α, πιο πρόσφατη ωστόσο και εξελιγμένη. Η Γραμμική Α αποτελείται όπως και η Γραμμική Β από συλλαβογράμματα (χαρακτήρες με συγκεκριμένη συλλαβική φωνητική αξία) και ιδεογράμματα (ή λογογράμματα, χαρακτήρες που αντιπροσωπεύουν αντικείμενα). Έχουν βρεθεί περί τα 60-70 συλλαβογράμματα και 60 ιδεογράμματα. Περίπου τα μισά από αυτά είναι κοινά με τους χαρακτήρες της Γραμμικής Β. Με βάση όσα γνωρίζουμε σήμερα, η γραφή αυτή υιοθετήθηκε αποκλειστικά για λογιστικούς σκοπούς. Πινακίδες χαραγμένες με την γραμμική γραφή Β βρέθηκαν στην Κνωσό, στα Χανιά αλλά και στην Πύλο, τις Μυκήνες, τη Θήβα και την Τίρυνθα. Σήμερα αποτελούν ένα σύνολο 10.000 τεμαχίων. Τα σχήματα των πινακίδων της γραφής αυτής ποικίλουν, επικρατούν όμως οι φυλλοειδείς και «σελιδόσχημες», οι οποίες διαφέρουν ως προς τις διαστάσεις, ανάλογα με τις προτιμήσεις του κάθε γραφέα. Έπλαθαν πηλό σε σχήμα κυλίνδρου, τον τοποθετούσαν σε λεία επιφάνεια και την πίεζαν μέχρι να γίνει επίπεδη, επιμήκης και συμπαγής πινακίδα, σαφώς διαφοροποιημένη σε δύο επιφάνειες: μία επίπεδη λειασμένη, που επρόκειτο να αποτελέσει την κύρια γραφική επιφάνεια και μία κυρτή, που συνήθως έμενε άγραφη. Πολλές φορές, όταν τα κείμενα απαιτούσαν περισσότερες από μία πινακίδες, έχουμε τις αποκαλούμενες «ομάδες» ή «πολύπτυχα» πινακίδων, οι οποίες εμφανίζουν κοινά χαρακτηριστικά και ως προς την αποξήρανση και το μίγμα του πηλού και κυρίως, ως προς το γραφικό χαρακτήρα του ίδιου του γραφέα. Τα πολύπτυχα αυτά φυλάσσονταν σε αρχειοφυλάκια και ταξινομούνταν κατά θέματα σε ξύλινα κιβώτια. Για να γνωρίζει ο ενδιαφερόμενος το περιεχόμενο των καλαθιών, κυρίως, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες.

Συστηματικά, με την γραφή αυτή, με την οποία είχε πραγματικό πάθος, ασχολήθηκε ο Άγγλος αρχιτέκτονας και ερασιτέχνης αρχαιολόγος Μ. Βέντρις. ο Μάικλ Βέντρις (Michael Ventris), ηλικίας τότε 30 ετών, ανακοίνωσε δημόσια ότι μπόρεσε να αποκρυπτογραφήσει μιαν άγνωστη μέχρι τότε γραφή, την κρητομυκηναϊκή γραμμική γραφή τύπου Β', στην οποία βρίσκονται γραμμένες πολλές πήλινες πινακίδες από την Κρήτη, τις Μυκήνες, την Πύλο κ.α. και, το κυριότερο, ότι η γλώσσα των πινακίδων αυτών είναι η Ελληνική. Η σπουδαιότητα τής ανακοίνωσης τού Βέντρις για την επιστήμη γενικότερα (που έλυνε, επιτέλους, το μυστήριο των πινακίδων τής γραμμικής γραφής Β') αλλά ιδίως για τον ελληνικό πολιτισμό, που η γραπτή του παράδοση μεταφερόταν επτά περίπου αιώνες νωρίτερα (από τον 8ο αιώνα π.Χ. στον 15ο), ήταν ανυπολόγιστης σημασίας. Αλλαζαν άρδην τα δεδομένα τής ιστορίας μας, αφού αυτή εξαρτάται και προσδιορίζεται χρονικά κατά κύριο λόγο από τις γραπτές μαρτυρίες.

Ο Μ. Βέντρις (1922-1956) ήταν χαρισματικό πνεύμα. Μπορούσε να μαθαίνει εύκολα ξένες γλώσσες, είχε μια σπάνια συνδυαστική φαντασία, ήταν ικανός να ξεχωρίζει τις κανονικότητες μέσα στην ποικιλία και γενικά, όπως γράφει ο J. Chadwick, ο Μ. Βέντρις «είχε τη δύναμη να διακρίνει την τάξη μέσα στο φαινομενικό χάος, το χάρισμα δηλ. που χαρακτηρίζει το έργο όλων των μεγάλων ανδρών». Αν υπάρχει μια λέξη που να συνοψίζει τον Βέντρις,αυτή είναι «αντισυμβατικός».Σχεδόν όλοι όσοι τον γνώριζαν,σημείωναν την άνεση και τη γοητεία της συντροφιάς του,αλλά μπορούσε να είναι και εξαιρετικά απόμακρος και λιγομίλητος. Πάνω από όλα όμως επεδείκνυε μια σεμνότητα που άγγιζε τα όρια της έλλειψης αυτοπεποίθησης αν και είχε τόσους λόγους να καυχιέται, όσους και ένας νομπελίστας. Δίχως την παραμικρή αμφιβολία, αυτή η απελευθέρωσή του από το συμβατικό τρόπο σκέψης και συμπεριφοράς στάθηκε το κλειδί της επιτυχίας του Βέντρις ως αποκρυπτογράφου της Γραμμικής Β.

Δεκατεσσάρων χρονών παιδί ακόμη (το 1936), ακούγοντας τον μεγάλο Αγγλο αρχαιολόγο Σερ Αρθρουρ Εβανς να εξηγεί σε μια διάλεξη στο Βρετανικό Μουσείο τα μυστήρια των αναποκρυπτογράφητων γραφών τής Κρήτης, αυτών που ο ίδιος ο Εβανς ονόμασε «μινωικές γραφές», και τη σημασία τους για τη γνώση τού μινωικού αλλά και τού μυκηναϊκού κόσμου, ο μικρός Βέντρις αποφάσισε να λύσει το μυστήριο τής ανάγνωσης των μινωικών γραφών. Ετσι άρχισε να ασχολείται από νωρίς με το θέμα, διαβάζοντας ό,τι σχετικό υπήρχε. Στον Β' Παγκόσμιο Πόλεμο ασχολήθηκε επίσης με το «σπάσιμο» μυστικών κωδίκων, γεγονός που όξυνε την ικανότητά του στη διερεύνηση τής λειτουργίας διαφόρων κωδικών συστημάτων. Με το θέμα τής αποκρυπτογράφησης τής γραμμικής γραφής Β' συνέχισε να ασχολείται ερασιτεχνικά, η δε ενασχόλησή του αυτή εντάθηκε μετά την επαγγελματική του αποκατάσταση ως επιτυχημένου αρχιτέκτονα.

Ο Βέντρις χρησιμοποίησε αρχικά το περιορισμένο υλικό που είχε δημοσιεύσει ο Εβανς από την Κνωσό. Το υλικό τής έρευνάς του αυξήθηκε με τις πινακίδες γραμμικής γραφής Β' από την Πύλο που βρήκε το 1939 ο Αμερικανός αρχαιολόγος Carl Blegen και που δημοσιεύτηκαν το 1951. Η μελέτη τού διευρυμένου υλικού ενίσχυσε την υπόθεση τού Βέντρις ότι η γλώσσα των πινακίδων τής γραμμικής γραφής Β' είναι η Ελληνική αντίθετα προς την άποψη που είχε μέχρι τότε επιβάλει με το κύρος του ο Εβανς, ότι οι μινωικές γραφές (τόσο η γραμμική Α' - που δεν έχει μέχρι σήμερα αποκρυπτογραφηθεί - όσο και η γραμμική Β') περιείχαν μια μινωική, μη ελληνική γλώσσα, αφού ο Εβανς πίστευε στη δύναμη τού μινωικού κόσμου και στην κυριαρχία των Μινωιτών και στον χώρο τής ηπειρωτικής Ελλάδας (Μυκήνες κ.α.). Ο Βέντρις βοηθήθηκε αρχικά στην αποκρυπτογράφηση συγκρίνοντας τα γράμματα τής γραμμικής Β' με υλικό από τις πινακίδες τής επίσης γραμμικής κυπριακής συλλαβικής γραφής («κυπριακό συλλαβάριο»). Τον βοήθησε ακόμη και το υλικό από τις έρευνες που είχαν πραγματοποιήσει άλλοι ερευνητές (Alice Kober, Emmett Bennett κ.ά.). Ετσι δοκίμασε δειλά και τελείως υποθετικά την ανάγνωση των πινακίδων τής γραμμικής Β' με βάση την ελληνική γλώσσα. Ο Chadwick αναφέρει: «Ο Ventris ξεκίνησε να δοκιμάσει την υπόθεση ότι η γλώσσα ήταν ελληνική, χωρίς να προσδοκά ότι θα οδηγούσε πουθενά. Αλλά καθώς εφάρμοζε τις αξίες του σε περισσότερες και περισσότερες λέξεις, συνέχιζαν να εμφανίζονται ελληνικές λέξεις».

Ο Βέντρις δεν ήταν φιλόλογος και δεν μπορούσε να συνεχίσει την ανακάλυψή του χωρίς την επικουρία ενός κλασικού φιλολόγου που θα μπορούσε να τον βοηθήσει να ταυτίσει τις αναγνώσεις του με αρχαιοελληνικές λέξεις και μάλιστα αρχαιότατες, ενίοτε και μη παραδεδομένες στη μετέπειτα Ελληνική. Αυτό επετεύχθη στο πρόσωπο τού Τζων Τσάντγουικ (John Chadwick), υφηγητή των κλασικών γραμμάτων στο Πανεπιστήμιο τού Καίμπριτζ. Μαζί επεξεργάστηκαν την επίσημη παρουσίαση τής αποκρυπτογράφησης τής γραμμικής γραφής Β', σε άρθρο τους που δημοσιεύθηκε στο έγκυρο επιστημονικό περιοδικό «Journal of Hellenic Studies» το 1953 με τίτλο «Μαρτυρίες για ελληνική διάλεκτο στα μυκηναϊκά αρχεία» (Evidence for Greek Dialect in Mycenaean Archives). Αντίγραφο τού άρθρου αυτού, προτού δημοσιευθεί, δόθηκε στον αρχαιολόγο Carl Blegen, ο οποίος μπόρεσε να διαβάσει την περίφημη «οιονεί δίγλωσση» πινακίδα τής Πύλου, την «πινακίδα των τριπόδων», εφαρμόζοντας τις αξίες των συλλαβογραμμάτων που είχαν επισημάνει οι Βέντρις - Τσάντγουικ. Αυτό έπεισε τους περισσότερους επιστήμονες να δεχθούν ότι η ανάγνωση ήταν ορθή και ότι έχρηζε περαιτέρω βελτιώσεων.

Ως προς την υφή τής γραμμικής γραφής Β', πρόκειται για «συλλαβογραφική γραφή», κάθε σημείο (γράμμα) δηλαδή δηλώνει συλλαβή και όχι μεμονωμένο φθόγγο. Αν λάβει κανείς υπ' όψιν ότι ο αριθμός των συλλαβών σε μια γλώσσα είναι τεράστιος, καταλαβαίνει ότι μια συλλαβογραφική γραφή - για λόγους οικονομίας - χρησιμοποιεί έναν μικρό μόνο αριθμό συλλαβογραμμάτων (γύρω στα 90), για να δηλώσει όλες τις συλλαβές. Ετσι λ.χ. το συλλαβόγραμμα **πε** δηλώνει επίσης και το **βε** και το **φε**. Δηλώνει ακόμη τις μακρόφωνες συλλαβές: **πη, βη, φη**. Και δηλώνει και τις συλλαβές με **ει** και **ηι: πει-πηι, βει-βηι, φει-φηι.** Το ίδιο συλλαβόγραμμα δηλαδή έχει 12 δυνατές αναγνώσεις! Πρόκειται δηλαδή για ένα ατελές σύστημα γραφής, το οποίο οι Ελληνες αντικατέστησαν με μια καθαρώς αλφαβητική γραφή, το γνωστό και μέχρι σήμερα χρησιμοποιούμενο ελληνικό αλφάβητο, το οποίο οι ίδιοι οι Ελληνες δημιούργησαν, επινοήσαντες χωριστά γράμματα να δηλώνουν τα φωνήεντα και χωριστά γράμματα να δηλώνουν τα σύμφωνα.

Οπωσδήποτε, οφείλουμε στη μεγαλοφυΐα τού Βέντρις το γεγονός ότι η ιστορία τής ελληνικής γλώσσας δεν αρχίζει πλέον όπως γνωρίζαμε μέχρι το 1952 τον 8ο αιώνα με την αλφαβητική γραφή τής οινοχόης τού Διπύλου (ή, κατ' άλλους, τού «ποτηρίου τού Νέστορος» που ανήκει στην ίδια περίοδο) αλλά από τα μέσα τού 15ου αιώνα με την ανάγνωση των πινακίδων τής γραμμικής γραφής Β' (Κνωσός, Φαιστός, Πύλος, Μυκήνες, Θήβα).

Αλήθεια, υπάρχει κανένας δρόμος τής Ελλάδος που να φέρει το όνομα αυτού τού μεγάλου επιστημονικού ευεργέτη τού Ελληνισμού; Ας σημειωθεί ότι η Μ. Βρετανία ετίμησε εν ζωή τον Βέντρις με το παράσημο τής Βρετανικής Αυτοκρατορίας, το Πανεπιστήμιο τού Λονδίνου τον ανακήρυξε επίτιμο ερευνητή και το Πανεπιστήμιο τής Ουψάλα τον ανακήρυξε επίτιμο διδάκτορα, προφταίνοντας να τον τιμήσουν, προτού χαθεί πρόωρα από τη ζωή (το 1956) σε ηλικία 34 ετών.

Ήταν ο πρώτος που κατάλαβε ότι επρόκειτο για κάποιο είδος ελληνικής γραφής, αλλά η άποψη του αυτή δεν έγινε δεκτή αρχικά από τους ειδικούς. Στην συνέχεια, όμως, αρκετοί προσχώρησαν στην άποψή

του. Ένας από αυτούς ήταν ο κρυπταναλυτής Τζον Τσάντγουικ, ο οποίος, στη διάρκεια του πολέμου, είχε εργασθεί στην ανάλυση της γερμανικής κρυπτομηχανής Enigma. Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Όμως, ο συνδυασμός των δύο επιστημόνων έφερε το πολυπόθητο αποτέλεσμα. Το 1953 κατέγραψαν τα συμπεράσματά τους στο μνημειώδες έργο «Μαρτυρίες για την ελληνική διάλεκτο στα μυκηναϊκά αρχεία», που έγινε το πιο διάσημο άρθρο κρυπτανάλυσης. Η αποκρυπτογράφηση της Γραμμικής Β απέδειξε ότι επρόκειτο για ελληνική γλώσσα, ότι οι Μινωίτες της Κρήτης μιλούσαν ελληνικά και ότι η δεσπόζουσα δύναμη εκείνη την εποχή ήταν οι Μυκήνες. Η αποκρυπτογράφηση της Γραμμικής Β θεωρήθηκε επίτευγμα ανάλογο της κατάκτησης του Έβερεστ, αλλά και της ανακάλυψης της δομής του DNA από τους Crick και Watson, τα οποία συνέβησαν την ίδια εποχή(1952-53). Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

### *1.2. Νεώτερη ιστορία και κρυπτογραφία – η μηχανή ENIGMA*

Στα τέλη του 19ου αιώνα, η κρυπτογραφία βρισκόταν σε αδιέξοδο. Από τότε που η ασφάλεια του κρυπτογράμματος Βινεζέρ καταστράφηκε ,οι κρυπτογράφοι αναζητούσαν ένα νέο κρυπτόγραμμα, κάτι που θα επανέφερε την ασφάλεια στις επικοινωνίες, επιτρέποντας στους επιχειρηματίες και τους στρατιωτικούς να επωφελούνται από την αμεσότητα του τηλεγράφου χωρίς να κινδυνεύουν οι επικοινωνίες τους να υποκλαπούν και να αποκρυπτογραφηθούν. Λίγο πριν από την αλλαγή του αιώνα ο ιταλός φυσικός Γουλιέλμος Μαρκόνι εφηύρε μια ακόμη πιο ισχυρή μορφή τηλεπικοινωνίας, που έκανε πιεστικότερη την ανάγκη για ασφαλή κρυπτογράφηση. Το 1894 ο Μαρκόνι πειραματιζόταν με μία περίεργη ιδιότητα των ηλεκτρικών κυκλωμάτων. Παρατήρησε ότι κάτω από ορισμένες συνθήκες, αν ένα κύκλωμα μετέφερε ένα ηλεκτρικό ρεύμα, αυτό μπορούσε να δημιουργήσει επαγωγικά ένα ρεύμα σε ένα άλλο απομονωμένο κύκλωμα το οποίο βρισκόταν σε κάποια απόσταση. Βελτιώνοντας το σχέδιο των 2 κυκλωμάτων, αυξάνοντας την ισχύ και προσθέτοντας κεραίες κατάφερε να μεταδίδει και να λαμβάνει παλμούς σε και από απόσταση ως και 2,5 χιλιομέτρων. Είχε επινοήσει τον ασύρματο ο οποίος είχε το σημαντικό πλεονέκτημα ότι επέτρεπε την άμεση επικοινωνία ανάμεσα σε οποιαδήποτε δύο σημεία χωρίς να χρειάζονται σύρματα που να τα ενώνουν. Ο ασύρματος θα επέτρεπε στους στρατηγούς να διευθύνουν τις εκστρατείες τους, κρατώντας τους σε διαρκή επαφή με τους λόχους, ανεξάρτητα από τις κινήσεις των τελευταίων. Ωστόσο αυτή η πανταχού παρουσία του ασυρμάτου είναι και η μεγαλύτερη στρατιωτική αδυναμία καθώς αναπόφευκτα τα μηνύματα φτάνουν όχι μόνο στον επιθυμητό παραλήπτη αλλά και στον εχθρό. Κατά συνέπεια, η αξιόπιστη κρυπτογράφηση ήταν αναγκαία καθώς αν ο εχθρός είχε τη δυνατότητα να υποκλέπτει όλα τα ραδιομηνύματα, τότε οι κρυπτογράφοι έπρεπε να βρουν ένα τρόπο να τον εμποδίζουν να τα αποκρυπτογραφεί.

Ο διττός αυτός χαρακτήρας του ασυρμάτου, ευκολία στην επικοινωνία αλλά και στην υποκλοπή, ήλθε έντονα στο προσκήνιο με την έναρξη του Ά Παγκοσμίου πολέμου. Όλες οι αντιμαχόμενες πλευρές επιθυμούσαν να εκμεταλλευτούν τη δύναμη του ασυρμάτου αλλά και ταυτόχρονα δεν ήξεραν πώς να εγγυηθούν την ασφάλεια των επικοινωνιών. Όλοι ήλπιζαν ότι θα βρισκόταν ένα νέο κρυπτόγραμμα που θα κατοχύρωνε και πάλι το στρατιωτικό απόρρητο. Ωστόσο μεταξύ 1914 και 1918 υπήρξε μόνο ένας κατάλογος κρυπτογραφικών αποτυχιών. Ένα από τα πιο διάσημα κρυπτογράμματα εκείνης της εποχής ήταν το γερμανικό κρυπτόγραμμα ADFGVX, το οποίο εμφανίστηκε λίγο πριν τη μεγάλη γερμανική επίθεση. Όπως σε κάθε τέτοια επιχείρηση, οι γερμανοί ήθελαν να εκμεταλλευτούν το στοιχείο του αιφνιδιασμού, και μια επιτροπή κρυπτογράφων επέλεξε το παραπάνω κρυπτόγραμμα πιστεύοντας ότι είχε τη μεγαλύτερη ασφάλεια λόγω της πολύπλοκης φύσης του, που ήταν μείγμα υποκατάστασης και μετάθεσης.

Από ότι αποδείχτηκε λίγο αργότερα όμως ούτε αυτό το κρυπτόγραμμα ήταν αρκετά ασφαλές αφού ένα μήνυμα κρυπτογραφημένο με το ADFGVX έσπασε από το Γάλλο κρυπταναλυτή Πενβέν κοστίζοντας στους Γερμανούς τη νίκη στην έφοδο του Παρισιού το 1918.Το γεγονός αυτό ήταν ένα τυπικό δείγμα της κατάστασης της κρυπτογραφίας κατά τη διάρκεια του Πρώτου Παγκοσμίου πολέμου καθώς παρότι υπήρξε πληθώρα νέων κρυπτογραμμάτων, όλα ήταν παραλλαγές ή συνδυασμοί ήδη σπασμένων κρυπτογραμμάτων του 19ου αιώνα.

Το μεγαλύτερο πρόβλημα των κρυπταναλυτών ήταν ο τεράστιος όγκος μηνυμάτων. Πριν από τον ασύρματο, τα υποκλεπτόμενα μηνύματα ήταν σπάνια και πολύτιμα αντικείμενα προσοχής. Όμως στον Ά Παγκόσμιο πόλεμο οι ραδιοεπικοινωνίες γνώρισαν μεγάλη ανάπτυξη, και όλα τα μηνύματα μπορούσαν να υποκλαπούν, δημιουργώντας μια συνεχή ροή κρυπτογραμμάτων που απασχολούσαν τα μυαλά των κρυπταναλυτών. Υπολογίζεται ότι στη διάρκεια του πολέμου οι Γάλλοι, οι οποίοι ήταν και οι πιο αποτελεσματικοί κρυπταναλυτές εκείνης της εποχής, υπέκλεψαν πάνω από 100.000.000 λέξεις των γερμανικών επικοινωνιών . Οι Γάλλοι ασχολούνταν με τις κρυπτογραφήσεις σε καθημερινή βάση και ανέπτυξαν βοηθητικές τεχνικές για να συγκεντρώνουν πληροφορίες μέσω των ραδιοεπικοινωνιών οι οποίες δεν περιλάμβαναν αποκρυπτογράφηση όπως για παράδειγμα την αναγνώριση της γροθιάς ενός ραδιοχειριστή. Ένα μήνυμα αφού κρυπτογραφηθεί, μεταδίδεται σε κώδικα Μορς ως μια σειρά από στιγμές και παύλες, και κάθε χειριστής μπορεί να αναγνωρίσει από τις παύσεις του, την ταχύτητα μετάδοσης και το σχετικό μήκος που έχουν οι στιγμές και οι παύλες του. Εκτός από τη λειτουργία σταθμών ακρόασης οι Γάλλοι εγκατέστησαν 6 σταθμούς εντοπισμού διεύθυνσης, που μπορούσαν να ανιχνεύουν τον τόπο προέλευσης κάθε μηνύματος. Ο κάθε σταθμός μετακινούσε την κεραία του μέχρι το σημείο που το σήμα ήταν ισχυρότερο, πράγμα που υποδείκνυε την κατεύθυνση της πηγής του μηνύματος. Συνδυάζοντας τα παραπάνω ήταν δυνατόν να αποκαλυφθεί η ταυτότητα και η θέση λόγου χάρη ενός συγκεκριμένου λόχου και κατά συνέπεια η πορεία του, ο προορισμός και οι στόχοι του. Αυτή η μορφή συλλογής πληροφοριών, γνωστή ως ανάλυση κυκλοφορίας, ήταν ιδιαίτερα πολύτιμη μετά την εισαγωγή ενός νέου κρυπτογράμματος. Κάθε νέο κρυπτόγραμμα αχρήστευε πρόσκαιρα τους αναλυτές όμως ακόμη κι αν ένα μήνυμα δεν μπορούσε να αποκρυπτογραφηθεί παρείχε και πάλι πληροφορίες μέσω της ανάλυσης κυκλοφορίας.
Ελλείψει γαλλικών ραδιοεπικοινωνιών, οι Γερμανοί δεν μπορούσαν να πραγματοποιήσουν πολλές υποκλοπές και έτσι δεν μπήκαν στον κόπο να αναπτύξουν το κρυπταναλυτικό τμήμα τους παρά μόνο 2 χρόνια μετά την έναρξη του πολέμου.

Βρετανοί και Αμερικάνοι συνέβαλαν επίσης σημαντικά στη συμμαχική κρυπτανάλυση. Η υπεροχή των συμμάχων κρυπταναλυτών και η επίδρασή τους στο Μεγάλο Πόλεμο καταδεικνύεται από την αποκρυπτογράφηση ενός γερμανικού τηλεγραφήματος που υπέκλεψαν οι Βρετανοί τον Ιανουάριο του 1917. Ο πρόεδρος των ΗΠΑ Ουίλσον, αρνείτο κατηγορηματικά τα 2 πρώτα χρόνια να στείλει αμερικανικά στρατεύματα προς ενίσχυση των Συμμάχων καθώς πίστευε ότι θα πρόσφερε καλύτερες υπηρεσίες στον κόσμο αν παρέμενε ουδέτερος και ενεργούσε ως διαμεσολαβητής.

Η Γερμανία το Νοέμβριο του 1916 διόρισε στο υπουργείο εξωτερικών τον Άρθουρ Μέρμαν ο οποίος ενώ κατά τον Ουίλσον έδειχνε να εγκαινιάζει μια νέα εποχή γερμανικής διπλωματίας, στην πραγματικότητα δεν είχε καμία πρόθεση να επιδιώξει την ειρήνη, αλλά συνωμοτούσε για να επεκτείνει τη στρατιωτική επιθετικότητα της Γερμανίας.

Βασικός στόχος του Μέρμαν ήταν να αναγκάσει τους Συμμάχους να παραδοθούν πριν μπορέσει η Αμερική να εισέλθει στο ευρωπαικό πολεμικό μέτωπο. Σύμφωνα με το σχέδιό του, θα πρότεινε συμμαχία με το Μεξικό και θα έπειθε τη χώρα αυτή να εισβάλει στις Η.Π.Α διεκδικώντας περιοχές όπως το Τέξας , το Νέο Μεξικό και η Αριζόνα, έχοντας την οικονομική και στρατιωτική υποστήριξη της Γερμανίας. Επιπλέον ο Μέρμαν ήθελε να ενεργήσει ο μεξικανός πρόεδρος ως διαμεσολαβητής και να πείσει την Ιαπωνία να επιτεθεί κι αυτή στην Αμερική. Με αυτόν τον τρόπο η Γερμανία θα απειλούσε την ανατολική ακτή των ΗΠΑ, η Ιαπωνία θα χτυπούσε από τα δυτικά και το Μεξικό θα εισέβαλε από το νότο. Έτσι η Αμερική θα είχε τέτοιο εσωτερικό πρόβλημα ώστε να μην μπορεί να στείλει στρατό στην Ευρώπη.

Ο Μέρμαν ανέπτυξε την πρότασή του σε ένα τηλεγράφημα προς το Γερμανό πρέσβη στην Ουάσιγκτον ο οποίος θα το μετέφερε στον Γερμανό πρέσβη στο Μεξικό που τελικά θα το παρέδιδε στο Μεξικανό πρόεδρο. Ο Μέρμαν αφού κρυπτογράφησε το μήνυμά του, λόγω της αποκοπής των υπερατλαντικών υποθαλάσσιων καλωδίων της Γερμανίας από τους Βρετανούς, αναγκάστηκε να το στείλει μέσω Σουηδίας αλλά και μέσω του πιο άμεσου καλωδίου αμερικανικής ιδιοκτησίας. Και οι δύο δρόμοι περνούσαν από την Αγγλία με αποτέλεσμα το τηλεγράφημα να υποκλαπεί και να διαβιβαστεί αμέσως στο Γραφείο Κρυπτογραμμάτων του Ναυαρχείου, γνωστό και ως «δωματιο 40». Μέσα σε λίγες ώρες το κωδικοθραυστικό ντουέτο των Μοντγκόμερι και ντε Γκρέι ανέσυρε κάποια θραύσματα κειμένου τα οποία ήταν αρκετά για να καταλάβουν ότι αποκάλυπταν ένα μήνυμα υψίστης σημασίας. Στο τέλος της μέρας που

ήταν σε θέση πια να διακρίνουν το περίγραμμα των τρομερών σχεδίων του Μέρμαν, παρέδωσαν το εν μέρει αποκρυπτογραφημένο τηλεγράφημα στο Ναύαρχο Ουίλιαμ Χολ με την προσδοκία ότι αυτός θα διαβίβαζε την πληροφορία στους Αμερικανούς παρασύροντάς τους έτσι στον πόλεμο. Ωστόσο ο Χολ δεν παρέδωσε το αποκρυπτογραφημένο μήνυμα, καθώς σκέφτηκε πως αν οι Βρετανοί έδιναν στους Αμερικάνους το τηλεγράφημα και εκείνοι καταδίκαζαν δημόσια τη γερμανική επίθεση, τότε οι Γερμανοί θα συμπέραιναν ότι οι Βρετανοί έσπασαν την κρυπτογραφική τους μέθοδο και θα ανέπτυσσαν νέο ισχυρότερο σύστημα κρυπτογραφίας φράζοντας έτσι ένα ζωτικό δίαυλο ροής πληροφοριών. Έτσι ο Χολ άφησε το μήνυμα να φτάσει στο γερμανό πρέσβη στο Μεξικό έχοντας πρώτα επιφέρει κάποιες μικρές αλλαγές, ο οποίος με τη σειρά του θα επέδιδε την αναθεωρημένη αυτή εκδοχή του τηλεγραφήματος στο μεξικανό πρόεδρο. Αν ο Χολ κατάφερνε με κάποιο τρόπο να πάρει στα χέρια του τη μεξικανική παραλλαγή τότε αυτό θα μπορούσε να δημοσιευτεί στις εφημερίδες και οι Γερμανοί θα υπέθεταν ότι οι Βρετανοί το έκλεψαν από τη μεξικανική πλευρά και όχι ότι το υπέκλεψαν και το αποκρυπτογράφησαν κατά τη διάρκεια της αποστολής του στην Αμερική. Το σχέδιο του Χολ ήλθε εις πέρας με τη βοήθεια ενός βρετανού πράκτορα στο Μεξικό ο οποίος πήρε τη μεξικανική παραλλαγή του τηλεγραφήματος. Αυτό είχε ως αποτέλεσμα το τηλεγράφημα να δοθεί στον τύπο, ο Μέρμαν να παραδεχτεί δημόσια ότι το είχε συντάξει ο ίδιος και οι έρευνες του υπουργείου εξωτερικών της Γερμανίας για το πώς έφτασε το τηλεγράφημα στα χέρια των Αμερικανών να καταλήξουν στο συμπέρασμα ότι η προδοσία διαπράχθηκε στο Μεξικό. Μετά από αυτές τις εξελίξεις ο Ουίλσον πρότεινε την αποδοχή του καθεστώτος πολέμου από το Κογκρέσο.

Η ιστορία αυτής της αποκρυπτογράφησης δείχνει πώς η κρυπτανάλυση μπορεί να επηρεάσει την πορεία ενός πολέμου στο ανώτατο επίπεδο και αποδεικνύει τις δυνητικά καταστροφικές συνέπειες της χρήσης ανεπαρκούς κρυπτογράφησης. Μέσα σε λίγες μέρες το αποκρυπτογραφημένο τηλεγράφημα έμμελε να υποχρεώσει την Αμερική να αναθεωρήσει την πολιτική ουδετερότητα που τηρούσε, με αποτέλεσμα να γείρει η πλάστιγγα του πολέμου.

Κατά τον Ά Παγκόσμιο Πόλεμο η κρυπτανάλυση γνώρισε μια σειρά από επιτυχίες, με αποκορύφωμα την αποκρυπτογράφηση του τηλεγραφήματος του Μέρμαν. Από τότε που έσπασαν το κρυπτόγραμμα Βιζενέρ το 19ο αιώνα οι κωδικοθραύστες είχαν το πάνω χέρι έναντι των κωδικοπλαστών. Προς το τέλος του πολέμου, και ενώ οι κρυπτογράφοι είχαν περιέλθει σε απελπιστική θέση, οι Αμερικανοί επιστήμονες πραγματοποίησαν ένα εκπληκτικό κατόρθωμα. Ανακάλυψαν ότι το κρυπτόγραμμα Βιζενέρ μπορούσε να χρησιμοποιηθεί ως βάση για μια νέα ισχυρότερη μορφή κρυπτογράφησης η οποία θα παρείχε απόλυτη ασφάλεια.

Η βασική αδυναμία του κρυπτογράμματος Βιζενέρ είναι η κυκλική του φύση. Αν η λέξη-κλειδί έχει μήκος πέντε γράμματα τότε κάθε πέμπτο γράμμα του κανονικού κειμένου κρυπτογραφείται σύμφωνα με το ίδιο κρυπτογραφικό αλφάβητο. Αν ο κρυπταναλυτής κατορθώσει να βρει το μήκος της λέξης κλειδιού, τότε το κρυπτογραφημένο κείμενο μπορεί να αντιμετωπιστεί σαν μια σειρά από πέντε μονοαλφαβητικά κρυπτογράμματα, καθένα από τα οποία μπορεί να σπάσει με την ανάλυση συχνοτήτων. Η καλύτερη λύση στο συγκεκριμένο πρόβλημα θα ήταν να χρησιμοποιηθεί ένα κλειδί που το μήκος του θα είναι όσο και το μήκος του μηνύματος. Κάτι τέτοιο όμως απαιτεί από τον κρυπτογράφο να δημιουργήσει ένα επίμηκες κλειδί. Αν το μήνυμα περιέχει εκατοντάδες γράμματα, τότε και το κλειδί πρέπει να περιλαμβάνει άλλα τόσα. Αντί να επινοήσει κανείς εκ του μηδενός ένα τόσο μακρύ κλειδί, θα μπορούσε για παράδειγμα να βασίσει το κλειδί σε μια σειρά από τυχαία επιλεγμένα ονόματα πουλιών. Ωστόσο, τέτοιου είδους κλειδιά είναι εγγενώς ελαττωματικά καθώς δημιουργήθηκαν από λέξεις με νόημα.

Το 1918 οι κρυπτογράφοι άρχισαν να πειραματίζονται με κλειδιά που στερούνταν δομής. Το αποτέλεσμα ήταν ένα άθραυστο κρυπτόγραμμα. Καθώς ο Μεγάλος Πόλεμος πλησίαζε στο τέλος του, ο ταγματάρχης των ΗΠΑ J.Manborgue εισήγαγε την έννοια ενός τυχαίου κλειδιού που αποτελείτο όχι από μια αναγνωρίσιμη αλλά από μια τυχαία σειρά λέξεων. Υποστήριζε τη χρήση τυχαίων τέτοιων κλειδιών ως μερών ενός κρυπτογράμματος Βιζενέρ ώστε να επιτευχθεί ένα άνευ προηγούμενου επίπεδο ασφάλειας.

Το πρώτο στάδιο ήταν να δημιουργηθεί ένα παχύ μπλοκ αποτελούμενο από εκατοντάδες φύλλα χαρτιού, το καθένα από τα οποία θα περιείχε ένα μοναδικό κλειδί με τη μορφή γραμμών από γράμματα σε

αυθαίρετη διαδοχή. Θα υπήρχαν δυο αντίγραφα του μπλοκ, ένα για τον αποστολέα και ένα για τον παραλήπτη. Ο αποστολέας θα εφάρμοζε το κρυπτόγραμμα Βιζενέρ χρησιμοποιώντας ως κλειδί το πρώτο φύλλο του μπλοκ. Ο παραλήπτης μπορεί εύκολα να αποκρυπτογραφήσει το κρυπτογραφικό κείμενο χρησιμοποιώντας το ίδιο ακριβώς κλειδί και αντιστρέφοντας το κρυπτόγραμμα Βιζενέρ. Από τη στιγμή που το μήνυμα θα σταλεί, θα ληφθεί και θα αποκρυπτογραφηθεί με επιτυχία, τόσο αποστολέας όσο και ο παραλήπτης καταστρέφουν το φύλλο που έπαιξε το ρόλο του κλειδιού, ώστε να μην ξαναχρησιμοποιηθεί. Επειδή κάθε κλειδί χρησιμοποιείται για μια και μοναδική φορά, το σύστημα αυτό είναι γνωστό ως *κρυπτόγραμμα του μπλοκ μιας χρήσης*.

Το παραπάνω κρυπτόγραμμα παρότι τέλειο στη θεωρία, στην πράξη πάσχει, επειδή παρουσιάζει δύο βασικές δυσκολίες.

Πρώτον, υπάρχει το πρακτικό πρόβλημα της παραγωγής μεγάλων ποσοτήτων τυχαίων κλειδιών. Μέσα σε μια μέρα ένας στρατός μπορεί να ανταλλάσει εκατοντάδες μηνύματα, που το καθένα περιέχει χιλιάδες χαρακτήρες, οπότε οι ραδιοχειριστές θα χρειάζονταν μια καθημερινή προμήθεια κλειδιών που θα ισοδυναμούσαν με εκατομμύρια τυχαία διατεταγμένα γράμματα. Η παραγωγή τόσο πολλών τυχαίων ακολουθιών γραμμάτων είναι τεράστιο έργο. Οι κρυπτογράφοι συνειδητοποίησαν ότι απαιτείται πολύς χρόνος, προσπάθεια και χρήμα για να δημιουργηθεί ένα τυχαίο κλειδί. Τα καλύτερα τυχαία κλειδιά δημιουργούνται με την τιθάσευση φυσικών διαδικασιών όπως η ραδιενέργεια, που είναι γνωστό ότι επιδεικνύει πραγματικά τυχαία συμπεριφορά.

Το δεύτερο πρόβλημα του συγκεκριμένου κρυπτογράμματος είναι η δυσκολία κατανομής των τυχαίων κλειδιών. Σε ένα πιθανό σενάριο πεδίου μάχης, εκατοντάδες διαχειριστές μετέχουν στο ίδιο δίκτυο επικοινωνιών. Κάθε διαχειριστής πρέπει να διαθέτει πανομοιότυπα αντίγραφα του μπλοκ μιας χρήσης. Στη συνέχεια όταν εκδίδονται νέα μπλοκ, πρέπει να διανέμονται σε όλους ταυτοχρόνως.

Τέλος, πρέπει όλοι να είναι συντονισμένοι, ώστε να χρησιμοποιούν το σωστό φύλλο του μπλοκ τη σωστή στιγμή. Η ευρεία διάδοση του μπλοκ μιας χρήσης θα γέμιζε το πεδίο μάχης με ταχυδρόμους και λογιστές. Επιπλέον, αν έστω και μια σειρά κλειδιών πέσει στα χέρια του εχθρού, τίθεται σε κίνδυνο όλο το σύστημα επικοινωνιών. Οι πρακτικές ατέλειες του θεωρητικά τέλειου μπλοκ μιας χρήσης σήμαιναν ότι ήταν αδύνατο να χρησιμοποιηθεί μέσα στο πεδίο της μάχης. Μετά τον Ά Παγκόσμιο Πόλεμο και όλες τις κρυπτογραφικές αποτυχίες του, συνεχίστηκε η αναζήτηση για ένα πρακτικό σύστημα που θα μπορούσε να χρησιμοποιηθεί στην επόμενη σύγκρουση. Προκειμένου να ενισχύσουν τα κρυπτογράμματά τους, οι κρυπτογράφοι αναγκάστηκαν να εγκαταλείψουν τη μέθοδο προσέγγισης που βασιζόταν στο μολύβι και στο χαρτί και να εκμεταλλευτούν την πιο πρόσφατη τεχνολογία για να αναδιατάσσουν τα μηνύματα.

Η πρώτη κρυπτογραφική μηχανή είναι ο κρυπτογραφικός δίσκος, που τον επινόησε το δέκατο πέμπτο αιώνα ο ιταλός αρχιτέκτων Λέον Αλμπέρτι, ένας από τους πατέρες του πολυαλφαβητικού κρυπτογράμματος. Πήρε δύο χάλκινους δίσκους, τον έναν φαρδύτερο από τον άλλο, και χάραξε το αλφάβητο στην περιφέρεια και των δύο. Τοποθετώντας το μικρότερο δίσκο πάνω στο μεγαλύτερο και στερεώνοντάς τους με μια βελόνα που ενεργεί ως άξονας, κατασκεύασε κάτι παρόμοιο με το δίσκο που παρουσιάζεται στην παρακάτω εικόνα. Οι δύο δίσκοι μπορούν να περιστρέφονται ανεξάρτητα, έτσι ώστε τα δύο αλφάβητα μπορούν να έχουν διαφορετικές σχετικές θέσεις, και έτσι να χρησιμοποιούνται για την κρυπτογράφηση ενός μηνύματος με ένα απλό κρυπτόγραμμα μετάθεσης τύπου Καίσαρα. Παρότι ο κρυπτογραφικός δίσκος είναι μια πολύ πρωτόλεια συσκευή, διευκολύνει σαφώς την κρυπτογράφηση και επέζησε για πέντε αιώνες. Μπορεί επίσης να θεωρηθεί ως «αναδιατάκτης»,που παίρνει κάθε γράμμα του κανονικού κειμένου και το μετατρέπει σε κάτι άλλο. Η διαδικασία που περιγράψαμε ως τώρα είναι απλή και το προκύπτον κρυπτόγραμμα μπορεί να σπάσει σχετικά εύκολα, όμως ο κρυπτογραφικός δίσκος μπορεί να χρησιμοποιηθεί και με πιο περίπλοκο τρόπο. Ο εφευρέτης του, ο Αλμπέρτι, πρότεινα την αλλαγή της διάταξης του δίσκου κατά τη διάρκεια του μηνύματος, κάτι που ουσιαστικά δημιουργεί ένα πολυαλφαβητικό κρυπτόγραμμα στη θέση του μονοαλφαβητικού. Για παράδειγμα ο Αλμπέρτι θα μπορούσε να χρησιμοποιήσει το δίσκο για να κρυπτογραφήσει τη λέξη goodbye(αντίο),χρησιμοποιώντας τη λέξη κλειδί LEON.Θα άρχιζε διευθετώντας το δίσκο του σύμφωνα με το πρώτο γράμμα της λέξης κλειδιού, μετακινώντας το εξωτερικό Α δίπλα στο εσωτερικό L. Στη συνέχεια θα κρυπτογραφούσε το πρώτο γράμμα

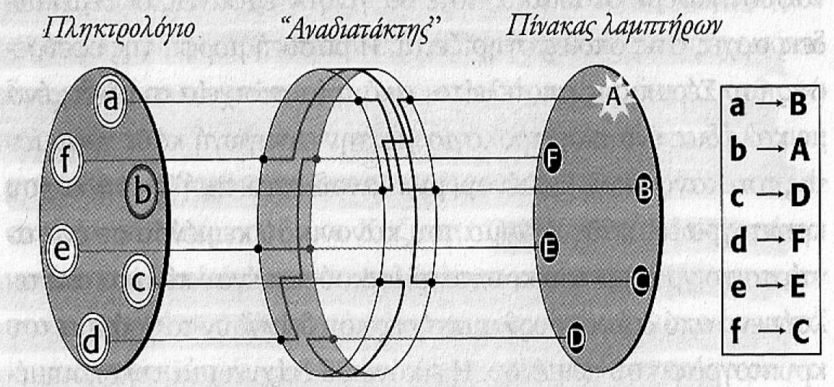
του μηνύματος, το g,βρίσκοντάς το στον εξωτερικό δίσκο και σημειώνοντας το αντίστοιχο γράμμα στον εσωτερικό,που είναι το R. Για να κρυπτογραφήσει το δεύτερο γράμμα της λέξης κλειδιού, μετακινώντας το εξωτερικό Α πλάι στο εσωτερικό Ε. Μετά θα κρυπτογραφούσε το **o** βρίσκοντάς το στον εξωτερικό δίσκο και σημειώνοντας το αντίστοιχο γράμμα στον εσωτερικό, που είναι το **S**.Η διαδικασία της κρυπτογράφησης συνεχίζεται με τον κρυπτογραφικό δίσκο να διευθετείται σύμφωνα με το γράμμα κλειδί **O**, μετά σύμφωνα με το **N**, ύστερα πάλι σύμφωνα με το **L** κ.ο.κ. Ο Αλμπέρτι κατόρθωσε πάντως να κρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας το κρυπτόγραμμα Βιζενέρ με το μικρό του όνομα να παίζει το ρόλο της λέξης κλειδιού. Ο κρυπτογραφικός δίσκος επιταχύνει την κρυπτογράφηση και περιορίζει τα λάθη σε σχέση με το τετράγωνο Βιζενέρ. Το σημαντικό χαρακτηριστικό της χρήσης του κρυπτογραφικού δίσκου με αυτόν τον τρόπο είναι το γεγονός ότι ο δίσκος αλλάζει μέθοδο αναδιάταξης κατά τη διάρκεια της κρυπτογράφησης. Παρότι αυτό το επιπλέον επίπεδο πολυπλοκότητας κάνει δυσκολότερο το σπάσιμο του κρυπτογράμματος, δεν το καθιστά άθραυστο, γιατί ουσιαστικά έχουμε να κάνουμε απλώς με μια μηχανική εκδοχή του κρυπτογράμματος Βιζενέρ το οποίο έσπασαν οι Μπάμπατζ και Καζίσκι.

Όμως, 500 χρόνια μετά τον Αλμπέρτι, μια πιο πολύπλοκη μετενσάρκωση του κρυπτογραφικού δίσκου έμελλε να οδηγήσει σε μια νέα γενιά κρυπτογραμμάτων, κατά μια τάξη μεγέθους δυσχερέστερα να αποκρυπτογραφηθούν από οτιδήποτε είχε χρησιμοποιηθεί προηγουμένως. Το 1918,ο γερμανός εφευρέτης Άρθουρ Σέρμπιους και ο στενός του φίλος Ρίτσαρντ Ρίτερ ίδρυσαν την εταιρία Σέρμπιους και Ρίτερ, μια καινοτόμο κατασκευαστική επιχείρηση που ασχολείτο με τα πάντα, από τουρμπίνες μέχρι θερμαινόμενα μαξιλάρια. Ο Σέρμπιους ήταν υπεύθυνος για την έρευνα και την ανάπτυξη, και συνεχώς αναζητούσε νέες ευκαιρίες. Ένα από τα αγαπημένα του σχέδια ήταν να καταργήσει τα αναποτελεσματικά συστήματα κρυπτογραφίας που χρησιμοποιούνταν κατά τον Πρώτο Παγκόσμιο πόλεμο, αντικαθιστώντας τα κρυπτογράμματα του τύπου μολύβι και χαρτί με μια μορφή κρυπτογράφησης που να εκμεταλλεύεται την τεχνολογία του εικοστού αιώνα. Έχοντας σπουδάσει ηλεκτρολόγος-μηχανολόγος, ανέπτυξε ένα μηχανικό κρυπτογραφικό σύστημα που ουσιαστικά ήταν μια ηλεκτρική παραλλαγή του κρυπτογραφικού δίσκου του Αλμπέρτι. Η εφεύρεση του Σέρμπιους, που έγινε γνωστή ως Αίνιγμα, έμελλε να γίνει το πρώτο επίφοβο σύστημα κρυπτογράφησης στην ιστορία.

Το Αίνιγμα του Σέρμπιους αποτελείτο από έναν αριθμό «έξυπνων» εξαρτημάτων τα οποία ο ίδιος συνδύασε σε μια καταπληκτική και περίπλοκη κρυπτογραφική μηχανή. Ωστόσο αν αποδομήσουμε τη μηχανή στα συστατικά της μέρη και την ανασυστήσουμε σταδιακά, τότε θα γίνουν εμφανείς οι θεμελιώδεις αρχές στις οποίες στηρίζεται. Η βασική μορφή της εφεύρεσης του Σέρμπιους αποτελείται από 3 στοιχεία συνδεδεμένα με καλώδια: ένα πληκτρολόγιο για την εισαγωγή κάθε γράμματος του κανονικού κειμένου, μια «αναδιατακτική μονάδα» που κρυπτογραφεί κάθε γράμμα του κανονικού κειμένου σε ένα αντίστοιχο γράμμα του κρυπτογραφικού και έναν πίνακα αποτελούμενο από διάφορους λαμπτήρες που δείχνουν το γράμμα του κρυπτογραφικού κειμένου. Η παρακάτω εικόνα δείχνει μια τυποποιημένη διάταξη της μηχανής, με ένα αλφάβητο 6 μόνο γραμμάτων για λόγους απλότητας. Προκειμένου να κρυπτογραφήσει ένα γράμμα του κανονικού κειμένου, ο χειριστής χτυπάει το αντίστοιχο γράμμα στο πληκτρολόγιο, το οποίο στέλνει έναν ηλεκτρικό παλμό μέσω της κεντρικής «αναδιατακτικής» μονάδας προς την άλλη πλευρά, όπου ανάβει το αντίστοιχο γράμμα του κρυπτογραφικού κειμένιου στον πίνακα με τους λαμπτήρες.

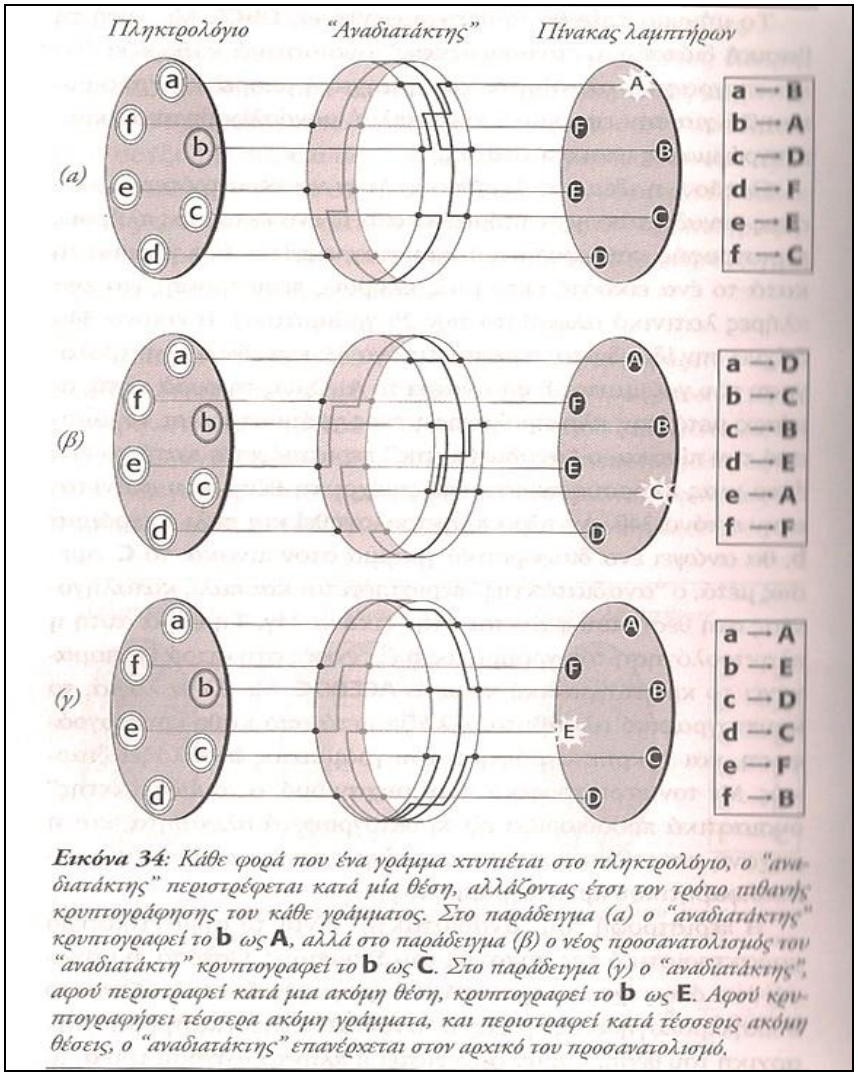
Ο αναδιατάκτης, ένας παχύς λαστιχιένιος δίσκος διάτρητος από καλώδια, είναι το σημαντικότερο τμήμα της μηχανής.Από το πληκτρολόγιο τα καλώδια εισέρχονται στον «αναδιατάκτη» σε 6 σημεία, και αφού περιελιχθούν μέσα σε αυτόν, εξέρχονται από 6 σημεία στην άλλη πλευρά. Οι εσωτερικές καλωδιώσεις του «αναδιατάκτη» καθορίζουν πώς θα κρυπτογραφηθούν τα γράμματα του κανονικού κειμένου. Για παράδειγμα στην παρακάτω εικόνα επιτάσσουν ότι:

Πληκτρολογώντας το **a** ανάβει το **B**, δηλαδή, το **a** κρυπτογραφείται ως **B**.
Πληκτρολογώντας το **b** ανάβει το **A**, δηλαδή, το **b** κρυπτογραφείται ως **A**.
Πληκτρολογώντας το **c** ανάβει το **D**, δηλαδή, το **c** κρυπτογραφείται ως **D**.
Πληκτρολογώντας το **d** ανάβει το **F**, δηλαδή, το **d** κρυπτογραφείται ως **F**.
Πληκτρολογώντας το **e** ανάβει το **E**, δηλαδή, το **e** κρυπτογραφείται ως **E**.
Πληκτρολογώντας το **f** ανάβει το **C**, δηλαδή, το **f** κρυπτογραφείται ως **C**.




***Εικόνα 33**: Απλοποιημένη εκδοχή του Αινίγματος, με αλφάβητο αποτελούμενο από έξι μόνο γράμματα. Το σημαντικότερο στοιχείο της μηχανής είναι ο "αναδιατάκτης". Όταν στο πληκτρολόγιο χτυπηθεί το **b**, ένα ηλεκτρικό ρεύμα εισέρχεται στον "αναδιατάκτη", ακολουθεί την πορεία των εσωτερικών καλωδιώσεων, και τέλος αναδύεται έτσι ώστε να φωτίσει τον λαμπτήρα **A**. Το πλαίσιο στα δεξιά δείχνει πώς κρυπτογραφείται το καθένα από τα έξι γράμματα.*

Το μήνυμα café θα κρυπτογραφηθεί ως DBCE.Με αυτή τη βασική διάταξη, ο «αναδιατάκτης» ουσιαστικά καθορίζει ένα κρυπτογραφικό αλφάβητο, και η μηχανή μπορεί να χρησιμοποιηθεί για την εφαρμογή ενός απλού μονοαλφαβητικού κρυπτογράμματος υποκατάστασης. Ωστόσο η ιδέα του Σέμπιους ήταν να περιστρέφεται ο δίσκος «αναδιατάκτης» αυτόματα από το ένα έκτο μιας πλήρους περιστροφής κάθε φορά που κρυπτογραφείται ένα γράμμα(ή το ένα εικοστό έκτο μιας πλήρους περιστροφής για ένα πλήρες λατινικό αλφάββητο των 26 γραμμάτων).Η εικόνα 34 α δείχνει την ίδια δίαταξη με την εικόνα 33:και εδώ η πληκτρολόγηση του γράμματος b θα ανάψει το γράμμα A .Όμως αυτή τη φορά, αμέσως μετά την πληκτρολόγηση ενός γράμματος και το φωτισμό του πίνακα, ο «αναδιατάκτης» περιστρέφεται κατά το ένα έκτο μιας πλήρους περιστροφής μέχρι τη θέση που φαίνεται στην εικόνα 34 β.Αν τώρα πληκτρολογηθεί και πάλι το γράμμα b,θα ανάψει ένα διαφορετικό γράμμα στον πίνακα, το C.Αμέσως μετά ο «αναδιατάκτης» περιστρέφεται και πάλι καταλήγοντας στη θέση που φαίνεται στην εικόνα 34 γ.Τη φορά αυτή η πληκτρολόγηση του γράμματος b έξι φορές στη σειρά θα παραγάγει το κρυπτογραφικό κείμενο ACEBDC.Με άλλα λόγια, το κρυπτογραφικό αλφάβητο αλλάζει μετά από κάθε κρυπτογράφηση, και η κτυπτογράφηση του γράμματος b αλλάζει διαρκώς. Με τον περιστροφικό αυτό μηχανισμό, ο «αναδιατάκτης» ουσιαστικά προσδιορίζει 6 κρυπτογραφικά αλφάβητα,και η μηχανή μπορεί να χρησιμοποιηθεί για την εφαρμογή ενός πολυαλφαβητικού κρυτπογράμματος.Η περιστροφή του αναδιατάκτη είναι το σημαντικότερο χαρακτηριστικό της μηχανής του Σέρμπιους.Ωστόσο η μηχανή πάσχει από μια προφανή αδυναμία. Όταν το b πληκτρολογηθεί 6 φορές, ο «¨αναδιατάκτης» επιστρέφει στην αρχική του θές, και αν συνεχιστεί η πληκτρολόγηση του b,το σχήμα της κρυπτογράφησης θα επαναλαμβάνεται. Γενικά οι κρυπτογράφοι θέλουν να αποφεύγουν την επανάληψη επειδή εισάγει στο κανονικό κείμενο κανονικότητα και δομή,συμπτώματα ασθενούς κρυπτογράμματος.Το πρόβλημα αυτό μπορεί να θεραπευτεί με την εισαγωγή ενός δεύτερου δίσκου-«αναδιατάκτη».

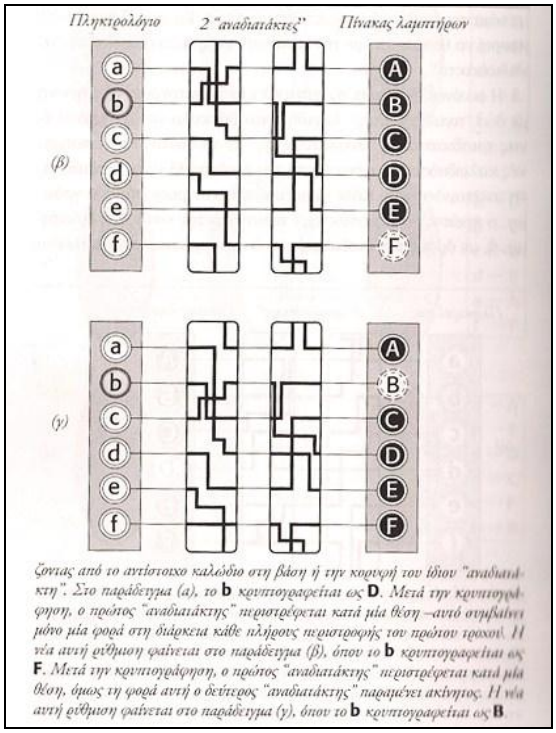



***Εικόνα 34**: Κάθε φορά που ένα γράμμα χτυπιέται στο πληκτρολόγιο, ο "αναδιατάκτης" περιστρέφεται κατά μία θέση, αλλάζοντας έτσι τον τρόπο πιθανής κρυπτογράφησης του κάθε γράμματος. Στο παράδειγμα (α) ο "αναδιατάκτης" κρυπτογραφεί το* **b** *ως* **A**, *αλλά στο παράδειγμα (β) ο νέος προσανατολισμός του "αναδιατάκτη" κρυπτογραφεί το* **b** *ως* **C**. *Στο παράδειγμα (γ) ο "αναδιατάκτης", αφού περιστραφεί κατά μια ακόμη θέση, κρυπτογραφεί το* **b** *ως* **E**. *Αφού κρυπτογραφήσει τέσσερα ακόμη γράμματα, και περιστραφεί κατά τέσσερις ακόμη θέσεις, ο "αναδιατάκτης" επανέρχεται στον αρχικό του προσανατολισμό.*

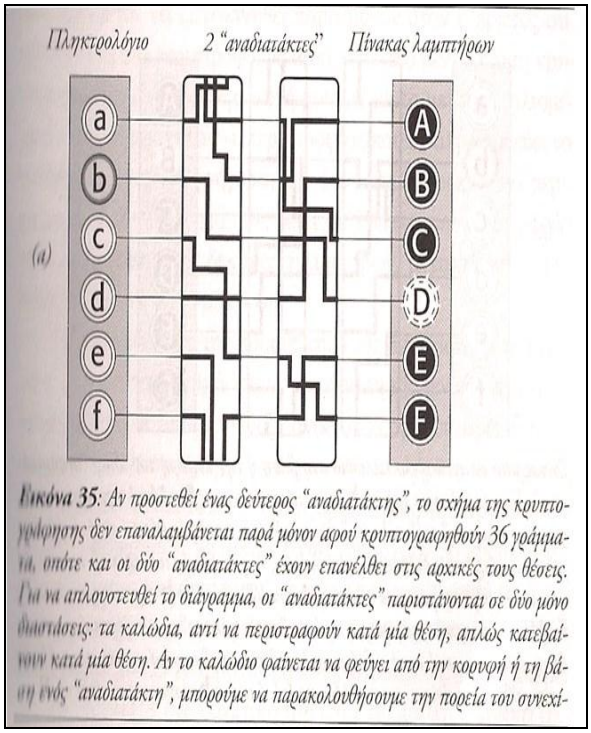
Ηεικόνα 35 δείχνει σχηματικά μια κρυπτογραφική μηχανή με δύο «αναδιατάκτες».

Επειδή είναι δύσκολο να σχεδιαστεί ένας τρισδιάστατος «αναδιατάκτης» με τρισδιάστετες εσωτερικές καλωδιώσεις η απεικόνιση της εικόνας 35 είναι δισδιάστατη αναπαράσταση.

Κάθε φορά που κρυπτογραφείται ένα γράμμα ο πρώτος «αναδιατάκτης» περιστρέφεται κατά ένα διάστημα, ή, με όρους του δισδιάστατου διαγράμματος,κάθε καλώδιο μετατοπίζεται κατά μια θέση. Αντίθετα,ο δεύτερος δίσκος-«αναδιατάκτης» παραμένει ακίνητος τον περισσότερο χρόνο.Κινείται μόνο όταν ο πρώτος «αναδιατάκτης» ολοκληρώσει μια πλήρη περιστροφή.Ο πρώτος «αναδιατάκτης» στερεώνεται με ένα δόντι, και μόνο όταν το δόντι αυτό φτάσει σε ένα ορισμένο σημείο, χτυπάει σε μια θέση το δεύτερο «αναδιατάκτη».




ζοντας από το αντίστοιχο καλώδιο στη βάση ή την κορυφή του ίδιου "αναδιατάκτη". Στο παράδειγμα (α), το **b** κρυπτογραφείται ως **D**. Μετά την κρυπτογράφηση, ο πρώτος "αναδιατάκτης" περιστρέφεται κατά μία θέση –αυτό συμβαίνει μόνο μία φορά στη διάρκεια κάθε πλήρους περιστροφής του πρώτου τροχού. Η νέα αυτή ρύθμιση φαίνεται στο παράδειγμα (β), όπου το **b** κρυπτογραφείται ως **F**. Μετά την κρυπτογράφηση, ο πρώτος "αναδιατάκτης" περιστρέφεται κατά μία θέση, όμως τη φορά αυτή ο δεύτερος "αναδιατάκτης" παραμένει ακίνητος. Η νέα αυτή ρύθμιση φαίνεται στο παράδειγμα (γ), όπου το **b** κρυπτογραφείται ως **B**.

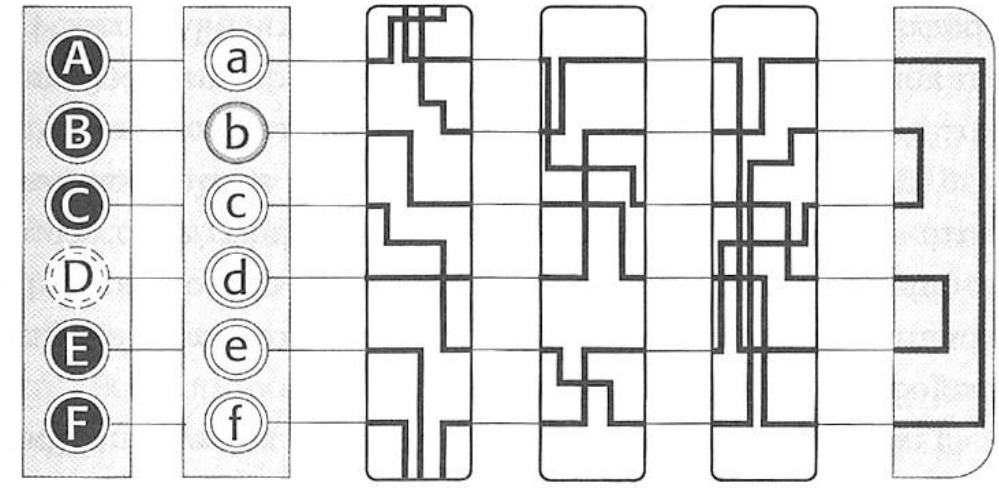



**Εικόνα 35**: Αν προστεθεί ένας δεύτερος "αναδιατάκτης", το σχήμα της κρυπτογράφησης δεν επαναλαμβάνεται παρά μόνον αφού κρυπτογραφηθούν 36 γράμματα, οπότε και οι δύο "αναδιατάκτες" έχουν επανέλθει στις αρχικές τους θέσεις. Για να απλουστευθεί το διάγραμμα, οι "αναδιατάκτες" παριστάνονται σε δύο μόνο διαστάσεις: τα καλώδια, αντί να περιστραφούν κατά μία θέση, απλώς κατεβαίνουν κατά μία θέση. Αν το καλώδιο φαίνεται να φεύγει από την κορυφή ή τη βάση ενός "αναδιατάκτη", μπορούμε να παρακολουθήσουμε την πορεία του συνεχί-

Στην εικόνα 35 α, ο πρώτος «αναδιατάκτης» βρίσκεται σε μια θέση που είναι έτοιμος να θέσει σε κίνηση τον δεύτερο.

Η πληκτρολόγηση και η κρυπτογράφηση ενός γράμματος μετακινεί το μηχανισμό στη διάταξη που φαίνεται στην εικόνα 35 β,όπου ο πρώτος «αναδιατάκτης» έχει μετακινηθεί κατά μία θέση και ο δεύτερος έχει τεθεί σε κίνηση ώστε να μετακινηθεί επίσης κατά μια θέση. Η πληκτρολόγηση και η κρυπτογράφηση ενός δεύτερου γράμματος μετακινεί και πάλι τον πρώτο «αναδιατάκτη» κατά μια θέση(εικόνα 35 γ),όμως αυτή τη φορά ο δεύτερος «αναδιατάκτης» έχει παραμείνει ακίνητος.Ο δεύτερος «αναδιατάκτης» δεν πρόκειται να ξανακινηθεί παρά μόνο όταν ο πρώτος συμπληρώσει μια περιστροφή,δηλαδή μετά από 5 ακόμη κρυπτογραφήσεις. Η διάταξη αυτή μοιάζει με το μετρητή χιλιομέτρων του αυτοκινήτου-ο περιστροφέας που αντιπροσωπεύει τα χιλιόμετρα γυρίζει γρήγορα,κι όταν συμπληρώσει μια περιστροφή φτάνοντας στο «9»,θέτει σε κίνηση τον περιστροφέα που εκπροσωπεί τις δεκάδες χιλιομέτρων μετακινώντας τον προς τα εμπρός κατά μια θέση.Το πλεονέκτημα της προσθήκης ενός δεύτερου αναδιατάκτη είναι ότι το σχήμα της κρυπτογράφησης δεν επαναλαμβάνεται μέχρις ότου ο δεύτερος αναδιατάκτης επιστρέψει στην αρχική του θέση,πράγμα που απιτεί 6 πλήρεις περιστροφές του πρώτου αναδιατάκτη,ή την κρυπτογράφηση συνολικά 36 γραμμάτων. Με άλλα λόγια υπάρχουν 36 ευδιάκριτες διατάξεις του αναδιατάκτη,πράγμα που ισοδυναμεί με αναλλαγή μεταξύ 36 κρυπτογραφικών αλφαβήτων. Με ένα πλήρες αλφάβητο των 26 γραμμάτων,η κρυπτογραφική μηχαν΄σ μπορεί να χρησιμοποιεί εναλλακτικά 676(26*26) κρυπτογραφικά αλφάβητα. Έτσι συνδυάζοντας τους αναδιατάκτες που ενίοτε αποκαλούνται και περιστροφείς,είναι δυνατόν να κατασκευάσουμε μια κρυπτογραφική μηχανή που εναλλάσεται συνεχώς μεταξύ διαφορετικών κρυπτογραφικών αλφαβήτων. Στη συνέχεια η διάταξη του «αναδιατάκτη» αλλάζε,έτσι ώστε όταν κρυπτογραφηθεί το επόμενο γράμμα,να κρυπτογραφηθεί σύμφωνα με ένα διαφορετικό κρυπτογραφικό αλφάβητο. Επιπλέον η όλη διαδικασία συντελείται με μεγάλη αποτελεσματικότητα και ακρίβεια,χάρη στην αυτόματη κίνηση των «αναδιατακτών» και την ταχύτητα του ηλεκτρισμού.

Πριν εξηγήσουμε λεπτομερώς πώς ήθελε ο Σέρμπιους να χρησιμοποιείται η κρυπτογραφική μηχανή του,είναι απαραίτητο να περιγράψουμε δυο ακόμη βασικά στοιχεία του Αινίγματος,τα οποία φαίνονται στην εικόνα 36.




***Εικόνα 36**: Το σχέδιο του Σέρμπιους για το Αίνιγμα περιλάμβανε έναν τρίτο "αναδιατάκτη" και έναν ανακλαστή που στέλνει το ρεύμα πίσω διαμέσου των "αναδιατακτών". Στη συγκεκριμένη ρύθμιση, η πληκτρολόγηση του* **b** *φωτίζει τελικά το* **D** *στον πίνακα λαμπτήρων, που εδώ απεικονίζεται δίπλα στο πληκτρολόγιο.*

Πρώτον η κρυπτογραφική μηχανή του Σέρμπιους χρησιμοποιούσε και τρίτο «αναδιατάκτη» για επιπλέον πολυπλοκότητα-για ένα πλήρες αλφάβητο, οι τρεις αναδιατάκτες παρέχουν 17.576 (26*26*26) διαφορετικούς συνδυασμούς. Δεύτερον ο Σέρμπιους πρόσθεσε στην εφεύρεσή του έναν ανακλαστή. Ο ανακλαστής μοιάζει κάπως με τον αναδιατάκτη κατά το ότι είναι ένας λαστιχιένιος δίσκος με εσωτερικές καλωδιώσεις, διαφέρει όμως από αυτόν επειδή δεν περιστρέφεται, και τα καλώδια εισέρχονται από τη μια πλευρά του και εξέρχονται πάλι από την ίδια πλευρά. Με αυτόν τον ανακλαστή στη θέση του, ο χειριστής πληκτρολογεί ένα γράμμα ,το οποίο στέλνει ένα ηλεκτρικό σήμα διαμέσου τριών «αναδιατακτών». Όταν ο ανακλαστής λάβει το εισερχόμενο σήμα, το στέλνει πίσω μέσω τριών ίδιων «αναδιατακτών», αλλά από διαφορετική οδό. Για παράδειγμα με τη διάταξη της εικόνας 36,η πληκτρολόγηση του γράμματος b στέλνει ένα σήμα, μέσω των τριών «αναδιατακτών» ,στον ανακλαστή, και το σήμα επιστρέφει μέσω των καλώδίων για να φτάσει στο γράμμα D.Το σήμα στην πραγματικότητα δεν εμφανίζεται μέσω του πληκτρολογίου όπως θα μπορούσε κανείς να συμπεράνει από την εικόνα 36,αλλά διοχετεύεται στον πίνακα με τους λαμπτήρες. Εκ πρώτης όψεως ο ανακλαστής, μοιάζει να είναι μια ανώφελη προσθήκη στη μηχανή, γιατί η στατική φύση του σημαίνει ότι δεν αυξάνει τον αριθμό των κρυπτογραφικών αλφαβήτων. Ωστόσο, τα οφέλη του θα γίνουν σαφή όταν δούμε πώς χρησιμοποιείτο στην πράξη η μηχανή για την κρυπτογράφηση και την αποκρυπτογράφηση και την αποκρυπτογράφηση ενός μηνύματος. Ένας χειριστής θέλει να στείλει ένα μυστικό μήνυμα.Πριν αρχίσει η κρυπτογράφηση, ο χειριστής πρέπει πρώτα να περιστρέψει τους αναδιατάκτες σε μια συγκεκριμένη θέση έναρξης. Υπάρχουν 17.576 πιθανές αναδιατάξεις, και επομένως 17.576 πιθανές θέσεις έναρξης. Η αρχική ρύθμιση των «αναδιατακτών» θα προσδιορίσει τον τρόπο κρυπτογράφησης του μηνύματος.

Το Αίνιγμα μπορεί να θεωρηθεί ως ένα γενικό κρυπτογραφικό σύστημα, και η αρχική ρύθμιση είναι αυτή που καθορίζει τις ακριβείς λεπτομέρειες της κρυπτογράφησης. Με άλλα λόγια η αρχική ρύθμιση παρέχει το κλειδί. Την αρχική ρύθμιση συνήθως την υπαγορεύει ένα κωδικό βιβλίο που καταγράφει το κλειδί για την κάθε μέρα και που είναι προσιτό σε όλους όσους μετέχουν στο δίκτυο επικοινωνιών. Η διανομή του κωδικού βιβλίου απαιτεί χρόνο και προσπάθεια, επειδή όμως απαιτείται μόνο ένα κλειδί τη μέρα, μπορεί να ληφθεί μέριμνα ώστε να στέλνεται μια φορά κάθε 4 εβδομάδες ένα κωδικό βιβλίο που να περιέχει 28 κλειδιά. Συγκριτικά αν ένας στρατός έπρεπε να χρησιμοποιήσει ένα κρυπτόγραμμα του μπλοκ μιας χρήσης, θα χρειαζόταν ένα νέο κλειδί για κάθε μήνυμα, και η διανομή των κλειδιών θα ήταν πολύ πιο επίπονο έργο. Όταν οι αναδιατάκτες διευθετηθούν σύμφωνα με τις καθημερινές οδηγίες του κωδικού βιβλίου, ο αποστολέας μπορεί να αρχίσει την κρυπτογράφηση. Πληκτρολογεί το πρώτο γράμμα του μηνύματος, βλέπει ποιο γράμμα ανάβει στον πίνακα με τους λαμπτήρες και το καταγράφει ως το πρώτο

γράμμα του κρυπτογραφικού κειμένου. Στη συνέχεια, αφού ο αναδιατάκτης προχωρήσει αυτόματα κατά μια θέση, ο αποστολέας πληκτρολογεί το δεύτερο γράμμα του μηνύματος κ.ο.κ. Όταν δημιουργήσει το πλήρες κρυπτογραφικό κείμενο, το παραδίδει σε έναν ραδιοχειριστή ο οποίος το διαβιβάζει στον παραλήπτη. Για να αποκρυπτογραφήσει το μήνυμα, ο παραλήπτης χρειάζεται να έχει μια δεύτερη μηχανή Αίνιγμα και ένα αντίγραφο του κωδικού βιβλίου που περιέχει την αρχική ρύθμιση του αναδιατάκτη για τη συγκεκριμένη ημέρα. Ρυθμίζει τη μηχανή σύμφωνα με το βιβλίο, πληκτρολογεί γράμμα-γράμμα το κρυπτογραφικό κείμενο, και ο πίνακας των λαμπτήρων δείχνει το κανονικό κείμενο. Με άλλα λόγια, ο αποστολέας πληκτρολόγησε το κανονικό κείμενο για να παραγάγει το κρυπτογραφικό, και τώρα ο παραλήπτης πληκτρολογεί το κρυπτογραφικό κείμενο για να παραγάγει το κανονικό-η κρυπτογράφηση και αποκρυπτογράφηση είναι αντικατοπτριζόμενες διαδικασίες. Η ευκολία της αποκρυπτογράφησης οφείλεται στον ανακλαστή. Από την εικόνα 36 μπορούμε να δούμε ότι αν πληκτρολογήσουμε το b και ακολουθήσουμε την ηλεκτρική διαδρομή, επιστρέφουμε στο D.Με τον ίδιο τρόπο να πληκτρολογήσουμε το d και ακολουθήσουμε την ηλεκτρική διαδρομή, επιστρέφουμε στο B.Η μηχανή κρυπτογραφεί ένα γράμμα του κανονικού κειμένου μετατρέποντάς το σε γράμμα του κρυπτογραφικού, και όσο η μηχανή βρίσκεται στη ίδια ρύθμιση, θα αποκρυπτογραφεί το ίδιο γράμμα του κρυπτογραφικού κειμένου στο ίδιο γράμμα του κανονικού.

Είναι προφανές ότι το κλειδί και το κωδικό βιβλίο που το περιέχει δεν πρέπει ποτέ να πέσουν σε εχθρικά χέρια. Είναι πιθανό μια μηχανή Αίνιγμα να περιέλθει στην κατοχή του εχθρού, αλλά αν δεν γνωρίζει τις αρχικές ρυθμίσεις που χρησιμοποιήθηκαν για την κρυπτογράφηση δεν μπορεί εύκολα να αποκρυπτογραφήσει ένα υποκλαπέν μήνυμα. Χωρίς το κρυπτογραφικό βιβλίο ο κρυπταναλυτής του εχθρού μπορεί να καταφύγει στον έλεγχο όλων των πιθανών κλειδιών, που σημαίνει να δοκιμάσει 17.576 πιθανές αρχικές ρυθμίσεις του «αναδιατάκτη». Ο απελπισμένος κρυπταναλυτής θα διευθετήσει τη μηχανή Αίνιγμα που έχει πέσει στα χέρια του με μια συγκεκριμένη ρύθμιση του «αναδιατάκτη», θα πληκτρολογήσει ένα μικρό τμήμα του κρυπτογραφικού κειμένου και θα δει αν το προκύπτον κανονικό κείμενο βγάζει κάποιο νόημα. Αν όχι, θα αλλάξει τη ρύθμιση του «αναδιατάκτη» και θα ξαναπροσπαθήσει. Αν είναι σε θέση να ελέγχει μια ρύθμιση του «αναδιατάκτη» ανά λεπτό και εργάζεται νυχθημερόν θα χρειαστεί περίπου δύο εβδομάδες για να ελέγξει όλες τις ρυθμίσεις. Πρόκειται για ένα σχετικά καλό επίπεδο ασφάλειας, αν όμως ο εχθρός στρώσει στη δουλειά δώδεκα άτομα τότε όλες οι ρυθμίσεις μπορούν να ελεγχθούν μέσα σε μία μέρα. Έτσι ο Σέρμπιους αποφάσισε να βελτιώσει την ασφάλεια της εφεύρεσής του αυξάνοντας τον αριθμό των αρχικών ρυθμίσεων και άρα και τον αριθμό των πιθανών κλειδιών. Θα μπορούσε να αυξήσει την ασφάλεια προσθέτοντας κι άλλους «αναδιατάκτες» (κάθε νέος αναδιατάκτης πολλαπλασιάζει επί 26 τον αριθμό των κλειδιών), όμως κάτι τέτοιο θα αύξανε το μέγεθος του Αινίγματος. Αντ' αυτού πρόσθεσε δύο άλλα στοιχεία. Πρώτον έκανε τους αναδιατάκτες κινητούς και αμοιβαία εναλλάξιμους. Έτσι για παράδειγμα, ο πρώτος δίσκος «αναδιατάκτης» μπορούσε να μετακινηθεί στην τρίτη θέση και ο τρίτος στην πρώτη. Η διευθέτηση των «αναδιατακτών» επηρεάζει την κρυπτογραφική διαδικασία, και συνεπώς η ακριβής τους θέση είναι καίριας σημασίας για την κρυπτογράφηση και την αποκρυπτογράφηση. Υπάρχουν 6 διαφορετικοί τρόποι διευθέτησης των τριών «αναδιατακτών», οπότε αυτό το χαρακτηριστικό πολλαπλασιάζει επί 6 τον αριθμό των αρχικών πιθανών ρυθμίσεων, δηλαδή τον αριθμό των κλειδιών. Το δεύτερο νέο χαρακτηριστικό ήταν η παρεμβολή ενός πίνακα βυσμάτων μεταξύ του πληκτρολογίου και του πρώτου «αναδιατάκτη». Για παράδειγμα ένα καλώδιο θα μπορούσε να χρησιμοποιηθεί για να συνδέσει τις υποδοχές a και b του πίνακα βυσμάτων, έτσι ώστε όταν ο κρυπτογράφος θέλει να αποκρυπτογραφήσει το γράμμα b, το ηλεκτρικό σήμα να ακολουθεί, μέσω των «αναδιατακτών» , τη διαδρομή που θα ακολουθούσε το a και αντίστροφα.

Ο χειριστής του Αινίγματος είχε 6 καλώδια και επομένως 6 ζευγάρια γραμμάτων μπορούσαν να ανταλλαγούν αφήνοντας δεκατέσσερα γράμματα ασύνδετα και μη ανταλλασσόμενα. Τα γράμματα τα οποία ανταλλάσσει ο πίνακας βυσμάτων αποτελούν μέρος της ρύθμισης της μηχανής και συνεπώς θα πρέπει να προσδιορίζονται στο κωδικό βιβλίο. Η εικόνα 37 δείχνει τη διάταξη της μηχανής περιλαμβανομένου του πίνακα βυσμάτων. Επειδή το διάγραμμα αναφέρεται σε αλφάβητο αποτελούμενο από 6 γράμματα, έχει ανταλλαγεί μόνο ένα ζευγάρι γραμμάτων, τα a και b. Η μηχανή του Σέρμπιους περιλαμβάνει ένα ακόμη στοιχείο, το δακτύλιο. Παρότι ο δακτύλιος έχει κάποια επίδραση στην κρυπτογράφηση, είναι το λιγότερο σημαντικό μέρος του Αινίγματος και γι αυτόν το λόγο δεν θα περιγραφεί παρακάτω. Αφού αναφέρθηκαν όλα τα κύρια στοιχεία του Αινίγματος, μπορεί τώρα να υπολογιστεί ο αριθμός των κλειδιών συνδυάζοντας τον αριθμό των πιθανών καλωδιώσεων του πίνακα βυσμάτων με τον αριθμό των πιθανών διευθετήσεων και προσανατολισμών των «αναδιατακτών».

Ο παρακάτω κατάλογος δείχνει την κάθε μεταβλητή της μηχανής και τον αντίστοιχο αριθμό πιθανοτήτων που αντιστοιχεί σε καθεμία:

*Προσανατολισμοί των «αναδιατακτών».* Καθένας από τους τρεις αναδιατάκτες μπορεί να ρυθμιστεί σε έναν από τους 26 προσανατολισμούς.
Υπάρχουν επομένως 26*26*26 ρυθμίσεις : 17.576

*Διάταξη των «αναδιατακτών».* Οι τρεις «αναδιατάκτες» (1,2 και 3) μπορούν να τοποθετηθούν με οποιαδήποτε από τις εξής σειρές: 123, 132, 213, 231, 312, 321 6

*Πίνακας βυσμάτων.* Ο αριθμός των τρόπων με τους οποίους μπορούν να συνδεθούν και άρα να εναλλάσσονται 6 από τα 26 γράμματα είναι τεράστιος: 100.391.791.500

*Σύνολο.* Ο συνολικός αριθμός των κλειδιών Είναι το γινόμενο των τριών παραπάνω αριθμών: 17.576*6*100.391.791.500 = 10.000.000.000.000.000

Εφόσον ο αποστολέας και ο παραλήπτης έχουν συμφωνήσει για τις καλωδιώσεις του πίνακα βυσμάτων, τη σειρά των «αναδιατακτών» και τους αντίστοιχους προσανατολισμούς των, δηλαδή τους τρεις παράγοντες που καθορίζουν το κλειδί μπορούν εύκολα να κρυπτογραφούν και να αποκρυπτογραφούν μηνύματα. Όμως ένας υποκλοπέας εχθρός που δεν ξέρει το κλειδί, θα πρέπει να ελέγξει ένα προς τα 10.000.000.000.000.000 πιθανά κλειδιά για να σπάσει το κρυπτογραφικό κείμενο. Για να γίνει πιο κατανοητό, ένας φιλότιμος κρυπταναλυτής που είναι σε θέση να ελέγχει μια ρύθμιση ανά λεπτό, θα χρειαζόταν περισσότερο χρόνο από την ηλικία του σύμπαντος για να ελέγξει όλες τις ρυθμίσεις. Εφόσον η μεγαλύτερη συμβολή στον αριθμό των κλειδιών προέρχεται από τον πίνακα βυσμάτων, θα μπορούσε κανείς να διερωτηθεί γιατί ο Σέρμπιους μπήκε στον κόπο να ασχοληθεί με τους «αναδιατάκτες». Ο πίνακας βυσμάτων από μόνος του θα έδινε ένα απλό κρυπτόγραμμα μονοαλφαβητικής υποκατάστασης εναλλάσσοντας μόλις 12 γράμματα. Το πρόβλημα με τον πίνακα βυσμάτων είναι ότι από την αρχή που θα αρχίσει η κρυπτογράφηση οι συνδέσεις δεν αλλάζουν οπότε από μόνος του θα δημιουργούσε ένα κρυπτογραφικό κείμενο που θα μπορούσε να σπάσει με ανάλυση συχνοτήτων και ταυτόχρονα την εφοδίασε με ένα τεράστιο αριθμό πιθανών κλειδιών.

Ο Σέρμπιους πήρε την πρώτη του ευρεσιτεχνία το 1918. Η κρυπτογραφική μηχανή του περιεχόταν σε ένα συμπαγές κουτί διαστάσεων μόλις 34*28*15 εκ. αλλά ζύγιζε 12 κιλά.

Η παρακάτω εικόνα δείχνει μια μηχανή Αίνιγμα με το εξωτερικό καπάκι ανοιχτό έτοιμη για χρήση. Φαίνεται το πληκτρολόγιο στο οποίο πληκτρολογούνται τα γράμματα του κανονικού κειμένου, και από πάνω του τον πίνακα των λαμπτήρων όπου εμφανίζεται το προκύπτον κρυπτογραφικό κείμενο. Κάτω από το πληκτρολόγιο βρίσκεται ο πίνακας βυσμάτων. Υπάρχουν περισσότερα από 6 ζευγάρια γραμμάτων τα οποία ανταλλάσσει ο πίνακας επειδή το συγκεκριμένο Αίνιγμα είναι μια λίγο μεταγενέστερη τροποποίηση του αρχικού μοντέλου το οποίο περιγράφηκε παραπάνω.

Ο Σέρμπιους πίστευε ότι το Αίνιγμα ήταν απόρθητο και ότι η κρυπτογραφική του ισχύς θα το έκανε περιζήτητο. Προσπάθησε να προωθήσει τη μηχανή του τόσο στη στρατιωτική όσο και στην επιχειρηματική κοινότητα, προσφέροντας διαφορετικές παραλλαγές στην καθεμία. Για παράδειγμα, στους επιχειρηματίες πρότεινε το βασικό μοντέλο του Αινίγματος, ενώ στο υπουργείο εξωτερικών ένα διπλωματικό μοντέλο πολυτελείας με εκτυπωτή στη θέση του πίνακα λαμπτήρων. Η τιμή της κάθε μονάδας ανερχόταν στο ποσό των 20.000 σημερινών αγγλικών λιρών.

Δυστυχώς το υψηλό κόστος της μηχανής αποθάρρυνε τους επίδοξους αγοραστές. Οι επιχειρηματίες έλεγαν ότι δεν μπορούσαν να ανταπεξέλθουν στα έξοδα που απαιτούσε η ασφάλεια την οποία τους παρείχε το Αίνιγμα αλλά ο Σέρμπιους πίστευε ότι δε μπορούσαν να κάνουν χωρίς αυτό. Πρόβαλλε το επιχείρημα ότι

η κλοπή ενός ζωτικού μηνύματος από έναν επαγγελματικό ανταγωνιστή μπορούσε να κοστίσει ολόκληρη περιουσία σε μια εταιρία, όμως ελάχιστοι ήταν οι επιχειρηματίες που έδιναν σημασία. Επίσης απρόθυμοι ήταν και οι γερμανοί στρατιωτικοί αφού αγνοούσαν τη ζημιά που τους είχαν προκαλέσει τα μη ασφαλή τους κρυπτογράμματα κατά τη διάρκεια του Μεγάλου Πολέμου. Για παράδειγμα είχαν παρασυρθεί να πιστέψουν ότι το τηλεγράφημα του Τσίτσερμαν είχε κλαπεί από αμερικάνους κατάσκοπους στο Μεξικό και έτσι έριχναν το φταίξιμο στη μεξικανική ασφάλεια. Δεν είχαν ακόμη αντιληφθεί ότι στην πραγματικότητα το τηλεγράφημα το είχαν υποκλέψει και αποκρυπτογραφήσει οι Βρετανοί και ότι το φιάσκο Τσίτσερμαν ήταν στην πραγματικότητα μια αποτυχία της γερμανικής κρυπτογραφίας.

Εκτός από τον Σέρμπιους, άλλοι τρεις εφευρέτες σε τρεις διαφορετικές χώρες είχαν συλλάβει ανεξάρτητα και σχεδόν ταυτόχρονα την ιδέα μιας κρυπτογραφικής μηχανής βασισμένης σε περιστρεφόμενους αναδιατάκτες αλλά για καμία από αυτές δεν εκδηλώθηκε και πάλι ενδιαφέρον.

Αμέσως μετά τον Πρώτο Παγκόσμιο Πόλεμο, η κυβέρνηση των ΗΠΑ είχε ιδρύσει το Αμερικανικό Μαύρο Δωμάτιο, ένα πολύ αποτελεσματικό κρυπτογραφικό γραφείο στελεχωμένο με μια ομάδα είκοσι κρυπταναλυτών με επικεφαλή τον περίφημο Χέρμπεν Γιάρντλει. Αργότερα ο Χέρμπεν έγραφε ότι το Μαύρο Δωμάτιο, αμπαρωμένο, κρυμμένο, φρουρούμενο βλέπει τα πάντα και ακούει τα πάντα. Το αμερικανικό Μαύρο Δωμάτιο έλυσε 45.000 κρυπτογράμματα σε μια δεκαετία.

Όταν όμως ο Χέρμπεν στα μέσα της δεκαετίας του 1920 έχτισε ένα εργοστάσιο αξίας 380.000 δολαρίων, Πρόεδρος των ΗΠΑ ήταν ο Χέρμπετ Χούβερ, ο οποίος προσπαθούσε να εγκαινιάσει μια νέα εποχή εμπιστοσύνης στις διεθνείς σχέσεις και διέλυσε το Μαύρο Δωμάτιο. Ο υπουργός εξωτερικών Χένρι Στίμσον δήλωνε ότι «οι κύριοι δεν θα πρέπει να διαβάζουν ο ένας τις επιστολές του άλλου». Αν ένα έθνος πιστεύει ότι είναι λάθος να διαβάζεις τα μηνύματα των άλλων τότε αρχίζει να πιστεύει ότι και οι άλλοι δεν θα διαβάζουν τα δικά του, οπότε δεν βλέπει σε τι χρειάζονται οι πολύπλοκες κρυπτογραφικές μηχανές. Ο Χέρμπεν πούλησε όλες κι όλες 12 μηχανές στη τιμή των 1.200 δολαρίων περίπου και το 1926 σύρθηκε σε δίκη από δυσαρεστημένους μετόχους και καταδικάστηκε με βάση το Διάταγμα περί Συντεχνιακής Ασφάλειας της Καλιφόρνιας. Ευτυχώς για τον Σέρμπιους οι Γερμανοί στρατιωτικοί αναγκάστηκαν εκ των πραγμάτων να εκτιμήσουν την αξία του Αινίγματος χάρη σε δύο βρετανικά ντοκουμέντα. Το πρώτο ήταν το κείμενο του Ουίστον Τσόρτσιλ «η παγκόσμια κρίση» που δημοσιεύτηκε το 1923 και το οποίο περιλάμβανε μια δραματική περιγραφή του πώς οι Βρετανοί είχαν αποκτήσει πρόσβαση σε ανεκτίμητης αξίας βρετανικό κρυπτογραφικό υλικό. Το υλικό αυτό είχε βοηθήσει τους κρυπταναλυτές του Δωματίου 40 να σπάζουν τα κρυπτογράμματα των Γερμανών. Τελικά, σχεδόν μια δεκαετία μετά, οι Γερμανοί συνειδητοποίησαν την αποτυχία της ασφάλειας των επικοινωνιών τους. Το 1923 επίσης, το Βρετανικό Βασιλικό Ναυτικό δημοσίευσε την επίσημη εκδοχή του της ιστορίας του Πρώτου Παγκοσμίου Πολέμου που επαναλάμβανε το γεγονός ότι η υποκλοπή και κρυπτανάλυση των γερμανικών επικοινωνιών είχε εξασφαλίσει στους Συμμάχους σαφές πλεονέκτημα. Αυτά τα σημαντικά επιτεύγματα της Βρετανικής Κατασκοπίας ισοδυναμούσαν με αμετάκλητη καταδίκη των υπευθύνων της γερμανικής ασφάλειας, που αναγκάστηκαν να παραδεχτούν στη αναφορά τους ότι η διοίκηση του γερμανικού στόλου της οποίας τα μηνύματα υποκλέπτονταν και αποκρυπτογραφούνταν από τους Άγγλους έπαιζε με ανοιχτά χαρτιά εναντίον της βρετανικής διοίκησης.

Οι Γερμανοί στρατιωτικοί διεξήγαγαν έρευνα για το πώς να αποφύγουν την επανάληψη των αποτυχιών του Πρώτου Παγκοσμίου Πολέμου και συμπέραναν ότι το Αίνιγμα πρόσφερε την καλύτερη λύση. Το 1925 ο Σέρμπιους άρχισε μαζική παραγωγή Αινιγμάτων, τα οποία την επόμενη χρονιά πήγαν στο στρατό και στη συνέχεια χρησιμοποιήθηκαν από την κυβέρνηση και από κρατικούς οργανισμούς όπως οι σιδηρόδρομοι. Τα Αινίγματα αυτά ήταν διαφορετικά από τις προηγούμενες μηχανές που είχε πουλήσει προηγουμένως στην επιχειρηματική κοινότητα επειδή οι «αναδιατάκτες» είχαν διαφορετική εσωτερική καλωδίωση. Έτσι οι κάτοχοι της εμπορικής παραλλαγής του Αινίγματος δεν είχαν πλήρη γνώση των κυβερνητικών και στρατιωτικών μοντέλων.

Στις δυο επόμενες δεκαετίες ο γερμανικός στρατός αγόρασε πάνω από 30.000 μηχανές Αίνιγμα. Η εφεύρεση του Σέρμπιους εφοδίασε τους Γερμανούς στρατιωτικούς με το ασφαλέστερο σύστημα κρυπτογράφησης στον κόσμο, κι όταν ξέσπασε ο Δεύτερος Παγκόσμιος Πόλεμος, οι επικοινωνίες τους προστατεύονταν από ένα πρωτόγνωρο επίπεδο κρυπογράφησης. Τότε φαινόταν ότι το Αίνιγμα θα έπαιζε ζωτικό ρόλο στην εξασφάλιση της νίκης των Ναζί, όμως εξασφάλισε την πτώση του Χίτλερ. Ο Σέρμπιους δεν έζησε αρκετά για να δει τις επιτυχίες και τις αποτυχίες του κρυπτογραφικού του συστήματος. Το 1929 έχασε τον έλεγχο της άμαξας που οδηγούσε με αποτέλεσμα να πεθάνει στις 30 Μαίου από εσωτερικές κακώσεις.

Τα χρόνια μετά τον πρώτο παγκόσμιο πόλεμο, οι βρετανοί κρυπταναλυτές του Δωματίου 40 εξακολούθησαν να παρακολουθούν τις γερμανικές επικοινωνίες. Το 1926 άρχισαν να υποκλέπτουν μηνύματα που τους έφερναν σε πλήρη σύγχυση. Είχε φτάσει το Αίνιγμα, και καθώς ο αριθμός των μηχανών αύξανε, η ικανότητα του δωματίου 40 να συγκεντρώνει πληροφορίες ελαττωνόταν με γρήγορους ρυθμούς. Αμερικάνοι και Γάλλοι καταπιάστηκαν και αυτοί με το κρυπτόγραμμα του Αινίγματος αλλά και οι δικές τους απόπειρες απέτυχαν, και σύντομα εγκατέλειψαν κάθε ελπίδα να το σπάσουν. Τώρα η Γερμανία διέθετε τις ασφαλέστερες επικοινωνίες στον κόσμο. Η γρήγορη παραίτηση των κρυπταναλυτών των συμμάχων από το σπάσιμο του Αινίγματος βρισκόταν στους αντίποδες της επιμονής τους μόλις μια δεκαετία πριν, στον Πρώτο Παγκόσμιο Πόλεμο. Αντιμέτωποι με την προοπτική της ήττας, εργάζονταν τότε νυχθημερόν για να εκπορθήσουν τα γερμανικά κρυπτογράμματα. Ο φόβος φαίνεται να ήταν η βασική κινητήρια δύναμη και η αντιξοότητα είναι ένα από τα θεμέλια του επιτυχημένου σπασίματος κωδίκων. Ωστόσο μετά τον Πρώτο Παγκόσμιο Πόλεμο οι Σύμμαχοι δεν φοβούνταν πλέον κανέναν. Η Γερμανία είχε ηττηθεί ολοσχερώς και οι Σύμμαχοι βρίσκονταν σε θέση ισχύος, με αποτέλεσμα να χάσουν τον κρυπταναλυτικό τους ζήλο. Οι κρυπταναλυτές τους λιγόστευαν σε αριθμό και οι ικανότητές τους μειώνονταν.

Ο αποστρατευμένος Γερμανός Χανς-Τίλο Σμιτ ήταν εκείνος που έκανε το πρώτο βήμα προς το σπάσιμο του κρυπτογράμματος του Αινίγματος. Είχε γεννηθεί στο Βερολίνο το 1888 και ήταν ο δευτερότοκος γιος ενός διακεκριμένου καθηγητή και της αριστοκράτισσας γυναίκας του. Ο Σμιτ επέλεξε να σταδιοδρομήσει στο γερμανικό στρατό και πολέμησε στον Πρώτο Παγκόσμιο Πόλεμο όμως δεν κρίθηκε αρκετά άξιος να παραμείνει στο στρατό μετά τι δραστικές περικοπές οι οποίες επιβλήθηκαν ως αποτέλεσμα της Συνθήκης των Βερσαλιών. Στη συνέχεια προσπάθησε να πετύχει ως επιχειρηματίας, όμως το εργοστάσιο σαπωνοποιίας του έκλεισε λόγω της μεταπολεμικής οικονομικής ύφεσης και του υπερπληθωρισμού. Μετά την κατάρρευση της επιχείρησής του ο Χανς-Τίλο βρήκε δουλειά στο Βερολίνο, στο Chiffrierstelle, δηλαδή στο γραφείο που είχε την ευθύνη για τη διαχείριση των κρυπτογραφημένων επικοινωνιών της Γερμανίας. Επρόκειτο για το διοικητικό κέντρο του Αινίγματος, ένα άκρως απόρρητο ίδρυμα που ασχολείτο με ιδιαίτερα ευαίσθητες πληροφορίες. Ο Χανς-Τίλο κέρδιζε χρήματα πουλώντας μυστικές πληροφορίες σχετικά με το Αίνιγμα σε ξένες δυνάμεις βλάπτοντας την ασφάλεια της χώρας του. Στις 8 Νοεμβρίου του 1931, ο Σμιτ έφτασε στο Γκραντ Οτέλ της βελγικής πόλης Βερβιέ για να συναντήσει ένα Γάλλο μυστικό πράκτορα με το κωδικό όνομα Ρεξ. Έναντι αμοιβής 10.000 μάρκων ο Σμιτ επέτρεψε στον Ρεξ να φωτογραφήσει δύο έγγραφα : «Gebrauchsanweisung fur die Chiffriersmaschine Enigma» (οδηγίες χρήσης για την κρυπτογραφική μηχανή Αίνιγμα) και « Schlusselanleitung fur die Chiffriersmaschine Enigma» ( επεξηγηματικές οδηγίες για την κρυπτογραφική μηχανή Αίνιγμα). Τα έγγραφα αυτά ήταν ουσιαστικά οδηγίες χρήσης για τη μηχανή Αίνιγμα και παρότι δεν περιλάμβαναν λεπτομερή περιγραφή των καλωδιώσεων στο εσωτερικό κάθε «αναδιατάκτη» περιείχαν όλες τις πληροφορίες που χρειάζονταν για να προκύψει η διάταξη των καλωδιώσεων αυτών. Χάρη στην προδοσία του Σμιτ οι Σύμμαχοι μπορούσαν να κατασκευάσουν ένα ακριβές αντίγραφο του γερμανικού στρατιωτικού μοντέλου του Αινίγματος. Ωστόσο αυτό δεν ήταν αρκετό για να αποκρυπτογραφηθούν μηνύματα κρυπτογραφημένα με τη μηχανή Αίνιγμα. Η ισχύς του κρυπτογράμματος δεν εξαρτάται από τη μυστικότητα της μηχανής, αλλά από τη μυστικότητα των αρχικών της ρυθμίσεων, δηλαδή του κλειδιού της κρυπτογράφησης. Αν ένας κρυπταναλυτής θέλει να αποκρυπτογραφήσει ένα υποκλαπέν μήνυμα τότε εκτός του να έχει αντίγραφο του Αινίγματος, πρέπει επιπλέον να ανακαλύψει ποιο από τα εκατομμύρια δισεκατομμυρίων των πιθανών κλειδιών χρησιμοποιήθηκε για την κρυπτογράφησή του. Ένα γερμανικό υπόμνημα το διατύπωνε ως εξής: «Για την αποτίμηση της ασφάλειας του κρυπτογραφικού συστήματος, έχουμε υποθέσει ότι ο εχθρός έχει στην κατοχή του τη μηχανή»

Το Bureau de Chiffre (Κρυπτογραφικό γραφείο) δεν μπήκε καν στον κόπο να κατασκευάσει αντίγραφο του στρατιωτικού Αινίγματος, επειδή πίστευε ότι το επόμενο στάδιο, δηλαδή το να βρουν το κλειδί που απαιτείτο για την αποκρυπτογράφηση ενός συγκεκριμένου μηνύματος κρυπτογραφημένου με το Αίνιγμα ήταν ακατόρθωτο. Έτσι οι Γάλλοι σύμφωνα με τους όρους της προ δεκαετίας συμφωνίας στρατιωτικής συνεργασίας με τους Πολωνούς, απλώς παρέδωσαν τις φωτογραφίες των εγγράφων στους συμμάχους του, μεταθέτοντας το χωρίς ελπίδα έργο του σπασίματος του Αινίγματος στο γραφείο Ζιφρόφ. Το Γραφείο συνειδητοποίησε ότι τα έγγραφα ήταν απλώς ένα σημείο εκκίνησης, σε αντίθεση όμως με τους Γάλλους, οι Πολωνοί είχαν ένα σημαντικό κίνητρο, το φόβο της εισβολής. Ήταν πεπεισμένοι ότι θα πρέπει να υπήρχε κάποιος σύντομος δρόμος για να βρουν το κλειδί ενός μηνύματος κρυπτογραφημένου με το Αίνιγμα και ότι θα μπορούσαν να τον ανακαλύψουν αν αφιέρωναν αρκετή προσπάθεια, επινοητικότητα και μυαλό. Τα έγγραφα του Σμιτ, εκτός του ότι αποκάλυψαν τις εσωτερικές καλωδιώσεις των «αναδιατακτών»

επιπλέον εξηγούσαν λεπτομερώς τη διάταξη των κωδικών βιβλίων που χρησιμοποιούσαν οι Γερμανοί. Κάθε μήνα οι χειριστές του Αινίγματος λάβαιναν ένα νέο κωδικό βιβλίο που προσδιόριζε ποιο κλειδί έπρεπε να χρησιμοποιηθεί για την κάθε μέρα.

Για παράδειγμα, την πρώτη μέρα του μήνα το κωδικό βιβλίο θα μπορούσε να προσδιορίσει το ακόλουθο *ημερήσιο κλειδί:*

1. *Ρύθμιση πίνακα βυσμάτων:* ***A/L – P/R – T/D – B/W – K/F – O/Y***
2. *Διάταξη «αναδιατακτών»:* 2 – 3 – 1
3. *Προσανατολισμοί «αναδιατακτών»:* ***Q – C – W***

Τα στοιχεία (2) και (3) συναποτελούν τις λεγόμενες ρυθμίσεις των «αναδιατακτών». Για να εφαρμόσει το συγκεκριμένο ημερήσιο κλειδί, ο χειριστής του Αινίγματος θα πρέπει να ρυθμίσει τη μηχανή του ως εξής:

1. *Ρύθμιση πίνακα βυσμάτων:* Όρισε εναλλαγή των γραμμάτων **A** και **L** συνδέοντάς τα με ένα καλώδιο στον πίνακα βυσμάτων. Με τον ίδιο τρόπο, όρισε εναλλαγή των **P** και **R**, έπειτα των **T** και **D**, **B** και **W**, **K** και **F** και τέλος των **O** και **Y.**

2. *Διάταξη «αναδιατακτών»:* Τοποθέτησε το 2$^{ο}$ «αναδιατάκτη» στην πρώτη υποδοχή της μηχανής, τον 3$^{ο}$ στη δεύτερη και τον 1$^{ο}$ στην τρίτη

3. *Προσανατολισμός «αναδιατακτών»:* Κάθε «αναδιατάκτης» έχει ένα αλφάβητο χαραγμένο στον εξωτερικό του δακτύλιο που επιτρέπει στο χειριστή να τον ρυθμίσει σε έναν συγκεκριμένο προσανατολισμό. Στη συγκεκριμένη περίπτωση ο χειριστής θα περιστρέψει τον «αναδιατάκτη» της πρώτης υποδοχής έτσι ώστε το **Q** να κοιτάζει προς τα πάνω και το ίδιο θα κάνει με το **C** στον «αναδιατάκτη» της δεύτερης υποδοχής και το **W** στον «αναδιατάκτη» της τρίτης υποδοχής.

Ένας τρόπος κρυπτογράφησης μηνυμάτων θα ήταν να κρυπτογραφεί ο αποστολέας όλη την κυκλοφορία της ημέρας σύμφωνα με το ημερήσιο κλειδί. Αυτό θα σήμαινε ότι για μια ολόκληρη ημέρα στη αρχή του κάθε μηνύματος όλοι οι χειριστές του Αινίγματος θα ρύθμιζαν τις μηχανές τους σύμφωνα με το ίδιο ημερήσιο κλειδί. Στη συνέχεια κάθε φορά που θα χρειαζόταν να σταλεί ένα μήνυμα, θα πληκτρολογείτο πρώτα στη μηχανή, στη συνέχεια θα καταγραφόταν το κρυπτογραφημένο αποτέλεσμα και θα παραδιδόταν στο ραδιοχειριστή για μεταβίβαση. Στην άλλη άκρη, ο ραδιοχειριστής δέκτης θα κατέγραφε το εισερχόμενο μήνυμα θα το παρέδιδε στο χειριστή του Αινίγματος και εκείνος θα το πληκτρολογούσε στη μηχανή του η οποία θα ήταν ήδη ρυθμισμένη σύμφωνα με το ίδιο ημερήσιο κλειδί. Το αποκρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν το αρχικό μήνυμα. Η διαδικασία αυτή είναι λογικά ασφαλής αλλά η αδυναμία της έγκειται στην επαναλαμβανόμενη χρήση ενός και μόνο ημερήσιου κλειδιού για την κρυπτογράφηση των εκατοντάδων μηνυμάτων που μπορεί να στέλνονται καθημερινά. Γενικά ισχύει ότι αν ένα και μόνο κλειδί χρησιμοποιείται για την κρυπτογράφηση τεράστιας ποσότητας υλικού, είναι ευκολότερο για ένα κρυπταναλυτή να το ανακαλύψει επαγωγικά. Μια μεγάλη ποσότητα υλικού κρυπτογραφημένου με τον ίδιο τρόπο παρέχει στον κρυπταναλυτή ανάλογα μεγαλύτερες πιθανότητες να προσδιορίσει το κλειδί. Για παράδειγμα για να αναφερθούμε σε απλούστερα κρυπτογραφήματα, είναι πολύ πιο εύκολο να σπάσει κανείς ένα μονοαλφαβητικό κρυπτόγραμμα με ανάλυση συχνοτήτων αν διαθέτει πολλές σελίδες κρυπτογραφημένου υλικού παρά αν έχει μόνο δύο φράσεις. Συνεπώς, ως επιπλέον προφύλαξη οι Γερμανοί φρόντισαν ευφυώς να χρησιμοποιούν τις ρυθμίσεις του ημερήσιου κλειδιού για να μεταδίδουν ένα νέο μήνυμα κλειδί για κάθε μήνυμα. Τα μηνύματα κλειδιά είχαν τις ίδιες ρυθμίσεις πίνακα βυσμάτων και την ίδια διάταξη «αναδιατακτών» με το ημερήσιο κλειδί, αλλά διαφορετικούς προσανατολισμούς «αναδιατακτών». Επειδή ο νέος προσανατολισμός «αναδιατακτών» δεν υπήρχε στο κωδικό βιβλίο, ο αποστολέας έπρεπε να τον διαβιβάζει με ασφάλεια στον παραλήπτη σύμφωνα με την ακόλουθη διαδικασία. Πρώτον, ο αποστολέας ρυθμίζει τη μηχανή του κατά το συμφωνημένο ημερήσιο

κλειδί, το οποίο περιλαμβάνει ένα προσανατολισμό «αναδιατακτών», για παράδειγμα τον **QCW.** Στη συνέχεια επιλέγει στην τύχη ένα νέο προσανατολισμό «αναδιατακτών» για το μήνυμα κλειδί, ας πούμε τον **PGH**. Κατόπιν κρυπτογραφεί τον σύμφωνα με το ημερήσιο κλειδί. Το μήνυμα-κλειδί πληκτρολογείται στο Αίνιγμα δυο φορές, ώστε ο παραλήπτης να μπορεί να κάνει διπλό έλεγχο. Για παράδειγμα, ο αποστολέας κρυπτογραφεί το μήνυμα-κλειδί **PGHPGH** ως **KIVBJE**. Σημειώστε ότι τα δυο κρυπτογραφούνται διαφορετικά (το πρώτο ως **KIV** και το δεύτερο ως **BJE** ) επειδή οι «αναδιατάκτες» του Αινίγματος μετακινούνται περιστροφικά μετά από κάθε γράμμα και αλλάζουν την όλη κρυπτογράφηση. Στη συνέχεια ο αποστολέας αλλάζει τη μηχανή του στη ρύθμιση **PGH** και κρυπτογραφεί το κύριο μήνυμα σύμφωνα με αυτό το μήνυμα-κλειδί. Στην πλευρά του παραλήπτη, η μηχανή ρυθμίζεται αρχικά σύμφωνα με το ημερήσιο κλειδί, το **QCW** . Ο παραλήπτης πληκτρολογεί τα 6 πρώτα γράμματα του εισερχόμενου μηνύματος, τα **KIVBJE**, και η αποκρυπτογράφησή τους δίνει **PGHPGH**. Τώρα ο παραλήπτης ξέρει ότι πρέπει να ξαναρυθμίσει τους «αναδιατάκτες» του σύμφωνα με τον προσανατολισμό που δίνει το μήνυμα κλειδί, το **PGH** , και έτσι μπορεί να αποκρυπτογραφήσει το κύριο σώμα του μηνύματος. Αυτό ισοδυναμεί με το να συμφωνούν ο αποστολέας και ο παραλήπτης σε ένα κύριο κρυπτογραφικό κλειδί. Στη συνέχεια, αντί να κρυπτογραφούν όλα τα μηνύματα σύμφωνα με αυτό το ένα κλειδί, το χρησιμοποιούν απλά για να κρυπτογραφούν ένα νέο κρυπτόγραμμα για κάθε μήνυμα και στη συνέχεια κρυπτογραφούν το κυρίως μήνυμα σύμφωνα με το νέο κλειδί.

Εκ πρώτης όψεως το φαινόταν απόρθητο όμως οι Πολωνοί κρυπταναλυτές δεν κατέθεταν τα όπλα. Στην πρώτη γραμμή της μάχης κατά του Αινίγματος βρισκόταν μια νέα γενιά κρυπταναλυτών. Το Αίνιγμα ήταν ένα μηχανικό κρυπτόγραμμα, και το Γραφείο Ζιφρόφ έκρινε ότι ένα πιο επιστημονικό πνεύμα ίσως να είχε μεγαλύτερες πιθανότητες να το σπάσει. Το Γραφείο διοργάνωσε σεμινάριο κρυπτογραφίας και προσκάλεσε 20 μαθηματικούς, που όλοι του έδωσαν όρκο μυστικότητας. Και οι 20 προέρχονταν από το πανεπιστήμιο του Πόνζαν το οποίο έιχε το πλεονέκτημα ότι βρισκόταν στο δυτικό τμήμα της χώρας, στα εδάφη δηλαδή που ως το 1918 ανήκαν στη Γερμανία και κατά συνέπεια όλοι ήξεραν άπταιστα γερμανικά. Τρεις από τους 20 επέδειξαν ικανότητες επίλυσης κρυπτογραμμάτων και στρατολογήθηκαν στο Γραφείο. Ο πιο προικισμένος από αυτούς ήταν ο Μάριαν Ρεζέφσκι. Στη διάρκεια της μαθητείας του έσπασε μια σειρά παραδοσιακά κρυπτογράμματα, και στη συνέχεια πέρασε στην πιο απαγορευτική πρόκληση του Αινίγματος. Η στρατηγική του Ρεζέφσκι για το σπάσιμο του Αινίγματος εστιαζόταν στο γεγονός ότι η επανάληψη είναι εχθρός της ασφάλειας. Η πιο εμφανής επανάληψη στην κρυπτογράφηση με το Αίνιγμα ήταν το μήνυμα κλειδί, που κρυπτογραφείτο δύο φορές στην αρχή κάθε μηνύματος. Οι Γερμανοί είχαν ζητήσει αυτή την επανάληψη για να αποφύγουν λάθη που θα μπορούσαν να προκληθούν από ραδιοφωνικά παράσιτα ή από σφάλμα του χειριστή. Όμως δεν είχαν προβλέψει ότι αυτό θα έθετε σε κίνδυνο την ασφάλεια της μηχανής. Καθημερινά ο Ρεζέφσκι είχε στα χέρια του και από ένα νέο πακέτο με υποκλαπέντα μηνύματα. Όλα άρχιζαν με τα έξι γράμματα του επαναλαμβανόμενου μηνύματος κλειδιού των τριών γραμμάτων, έξι γράμματα κρυπτογραφημένα σύμφωνα με το ίδιο ημερίσιο κλειδί. Για παράδειγμα μπορούσε να έχει τέσσερα μηνύματα που άρχιζαν με τα ακόλουθα κρυπτογραφημένα μηνύματα κλειδιά:

| | $1^{ο}$ | $2^{ο}$ | $3^{ο}$ | $4^{ο}$ | $5^{ο}$ | $6^{ο}$ |
|---|---|---|---|---|---|---|
| *$1^{ο}$ μήνυμα* | ***L*** | ***O*** | ***K*** | ***R*** | ***G*** | ***M*** |
| *$2^{ο}$ μήνυμα* | ***M*** | ***V*** | ***T*** | ***X*** | ***Z*** | ***E*** |
| *$3^{ο}$ μήνυμα* | ***J*** | ***K*** | ***T*** | ***M*** | ***P*** | ***E*** |
| *$4^{ο}$ μήνυμα* | **D** | **V** | **W** | **P** | **Z** | **X** |

Σε όλες τις περιπτώσεις το $1^{ο}$ και $4^{ο}$ γράμμα είναι κρυπτογραφήσεις του ίδιου γράμματος δηλαδή του πρώτου γράμματος του μηνύματος κλειδιού, Επίσης, το $2^{ο}$ και $5^{ο}$ γράμμα είναι

κρυπτογραφήσεις του ίδιου γράμματος, δηλαδή του δεύτερου γράμματος του μηνύματος κλειδιού. Για παράδειγμα, στην πρώτη περίπτωση τα και είναι κρυπτογραφήσεις του ίδιου γράμματος, του πρώτου γράμματος του μηνύματος κλειδιού. Ο λόγος για τον οποίο το ίδιο γράμμα κρυπτογραφείται διαφορετικά, πρώτα σαν **L** και μετά σαν **R**, είναι ότι μεταξύ των δύο κρυπτογραφήσεων ο πρώτος «αναδιατάκτης» του Αινίγματος έχει μετατοπιστεί κατά τρείς θέσεις, αλλάζοντας τον όλο τρόπο αναδιάταξης. Το γεγονός ότι τα **L** και **R** είναι κρυπτογραφήσεις του ίδιου γράμματος επέτρεψε στον Ρεζέφσκι να συμπεράνει κάποιον μικρό περιορισμό στην αρχική ρύθμιση της μηχανής. Η αρχική ρύθμιση των «αναδιατακτών» , η οποία είναι άγνωστη, κρυπτογράφησε το πρώτο γράμμα του επίσης αγνώστου ημερήσιου κλειδιού ως **L,** και στη συνέχεια μια άλλη επίσης άγνωστη ρύθμιση των «αναδιατακτών»,τρεις θέσεις μετά την αρχική, κρυπτογράφησε το ίδιο γράμμα του ημερήσιου κλειδιού που παραμένει επίσης άγνωστο, ως **R.** Ο περιορισμός αυτός αποδεικνύει ότι τα γράμματα και συνδέονται στενά μέσω της αρχικής ρύθμισης του Αινίγματος, που αποτελεί το ημερήσιο κλειδί. Καθώς αυξάνει ο αριθμός των υποκλεπτομένων μηνυμάτων, είναι δυνατόν να εντοπιστούν κι άλλες σχέσεις μεταξύ $1^{ου}$ και $4^{ου}$ γράμματος του επαναλαμβανομένου μηνύματος κλειδιού. Όλες αυτές οι σχέσεις εκπορεύονται από την αρχική ρύθμιση του Αινίγματος. Λ.χ το δεύτερο μήνυμα του παραδείγματος μας λέει ότι τα **M** και **X** σχετίζονται, το τρίτο ότι τα **J** και **M** σχετίζονται και το τέταρτο ότι τα **D** και **P** σχετίζονται. Ο Ρεζέφσκι άρχισε να συνοψίζει αυτές τις σχέσεις εντάσσοντές τες σε πίνακες. Για τα τέσσερα μηνύματα που έχουμε ως τώρα, ο πίνακας θα αντικατόπτριζε τις σχέσεις μεταξύ **( L,R), (M,X), (J,M),** και **(D,P):**

| | |
|---|---|
| *$1^{ο}$ γράμμα* | **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z** |
| *$4^{ο}$ γράμμα* | **P M R X** |

Ο πίνακας που ακολουθεί δείχνει μια τέτοια συμπληρωμένη σειρά σχέσεων:

| | |
|---|---|
| *$1^{ο}$ γράμμα* | **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z** |
| *$4^{ο}$ γράμμα* | **F Q H P L W O G B M V R X U Y C Z I T N J E A S D *K*** |

Ο Ρεζέφσκι δεν ήξερε τίποτα για το ημερήσιο κλειδί ούτε και γι ατα μηνύματα κλειδιά που επιλέγονταν, αλλά ήξερε ότι κατέληγαν στον παραπάνω πίνακα σχέσεων. Αν το ημερήσιο κλειδί ήταν κάποιο άλλο, ο πίνακας των σχέσεων θα ήταν εντελώς διαφορετικός. Το επόμενο ερώτημα ήταν αν υπήρχε κάποιος τρόπος προσδιορισμού του ημερήσιου κλειδιού διερευνώντας τον πίνακα σχέσεων. Ο Ρεζέφσκι άρχισε να ψάχνει για σχήματα μέσα στον πίνακα, για κάποιες δομές που θα μπορούσαν να υποδεικνύουν το ημερήσιο κλειδί. Τελικά άρχισε να μελετάει έναν ιδιαίτερο τύπο σχήματος που εμφάνιζε αλυσίδες γραμμάτων. Λ.χ στον παραπάνω πίνακα το **A** στην πάνω σειρά συνδέεται με το **F** στην κάτω, οπότε στη συνέχεια θα έψαχνε το **F** στην πάνω σειρά. Αυτό προκύπτει ότι συνδέεται με το **W** και έτσι θα έψαχνε το στην πάνω σειρά το **W** οποίο συνδέεται με το **A** από όπου ξεκινήσαμε. Η αλυσίδα έχει συμπληρωθεί. Με τα υπόλοιπα γράμματα του αλφαβήτου ο Ρεζέφσκι σχημάτιζε κι άλλες αλυσίδες τις οποίες και κατέγραφε σημειώνοντας τον αριθμό των δεσμών σε καθεμία:

| | |
|---|---|
| **A→F→W→A** | *3 δεσμοί* |
| **B→Q→Z→K→V→E→L→R→I→B** | *9 δεσμοί* |
| **C→H→G→O→Y→D→P→C** | *7 δεσμοί* |
| **J→M→X→S→T→N→U→J** | *7 δεσμοί* |

Μέχρι τώρα εξετάσαμε μόνο τους δεσμούς ανάμεσα στο $1^{ο}$ και το $4^{ο}$ γράμμα του εξαγράμματου επαναλαμβανόμενου κλειδιού. Στην πραγματικότητα, ο Ρεζέφσκι επαναλάμβανε όλη αυτή την άσκηση για τις σχέσεις ανάμεσα στο $2^{ο}$ και το $5^{ο}$ καθώς και ανάμεσα στο $3^{ο}$ και το $6^{ο}$ γράμμα, εντοπίζοντας σε κάθε περίπτωση τις αλυσίδες και σημειώνοντας τον αριθμό των δεσμών σε κάθε αλυσίδα. Ο Ρεζέφσκι παρατήρησε ότι οι αλυσίδες άλλαζαν κάθε μέρα. Άλλοτε υπήρχαν πολλές σύντομες αλυσίδες και άλλες φορές λίγες και μακριές. Και φυσικά τα γράμματα μέσα στις αλυσίδες άλλαζαν. Τα χαρακτηριστικά των αλυσίδων ήταν εμφανώς αποτέλεσμα της ρύθμισης του ημερήσιου κλειδιού, μια περίπλοκη συνέπεια των ρυθμίσεων του πίνακα βυσμάτων, ης διάταξης των «αναδιατακτών» και του προσανατολισμού τους. Παρέμενε οστώσο το ερώτημα πώς θα μπορούσε ο Ρεζέφσκι να προσδιορίσει

με βάση αυτές τις αλυσίδες το ημερήσιο κλειδί. Ποιο από τα 10.000.000.000.000.000 πιθανά ημερήσια κλειδιά σχετιζόταν με ένα συγκεκριμένο σχήμα αλυσίδων; Ο αριθμός των πιθανοτήτων ήταν απλούστατα πολύ μεγάλος. Στο σημείο αυτό ο Ρεζέφσκι είχε μια καταπληκτική έμπνευση. Παρότι οι ρυθμίσεις τόσο του πίνακα βυσμάτων όσο και των «αναδιατακτών» , επηρεάζουν τις λεπτομέρειες των αλυσίδων, οι αντίστοιχες συμβολές τους μπορούν ως ένα βαθμό να διαχωριστούν. Υπάρχει συγκεκριμένα μια πτυχή των αλυσίδων που εξαρτάται απόλυτα από τις ρυθμίσεις των «αναδιατακτών» και που δεν έχει να κάνει σε τίποτα με τις ρυθμίσεις του πίνακα βυσμάτων : ο αριθμός των δεσμών στις αλυσίδες προκύπτει αποκλειστικά από τις ρυθμίσεις των «αναδιατακτών». Ας πάρουμε το παραπάνω παράδειγμα και ας θεωρήσουμε ότι το ημερήσιο κλειδί απαιτούσε την εναλλαγή των γραμμάτων και ως μέρος της ρύθμισης του πίνακα βυσμάτων. Αν αλλάξουμε αυτό το στοιχείο του ημερήσιου κλειδιού αφαιρώντας το καλώδιο που ανταλλάσει τα και χρησιμοποιώντας το για να συνδέσουμε τα και, ώστε να εναλλάσσονται αυτά, τότε οι αλυσίδες θα αλλάξουν και θα προκύψουν οι εξής:

| | |
|---|---|
| **A→F→W→A** | *3 δεσμοί* |
| **B→Q→Z→T→V→E→L→R→I→B** | *9 δεσμοί* |
| **C→H→S→O→Y→D→P→C** | *7 δεσμοί* |
| **J→M→X→G→K→N→U→J** | *7 δεσμοί* |

Κάποια από τα γράμματα στις αλυσίδες έχουν αλλάξει αλλά το πιο σημαντικό είναι ότι ο αριθμός των δεσμών παραμένει σταθερός. Ο Ρεζέφσκι είχε εντοπίσει μια πτυχή των αλυσίδων που αντανακλούσε αποκλειστικά στις ρυθμίσεις των «αναδιατακτών». Ο συνολικός αριθμός των ρυθμίσεων των «αναδιατακτών» είναι το γινόμενο του αριθμού των «διατάξεών» τους (6) επί τον αριθμό των προσανατολισμών τους (17.576), δηλαδή 105.456. Αντί λοιπόν να ανησυχεί για το ποιο από τα 10.000.000.000.000.000 ημερήσια κλειδιά συνδεόταν με μια συγκεκριμένη σειρά αλυσίδων, ο Ρεζέφσκι μπορούσε να καταπιαστεί με ένα ριζικά απλούστερο πρόβλημα: ποια από τις 105.456 ρυθμίσεις των «αναδιατακτών» συνδεόταν με τους αριθμούς των δεσμών μέσα σε μια σειρά αλυσίδων; Ο αριθμός αυτός είναι και πάλι μεγάλος, είναι όμως εκατό δισεκατομμύρια φορές μικρότερος από το συνολικό αριθμό των πιθανών ημερήσιων κλειδιών. Με δυο λόγια το έργο έγινε κατά εκατό δισεκατομμύρια φορές ευκολότερο, οπωσδήποτε εντός των ορίων του ανθρωπίνως εφικτού. Ο Ρεζέφσκι προχώρησε ως εξής: Χάρη στην κατασκοπεία του Χανς-Τίλο Σμιτ, είχε πρόσβαση σε μηχανές – αντίγραφα του Αινίγματος. Η ομάδα του ανέλαβε ένα επίπονο έργο: να ελέγχει μία προς μία τις 105.456 ρυθμίσεις των «αναδιατακτών» και να καταλογογράφει τα μήκη των αλυσίδων που προέκυπταν από την καθεμιά τους. Χρειάστηκε ένας ολόκληρος χρόνος για να ολοκληρωθεί ο κατάλογος, όταν όμως το Γραφείο συγκέντρωσε όλα τα στοιχεία ο Ρεζέφσκι μπορούσε επιτέλους να αρχίσει να αποκαλύπτει το κρυπτόγραμμα του Αινίγματος. Κάθε μέρα εξέταζε τα κρυπτογραφημένα μηνύματα κλειδιά δηλαδή τα 6 πρώτα γράμματα όλων των υποκλεπτομένων μηνυμάτων και χρησιμοποιούσε τις εξαγόμενες πληροφορίες για να καταρτίζει τον πίνακα των σχέσεων. Αυτό του επέτρεπε να ανιχνεύει τις αλυσίδες και να προσδιορίζει τον αριθμό των δεσμών στην καθεμιά τους. Για παράδειγμα η ανάλυση του $1^{ου}$ και του $4^{ου}$ γράμματος μπορούσε να δώσει 4 αλυσίδες , με 3,9,7 και 7 δεσμούς αντίστοιχα. Η ανάλυση του $2^{ου}$ και του $5^{ου}$ γράμματος μπορούσε να δώσει επίσης 4 αλυσίδες με 2,3,9 και 12 δεσμούς αντίστοιχα. Τέλος η ανάλυση του $3^{ου}$ και $6^{ου}$ γράμματος μπορούσε να δώσει 5 αλυσίδες με 5,5,5,3 και 8 δεσμούς αντίστοιχα. Μέχρι αυτό το σημείο ο Ρεζέφσκι εξακολουθούσε να αγνοεί το ημερήσιο κλειδί, ήξερε όμως ότι από αυτό προκύπτουν 3 σειρές αλυσίδων, με την κάθε σειρά να περιέχει τους ακόλουθους αριθμούς αλυσίδων και δεσμών στην καθεμιά τους:

*4 αλυσίδες από το $1^{ο}$ και το $4^{ο}$ γράμμα με 3, 9, 7 και 7 δεσμούς*
*4 αλυσίδες από το $2^{ο}$ και το $5^{ο}$ γράμμα με 2, 3, 9 και 12 δεσμούς*
*5 αλυσίδες από το $3^{ο}$ και το $6^{ο}$ γράμμα με 5, 5, 5, 3 και 8 δεσμούς*

Τώρα ο Ρεζέφσκι μπορούσε να ανατρέξει στον κατάλογό του ο οποίος περιείχε όλες τις ρυθμίσεις των «αναδιατακτών» καταγραμμένες σύμφωνα με το είδος των αλυσίδων που δημιουργούσαν. Βρίσκοντας το λήμμα του καταλόγου που περιείχε το σωστό αριθμό των δεσμών στην καθεμιά τους, ήξερε αμέσως τις ρυθμίσεις των «αναδιατακτών» για το συγκεκριμένο ημερήσιο κλειδί. Οι αλυσίδες ήταν στην ουσία δακτυλικά αποτυπώματα, η μαρτυρία που πρόδιδε την αρχική διάταξη και

τους αρχικούς προσανατολισμούς των «αναδιατακτών». Ο Ρεζέφσκι έπρεπε ακόμη να προσδιορίσει τις ρυθμίσεις του πίνακα βυσμάτων. Αν και υπάρχουν περίπου εκατό δισεκατομμύρια πιθανότητες για τις ρυθμίσεις του πίνακα βυσμάτων, το έργο του Ρεζέφσκι ήταν σχετικά απλό. Πρώτα πρώτα διευθετούσε τους «αναδιατάκες» του αντίγραφο του Αινίγματος σύμφωνα με το πρόσφατα εντοπισμένο μέρος του ημερήσιου κλειδιού που καθορίζεται από τους «αναδιατάκτες». Στη συνέχεια αποσυνέδεε όλα τα καλώδια από τον πίνακα βυσμάτων, ώστε αυτός να μην ασκεί καμία επιρροή. Τέλος, έπαιρνε ένα κομμάτι υποκλαπέντος κρυπτογραφικού κειμένου και το πληκτρολογούσε στο Αίνιγμα. Το αποτέλεσμα ήταν εν πολλοίς ασυνάρτητο, επειδή οι καλωδιώσεις του πίνακα βυσμάτων ήταν άγνωστες και έλειπαν. Ωστόσο, εμφανίζονταν πού και πού κάποιες κατά προσέγγιση αναγνωρίσιμες φράσεις όπως **alliveinbelrin** κατά πάσα πιθανότητα αυτό θα ήταν *arrive in Berlin* (άφιξη στο Βερολίνο). Αν και η υπόθεση αυτή είναι σωστή, υποδεικνύει ότι τα γράμματα **R** και **L** θα πρέπει να συνδέονται και να ανταλλάσσονται μέσω ενός καλωδίου του πίνακα βυσμάτων, ενώ τα A, I, V, E, B και N όχι. Αναλύοντας και άλλες φράσεις είναι δυνατόν να εντοπιστούν και τα άλλα πέντε ζεύγη γραμμάτων που ανταλλάσσονται μέσω του πίνακα βυσμάτων. Έχοντας προσδιορίσει τις ρυθμίσεις του πίνακα βυσμάτων και έχοντας ήδη ανακαλύψει τις ρυθμίσεις των «αναδιατακτών», ο Ρεζέφσκι είχε το πλήρες ημερήσιο κλειδί και μπορούσε πλέον να αποκρυπτογραφήσει οποιοδήποτε μήνυμα στελνόταν εκείνη τη μέρα. Ο Ρεζέφσκι είχε απλοποιήσει δραστικά το έργο της ανεύρεσης του ημερήσιου κλειδιού με το να διαχωρίσει το πρόβλημα του εντοπισμού των ρυθμίσεων των «αναδιατακτών» από το πρόβλημα του εντοπισμού των ρυθμίσεων του πίνακα βυσμάτων. Το καθένα από αυτά τα προβλήματα ήταν από μόνο του επιλύσιμο. Αρχικά είχαμε υπολογίσει ότι θα χρειαζόταν περισσότερος χρόνος από τη ζωή όλου του σύμπαντος για να ελεγχθούν όλα τα πιθανά κλειδιά του Αινίγματος. Ωστόσο ο Ρεζέφσκι χρειάστηκε μόνο ένα έτος για να καταρτίσει τον κατάλογό του με τα μήκη των αλυσίδων, και από κει και πέρα μπορούσε να βρει το ημερήσιο κλειδί πριν τελειώσει η μέρα. Από τη στιγμή που είχε το ημερήσιο κλειδί, κατείχε την ίδια πληροφορία με τον αποδέκτη των μηνυμάτων και μπορούσε εξίσου εύκολα να τα αποκρυπτογραφεί. Μετά το κατόρθωμα του Ρεζέφσκι, οι γερμανικές επικοινωνίες δεν είχαν πια μυστικά. Η Πολωνία δεν βρισκόταν σε πόλεμο με τη Γερμανία αλλά επειδή υπήρχε πάντα η απειλή της εισβολής, η ανακούφιση των Πολωνών για την κατάκτηση του Αινίγματος ήταν τεράστια. Η πολωνική επιτυχία με το σπάσιμο του κρυπτογράμματος του Αινίγματος μπορεί να αποδοθεί σε τρεις παράγοντες: το φόβο, τα μαθηματικά και την κατασκοπεία. Χωρίς το φόβο της εισβολής, οι Πολωνοί θα αποθαρρύνονταν από το φαινομενικά άτρωτο χαρακτήρα του Αινίγματος. Χωρίς τα μαθηματικά, ο Ρεζέφσκι δεν θα ήταν σε θέση να αναλύσει τις αλυσίδες . Τέλος χωρίς τον Σμιτ και τα έγγραφά του, οι καλωδιώσεις των «αναδιατακτών» δεν θα γίνονταν γνωστές και η κρυπτανάλυση δεν θα μπορούσε καν να αρχίσει.

Οι Πολωνοί χρησιμοποιούσαν με επιτυχία για αρκετά χρόνια την τεχνική του Ρεζέφσκι. Ακόμα και όταν οι Γερμανοί επέφεραν μια μικρή τροποποίηση στον τρόπο μετάδοσης των μηνυμάτων τους ο Ρεζέφσκι αντεπιτέθηκε. Ο παλιός κατάλογος με τα μήκη των αλυσίδων ήταν άχρηστος, αντί όμως να τον ξαναγράψει, επινόησε μια μηχανοποιημένη εκδοχή του δικού του συστήματος καταλογογράφησης, η οποία έψαχνε αυτόματα για τις σωστές ρυθμίσεις των «αναδιατακτών». Η επινόηση του Ρεζέφσκι ήταν μια προσαρμογή του Αινίγματος ικανή να ελέγχει γρήγορα μία προς μία τις 17.576 ρυθμίσεις ώσπου να εντοπίσει εκείνη που ταίριαζε. Εξαιτίας των 6 πιθανών διατάξεων των «αναδιατακτών» ήταν απαραίτητο να υπάρχουν 6 μηχανές του Ρεζέφσκι που δούεθαν ταυτόχρονα με την καθεμιά τους να αντιπροσωπεύει μια απότ ις πιθανές διατάξεις. Όλες μαζί σχημάτιζαν μια μονάδα ύψους περίπου ενός μέτρου, ικανή να βρίσκει το ημερήσιο κλειδί σε δύο περίπου ώρες. Οι μονάδες αποκαλούνταν *μπόμπες* , ένα όνομα που ίσως να οφείλεται στο ρυθμικό θόρυβο που έκαναν όταν έλεγχαν τις ρυθμίσεις των «αναδιατακτών». Οι *μπόμπες* όντως μηχανοποίησαν τη διαδικασία της κρυπρογράφησης. Ήταν μια φυσική απάντηση στη μηχανοποίηση της κρυπτογράφησης, στο Αίνιγμα. Κατά το μεγαλύτερο μέρος της δεκαετίας του 1930 ο Ρεζέφσκι και οι συνεργάτες του εργάζονταν ακούραστα για την αποκάλυψη των κλειδιών του Αινίγματος. Έπρεπε συνεχώς να διορθώνουν τις μηχανικές βλάβες στις μπόμπες και συνεχώς είχαν να αντιμετωπίσουν την αδιάκοπη ροή των κρυπτογραφημένων μηνυμάτων. Ωστόσο εν αγνοία των πολωνών κρυπταναλυτών μεγάλο μέρος της δουλειάς τους ήταν άχρηστο. Ο επικεφαλής του Γραφείου, Ταγματάρχης Γκουίντο Λάνγκερ είχε ήδη στην κατοχή του τα ημερήσια κλειδιά του Αινίγματος αλλά τα κρατούσε κρυφά. Ο Λάνγκερ εξακολουθούσε να δέχεται πληροφορίες από τον Σμιτ. Οι δραστηριότητες του Γερμανού κατασκόπου συνεχίστηκαν για επτά ακόμη χρόνια. Συνάντησε το Γάλλο μυστικό πράκτορα Ρεξ είκοσι φορές και σε κάθε συνάντηση ο Σμιτ παρέδιδε ένα ή

περισσότερα κωδικά βιβλία, που το καθένα τους περιείχε τα ημερήσια κλειδιά ενός μήνα. Ήταν τα κωδικά βιβλία που διανέμονταν σε όλους τους Γερμανούς χειριστές του Αινίγματος και τα οποία περιείχαν όλες τις πληροφορίες που χρειάζονταν για την κρυπτογράφηση και την αποκρυπτογράφηση των μηνυμάτων. Συνολικά παρέδωσε κωδικά βιβλία που περιείχαν ημερήσια κλειδιά 38 μηνών. Τα κλειδιά θα είχαν γλιτώσει το Ρεζέφσκι από τεράστιο κόπο και χρόνο, ωστόσο ο Λάνγκερ αποφάσισε να μην αποκλύψει στον Ρεζέφσκι την ύπαρξη των κλειδιών καθώς πίστευε ότι έτσι τον προετοίμαζε για την εποχή που αναπόφευκτα τα κλειδιά δεν θα ήταν πλέον διαθέσιμα.

Οι δεξιότητες του Ρεζέφσκι έφτασαν στα όριά τους το Δεκέμβριο του 1938 όταν οι Γερμανοί κρυπτογράφοι ενίσχυσαν την ασφάλεια του Αινίγματος. Σε όλους τους χειριστές του Αινίγματος δόθηκαν δυο νέοι «αναδιατάκτες» έτσι ώστε η διευθέτηση των «αναδιατακτών» να περιλαμβάνει οποιουσδήποτε τρεις από τους πέντε διαθέσιμους «αναδιατάκτες». Προηγουμένως υπήρχαν μόνο τρεις «αναδιατάκτες» (οι 1, 2 και 3) για να επιλέξει ο χειριστής και μόνο έξι τρόποι διευθέτησής τους, τώρα όμως που υπήρχαν δυο επιπλέον (οι 4 και 5) για να επιλέξει, ο αριθμός των διατάξεων ανέβηκε σε 60, όπως φαίνεται στον παρακάτω πίνακα. Η πρώτη πρόκληση που είχε να αντιμετωπίσει ο Ρεζέφσκι ήταν να ανακαλύψει τις εσωτερικές καλωδιώσεις των δυο νέων «αναδιατακτών». Το πιο ανησυχητικό όμως ήταν ότι έπρεπε να κατασκευάσει 10 φορές περισσότερες μπόμπες που η καθεμιά τους να εκπροσωπεί μια διαφορετική διάταξη «αναδιατακτών». Το κόστος κατασκευής μιας τέτοιας συστοιχίας από μπόμπες ισοδυναμούσε με ολόκληρο τον προυπολογισμό εξοπλισμού του Γραφείου πολλαπλασιασμένου επί 15. Η κατάσταση επιδεινώθηκε όταν ο ριθμός των πινάκων βυσμάτων αυξήθηκε από 6 σε 10. Αντί για 12 γράμματα που ανταλλάσσονταν ανά δύο πριν εισαχθούν στους «αναδιατάκτες» τώρα υπήρχαν 20 ανταλλασσόμενα γράμματα. Ο αριθμός των πιθανών κλειδιών αυξήθηκε σε 159.000.000.000.000.000.000.

Το νέο άτρωτο Αίνιγμα ήταν εξοντωτικό πλήγμα για την Πολωνία γιατί τώρα η κρυπτογραφική μηχανή δεν ήταν απλώς ένα μέσον επικοινωνίας αλλά η καρδιά της στρατηγικής του Χίτλερ που είχε ως επίκεντρο τον πόλεμο – αστραπή (blitzkrierg). Ο πόλεμος αστραπή γρήγορη εντατική και συντονισμένη επίθεση, πράγμα που σήμαινε ότι μεγάλες μεραρχίες τεθωρακισμένων έπρεπε να επικοινωνούν τόσο μεταξύ τους όσο και με το ιππικό και το πυροβολικό. Επιπλέον, οι χερσαίες δυνάμεις έπρεπε να έχουν ενιαία υποστήριξη από βομβαρδιστικά κάθετης εφόρμησης, πράγμα που απαιτούσε αποτελεσματικές και ασφαλείς επικοινωνίες ανάμεσα στα στρατεύματα της πρώτης γραμμής και τις αεροπορικές βάσεις. Η φιλοσοφία του πολέμου – αστραπή ήταν «ταχύτητα επίθεσης μέσω της ταχύτητας των επικοινωνιών». Αν οι Πολωνοί δεν μπορούσαν να σπάσουν το Αίνιγμα δεν είχαν καμία ελπίδα να σταματήσουν τη γερμανική επέλαση. Η Γερμανία είχε ήδη καταλάβει τη Σουηδία και στις 27 Απριλίου του 1939 κατήγγειλε το σύμφωνο μη επίθεσης με την Πολωνία. Στις 30 Ιουλίου επιφανείς Γάλλοι και Βρετανοί κρυπταναλυτές έφτασαν στο αρχηγείο του Γραφείου όπου ο Λάνγκερ τους αποκάλυψε μια από τις μπόμπες του Ρεζέφσκι. Οι επισκέπτες έμειναν εμβρόντητοι ακούγοντας με ποιο τρόπο ο Ρεζέφσκι λεσπαγε επί χρόνια το Αίνιγμα. Ο Λάνγκερ πρόσφερε στους Βρετανούς και στους Γάλλους δύο αντίγραφα του Αινίγματος και σχεδιαγράμματα για τις μπόμπες τα οποία θα μεταφέρονταν στο Παρίσι σε διπλωματικούς σάκους και από εκεί το ένα αντίγραφο προωθήθηκε στο Λονδίνο. Την 1$^{η}$ Σεπτεμβρίου ο Χίτλερ εισέβαλε στην Πολωνία και ο πόλεμος άρχισε.

Επί 13 χρόνια οι Βρετανοί και οι Γάλλοι θεωρούσαν ότι το κρυπτόγραμμα του Αινίγματος ήταν άθραυστο. Οι πολωνικές όμως αποκαλύψεις είχαν αποδείξει ότι το Αίνιγμα ήταν ελαττωματικό πράγμα που ανύψωσε το ηθικό των κρυπταναλυτών των Συμμάχων. Η πρόοδος των Πολωνών είχε ανακοπεί εξαιτίας της εισαγωγής των νέων «αναδιατακτών» και των επιπλέον καλωδίων στους πίνακες βυσμάτων, παρέμενε όμως το γεγονός ότι το Αίνιγμα δεν θεωρείτο πλέον τέλειο κρυπτόγραμμα. Επιπλέον τα πολωνικά στρατεύματα απέδειξαν στους Συμμάχους την αξία της πρόσληψης μαθηματικών για το σπάσιμο κωδίκων. Στο βρετανικό Δωμάτιο 40 κυριαρχούσαν πάντα οι γλωσσολόγοι και οι κλασικοί φιλόλογοι, τώρα όμως υπήρχε μιαι συντονισμένη προσπάθεια εξισορρόπησης του προσωπικού με μαθηματικούς και επιστήμονες. Αυτοί στρατολογούνταν με τη μέθοδο του δικτύου παλιών συμφοιτητών: τα μέλη του Δωματίου 40 έρχονταν σε επαφή με τους πρώην συμφοιτητές τους από την Οξφόρδη και το Κέμπριτζ. Υπήρχε και δίκτυο πρώην συμφοιτητριών που στρατολογούσε γυναίκες από ιδρύματα όπως το Νιούχαμ Κόλετζ και το Γκίρτον Κόλετζ του Κέμπριτζ. Τα νέα μέλη δεν πήγαιναν στο Δωμάτιο 40 στο Λονδίνο αλλά στο Μπλίτσλει Παρκ του Μπακιγχαμσαιρ, έδρα της Κυβερνητικής Σχολής Κωδίκων και Κρυπτογραμμάτων ( GC&CS: Government Code and Cypher School), ενός νεοσύστατου κρυπταναλυτικού οργανισμού που

διαδέχτηκε το Δωμάτιο 40. Το Μπλίτσλει Παρκ μπορούσε να στεγάσει πολύ περισσότερο προσωπικό πράγμα απαραίτητο εφόσον με την έναρξη του πολέμου αναμενόταν ένας κατακλυσμός από κρυπτογραφημένα προιόντα υποκλοπής. Κατά τη διάρκεια του Πρώτου Παγκοσμίου Πολέμου η Γερμανία μετέδιδε δύο εκατομμύρια λέξεις το μήνα, όμως η αύξηση του αριθμού των διαθέσιμων ασυρμάτων οδηγούσε στην πρόβλεψη ότι κατά το Δεύτερο Παγκόσμιο Πόλεμο θα μεταδίδονταν δύο εκατομμύρια λέξεις τη μέρα. Στο Μπλίτσλει Παρκ κατασκευάστηκαν επίσης πολυάριθμα παραπήγματα, πρόχειρα ξύλινα κτίσματα τα οποία στέγαζαν τις διάφορες δραστηριότητες της οργάνωσης. Για παράδειγμα το Παράπηγμα 6 ειδικευόταν στο να προσβάλλει τις επικοινωνίες του Γερμανικού στρατού που ήταν κωδικοποιημένες με το Αίνιγμα. Το Παράπηγμα 6 προωθούσε τα κείμενα που αποκρυπτογραφούσε το Παράπηγμα 3, όπου τα στελέχη των υπηρεσιών κατασκοπείας μετέφραζαν τα μηνύματα και προσπαθούσαν να εκμεταλλευτούν τις πληροφορίες που αντλούσαν. Το Παράπηγμα 8 ειδικευόταν στο Αίνιγμα του Γερμανικού Ναυτικού και τα προιόντα των αποκρυπτογραφήσεών τους διαβιβάζονταν στο Παράπηγμα 4 για μετάφραση και συλλογή πληροφοριών. Αρχικά το Μπλίτσλει Παρκ είχε προσωπικό διακοσίων μόνο ατόμων, όμως μέσα σε πέντε χρόνια η έπαυλη και τα παραπήγματα έφτασαν να στεγάζουν επτά χιλιάδες άνδρες και γυναίκες.

Κάθε εικοσιτετράωρο οι Βρετανοί κωδικοθραύστες περρνούσαν από τη ίδια ρουτίνα. Τα μεσάνυχτα οι Γερμανοί χειριστές του Αινίγματος άλλαζαν τις ρυθμίσεις των μηχανών τους σύμφωνα με το νέο ημερήσιο κλειδί, οπότε οι όποιες πρόοδοι είχαν επιτευχθεί από το Μπλίτσλει την προηγούμενη ήταν πλέον άχρηστες για την αποκρυπτογράφηση μηνυμάτων. Οι κωδικοθραύστες έπρεπε τώρα να αναλάβουν το έργο της απόπειρας εντοπισμού του νέου ημερήσιου κλειδιού. Αυτό τους έπαιρνε αρκετές ώρες, μόλις όμως ανακάλυπταν τις ρυθμίσεις του Αινίγματος για τη συγκεκριμένη μέρα, το προσωπικό του Μπλίτσλει μπορούσε να αρχίσει την αποκρυπτογράφηση των γερμανικών μηνυμάτων που είχαν ήδη συσσωρευτεί, αποκαλύπτοντας πληροφορίες ανεκτίμητης αξίας για την πολεμική προσπάθεια. Αν το Μπλίτσλει κατόρθωνε να σπάσει το Αίνιγμα, τα γερμανικά σχέδια θα αποκαλύπτονταν και οι Βρετανοί θα ήταν σε θέση να διαβάζουν τη σκέψη της Γερμανικής Ανώτατης Διοίκησης. Αν οι Βρετανοί πληροφορούνταν μια επικείμενη επίθεση, θα μπορούσαν να στείλουν ενισχύσεις ή να οργανώσουν επιχείρηση διαφυγής. Αν οι Σύμμαχου μπορούσαν να αποκρυπτογραφήσουν τα όσα συζητούσαν οι Γερμανοί για τις δικές τους αδυναμίες, θα ήταν σε θέση να επικεντρώσουν στα σωστά σημεία τις επιθετικές τους ενέργειες. Οι αποκρυπτογραφήσεις του Μπλίτσλει ήταν ζωτικής σημασίας. Για παράδειγμα όταν οι Γερμανοί εισέβαλαν στη Δανία και τη Νορβηγία τον Απρίλιο του 1940, το Μπλίτσλει έδωσε λεπτομερή εικόνα των γερμανικών επιχειρήσεων. Με τον ίδιο τρόπο, στη μάχη της Βρετανίας, οι κρυπταναλυτές ήταν σε θέση να προειδοποιούν από πριν για τους αεροπορικούς βομβαρδισμούς δίνοντας ακριβή χρόνο και τόπο. Επίσης παρείχαν διαρκή ενημέρωση για την κατάσταση της Λούφτβαφε, όπως τον αριθμό των χαμένων αεροπλάνων και την ταχύτητα αποκατάστασής τους. Το Μπλίτσλει έστελνε όλες αυτές τις πληροφορίες στο αρχηγείο της Μ16 που στη συνέχεια τις διαβίβαζε στο Γραφείο Πολέμου, το Υπουργείο Αεροπορίας και το Ναυαρχείο.

Από τη στιγμή που έγιναν κάτοχοι των πολωνικών τεχνικών, οι κρυπταναλυτές του Μπλίτσλει άρχισαν να επινοούν τους δικούς τους σύντομους δρόμους για την ανακάλυψη των κλειδιών του Αινίγματος. Για παράδειγμα είχαν επισημάνει ότι οι Γερμανοί χειριστές του Αινίγματος ενίοτε επέλεγαν προφανή μηνύματα κλειδιά. Για κάθε μήνυμα υποτίθεται ότι ο χειριστής έπρεπε να επιλέξει ένα διαφορετικό μήνυμα κλειδί, τρία γράμματα διαλεγμένα στην τύχη. Ωστόσο, μέσα στη φωτιά της μάχης, οι καταπονημένοι χειριστές κάποιες φορές διάλεγαν τρία συνεχόμενα γράμματα από το πληκτρολόγιο του Αινίγματος όπως τα **QWE** ή **BNM**. Αυτά τα προβλέψιμα μηνύματα κλειδιά έγιναν γνωστά ως *cillies*. Μια άλλη μορφή τους ήταν η επαναλαμβανόμενη χρήση του ίδιου μηνύματος κλειδιού, ίσως των αρχικών της κοπέλας του χειριστή – ίσως μάλιστα ο όρος να προήλθε από μια τέτοια σειρά αρχικών, τα C.I.L. Πριν σπάσουν το Αίνιγμα με το δύσκολο τρόπο έγινε συνήθεια στους κρυπταναλυτές να δοκιμάζουν τα cillies, και ενίοτε τα προαισθήματά τους επαληθεύονταν. Τα cillies δεν ήταν εγγενείς αδυναμίες του Αινίγματος, αλλά αδυναμίες στον τρόπο χρήσης της μηχανής. Όμως και στα υψηλότερα κλιμάκια η ανθρώπινη πλάνη έθετε σε κίνδυνο την ασφάλεια του κρυπτογράμματος του Αινίγματος. Οι υπεύθυνοι για τη συγγραφή των κωδικών βιβλίων έπρεπε να αποφασίζουν ποιοι «αναδιατάκτες» θα χρησιμοποιούνταν κάθε μέρα και σε ποιες θέσεις. Προσπαθούσαν να διασφαλίσουν το απρόβλεπτο των ρυθμίσεων των «αναδιατακτών» με το να μην επιτρέπουν σε κανένα «αναδιατάκτη» να παραμείνει στην ίδια θέση για δύο συνεχόμενες μέρες. Έτσι, αν ονομάσουμε τους «αναδιατάκτες» 1,

2, 3, 4, και 5 και την πρώτη μέρα έχουμε τη διάταξη 134, τότε τη δεύτερη μέρα μπορούμε να έχουμε τη διάταξη 215, αλλά όχι τη 214, επειδή ο «αναδιατάκτης» με τον αριθμό 4 δεν επιτρέπεται να παραμείνει στην ίδια θέση για δύο συνεχόμενες μέρες.

Αυτή η στρατηγική μπορεί να μοιάζει λογική επειδή οι «αναδιατάκτες» αλλάζουν συνεχώς θέση, όμως στην πράξη η εφαρμογή ενός τέτοιου κανόνα κάνει τη ζωή του κρυπταναλυτή ευκολότερη. Ο αποκλεισμός ορισμένων συνδυασμών ώστε να αποφευχθεί η παραμονή του «αναδιατάκτη» στην ίδια θέση είχε ως συνέπεια οι συγγραφείς των κωδικών βιβλίων να μειώσουν στο μισό τον αριθμό των πιθανών διευθετήσεων των «αναδιατακτών». Οι κρυπταναλυτές του Μπλίτσλει αντιλήφθηκαν τι συνέβαινε και το εκμεταλλεύτηκαν στο έπακρο. Από τη στιγμή που εντόπιζαν τη διάταξη των «αναδιατακτών» για μια συγκεκριμένη μέρα, αμέσως απέκλειαν τους μισούς πιθανούς συνδυασμούς για την επόμενη. Έτσι, ο όγκος της δουλειάς τους μειωνόταν στο μισό. Επίσης υπήρχε ένας κανόνας σύμφωνα με τον οποίο οι ρυθμίσεις του πίνακα βυσμάτων δεν μπορούσαν να περιλαμβάνουν ανταλλαγή μεταξύ γειτονικών γραμμάτων του αλφαβήτου, πράγμα που σήμαινε ότι το S μπορούσε να ανταλλάσσεται με οποιοδήποτε γράμμα εκτός των R και T. Η θεωρία ήταν ότι τέτοιες εμφανείς ανταλλαγές θα έπρεπε εσκεμμένα να αποφεύγονται, και πάλι όμως η εφαρμογή του κανόνα μείωνε δραστικά τον αριθμό των πιθανών κλειδιών.

Η αναζήτηση νέων κρυπταναλυτικών σύντομων δρόμων ήταν απαραίτητη επειδή το Αίνιγμα εξακολουθούσε να εξελίσσεται στη διάρκεια του πολέμου. Οι κρυπταναλυτές ήταν διαρκώς υποχρεωμένοι να καινοτομούν, να σχεδιάζουν εκ νέου και να βελτιώνουν τις μπόμπες και να επινοούν εντελώς νέες στρατηγικές. Η επιτυχία τους οφειλόταν εν μέρει στον περίεργο συνδυασμό μαθηματικών, θετικών επιστημόνων, γλωσσολόγων, κλασσικών φιλολόγων, μεγάλων δασκάλων του σκακιού και φανατικών των σταυρολέξων μέσα σε κάθε παράπηγμα, Ένα δυσεπίλυτο πρόβλημα έκανε το γύρο του παραπήγματος μέχρι να φτάσει στα χέρια κάποιου που διέθετε τον κατάλληλο διανοητικό εξοπλισμό για να το λύσει ή κάποιου που μπορούσε να το λύσει εν μέρει πριν το δώσει σε κάποιον άλλο.

Υπήρχαν πολλοί μεγάλοι κρυπταναλυτές και πολλές σημαντικές πρόοδοι, και θα χρειάζονταν πολλοί ογκώδεις τόμοι για να περιγράψει κανείς λεπτομερώς τις ατομικές συμβολές τους. Ωστόσο, αν υπάρχει μια μορφή που αξίζει να την ξεχωρίσουμε είναι ο Άλαν Τιούρινγκ, που εντόπισε τη μεγαλύτερη αδυναμία του Αινίγματος και την εκμεταλλεύτηκε κατά τον πιο αδίστακτο τρόπο. Χάρη στον Τιούρινγκ, κατέστη δυνατό το σπάσιμο του κρυπτογράμματος του Αινίγματος ακόμη και κάτω από τις δυσκολότερες συνθήκες.

Το 1926, σε ηλικια 14 χρονών ο Τιούρινγκ γράφτηκε στη σχολή Σέρμπορν, στο Ντόρσετ. Σκοπός του Σέρμπορν ήταν να κάνει τα αγόρια ολοκληρωμένους άντρες, ικανούς να διοικούν την Αυτοκρατορία, όμως ο Τιούρινγκ δε συμμεριζόταν αυτή τη φιλοδοξία και γενικά τα σχολικά του χρόνια δεν ήταν ευτυχισμένα. Ο μοναδικός πραγματικός φίλος του στο Σέρμπορν ήταν ο Κρίστοφερ Μόρκομ, που όπως και ο Τιούρινγκ ενδιαφερόταν για θετικές επιστήμες. Μαζί συζητούσαν τα τελευταία επιστημονικά νέα και έκαναν τα δικά τους πειράματα. Η σχέση αυτή διέγειρε την επιστημονική περιέργεια του Τιούρινγκ, αλλά το πιο σημαντικό ήταν ότι ασκούσε πάνω του μια βαθιά συναισθηματική επίδραση. Όταν το Φεβρουάριο του 1930 ο Κρίστοφερ Μόρκομ πέθανε ξαφνικά από φυματίωση ο Τιούρινγκ συγκλονίστηκε και εστίασε το ενδιαφέρον του στις επιστημονικές του σπουδές, σε μια απόπειρα να εκπληρώσει αυτά που ενδεχομένως θα πραγματοποιούσε ο φίλος του. Ο Τιούρινγκ πίστευε ότι ήταν χρέος του να κερδίσει κι αυτός μια θέση στο Κέμπριτζ, και στη συνέχεια να πραγματοποιήσει τις ανακαλύψεις που θα είχε κάνει ο φίλος του αν ζούσε.

Ο Τιούρινγκ έγινε δεκτός στο Κινγκς Κόλετζ του Κέμπριτζ το 1931, σε μια περίοδο έντονης διαμάχης με αντικείμενο τη φύση των μαθηματικών και της λογικής, περιστοιχιζόμενος από εξέχουσες μορφές σαν τον Λούντβιχ Βίτγκεωστάιν. Στο επίκεντρο της διαμάχης βρισκόταν το ζήτημα της μη αποδειξιμότητας, μιας αμφιλεγόμενης ιδέας που ανέπτυξε ο μελετητής της Λογικής Κουρτ Γκέντελ. Ανέκαθεν ίσχυε η υπόθεση ότι, θεωρητικά ουλάχιστον, όλα τα μαθηματικά ζητήματα μπορούν να απαντηθούν. Ωστόσο, ο Γκέντελ απέδειξε ότι μπορούσε να υπάρχει μια μειοψηφία ζητημάτων που βρίσκονται πέρα από την εμβέλεια της λογικής απόδειξης, τα λεγόμενα μη αποδείξημα ζητήματα. Η είδηση ότι τα μαθηματικά δεν ήταν η παντοδύναμη επιστήμη που πάντα πίστευαν ήταν τραυματική για τους μαθηματικούς. Επιχείρησαν λοιπόν να σώσουν το επιστημονικό τους αντικείμενο προσπαθώντας να βρουν ένα τρόπο για να εντοπίσουν τα ενοχλητικά μη αποδείξιμα ζητήματα, έτσι ώστε να τα βάλουν με ασφάλεια παράμερα. Αυτός ήταν πιθανότατα ο στόχος που ενέπνευσε τον Τιούρινγκ να γράψει το

σημαντικότερο μαθηματικό άρθρο του με τίτλο «Περί των υπολογίσιμων αριθμών», που δημοσιεύτηκε το 1937.

Στην προσπάθειά του να εντοπίσει τα μη αποδείξιμα ζητήματα, το άρθρο του Τιούρινγκ περιέγραφε μια φανταστική μηχανή σχεδιασμένη να εκτελεί μια συγκεκριμένη μαθηματική πράξη, ή αλγόριθμο. Με άλλα λόγια, η μηχανή θα είχε την ικανότητα να εκτελεί διαδοχικά μια σταθερή, προκαθορισμένη σειρά από βήματα τα οποία θα πολλαπλασίαζαν, λ.χ, δύο αρθμούς. Ο Τιούρινγκ είχε σκεφτεί ότι οι δύο προς πολλαπλασιασμό αριθμοί θα μπορολυσαν να εισαχθούν στη μηχανή μέσω μιας ταινίας από χαρτί, κάτι σαν τη διάτρητη ταινία που χρησιμοποιείται για την εισαγωγή ενός μουσικού σκοπού σε μια Πιανόλα. Το γινόμενο του πολλαπλασιασμού θα εξερχόταν μέσω μιας δεύτερης ταινίας. Ο Τιούρινγκ φανταζόταν μια ολόκληρη σειρά από τέτοιες μηχανές Τιούρινγκ, που η καθεμιά τους θα ήταν ειδικά σχεδιασμένη για να εκτελεί ένα συγκεκριμένο έργο όπως η διαίρεση, ο τετραγωνισμός ή η ανάλυση κατά παράγοντες. Στη συνέχεια ο Τιούρινγκ έκανε ένα ακόμη πιο ριζοσπαστικό βήμα. Φαντάστηκε μια μηχανή της οποίας οι εσωτερικές συνδέσεις θα τροποποιούνταν έτσι ώστε να μπορεί να εκτελεί όλες τις λειτουργίες όλων των δυνατών μηχανών Τιούρινγκ. Οι τροποποιήσεις θα γίνονταν με την εισαγωγή προσεκτικά επιλεγμένων ταινιών που θα μετέτρεπαν τη μία πολυδύναμη μηχανή σε μηχανή διαίρεσης, πολλαπλασιασμού ή οποιουδήποτε άλλου τύπου. Ο Τιούρινγκ ονόμασε την υποθετική αυτή συσκευή καθολική μηχανή Τιούρινγκ, επειδή θα ήταν ικανή να απαντά σε οποιοδήποτε ερώτημα που θα μπορούσε να απαντηθεί λογικά. Δυστυχώς αποδείχτηκε ότι δεν είναι πάντα λογικά δυνατό να αποδειχτεί ερώτημα σχετικό με τη μη αποδειξιμότητα ενός άλλου ερωτήματος και συνεπώς ούτε η καθολική μηχανή Τιούρινγκ ήταν ικανή να προσδιορίσει όλα τα μν αποδείξιμα ερωτήματα.

Η καθολική μηχανή Τιούρινγκ μπορεί να θεωρηθεί ως μετενσάρκωση της καθολικής μηχανής αρ.2. Στην πραγματικότητα ο Τιούρινγκ είχε προχωρήσει πολύ πιο πέρα: εφοδίασε τον υπολογισμό με μία στέρεη θεωρητική βάση, εμπλουτίζοντας τον υπολογιστή με δυνατότητες που ως τότε ήταν αδιανόητες. Όμως ήταν ακόμη δεκαετία του 1930 και δεν υπήρχε η τεχνολογία που θα έκανε πραγματικότητα την καθολική μηχανή Τιούρινγκ.

Το 1939 η ακαδημαική σταδιοδρομία του Τιούρινγκ διακόπηκε απότομα. Η Κυβερνητική Σχολή Κωδίκων και Κρυπτογραμμάτων τον κάλεσε να γίνει κρυπταναλυτής στο Μπλίτλει, και στις 4 Σεπτεμβρίου του ίδιου έτους, την επόμενη της κήρυξης του πολέμου κατά της Γερμανίας από τον Νέβιλ Τσάμπερλεν, ο Τιούρινγκ μετακόμισε από την τετράγωνη αυλή του Κέμπριτζ στο Πανδοχείο του Στέμματος, το Σένλει Μπρουκ Εντ.

Ο Τιούρινγκ εστίασε το ενδιαφέρον του στο τι θα συνέβαινε αν οι Γερμανοί στρατιωτικοί άλλαζαν το σύστημα με το οποίο αντάλλασσαν τα μηνύματα κλειδιά. Οι πρώτες επιτυχίες του Μπλίτλει είχαν στηριχθεί στη δουλειά του Ρεζέφσκι, ο οποίος είχε εκμεταλλευτεί το γεγονός ότι οι χειριστές του Αινίγματος κρυπτογραφούσαν κάθε μήνυμα κλειδί δύο φορές. Αυτή η επανάληψη εξασφάλιζε, υποτίθεται, ότι ο παραλήπτης δεν θα έκανε λάθος, παράλληλα όμως δημιουργούσε μια ρωγμή στην ασφάλεια του Αινίγματος. Οι Βρετανοί κρυπταναλυτές προέβλεπαν ότι σύντομα οι Γερμανοί θα παρατηρούσαν πως η επανάληψη του κλειδιού υπονόμευε το κρυπτόγραμμα του Αινίγματος, και τότε θα έδιναν εντολή στους χειριστές να την εγκαταλείψουν, πράγμα που θα αποτελούσε πλήγμα για τις ως τότε κρυπταναλυτικές τεχνικές του Μπλίτλει. Δουλειά του Τιούρινγκ ήταν να βρει έναν εναλλακτικό τρόπο προσβολής του Αινίγματος, έναν τρόπο που δεν θα βασιζόταν στο επαναλαμβανόμενο μήνυμα κλειδί. Με το πέρασμα των εβδομάδων ο Τιούρινγκ αντιλήφθηκε ότι το Μπλίτλει συσσώρευε μια τεράστια βιβλιοθήκη αποκρυπτογραφημένων μηνυμάτων, και παρατήρησε ότι πολλά από αυτά ακολουθούσαν μια αυστηρή δομή. Μελετώντας τα παλιά αποκρυπτογραφημένα μηνύματα, πίστευε ότι μπορούσε ενίοτε να προβλέπει ένα μέρος του περιεχόμενου ενός μη αποκρυπτογραφημένου μηνύματος, στηριζόμενος στο χρόνο αποστολής και στην πηγή προέλευσής του. Για παράδειγμα, η εμπειρία έδειχνε ότι οι Γερμανοί έστελναν καθημερινά ένα τακτικό κρυπτογραφημένο δελτίο καιρού λίγο μετά τις 6π.μ. Έτσι ένα κρυπρογραφημένο μήνυμα που θα υποκλεπτόταν στις 6:05 π.μ θα περιείχε σχεδόν στα σίγουρα τη λέξη wetter που στα γερμανικά σημαίνει καιρός. Το αυστηρό πρωτόκολλο που χρησιμοποιούν οι στρατιωτικές οργανώσεις επέβαλε τα μηνύματα αυτά να ακολουθούν μια συγκεκριμένη σύνταξη, και έτσι ο Τιούρινγκ μπορούσε να είναι σίγουρος ακόμα και για τη θέση της λέξης wetter μέσα στο κρυπτογραφημένο μήνυμα. Για παράδειγμα, η εμπειρία μπορεί να του υποδείκνυε ότι τα έξι πρώτα γράμματα ενός συγκεκριμένου κρυπτογραφικού κειμένου αντιστοιχούσαν στα γράμματα wetter στο κανονικό κείμενο. Όταν ένα τμήμα κρυπτογραφικού κειμένου μπορεί να συνδεθεί με ένα τμήμα κανονικού κειμένου, ο συνδυασμός αυτός είναι γνωστός σαν *τυφλοσούρτης*. Ο

Τιούρινγκ ήταν σίγουρος ότι μπορούσε να εκμεταλλευτεί τους τυφλοσούρτες για να σπάσει το Αίνιγμα. Αν είχε στα χέρια του ένα κρυπτογραφικό κείμενο ήξερε ότι ένα συγκεκριμένο τμήμα του, για παράδειγμα το **ETJWPX** αντιπροσώπευε το **wetter**, τότε η πρόκληση ήταν να προσδιορίσει τις ρυθμίσεις του Αινίγματοσπου θα μετέτρεπαν το **wetter** σε **ETJWPX**. Ο πιο ευθύς αλλά μη πρακτικός τρόπος για να γίνει αυτό θα ήταν να πάρει ο κρυπταναλυτής μια μηχανή αντίγραφο του Αινίγματος, να πληκτρολογήσει **wetter** και να δει αν θα έβγαινε το σωστό κρυπτογραφικό κείμενο. Αν δεν έβγαινε, τότε θα άλλαζε τις ρυθμίσεις της μηχανής ανταλλάσσοντας τα καλώδια του πίνακα βυσμάτων ή τροποποιώντας τη διάταξη ή τον προσανατολισμό των «αναδιατακτών», και στη συνέχεια θα πληκτρολογούσε και πάλι **wetter.** Αν δεν προέκυπτε το σωστό κρυπτογραφικό κείμενο θα άλλαζε πάλι τις ρυθμίσεις ξανά και ξανά μέχρι να βρει τη σωστή. Το μόνο πρόβλημα με αυτή τη προσέγγιση δια της δοκιμής και πλάνης είναι ότι οι πιθανές ρυθμίσεις ανέρχονται σε 159.000.000.000.000.000.000 και επομένως το να βρει ο κρυπταναλυτής ποια από αυτές μετέτρεπε το **wetter** σε **ETJWPX** ήταν φαινομενικά αδύνατο.

Για να απλουστεύσει το πρόβλημα ο Τιούρινγκ επιχείρησε να ακολουθήσει τη στρατηγική του Ρεζέφσκι με το διαχωρισμό των ρυθμίσεων. Ήθελε να διαχωρίσει το πρόβλημα τη ανεύρεσης των ρυθμίσεων των «αναδιατακτών»(ποιος αναδιατάκτης βρίσκεται σε ποια υποδοχή και ποιοι είναι οι αντίστοιχοι προσανατολισμοί τους) από το πρόβλημα της ανεύρεσης των καλωδιώσεων του πίνακα βυσμάτων. Για παράδειγμα, αν μπορούσε να εντοπίσει στον τυφλοσούρτη κάτι που να ήταν εντελώς ανεξάρτητο από τις καλωδιώσεις του πίνακα βυσμάτων, τότε θα ήταν εφικτό να ελέγξει έναν προς έναν τους υπόλοιπους 1.054.560 συνδυασμούς των «αναδιατακτών»(60 διευθετήσεις επί 17.576 προσανατολισμούς). Έχοντας βρει τις σωστές ρυθμίσεις των «αναδιατακτών» θα μπορούσε πλέον να συμπεράνει τις καλωδιώσεις του πίνακα βυσμάτων. Τελικά η σκέψη του επικεντρώθηκε σε έναν ιδιαίτερο τύπο τυφλοσούρτη που περιείχε εσωτερικές κυκλικές δομές(βρόχους), όμοιες με τις αλυσίδες που είχε εκμεταλλευτεί ο Ρεζέφσκι. Οι αλυσίδες του Ρεζέφσκι συνέδεαν γράμματα μέσα στο μήνυμα κλειδί. Αντίθετα οι βρόχοι του Τιούρινγκ δεν είχαν καμία σχέση με το τελευταίο(ο Τιούρινγκ εργαζόταν πάνω στη υπόθεση ότι οι Γερμανοί σύντομα θα σταματούσαν να στέλνουν επαναλαμβανόμενα μηνύματα κλειδιά), και απλώς συνέδεαν γράμματα του κανονικού κειμένου με γράμματα του κρυπτογραφικού κειμένου μέσα σε έναν τυφλοσούρτη. Για παράδειγμα, ο τυφλοσούρτης που φαίνεται στην εικόνα 48 περιέχει έναν βρόχο. Επισημαίνεται ότι οι τυφλοσούρτες είναι απλώς υποθέσεις, αν όμως θεωρήσουμε ότι ένας τυφλοσούρτης είναι σωστός, μπορούμε να συνδέσουμε τα γράμματα: **w→E, e→T, t→W**. Παρότι δεν γνωρίζουμε καμιά από τις ρυθμίσεις του Αινίγματος, μπορούμε να ονομάσουμε την πρώτη ρύθμιση, όποια κι αν είναι αυτή, S. Στην πρώτη αυτή ρύθμιση ξέρουμε ότι το **w** κρυπτογραφείται ως **E**.Μετά από αυτή τη κρυπτογράφηση, ο πρώτος αναδιατάκτης μετακινείται κατά μία θέση, στη ρύθμιση S+1, και το γράμμα **e** κρυπτογραφείται ως **T**. Ο «αναδιατάκτης μετακινείται κατά μία ακόμη θέση και κρυτπογραφεί ένα γράμμα που δεν αποτελεί μέρος του βρόχου, οπότε αγνοούμε αυτή τη κρυπτογράφηση. Στη συνέχεια ο «αναδιατάκτης» προχωρεί άλλη μία θέση, και τη φορά αυτή βρίσκουμε και πάλι ένα γράμμα που αποτελεί μέρος του βρόχου. Στη ρύθμιση S+3, ξέρουμε ότι το γράμμα **t** κρυπτογραφείται ως **W**. Συνοπτικά γνωρίζουμε ότι:

*Στη ρύθμιση S, το Αίνιγμα κρυπτογραφεί το **w** ως **E***
*Στη ρύθμιση S+1, το Αίνιγμα κρυπτογραφεί το **e** ως **T***
*Στη ρύθμιση S+3, το Αίνιγμα κρυπτογραφεί το **t** ως **W***

Μέχρι εδώ ο βρόχος μοιάζει απλώς με περίεργο σχήμα, όμως ο Τιούρινκ παρακολούθησε με επιμονή τις συνέπειες των σχέσεων μέσα στο βρόχο και είδε ότι του παρείχαν το δραστικά γρήγορο δρόμο που χρειαζόταν για να σπάσει το Αίνιγμα. Αντί να δουλεύει με μία μόνο μηχανή Αίνιγμα για να ελέγχει κάθε ρύθμιση, ο Τιούτινγκ άρχισε να φαντάζεται 3 ξεχωριστές μηχανές, που η καθεμιά τους θα ασχολείτο με την κρυτπογράφηση ενός στοιχείου του βρόχου. Η πρώτη μηχανή θα επιχειρούσε να κρυπτογραφήσει το w ως E, η δεύτερη το e ως T και η τρίτη το t ως W. Και οι τρεις μηχανές θα είχαν τις ίδιες ακριβώς ρυθμίσεις με τη μόνη διαφορά ότι στη δεύτερη οι προσανατολισμοί των «αναδιατακτών» θα βρίσκονταν μια θέση μπροστά από ότι στην πρώτη(ρύθμιση S+1) και στην τρίτη οι προσανατολισμοί των «αναδιατακτών» θα βρίσκονταν τρεις θέσεις μπροστά (ρύθμιση S+3). Στη συνέχεια ο Τιούρινγκ φαντάστηκε έναν κρυπταναλυτή να αλλάζει συνεχώς και με φρενήρη ρυθμό τα καλώδια στους πίνακες βυσμάτων, να ανταλλάσσει τις διατάξεις των «αναδιατακτών» και να

τροποποιεί τους προσανατολισμούς τους έτσι ώστε να πετύχει τις σωστές κρυπτογραφήσεις. Όσα καλώδια άλλαζαν στην πρώτη μηχανή θα άλλαζαν και στις άλλες δύο. Και το σημαντικότερο, η δεύτερη μηχανή θα είχε τον ίδιο προσανατολισμό με την πρώτη, αλλά μετατεθειμένο κατά μία θέση, ενώ στην τρίτη ο ίοδιος προσανατολισμός θα είχε προχωρήσει κατά τρεις θέσεις. Μέχρι αυτό το σημείο ο Τιούρινγκ δεν φαίνεται να έχει πετύχει πολλά πράγματα αφού ο κρυπταναλυτής είναι ακόμα υποχρεωμένος να ελέγξει και τις 159.000.000.000.000.000.000 πιθανές ρυθμίσεις και μάλιστα να το κάνεις ταυτόχρονα σε τρεις μηχανές αντί για μία. Ωστόσο το επόμενο στάδιο της ιδέας του Τιούρινγκ αλλάζει τα δεδομένα του προβλήματος και το απλοποιεί κατά πολύ. Η σκέψη του ήταν να συνδέσει τις τρεις μηχανές περνώντας ηλεκτρικά καλώδια ανάμεσα στις εισόδους και τις εξόδους της καθεμιάς, όπως φαίνεται στην παρακάτω εικόνα. Ουσιαστικά η θηλιά στον τυφλοσούρτη αντιστοιχεί με τη θηλιά στο ηλεκτρικό κύκλωμα. Ο Τιούρινγκ φαντάστηκε τις μηχανές να αλλάζουν ρυθμίσεις στους πίνακες βυσμάτων και τους αναδιατάκτες τους, όπως περιγράφηκε παραπάνω, αλλά το κύκλωμα θα συμπληρωνόταν μόνο όταν όλες οι ρυθμίσεις θα ήταν σωστές για όλες τις μηχανές, επιτρέποντας σε ένα ηλεκτρικό ρεύμα να ρέει μέσα και από τις τρεις. Αν ο Τιούρινγκ ενσωμάτωνε έναν ηλεκτρικό λαμπτήρα μέσα στο κύκλωμα, τότε το ρεύμα θα τον άναβε, σημαίνοντας ότι είχαν βρεθεί οι σωστλές ρυθμίσεις. Στο σημείο αυτό οι τρεις μηχανές είναι ακόμη υποχρεωμένες να ελέγχουν και τις 159.000.000.000.000.000.000 πιθανές ρυθμίσεις για να ανάψουν το λαμπτήρα. Όμως όλα όσα έγιναν μέχρι εδώ δεν ήταν παρά μία προετοιμασία για το τελικό λογικό λογικό άλμα του Τιούρινγκ, ένα άλμα που θα έκανε μεμιάς το έργο των μηχανών πάνω από εκατό εκατομμύρια φορές ευκολότερο.

Ο Τιούρινγκ είχε κατασκευάσει το ηλεκτρικό του κύκλωμα κατά τέτοιο τρόπο, ώστε να μηδενίζει την επίδραση του πίνακα βυσμάτων, πράγμα που του επέτρεπε να αγνοεί τα δισεκατομμύρια των πιθανών ρυθμίσεων του τελευταίου. Η εικόνα δείχνει ότι στο πρώτο Αίνιγμα, το ηλεκτρικό ρεύμα εισέρχεται στους «αναδιατάκτες» και εξέρχεται σε κάποιο άγνωστο γράμμα, το οποίο θα ονομάσουμε Γ1. Στη συνέχεια το ρεύμα διέρχεται από τον πίνακα βυσμάτων, που μετατρέπει το Γ1 σε Ε. Αυτό το Ε συνδέεται μέσω ενός καλωδίου με το γράμμα e του δεύτερου Αινίγματος, και καθώς το ρεύμα διέρχεται μέσω του δεύτερου πίνακα βυσμάτων, μετατρέπεται πάλι σε Γ1. Με άλλα λόγια οι δύο πίνακες βυσμάτων αλληλοεξουδετερώνονται. Με τον ίδιο τρόπο, το ρεύμα που εξέρχεται από τους «αναδιατάκτες» του δεύτερου Αινίγματος εισέρχεται στον πίνακα βυσμάτων στο γράμμα Γ2 πριν αυτό μετατραπεί σε Τ. Αυτό το Τ συνδέεται μέσω ενός καλωδίου με το γράμμα t του τρίτου Αινίγματος, και καθώς το ρεύμα διέρχεται μέσω του τρίτου πίνακα βυσμάτων, μετατρέπεται πάλι σε Γ2. Με δύο λόγια οι πίνακες βυσμάτων εξουδετερώνονται μέσα στο όλο κύκλωμα, κι έτσι ο Τιούρινγκ μπορούσε να τους αγνοήσει εντελώς. Το μόνο που χρειαζόταν τώρα ο Τιούρινγκ ήταν να συνδέσει την έξοδο της πρώτης σειράς «αναδιατακτών», Γ1, κατευθείαν στη είσοδο της δεύτερης σειράς, Γ1 επίσης κ.ο.κ. Δυστυχώς δεν ήξερε την ταυτότητα του γράμματος Γ1 οπότε έπρεπε να συνδέσει και τις 26 εξόδους της πρώτης σειράς «αναδιατακτών» με τις 26 αντίστοιχες εισόδους της δεύτερης σειράς κ.ο.κ. Στην πραγματικότητα υπήρχαν τώρα 26 ηλεκτρικές θηλιές και η καθεμιά τους έπρεπε να διαθέτει από έναν ηλεκτρικό λαμπτήρα, για να σημαίνει την ολοκλήρωση ενός ηλεκτρικού κυκλώματος. Στη συνέχεια οι τρεις σειρές των «αναδιατακτών» μπορούσαν απλώς να ελέγξουν έναν προς έναν τους 17.576 προσανατολισμούς με τη δεύτερη σειρά να βρίσκεται πάντα μια θέση μπροστά από την πρώτη και την Τρίτη δύο θέσεις μπροστά από την δεύτερη. Μετά την ανεύρεση και των σωστών προσανατολισμών των «αναδιατακτών», το ένα κύκλωμα θα συμπληρωνόταν και ο λαμπτήρας θα άναβε. Αν οι «αναδιατάκτες» άλλαζαν προσανατολισμό κάθε δευτερόλεπτο, θα χρειαζόταν μόλις 5 ώρες για να ελεγχθούν όλοι οι προσανατολισμοί. Παρέμεναν μόνο δύο προβήματα. Πρώτον, οι τρεις μηχανές μπορεί να τρέχουν με λάθος διάταξη των «αναδιατακτών», επειδή το Αίνιγμα λειτουργεί με οποιουσδήποτε τρεις από τους πέντε διαθέσιμους «αναδιατάκτες» τοποθετημένους με οποιαδήποτε σειρά, πράγμα που μας δίνει εξήντα πιθανούς συνδυασμούς. Επομένως, αν ελεγχθούν και οι 17.576 προσανατολισμοί και ο λαμπτήρας δεν ανάψει, είναι απαραίτητο να δοκιμάσουμε έναν άλλο συνδυασμό από τους εξήντα πιθανούς, αι να συνεχίσουμε έτσι μέχρι να ολοκληρωθεί το κύκλωμα. Σαν εναλλακτική λύση, ο κρυπταναλυτής μπορούσε να έχει εξήντα συστήματα των τριών Αινιγμάτων, τα οποία θα λειτουργούσαν ταυτόχρονα.

Το δεύτερο πρόβλημα σχετιζόταν με την ανεύρεση των καλωδιώσεων στους πίνακες βυσμάτων, μετά τον εντοπισμό των διατάξεων και των προσανατολισμών των «αναδιατακτών». Χρησιμοποιώντας μια μηχανή Αίνιγμα με τις σωστές ρυθμίσεις των «αναδιατακτών», ο κρυπταναλυτής πληκτρολογεί το κρυπτογραφικό κείμενο και κοιτάζει το προκύπτον κανονικό κείμενο. Αν το αποτέλεσμα είναι **tewwer**

αντί για **wetter**, τότε είναι προφανές ότι πρέπει να εισαχθούν στον πίνακα βυσμάτων καλώδια κατά τέτοιο τρόπο ώστε να ανταλλάσσουν τα w και t. Η πληκτρολόγηση και άλλων τμημάτων ρυπτογραφικού κειμένου θα αποκαλύψει και άλλες καλωδιώσεις του πίνακα βυσμάτων. Ο συνδυασμός του τυφλοσούρτη, των θηλιών και των ηλεκτρικά συνδεδεμένων μηχανών είχε ως αποτέλεσμα ένα εκπληκτικό κρυπτογραφικό επίτευγμα, κάτι που μόνο ο Τιούρινγκ με το μοναδικό του υπόβαθρο στις μαθηματικές μηχανές μπορούσε να κατορθώσει. Οι ρεμβασμοί του γι ατις φανταστικές μηχανές Τιούρινγκ είχαν σκοπό να απαντήσουν σε φιλοσοφικά ερωτήματα σχετικά με τη μαθηματική μη αποδειξιμότητα, όμως αυτή η καθαρά ακαδημαική του έρευνα τον είχε τοποθετήσει στο σωστό διανοητικό πλαίσιο που θα του επέτρεπε να σχεδιάσει μια υπαρκτή μηχανή κατάλληλη να λύνει πραγματικά προβήματα.

Το Μπλίτσλει ήταν σε θέση να βρει 100.000 λίρες ώστε να μετατρέψει την ιδέα του Τιούρινγκ σε λειτουργικές συσκευές, οι οποίες ονομάστηκαν μπόμπες, επειδή η μηχανική τους προσέγγιση παρουσίαζε κάποια φευγαλέα ομοιότητα με την μπόμπα του Ρεζέφσκι. Κάθε μπόμπα του Τιούρινγκ θα αποτελείτο από 12 σειρές ηλεκτρικά συνδεδεμένων «αναδιατακτών» Αινίγματος, και έτσι θα μπορούσε να αντιμετωπίζει πολύ μακρύτερες θηλιές γραμμάτων. Η πλήρης μονάδα θα είχε περίπου 2 μέτρα ύψος, 2 μέτρα μήκος και 1 μέτρο πλάτος. Ο Τιούρινγκ τελειοποίησε το σχέδιο στις αρχές του 1940.

Ωστόσο όλα όσα συνέβαιναν στην Κυβερνητική Σχολή Κωδίκων και Κρυπτογραμμάτων ήταν άκρως απόρρητα και έτσι κανείς έξω από το Μπλίτσλει Παρκ δεν γνώριζε το αξιόλογο επίτευγμα του Τιούρινγκ.

Η πρώτη πρωτότυπη μπόμπα, που τη βάφτισαν Νίκη, έφτασε στο Μπλίτσλει στις 14 Μαρτίου 1940. Η μηχανή τέθηκε αμέσως σε λειτουργία, αλλά τα αρχικά αποτελέσματα κάθε άλλο παρά ικανοποιητικά ήταν. Η μηχανή αποδείχτηκε πολύ πιο αργή από το αναμενόμενο: χρειαζόταν μια βδομάδα για να βρει ένα συγκεκριμένο κλειδί. Υπήρξε μια συντονισμένη προσπάθεια για να αυξηθεί η αποτελεσματικότητα της μπόμπας και λίγες βδομάδες μετά υπεβλήθη νέο τροποποιημένο σχέδιο. Θα χρειάζονταν 4 ακόμη μήνες για να κατασκευαστεί η αναβαθμισμένη μπόμπα. Στο μεταξύ οι κρυπταναλυτές είχαν να αντιμετωπίσουν τη συμφορά που από καιρό φοβόντουσαν. Την 1η Μαιου 1940, οι Γερμανοί άλλαξαν το πρωτόκολλο ανταλλαγής κλειδιών. Σταμάτησαν να επαναλαμβάνουν το μήνυμα κλειδί και από τότε ο αριθμός των επιτυχημένων αποκρυπτογραφήσεων του Αινίγματος μειώθηκε δραματικά. Το μπλακαουτ στην πληροφόρηση κράτησε μέχρι την άφιξη της νέας μπόμπας. Η μηχανή αυτή που τη βάφτισαν Agnus Dei ( Αμνός του Θεού) ή για συντομία Άγκνες έμελλε να εκπληρώσει τις προσδοκίες του Τιούρινγκ. Μέσα σε 18 μήνες είχαν τεθεί σε λειτουργία άλλες 15 μπόμπες που εκμεταλλεύονταν τους τυφλοσούρτες, έλεγχαν τις ρυθμίσεις των «αναδιατακτών» και αποκάλυπταν τα κελιδιά. Αν όλα πήγαιναν καλά, μια μπόμπα μπορούσε να βρει ένα κλειδί του Αινίγματος μέσα σε μια ώρα. Από τη στιγμή που για ένα συγκεκριμένο μήνυμα είχαν εντοπιστεί οι καλωδιώσεις του πίνακα βυσμάτων και οι ρυθμίσεις των «αναδιατακτών» (δηλαδή το μήνυμα κλειδί), ήταν εύκολο να συμπεράνουν το ημερήσιο κλειδί. Όλα τα άλλα μηνύματα που στέλνονταν την ίδια μέρα μπορούσαν τότε να αποκρυπτογραφηθούν. Παρότι οι μπόμπες αποτελούσαν ζωτικής σημασίας επίτευγμα στην κρυπτανάλυση, η αποκρυπτογράφηση δεν έγινε ποτέ υπόθεση ρουτίνας. Υπήρχαν πολλά εμπόδια που έπρεπε να υπερκεραστούν πριν μπορέσουν οι μπόμπες έστω και να αρχίσουν να ψάχνουν για ένα κλειδί. Για παράδειγμα για να λειτουργήσει μια μπόμπα χρειαζόταν πρώτα ένας τυφλοσούρτης. Οι κρυπταναλυτές των υψηλών κλιμακίων έδιναν τυφλοσούρτες στους χειριστές της μπόμπας, όμως δεν υπήρχε εγγύηση ότι είχαν ναμτέψει το σωστό νόημα του κρυπτογραφικού κειμένου. Αλλά ακόμη κι αν είχαν το σωστό τυφλοσούρτη, μπορεί αυτός να βρισκόταν σε λάθος θέση – οι κρυπταναλυτές μπορεί να είχαν μαντέψει ότι ένα κρυπτογραφημένο μήνυμα περιείχε μια συγκεκριμένη φράση, αλλά να είχαν συνδέσει τη φράση αυτή με λάθος τμήμα του κρυπτογραφικού κειμένου. Υπήρχε ωστόσο ένα έξυπνο κόλπο για να ελέγχουν αν ένας τυφλοσούρτης βρισκόταν στη σωστή θέση.

Στον τυφλοσούρτη που ακολουθεί, ο κρυπταναλυτής έχει τη βεβαιότητα ότι το κανονικό κείμενο είναι σωστό, αλλά δεν είναι σίγουρος αν το συνταίριαξε με τα σωστά γράμματα του κρυπτογραφικού κειμένου.

*Εικαζόμενο κείμενο* ***w e t t e r n u l l s e c h s***
*Γνωστό κρυπτογραφικό κείμενο* ***I P R E N L W K M J J S X C P L E J W Q***

Ένα από τα χαρακτηριστικά του Αινίγματος ήταν ότι, εξαιτίας του ανακλαστή δεν μπορούσε να κρυπτογραφήσει ένα γράμμα ως τον εαυτό του. Το γράμμα a δεν μπορούσε ποτέ να κρυπτογραφηθεί A, το b ποτέ ως B κ.ο.κ. Επομένως ο συγκεκριμένος τυφλοσούρτης του παραπάνω παραδείγματος θα πρέπει να έχει αντιστοιχηθεί εσφαλμένα, επειδή το πρώτο **e** του **wetter** έχει συνταιριαστεί με **E** στο κρυπρογραφικό κείμενο. Για να βρούμε τη σωστή αντιστοίχηση απλώς μετακινούμε το απλό κείμενο προς το κρυπτογραφικό, μέχρι που κανέναν γράμμα να μην συνταιριάζεται με τον εαυτό του. Αν μετακινήσουμε το κανονικό κείμενο κατά μία θέση προς τα αριστερά, η αντιστοίχηση και πάλι αποτυγχάνει επειδή αυτή τη φορά το πρώτο s του sechs συνταιριάζει με S στο κρυπτογραφικό κείμενο. Αν όμως μετακινήσουμε το κανονικό κείμενο κατά μια θέση προς τα δεξιά, δεν υπάρχουν αντικανονικές κρυπτογραφήσεις. Τώρα λοιπόν ο τυφλοσούρτης φαίνεται να είναι στη σωστή θέση και μπορεί να χρησιμοποιηθεί ως βάση για την αποκρυπτογράφηση με τη μπόμπα:

*Εικαζόμενο κείμενο* ***w e t t e r n u l l s e c h s***
*Γνωστό κρυπτογραφικό κείμενο* ***I P R E N L W K M J J S X C P L E J W Q***

Οι πληροφορίες που συγκεντρώνονταν στο Μπλίτσλει διαβιβάζονταν μόνο στους ανώτερους αξιωματικούς και σε επίλεκτα μέλη του πολεμικού επιτελείου. Ο Ουίνστον Τσόρτσιλ γνώριζε καλά πόσο σημαντικές ήταν οι αποκρυπτογραφήσεις του Μπλίτσλει και στις 6 Σεπτεμβρίου 1941 επισκέφτηκε τους κρυπταναλυτές. Συναντώντας μερικούς από αυτούς, έμεινε έκπληκτος με το παράξενο κράμα των ανθρώπων που του παρείχαν τόσο πολύτιμες πληροφορίες: εκτός από μαθηματικούς και γλωσσολόγους υπήρχε και ένας ειδικός στην κεραμική, ένας έφορος από το μουσείο της Πράγας, ο πρωταθλητής σκακιού της Βρετανίας και πολλοί εξπέρ του μπριτζ. Σκοπός της επίσκεψης ήταν να τονώσει το ηθικό των κρυπταναλυτών δείχνοντάς τους πως το έργο τους εκτιμάτο στα ανώτατα κλιμάκια. Παράλληλα, έδωσε στον Τιούρινγκ και τους συνεργάτες του το θάρρος να απευθυνθούν κατευθείαν στον Τσόρτσιλ όταν ξέσπασε μια κρίση. Για να εκμεταλλευτεί πλήρως τις μπόμπες ο Τιούρινγκ χρειαζόταν περισσότερο προσωπικό, αλλά το αίτημά του προσέκρουσε στο Διοικητή Έντουαρντ Τράβις, που είχε αναλάβει επικεφαλής του Μπλίτσλει και που είχε την άποψη ότι δεν μπορούσε να δικαιολογήσει την πρόσληψη και άλλων ατόμων. Έτσι οι κρυπταναλυτές αποφάσισαν να αψηφήσουν την ιεραρχία και να απευθυνθούν κατευθείαν στον Τσόρτσιλ, μέσω επιστολής η οποία επισήμαινε την καθυστέρηση του σπασίματος των γερμανικών κωδίκων λόγω έλλειψης προσωπικού. Ο Τσόρτσιλ αμέσως έστειλε μνημόνιο στον αρχηγό του επιτελείου του με την εντολή να παραχωρηθεί στην ομάδα κρυπταναλυτών ότι επιθυμούσαν με άμεση προτεραιότητα.

Στο εξής δεν επρόκειτο να τεθούν άλλοι περιορισμοί σε έμψυχο ή άψυχο υλικό. Ως το τέλος του 1942 υπήρχαν 49 μπόμπες και ένας νέος σταθμός άνοιξε στην Έπαυλη Γκέιχαρστ, βόρεια του Μπλίτσλει. Ως μέρος της προσπάθειας στρατολόγησης, η κυβερνητική σχολή κωδίκων και κρυπτογραμμάτων δημοσίευσε μια επιστολή στην Daily telegraph, απευθύνοντας ανώνυμη πρόκληση στους αναγνώστες της εφημερίδας. Το ερώτημα ήταν αν κάποιος μπορούσε να λύσει το σταυρόλεξό της σε λιγότερο από 12 λεπτά. Πίστευαν ότι οι έμπειροι λύτες σταυρολέξων θα ήτα και καλοί κρυπταναλυτές, συμπληρώνοντας τα επιστημονικά πνεύματα που υπηρετούσαν ήδη στο Μπλίτσλει – αλλά φυσικά και στην εφημερίδα δεν αναφερόταν τίποτε από αυτά. Οι 25 αναγνώστες που απάντησαν, προσεκλήθησαν στην Οδό Φλιτ, για να περάσουν από ένα τεστ σταυρολέξου. Πέντε από αυτούς τελείωσαν το σταυρόλεξο μέσα στα καθορισμένα χρονικά όρια, και άλλος ένας δεν είχε βρει μόνο μια λέξη όταν πέρασαν τα 12 λεπτά. Λίγες εβδομάδες αργότερα, και οι έξι έδωσαν συνέντευξη σε υπεύθυνους στρατιωτικής κατασκοπίας και προσελήφθησαν ως κρυπταναλυτές στο Μπλίτσλει Παρκ.

Η κυκλοφορία μηνυμάτων του Αινίγματος δεν ήταν ένα γιγάντιο σύστημα επικοινωνιών, υπήρχαν περισσότερα ανεξάρτητα δίκτυα. Ο Γερμανικός Στρατός στη Βόρειο Αφρική, για παράδειγμα, διέθετε δικό του, χωριστό δίκτυο, και οι εκεί χειριστές του Αινίγματος είχαν κωδικά βιβλία διαφορετικά από αυτά της Ευρώπης. Επομένως, αν το Μπλίτσλει κατόρθωνε να προσδιορίσει το βορειοαφρικανικό ημερήσιο κλειδί θα ήταν σε θέση να αποκρυτπογραφεί όλα τα γερμανικά μηνύματα που θα στέλνονταν εκείνη τη μέρα από τη Βόρειο Αφρική, όμως το κλειδί αυτό θα ήταν άχρηστο για το σπάσιμο των μηνυμάτων που διαβιβάζονταν στην Ευρώπη. Ορισμένα δίκτυα ήταν δυσκολότερο να σπάσουν σε σύγκριση με κάποια άλλα. Το δυσκολότερο από όλα ήταν το δίκτυο του Πολεμικού Ναυτικού, επειδή χειριζόταν μια πιο εξελιγμένη παραλλαγή του Αινίγματος. Για παράδειγμα, οι χειριστές του Ναυτικού Αινίγματος μπορούσαν να επιλέξουν ανάμεσα σε οκτώ και όχι μόνο ανάμεσα σε πέντε «αναδιατάκτες»,

πράγμα που σήμαινε ότι υπήρχαν σχεδόν έξι φορές περισσότερες διευθετήσεις των «αναδιατακτών», και συνεπώς σχεδόν έξι φορές περισσότερα κλειδιά που έπρεπε να ελέγξει το Μπλίτσλει. Η δεύτερη διαφορά του Ναυτικού Αινίγματος αφορούσε στον ανακλαστή, ο οποίος έστελνε πίσω το ηλεκτρικό σήμα μέσω των «αναδιατακτών». Στο τυποποιημένο Αίνιγμα, ο ανακλαστής ήταν μονίμως στερεωμένος σε ένα συγκεκριμένο προσανατολισμό όμως στο Ναυτικό Αίνιγμα μπορούσε να στερεώνεται σε οποιονδήποτε από τους 26 προσανατολισμούς. Επομένως ο αριθμός των πιθανών κλειδιών πολλαπλασιαζόταν επί 26.

Την κρυπτανάλυση του Ναυτικού Αινίγματος την καθιστούσαν ακόμη δυσχερέστερη οι χειριστές του, που πρόσεχαν να μην στέλνουν στερεότυπα μηνύματα, στερώντας έτσι τους τυφλοσούρτες από το Μπλίτσλει. Επιπλέον, το γερμανικό πολεμικό ναυτικό εγκαθίδρυσε ένα νέο ασφαλέστερο σύστημα για να επιλέγει και να διαβιβάζει τα μηνύματα κλειδιά. Οι επιπρόσθετοι «αναδιατάκτες», ο μεταβλητού προσανατολισμού ανακλαστής, τα μη στερεότυπα μηνύματα και το νέο σύστημα ανταλλαγής μηνυμάτων κλειδιών, όλα αυτά μαζί συνέτειναν ώστε οι επικοινωνίες του γερμανικού ναυτικού να είναι αδιαπέραστες.

Η αποτυχία του Μπλίτσλει να σπάσει το Ναυτικό Αίνιγμα είχε ως συνέπεια το Γερμανικό Πολεμικό Ναυτικό να έχει σταθερά το πάνω χέρι στη μάχη του Ατλαντικού. Ο Ναύαρχος Καρλ Ντένιτς είχε αναπτύξει μια άκρως αποτελεσματική στρατηγική ναυτικού πολέμου σε δύο στάδια η οποία άρχιζε με τη διασπορά των υποβρυχίων του, που όργωναν τον Ατλαντικό αναζητώντας συμμαχικές νηοπομπές. Μόλις ένα υποβρύχιο εντόπιζε ένα στόχο έθετε σε εφαρμογή το δεύτερο στάδιο της στρατηγικής καλώντας τα υπόλοιπα υποβρύχια στη συγκεκριμένη περιοχή. Η επίθεση άρχιζε μόνο όταν συγκεντρωνόταν μεγάλος αριθμός υποβρυχίων. Για να πετύχει αυτή η στρατηγική της συντονισμένης επίθεσης, ήταν σημαντικό να έχει το πολεμικό ναυτικό πρόσβαση σε ασφαλείς επικοινωνίες. Το Ναυτικό Αίνιγμα εξασφάλιζε αυτήν την παράμετρο και οι επιθέσεις των γερμανικών υποβρυχίων κατέφεραν συντριπτικά πλήγματα στα συμμαχικά πλοία τα οποία εφοδίαζαν τη Βρετανία με τρόφιμα και όπλα που τόσο χρειάζονταν.

Όσο οι επικοινωνίες των υποβρυχίων παρέμεναν ασφαλείς, οι Σύμμαχοι αγνοούσαν εντελώς τις θέσεις τους και δεν μπορούσαν να χαράξουν ασφαλείς πορείες για τις νηοπομπές τους. Εκτός από την αφόρητη καταστροφή των πλοίων τρομερό ήταν και το κόστος σε ανθρώπινες ζωές. Η πολωνική εμπειρία και η περίπτωση του Χανς – Τίλο Σμιτ είχε διδάξει το Μπλίτσλει Παρκ ότι αν η διανοητική προσπάθεια αποτύχει να σπάσει ένα κρυπτόγραμμα, τότε είναι απαραίτητη η προσφυγή στην κατασκοπία, τη διάβρωση και την κλοπή ώστε να αποκτηθούν τα κλειδιά του εχθρού. Πού και πού το Μπλίτσλει κέρδιζε μια νίκη στη μάχη κατά του Ναυτικού Αινίγματος χάρη σε ένα έξυπνο τέχνασμα της RAF. Τα βρετανικά αεροπλάνα έριχναν νάρκες σε ένα συγκεκριμένο σημείο προκαλώντας τα γερμανικά σκάφη να στέλνουν μηνύματα στα άλλα πλοία. Αυτά τα κρυπτογραφημένα με το Αίνιγμα μηνύματα αναπόφευκτα περιλάμβαναν αναφορά σε ένα χάρτη, όμως η αναφορά αυτή ήταν ήδη γνωστή στους Βρετανούς, και έτσι μπορούσε να χρησιμοποιηθεί ως τυφλοσούρτης. Με άλλα λόγια, το Μπλίτσλει γνώριζε ότι ένα συγκεκριμένο τμήμα κρυπτογραφικού κειμένου αντιπροσώπευε μια συγκεκριμένη δέσμη συντεταγμένων. Η διασπορά των ναρκών με σκοπό να αποκτηθούν τυφλοσούρτες, γνωστή σαν κηπουρική, απαιτούσε να πετούν τα αεροπλάνα της RAF σε ειδικές αποστολές, πράγμα που δεν ήταν δυνατό να γίνεται τακτικά. Το Μπλίτσλει έπρεπε να βρει έναν άλλο τρόπο να σπάσει το Ναυτικό Αίνιγμα. Μια εναλλακτική στρατηγική εξαρτάτο από την κλοπή των κλειδιών. Ένα από τα πιο παράτολμα σχέδια για την κλοπή των κλειδιών το κατέστρωσε ο Ίαν Φλέμινγκ. Πρότεινα νε συντρίψουν ένα γερμανικό βομβαρδιστικό, το οποίο είχαν αιχμαλωτίσει στη Μάγχη, κοντά σε ένα γερμανικό πλοίο. Οι Γερμανοί ναύτες θα πλησίαζαν το αεροπλάνο για να σώσουν τους συμπολεμιστές τους, και τότε το πλήρωμα του αεροπλάνου, δηλαδή Βρετανοί πιλότοι που θα παρίσταναν τους Γερμανούς, θα ανέβαιναν στο πλοίο και θα έκλεβαν τα κωδικά βιβλία του. Τα βιβλία αυτά περιείχαν όλες τις πληροφορίες που απαιτούνταν για τον εντοπισμό του κλειδιού της κρυπτογράφησης, και επειδή τα πλοία βρίσκονταν συχνά μακριά από τη βάση τους για μεγάλες περιόδους, τα κωδικά βιβλία θα ίσχυαν για τουλάχιστον ένα μήνα.

Η Βρετανική Υπηρεσία Πληροφοριών ενέκρινε το σχέδιο του Φλέμινγκ γνωστό ως *Επιχείρηση Αδίστακτος*, και άρχισε να ετοιμάζει ένα βομβαρδιστικό τύπου Χάινκελ για τη συντριβή, ενώ συγκέντρωσε και ένα πλήρωμα από γερμανόφωνους Άγγλους. Ο Φλέμινγκ πήγε στο Ντόβερ για να επιβλέψει την επιχείρηση, δυστυχώς όμως δεν υπήρχαν γερμανικά πλοία στην περιοχή, και η εφαρμογή του σχεδίου αναβλήθηκε επ’ αόριστον. Τελικά η επιχείρηση ματαιώθηκε, όμως τα κωδικά βιβλία του

Γερμανικού Ναυτικού έπεσαν στα χέρια των Βρετανών στη διάρκεια καταιγιστικών επιδρομών εναντίον μετεωρολογικών πλοίων και υποβρυχίων. Έτσι το Μπλίτσλει πήρε τα έγγραφα που χρειαζόταν για να θέσει τέρμα στο μπλακάουτ των πληροφοριών. Έχοντας σπάσει το Ναυτικό Αίνιγμα, το Μπλίτσλει μπορούσε να εντοπίσει τη θέση των γερμανικών υποβρυχίων, και η Μάχη του Ατλαντικού άρχισε να γέρνει προς την πλευρά των Συμμάχων. Το σημαντικό ήταν να μην υποπτευθεί ποτέ η Γερμανική Ανώτατη Διοίκηση ότι οι Άγγλοι είχαν στην κατοχή τους τα κωδικά βιβλία του Αινίγματος. Αν οι Γερμανοί ανακάλυπταν ότι η ασφάλεια του Αινίγματος είχε παραβιαστεί θα αναβάθμιζαν τις μηχανές τους και το Μπλίτσλει θα έπρεπε να ξαναρχίσει από το μηδέν. Όπως και με το επεισόδιο του τηλεγραφήματος Τσίμερμαν, οι Βρετανοί πήραν διάφορες προφυλάξεις ώστε να μην εγείρουν υποψίες, λ.χ αφού έπαιρναν τα κωδικά βιβλία ενός πλοίου, στη συνέχεια το βύθιζαν. Αυτό θα έπειθε το Ναύαρχο Ντένιτς ότι το κρυπτογραφικό υλικό είχε χαθεί στο βυθό της θάλασσας και δεν είχε πέσει σε βρετανικά χέρια. Μετά τη μυστική κλοπή του υλικού, οι Βρετανοί έπρεπε να πάρουν επιπρόσθετες προφυλάξεις πριν χρησιμοποιήσουν τις πληροφορίες που είχαν συλλέξει. Για παράδειγμα, οι αποκρυπτογραφήσεις του Αινίγματος έδιναν τις θέσεις πολλών γερμανικών υποβρυχίων, όμως δεν θα ήταν φρόνιμο να τα προσβάλουν όλα. Οι Σύμμαχοι άφηναν επίτηδες μερικά υποβρύχια να διαφύγουν και προσέβαλαν τα υπόλοιπα μόνο αφού έστελναν από πάνω τους ένα αναγνωριστικό αεροπλάνο δικαιολογώντας έτσι τον κατάπλου ενός αντιτορπιλικού λίγες ώρες μετά. Εναλλακτικά, οι Σύμμαχοι έστελναν πλαστά μηνύματα που περιέγραφαν εντοπισμούς υποβρυχίων από αέρος, πράγμα που επίσης εξηγούσε επαρκώς την επίθεση που ακολουθούσε. Σε μια περίπτωση, το Μπλίτσλει αποκρυπτογράφησε ένα μήνυμα του Αινίγματος που έδινε την ακριβή θέση μιας ομάδας εννιά γερμανικών δεξαμενοπλοίων και πλοίων ανεφοδιασμού. Το Ναυαρχείο αποφάσισε να μην βυθίσει όλα τα πλοία γιατί μια ολική καταστροφή των στόχων θα προκαλούσε τις υποψίες των Γερμανών. Πληροφόρησε λοιπόν τα αντιτορπιλικά για τη θέση των επτά από τα εννιά πλοία τα όντως βυθίστηκαν. Κάποια αντιτορπιλικά όμως του Βασιλικού Ναυτικού συνάντησαν κατά τύχη τα δύο που έπρεπε υποτίθεται να διασωθούν και τα βύθισαν και αυτά. Στο Βερολίνο ο Ναύαρχος Κουρτ Φρίκε διέταξε έρευνα για τη συγκεκριμένη επίθεση και για άλλες παρόμοιες διερευνώντας την πιθανότητα να είχαν σπάσει οι Βρετανοί το Αίνιγμα. Η αναφορά κατέληξε στο συμπέρασμα ότι οι μεγάλες απώλειες ήταν αποτέλεσμα φυσικής κακοτυχίας αφού το σπάσιμο του Αινίγματος θεωρείτο ανέφικτο και αδιανόητο. Το Μπλίτσλει Παρκ κατόρθωσε επιπλέον να αποκρυπτογραφήσει ιταλικά και ιαπωνικά μηνύματα. Οι πληροφορίες που συλλέγονταν από τις τρεις αυτές πηγές χαρακτηρίζονταν με το κωδικό όνομα *Ούλτρα*. Τα αρχεία πληροφοριών της Ούλτρα έδιναν στους Συμμάχους σαφές πλεονέκτημα σε όλους τους σημαντικούς τομείς της σύγκρουσης. Η Ούλτρα προειδοποίησε τους Συμμάχους και για τη γερμανική εισβολή στην Ελλάδα, πράγμα που επέτρεψε στα βρετανικά στρατεύματα να αποχωρήσουν χωρίς βαριές απώλειες. Ουσιαστικά η Ούλτρα έδινε λεπτομερείς αναφορές για την κατάσταση του εχθρού σε ολόκληρη τη Μεσόγειο. Οι πληροφορίες αυτές στάθηκαν ιδιαίτερα πολύτιμες για τη συμμαχική απόβαση στην Ιταλία και τη Σικελία το 1943.

Σε όλη τα διάρκεια του Πολέμου, οι κρυπταναλυτές του Μπλίτσλει γνώριζαν ότι οι αποκρυπτογραφήσεις τους ήταν ζωτικής σημασίας, όμως δεν τους έδιναν ποτέ καμιά επιχειρησιακή πληροφορία, ούτε τους έλεγαν με ποιον τρόπο χρησιμοποιούνταν οι αποκρυπτογραφήσεις τους. Για παράδειγμα οι κρυπταναλυτές δεν διέθεταν καμία πληροφορία για τη μέρα της απόβασης. Εκείνη τη μέρα η γαλλική αντίσταση κατέστρεψε τις χερσαίες γραμμές, αναγκάζοντας τους Γερμανούς να επικοινωνούν μόνο με τον ασύρματο, γεγονός που με τη σειρά του έδωσε στο Μπλίτσλει την ευκαιρία να εφοδιάσει τους Συμμάχους με μια ακόμη λεπτομερέστερη εικόνα των γερμανικών στρατιωτικών επιχειρήσεων.

Έχει υποστηριχθεί ότι τα επιτεύγματα του Μπλίτσλει Παρκ ήταν ο αποφασιστικός παράγων στη νίκη των Συμμάχων. Το βέβαιο είναι ότι οι κρυπταναλυτές του Μπλίτσλει συντόμευσαν σημαντικά τη διάρκεια του πολέμου γεγονός που έσωσε πολλές ζωές.

Μετά τον πόλεμο, τα επιτεύγματα του Μπλίτσλει παρέμειναν επτασφράγιστο μυστικό. Η Βρετανία, έχοντας αποκρυπτογραφήσει με επιτυχία τα εχθρικά μηνύματα στη διάρκεια του πολέμου, ήθελε να συνεχίσει τις επιχειρήσεις συλλογής πληροφοριών και δεν είχε σκοπό να δημοσιοποιήσει τις δυνατότητές της. Πράγματι, οι Βρετανοί κατάσχεσαν εκατοντάδες μηχανές – Αινίγματα και τις διένειμαν στις πρώην αποικίες τους, οι οποίες πίστευαν ότι το κρυπτόγραμμα ήταν εξίσου ασφαλές όπως φαινόταν στους Γερμανούς. Οι Βρετανοί δεν έκαναν τίποτα για να τους βγάλουν από την πλάνη τους, και αποκρυπτογραφούσαν κανονικά τις μυστικές τους επικοινωνίες όλα τα επόμενα χρόνια. Στο μεταξύ η Κυβερνητική Σχολή Κωδίκων και Κρυπτογραμμάτων έκλεισε, και οι χιλιάδες άντρες και

γυναίκες που είχαν συμβάλει στη δημιουργία της Ούλτρα διασκορπίστηκαν. Οι μπόμπες αποσυναρμολογήθηκαν, και το παραμικρό κομμάτι χαρτιού που αναφερόταν στις αποκρυπτογραφήσεις της πολεμικής περιόδου κάηκε ή κλειδώθηκε. Οι κωδικοθραυστικές δραστηριότητες της Βρετανίας μεταφέρθηκαν επίσημα στο Νεοσύστατο Κυβερνητικό Αρχηγείο επικοινωνιών στο Λονδίνο, που στη συνέχεια το 1952, μετακόμισε στο Τσέλτενχαμ. Οι περισσότεροι κρυπταναλυτές επέστρεψαν στη συνηθισμένη τους ζωή ως απλοί πολίτες, αφού πρώτα έδωσαν όρκο μυστικότητας που τους απαγόρευε να αποκαλύψουν τον κομβικό ρόλο τους στη συμμαχική πολεμική προσπάθεια. Ύστερα από τρεις δεκαετίες σιωπής, τελικά η μυστικότητα που περιέβαλε το Μπλίτσλει Παρκ πήρε τέλος στις αρχές της δεκαετίας του 1970. Ο Λοχαγός Φ. Ου. Ουίντερμοθαμ, που είχε την ευθύνη της διανομής πληροφοριών της Ούλτρα, άρχισε να ενοχλεί τη Βρετανική Κυβέρνηση, προβάλλοντας το επιχείρημα ότι οι χώρες της Κοινοπολιτείας είχαν σταματήσει να χρησιμοποιούν το Αίνιγμα, και επομένως η Βρετανία δεν είχε πλέον τίποτε να κερδίσει αποκρύπτοντας το γεγονός ότι το είχε σπάσει. Οι υπηρεσίες πληροφοριών συμφώνησαν απρόθυμα, και του επέτρεψαν να γράψει ένα βιβλίο για το έργο που είχε συντελεσθεί στο Μπλίτσλει Παρκ. Το βιβλίο του Ουίντερμοθαμ με τίτλο *Το μυστικό της Ούλτρα*, που εκδόθηκε το καλοκαίρι του 1974, έδωσε το έναυσμα στο προσωπικό του Μπλίτσλει ότι ήταν πλέον ελεύθεροι να συζητούν τις δραστηριότητές τους κατά τον πόλεμο. Η σημαντικότερη ίσως συνέπεια των αποκαλύψεων του Ουίντερμοθαμ ήταν ότι ο Ρεζέφσκι συνειδητοποίησε τις καταλυτικές συνέπειες των προπολεμικών του επιτευγμάτων κατά του Αινίγματος. Μετά την εισβολή στην Πολωνία ο Ρεζέφσκι είχε διαφύγει στη Γαλλία, και όταν κατελήφθη και η Γαλλία, ζήτησε καταφύγιο στη Βρετανία. Το φυσικό θα ήταν να λάβει μέρος στη βρετανική προσπάθεια αποκρυπτογράφησης του Αινίγματος, όμως τον υποβάθμισαν να ασχολείται με ασήμαντα κρυπτογράμματα σε μια ελάσσονος σημασίας μονάδα πληροφοριών. Δεν είναι σαφές γιατί ένα τέτοιο λαμπρό μυαλό αποκλείστηκε από το Μπλίτσλει Παρκ, το αποτέλεσμα πάντως ήταν ότι αγνοούσε εντελώς τις δραστηριότητες της κυβερνητικής σχολής κωδίκων και κρυπτογραμμάτων.

Ένας άλλος κρυπταναλυτής που δεν έζησε αρκετά για να προλάβει τη δημόσια αναγνώριση ήταν ο Άλαν Τιούρινγκ ο οποίος αντί να επευφημηθεί ως ήρωας, διώχθηκε για την ομοφυλοφιλία του. Η Βρετανική Κυβέρνηση του αφαίρεσε την άδεια ασφαλείας και του απαγορεύτηκε να εργάζεται σε ερευνητικά προγράμματα σχετικά με την ανάπτυξη του υπολογιστή. Τα επόμενα 2 χρόνια υπέφερε από βαριά κατάθλιψη και στις 7 Ιουνίου 1954, σε ηλικία 42 ετών αυτοκτόνησε δαγκώνοντας ένα μήλο βουτηγμένο σε υδροκυάνιο.

Την εποχή που οι Βρετανοί κρυπταναλυτές έσπαζαν ο γερμανικό κρυπτόγραμμα του Αινίγματος και άλλαζαν την πορεία του πολέμου στη Ευρώπη, οι Αμερικάνοι συνάδελφοί τους ασκούσαν εξίσου σημαντική επίδραση στα γεγονότα του θεάτρου του Ειρηνικού σπάζοντας το Ιαπωνικό κρυπτόγραμμα γνωστό ως Πορφυρό.

Παρότι το Πορφυρό και το Αίνιγμα τελικά έσπασαν, παρείχαν ωστόσο κάποια ασφάλεια όταν αρχικά εφαρμόστηκαν και αποτέλεσαν πραγματική πρόκληση για τους Αμερικανούς και τους Βρετανούς κρυπταναλυτές. Πράγματι, αν οι κρυπτογραφικές μηχανές είχαν χρησιμοποιηθεί σωστά – χωρίς επαναλαμβανόμενα μηνύματα κλειδιά, χωρίς cillies, χωρίς περιορισμούς στις ρυθμίσεις του πίνακα βυσμάτων και στις διευθετήσεις των «αναδιατακτών», και χωρίς στερεότυπα μηνύματα που έδιναν τυφλοσούρτες – είναι πολύ πιθανό ότι θα περέμεναν άθραυστες. Την πραγματική ισχύ και τις δυνατότητες των μηχανικών κρυπτογραμμάτων τις απέδειξε η κρυπτογραφική μηχανή Typex, την οποία χρησιμοποιούσε ο βρετανικός στρατός και η αεροπορία καθώς και η αντίστοιχη αμερικανική SIGABA. Και οι δύο αυτές μηχανές ήταν πιο πολύπλοκες από το Αίνιγμα και χρησιμοποιούνταν και οι δύο σωστά, με συνέπεια να παραμείνουν άθραυστες σε όλη τη διάρκεια του πολέμου. Οι κρυπτογράφοι των Συμμάχων είχαν την πεποίθηση ότι τα περίπλοκα ηλεκτρομηχανικά κρυπτογράμματα μπορούσαν να προσφέρουν ασφαλείς επικοινωνίες. Ωστόσο, οι πολύπλοκες κρυπτογραφικές μηχανές δεν είναι ο μόνος τρόπος αποστολής ασφαλών μηνυμάτων. Μία από τις ασφαλέστερες μορφές κρυπτογράφησης που χρησιμοποιούνταν κατά το Δεύτερο Παγκόσμιο Πόλεμο ήταν ταυτόχρονα και μια από τις απλούστερες.

### *1.3. <u>Κώδικας Ναβάχο</u>*

Στη διάρκεια της εκστρατείας του Ειρηνικού, οι αμερικανοί διοικητές άρχισαν να συνειδητοποιούν ότι οι κρυπτογραφικές μηχανές όπως η SIGABA παρουσίαζαν ένα σοβαρό

μειονέκτημα. Παρότι η ηλεκτρομηχανική κρυπτογράφηση παρείχε σχετικά υψηλά επίπεδα ασφαλείας, ήταν επώδυνα αργή. Τα μηνύματα έπρεπε να πληκτρολογούνται στη μηχανή γράμμα προς γράμμα και μετά να διαβιβάζεται από το ραδιοχειριστή. Στη συνέχεια, ο ραδιοχειριστής που λάμβανε το κρυπτογραφημένο μήνυμα έπρεπε να το παραδώσει σε έναν ειδικό κρυπταναλυτή, ο οποίος θα επέλεγε προσεκτικά το σωστό κλειδί και θα πληκτρολογούσε το κρυπτογραφικό κείμενο σε μια κρυπτογραφική μηχανή, για να το αποκρυπτογραφήσει γράμμα προς γράμμα. Ο απαραίτητος χρόνος καθώς και ο κατάλληλος χώρος για τέτοιες λεπτές διαδικασίες, είναι προυποθέσεις που καλύπτονται μέσα σε ένα στρατηγείο ή σε ένα πλοίο, αλλά η μηχανική κρυπτογράφηση δεν ήταν ιδεώδης για πιο εχθρικά περιβάλλοντα, όπως τα νησιά του Ειρηνικού.

Δυστυχώς για τους Αμερικανούς, πολλοί Ιάπωνες στρατιώτες γνώριζαν άπταιστα αγγλικά. Πολύτιμες πληροφορίες για την αμερικανική στρατηγική και τακτική περιέχονταν στα χέρια του εχθρού. Ένας από τους πρώτους που αντέδρασαν σε αυτό το πρόβλημα ήταν ο Φίλιπ Τζόνστον, ένας μηχανικός με έδρα το Λος Άντζελες, που ήτα πολύ ηλικιωμένος για να πολεμήσει, αλλά που ωστόσο επιθυμούσε να συμβάλει στη πολεμική προσπάθεια. Ο Τζόνστον είχε ανατραφεί στις ειδικές περιοχές των Ναβάχο στην Αριζόνα, με αποτέλεσμα να διαποτιστεί ολοκληρωτικά από τον πολιτισμό τους. Ήταν ένας από τους ελάχιστους ανθρώπους εκτός της φυλής τους που μιλούσε άπταιστα τη γλώσσα τους, πράγμα που του επέτρεπε να παίζει το ρόλο του διερμηνέα στις συζητήσεις μεταξύ των Ναβάχο και των κυβερνητικών πρακτόρων. Η εργασία του με αυτή του την ιδιότητα κορυφώθηκε με μία επίσκεψη στο Λευκό Οίκο, όταν ο εννιάχρονος τότε Τζόνστον μετέφραζε για λογαριασμό δύο Ναβάχο που έκαναν έκκληση στον πρόεδρο για δικαιότερη μεταχείριση της κοινότητάς τους. Έχοντας πλήρη συνείδηση του πόσο αδιαπέραστη ήταν η γλώσσα των Ναβάχο για τους εκτός φυλής, ο Τζόνστον συνέλαβε την ιδέα ότι η συγκεκριμένη γλώσσα, ή οποιαδήποτε άλλη γλώσσα των Γηγενών Αμερικανών, μπορούσε να χρησιμοποιηθεί ως εν δυνάμει άθραυστος κώδικας. Αν κάθε λόχος στον Ειρηνικό χρησιμοποιούσε δύο Γηγενείς Αμερικανούς ως ραδιοχειριστές, οι ασφαλείς επικοινωνίες ήταν εγγυημένες. Ο Τζόνστον υπέβαλε την ιδέα του στον αντισυνταγματάρχη Τζέιμς Τζόουνς και δεν χρειάστηκε παρά να πετάξει λίγες φράσεις των Ναβάχο για να πείσει τον αξιωματικό διαβιβάσεων της περιοχής, ότι ι ιδέα του άξιζε να ληφθεί υπόψη. Δεκαπέντε μέρες αργότερα ο Τζόνστον επέστρεψε με δύο Ναβάχο έτοιμους να προβούν σε τεστ επίδειξης ενώπιον ανώτατων αξιωματικών του Ναυτικού. Οι Ναβάχο ήταν απομονωμένοι ο ένας από τον άλλο. Στον έναν έδωσαν έξι τυπικά μηνύματα στα αγγλικά, τα οποία μετέφρασε στη γλώσσα του και τα έδωσε στον ομόφυλό του μέσω ασυρμάτου. Ο άλλος Ναβάχο, ο αποδέκτης, ξαναμετέφρασε τα μηνύματα στα αγγλικά, τα κατέγραψε και τα παρέδωσε στους αστυνομικούς, που τα συνέκριναν με τα πρωτότυπα. Το σύστημα αποδείχτηκε άψογο και οι αξιωματικοί του Ναυτικού έδωσαν την άδεια να εφαρμοστεί ένα πιλοτικό σχέδιο και διέταξαν να αρχίσει αμέσως η στρατολόγηση.

Ωστόσο, πριν στρατολογήσουν οποιονδήποτε, ο αντισυνταγματάρχης Τζόουνς και ο Φίλιπ Τζόνστον έπρεπε να αποφασίσουν αν θα διενεργούσαν την πιλοτική μελέτη με τους Ναβάχο ή αν θα επέλεγαν άλλη φυλή. Το σημαντικότερο κριτήριο επιλογής ήταν απλώς θέμα αριθμών: οι πεζοναύτες έπρεπε να βρουν μια φυλή ικανή να παρέχει μεγάλο αριθμό αντρών που να γνωρίζουν καλά τα αγγλικά και να είναι εγγράμματοι. Η απουσία κυβερνητικών επενδύσεων είχε ως αποτέλεσμα το πολύ υψηλό ποσοστό αναλφαβητισμού στις περισσότερες ειδικές περιοχές, και συνεπώς η προσοχή εστιάστηκε στις τέσσερις μεγαλύτερες φυλές: τους Ναβάχο, τους Σιού, τους Τσιπέουα και τους Πίμα – Παπάγκο. Οι Ναβάχο ήταν η μεγαλύτερη φυλή αλλά και η πιο αναλφάβητη ενώ η Πίμα – Παπάγκο ήταν η πιο εγγράμματη αλλά πολύ πιο ολιγάριθμη. Δεν υπήρχαν και μεγάλα περιθώρια επιλογής ανάμεσα στις τέσσερις φυλές και έτσι η τελική απόφαση εξαρτήθηκε από την αναφορά του Τζόνστον, η οποία επεσήμαινε ότι οι Ναβάχο ήταν η μόνη φυλή η οποία δεν είχε κατακλυστεί ακόμα από γερμανούς σπουδαστές καθώς και ο γεγονός ότι οι Γερμανοί που μελετούσαν τις διάφορες διαλέκτους των φυλών, είχαν αποκτήσει αρκετές γνώσεις όλων των διαλέκτων των φυλών εκτός από αυτή των Ναβάχο. Σημαντική επίσης ήταν η αναφορά του στο γεγονός ότι η διάλεκτος των Ναβάχο ήταν εντελώς ακατανόητη σε όλες τις υπόλοιπες φυλές, εκτός ίσως από 28 Αμερικάνους που την έχουν μελετήσει και έτσι η διάλεκτος αυτή αποτελεί μυστικό κώδικα ως προς τον εχθρό και προσφέρεται θαυμάσια για γρήγορη και ασφαλή επικοινωνία.

Την εποχή που οι ΗΠΑ εισήλθαν στο Δεύτερο Παγκόσμιο Πόλεμο, οι Ναβάχο ζούσαν υπό άθλιες συνθήκες και τους μεταχειρίζονταν ως υπανθρώπους. Ωστόσο το συμβούλιο της φυλής τους υποστήριξε την πολεμική προσπάθεια. Δεν υπήρχε καμία δυσκολία να βρεθούν κατάλληλοι υποψήφιοι

για να υπηρετήσουν ως ομιλητές κωδίκων Ναβάχο, όπως έγιναν γνωστοί. Μέσα σε 4 μήνες από το βμβαρδισμό του Περλ Χάρμπορ, 29 Ναβάχο, μερικοί από τους οποίους ήταν μόλις δεκαπέντε ετών, άρχισαν μαθήματα επικοινωνιών, διαρκείας οκτώ εβδομάδων, με το Σώμα των πεζοναυτών. Πριν αρχίσει η εκπαίδευση, το Σώμα των Πεζοναυτών έπρεπε να λύσει το πρόβλημα το οποίο δημιουργούσε το γεγονός ότι η γλώσσα των Ναβάχο δεν διέθετε λέξεις αντίστοιχες της στρατιωτικής ορολογίας. Το Σώμα των Πεζοναυτών φρόντισε να καταρτίσει ένα λεξικό όρων των Ναβάχο που θα αντικαθιστούσαν τις αγγλικές λέξεις, οι οποίες διαφορετικά θα ήταν αμετάφραστες, έτσι ώστε να αρθεί οποιαδήποτε αμφισημία. Οι εκπαιδευόμενοι βοήθησαν στη κατάρτιση του λεξικού, επιλέγοντας λέξεις που περιέγραφαν το φυσικό νόμο για να υποδεικνύουν ειδικούς στρατιωτικούς όρους. Έτσι για αεροπλάνα χρησιμοποιούσαν ονόματα πουλιών και για τα πλοία ονόματα ψαριών. Παρότι το πλήρες λεξικό περιλάμβανε 274 λέξεις, παρέμενε το πρόβλημα της μετάφρασης λιγότερο προβλέψιμων λέξεων, καθώς και των ονομάτων χωρών και λαών. Η λύση ήταν να επινοήσουν ένα κωδικοποιημένο φωνητικό αλφάβητο για να γράφουν τις δύσκολες λέξεις. Για παράδειγμα, η λέξη Pacific(Ειρηνικός) θα γραφόταν pig, ant, cat, ice,fox, ice, cat (χοίρος, μυρμήγκι, γάτα, πάγος, αλεπού, πάγος, γάτα), που στη συνέχεια θα μεταφραζόταν στη γλώσσα των Ναβάχο ως bi – sodih, wol – la – chee, moasi, tkin, ma – e, tkin, moasi.

Το πλήρες αλφάβητο των Ναβάχο δίνεται στον παρακάτω πίνακα.

*Το κωδικό αλφάβητο Ναβάχο*

- **A** Ant (μυρμήγκι) **Wol – la – chee**
- **B** Bear (αρκούδα) **Shush**
- **C** Cat (γάτα) **Moasi**
- **D** Deer (ελάφι) **Be**
- **E** Elk (τάρανδος) **Dzeh**
- **F** Fox (αλεπού) **Ma-e**
- **G** Goat (κατσίκα) **Klizzie**
- **H** Horse (άλογο) **Lin**
- **I** Ice (πάγος) **Tkin**
- **J** Jackass (γαιδούρι) **Tkele-cho-gi**
- **K** Kid (παιδί) **Klizzie-yazzi**
- **L** Lamp (αρνί) **Dibeh-yazzi**
- **M** Mouse (ποντίκι) **Na-as-tso-si**
- **N** Nut (καρύδι) **Nesh-chee**
- **O** Owl (κουκουβάγια) **Ne-ahs-jsh**
- **P** Pig (γουρούνι) **Bi-sodih**
- **Q** Quiver (φαρέτρα) **Ca-yeilth**
- **R** Rabbit (λαγός) **Gah**
- **S** Sheep (πρόβατο) **Dibeh**
- **T** Turkey (γαλοπούλα) **Than-zie**
- **U** Ute (φορτηγό) **No-da-ih**
- **V** Victor (νικητής) **A-keh-di-glini**
- **W** Weasel (νυφίτσα) **Gloe-ih**
- **X** Cross (σταυρός) **Al-an-as-dzoh**
- **Y** Yucca (γιούκα) **Tsah-as-zih**
- **Z** Zinc (ψευδάργυρος) **Besh-do-gliz**

Μέσα σε οκτώ εβδομάδες, οι εκπαιδευόμενοι ομιλητές κωδίκων είχαν μάθει απέξω όλο το λεξικό και το αλφάβητο, καθιστώντας περττή την ύπαρξη κωδικών βιβλίων που θα μπορούσαν να

πέσουν σε εχθρικά χέρια. Για τους Ναβάχο, το να μάθουν τα πάντα από μνήμης ήταν εύκολο, επειδή παραδοσιακά η γλώσσα τους δεν διέθετε γραπτό λόγο και έτσι ήταν συνηθισμένοι να απομνημονεύουν τις λαικές και οικογενειακές τους ιστορίες. Μετά την ολοκλήρωση της εκπαίδευσής τους, οι Ναβάχο πέρασαν από τεστ. Οι αποστολείς μετέφραζαν μια σειρά μηνυμάτων από τα αγγλικά στη γλώσσα των Ναβάχο, τα διαβίβαζαν και στη συνέχεια οι παραλήπτες τα μετέφραζαν πάλι στα αγγλικά χρησιμοποιώντας, όπου αυτό ηταν απαραίτητο, το λεξικό και το αλφάβητο τα οποία είχαν απομνημονεύσει. Τα αποτελέσματα ήταν άριστα. Για να ελέγξουν την ισχύ του συστήματος, έδωσαν μια μαγνητοταινία όπου είχαν καταγράψει τις μεταδόσεις στη Ναυτική Υπηρεσία Πληροφοριών, που είχε σπάσει το δυσκολότερο ιαπωνικό κρυπτόγραμμα, το Πορφυρό. Ύστερα από τρεις εβδομάδες εντατικής προσπάθειας οι κρυπταναλυτές του Ναυτικού εξακολουθούσαν να μην βγάζουν καμιά άκρη από τα μηνύματα. Ο κώδικας Ναβάχο θεωρήθηκε επιτυχής. Δύο στρατιώτες Ναβάχο, οι Τζον Μπέναλι και Τζόνι Μανουελίτο, παρέμειναν για να εκπαιδεύσουν την απόμενη σειρά, ενώ οι υπόλοιποι 27 ομιλητές κωδίκων Ναβάχο τοποθετήθηκαν σε τέσσερα συντάγματα και στάλθηκαν στον Ειρηνικό.

Παρότι οι Ναβάχο ήταν πεπεισμένοι ότι οι ικανότητές τους θα ήταν ευλογία για τους πεζοναύτες, οι πρώτες απόπειρες μόνο σύγχυση προκάλεσαν. Πολλοί από τους κανονικούς χειριστές σημάτων αγνοούσαν το νέο κώδικα και άρχισαν να στέλνουν μηνύματα πανικού σε όλο το νησί δηλώνοντας ότι οι Ιάπωνες εξέπεμπαν σε αμερικάνικες συχνότητες. Ο υπεύθυνος συνταγματάρχης σταμάτησε αμέσως τις επικοινωνίες με τον κώδικα Ναβάχο μέχρι πουν α πειστεί ότι το νέο σύστημα άξιζε να συνεχιστεί.

Όταν ο κώδικας ξαναμπήκε σε εφαρμογή μετά από ακόμα ένα τεστ, οι ομιλητές κωδίκων σύντομα απέδειξαν την αξία τους στο πεδίο της μάχης. Η φήμη των ομιλητών κωδίκων σύντομα διαδόθηκε και στο τέλος του 1942 ζητήθηκαν 83 ακόμη άντρες. Οι Ναβάχο υπηρετούσαν πλέον και στις 6 μεραρχίες του Σώματος των Πεζοναυτών, και ενίοτε τους δανείζονταν και άλλες αμερικανικές δυνάμεις. Ο πόλεμος των λέξεων δεν άργησε να μετατρέψει τους Ναβάχο σε ήρωες. Σε τρεις τουλάχιστον περιπτώσεις οι ομιλητές κωδίκων εκλήφθησαν ως ιάπωνες στρατιώτες και αιχμαλωτίστηκαν από Αμερικανούς, οι οποίοι τους απελευθέρωσαν μόνο όταν εγγυήθηκαν γι αυτούς οι συμπολεμιστές τους από το ίδιο τάγμα. Η μη διαπερατότητα του κώδικα Ναβάχο οφειλόταν εξ ολοκλήρου στο γεγονός ότι η γλώσσα των Ναβάχο ανήκει στη γλωσσική οικογένεια Να-Ντένε, που δεν έχει καμία σχέση με οποιαδήποτε ευρωπαική ή ασιατική γλώσσα. Για παράδειγμα, το ρήμα κλείνεται όχι μόνο σύμφωνα με το υποκείμενο αλλά και σύμφωνα με το αντικείμενό του και η κατάληξη του ρήματος εξαρτάται από την κατηγορία στην οποία ανήκει το αντικείμενο.

Παρά τα ισχυρά σημεία του, ο κώδικας Ναβάχο εξακολουθούσε να πάσχει από δύο σημαντικά μειονεκτήματα. Πρώτον, οι λέξεις που δεν περιλαμβάνονταν ούτε στο φυσικό λεξιλόγιο των Ναβάχο ούτε στον κατάλογο των 274 επίσημων κωδικών λέξεων, έπρεπε να γράφονται με το ειδικό αλφάβητο. Επειδή αυτό ήταν χρονοβόρο, αποφάσισαν να προσθέσουν άλλους 234 κοινούς όρους στο λεξικό. Το δεύτερο πρόβλημα αφορούσε τις λέξεις που παρά τις παραπάνω προσθήκες έπρεπε και πάλι να γράφονται γράμμα προς γράμμα. Αν οι Ιάπωνες αντιλαμβάνονταν ότι συνέβαινε κάτι τέτοιο, θα χρησιμοποιούσαν την ανάλυση συχνοτήτων για να εντοπίσουν ποιες λέξεις των Ναβάχο αντιπροσώπευαν συγκεκριμένα γράμματα. Σύντομα θα έβλεπαν ότι η πιο συνηθισμένη λέξη ήταν **dzeh** που σημαίνει τάρανδος (στα αγγλικά **elk** ) και εκπροσωπεί το γράμμα **e** το πιο κοινό γράμμα του αγγλικού αλφαβήτου. Αν το όνομα του νησιού Γκουανταλκανάλ γραφόταν με αυτόν τον τρόπο, θα περιλάμβανε τέσσερις φορές τη λέξη la-chee που σημαίνει μυρμήγκι (στα αγγλικά ant), αποτελώντας σαφή ένδειξη για το ποια λέξη εκπροσωπούσε το γράμμα a. Η λύση ήταν να προσθέσουν περισσότερες λέξεις που να λειτουργούν ως επιπλέον υποκατάστατα(ομόφωνα) για τα πιο συνηθισμένα γράμματα. Εισήγαγαν λοιπόν δύο επιπλέον λέξεις ως εναλλακτικές λύσεις για τα έξι πιο κοινά γράμματα της αγγλικής (e, t, a, o, i, n) και μια επιπλέον λέξη για τα έξι επόμενα κοινά γράμματα (s, h, r, d, l, u).

Καθώς ο πόλεμος του Ειρηνικού εντεινόταν και οι Αμερικάνοι προωθούνταν στα νησιά του Σολομώντος προς την Οκινάβα, ο ρόλος των ομιλητών κωδίκων Ναβάχο γινόταν όλο και πιο σημαντικός. Η συνεισφορά των Ναβάχο είναι ιδιαίτερα αξιοσημείωτη αν λάβουμε υπόψην ότι, για να εκπληρώσουν τα καθήκοντά τους έπρεπε να ξεπερνούν τους βαθιά ριζωμένους πνευματικούς φόβους τους. Οι Ναβάχο πιστεύουν ότι τα *τσίντι*, τα πνεύματα δηλαδή των νεκρών, ζητούν εκδίκηση από τους ζωντανούς αν το νεκρό σώμα δεν ταφεί με το θρησκευτικό τους τελετουργικό. Ο πόλεμος στον Ειρηνικό ήταν ιδιαίτερα αιματηρός και τα πεδία της μάχης διάσπαρτα με πτώματα. Ωστόσο, οι ομιλητές

κωδίκων επιστράτευσαν όλο τους το θάρρος και συνέχιζαν το έργο τους αψηφώντας τα *τσίντι* που τους στοίχειωναν.

Συνολικά υπήρχαν 240 ομιλητές κωδίκων Ναβάχο. Η γενναιότητά τους ως πολεμιστών αναγνωρίστηκε, όμως ο ειδικός ρόλος τους στη διασφάλιση των επικοινωνιών χαρακτηρίστηκε απόρρητη πληροφορία. Η κυβέρνηση τους απαγόρευσε να μιλούν για το έργο τους και η απαράμιλλη συνεισφορά τους δεν δημοσιοποιήθηκε. Όπως και στη περίπτωση του Μπλίτσλει Παρκ,οι Ναβάχο αγνοήθηκαν επί δεκαετίες. Ωστόσο ο μεγαλύτερος φόρος τιμής στο έργο των Ναβάχο, είναι το γεγονός ότι ο κώδικάς τους είναι από τους ελάχιστους στην ιστορία που δεν έσπασαν ποτέ.

Στη διάρκεια του Δεύτερου Παγκοσμίου Πολέμου, οι βρετανοί κωδικοθραύστες είχαν το πάνω χέρι στη μάχη με τους γερμανούς κωδικοπλάστες, κυρίως επειδή οι γυναίκες και οι άντρες του Μπλίτσλει, ακολουθώντας τα βήματα των Πολωνών, ανέπτυξαν την πρώτη κωδικοθραυστική τεχνολογία. Εκτός από τις μπόμπες του Τιούρινγκ, που χρησιμοποιούνταν για το σπάσιμο του κρυπτογράμματος του Αινίγματος, οι Βρετανοί επινόησαν και μια άλλη κωδικοθραυστική συσκευή, τον Κολοσσό, προκειμένου να αντιμετωπίσουν μια ακόμη ισχυρότερη μορφή κρυπτογράφησης, το γερμανικό κρυπτόγραμμα Λόρεντς. Από τις δυο κρυπτογραφικές μηχανές ο Κολοσσός ήταν αυτός που έμελλε να καθορίσει την ανάπτυξη της κρυπτογραφίας κατά το δεύτερο μισό του εικοστού αιώνα. Το κρυπτόγραμμα Λόρεντς χρησιμοποιείτο για την κρυτπογράφηση των επικοινωνιών του Χίτλερ με τους στρατηγούς του. Την κρυπτογράφηση πραγματοποιούσε η μηχανή Λόρεντς SZ40, που λειτουργούσε παρόμοια με το Αίνιγμα αλλά ήταν πολύ πιο πολύπλοκη, και έτσι αποτελούσε πολύ μεγαλύτερη πρόκληση για τους κρυπταναλυτές του Μπλίτσλει. Τελικά όμως, δύο από αυτούς, οι Τζον Τίλτμαν και Μπιλ Τιουτ, ανακάλυψαν μια αδυναμία στον τρόπο που λειτουργούσε το κρυπτόγραμμα Λόρεντς, ένα ελάττωμα που το Μπλίτσλει θα μπορούσε να το εκμεταλλευτεί και συνεπώς να διαβάζει τα μηνύματα του Χίτλερ. Το σπάσιμο του κρυπτογράμματος Λόρεντς απαιτούσε ένα κράμα έρευνας, συνδυαστικής ικανότητας, στατιστικής ανάλυσης και ορθής κρίσης, πράγματα δηλαδή που βρίσκονταν πέρα από τις τεχνικές δυνατότητες που διέθεταν οι μπόμπες. Οι μπόμπες μπορούσαν να εκτελούν μια συγκεκριμένη λειτουργία με μεγάλη ταχύτητα όμως δεν ήταν αρκετά ευέλικτες ώστε να αντιμετωπίσουν την πολυπλοκότητα του Λόρεντς. Οι κρυπταναλυτές του Μπλίτσλει  ήταν αναγκασμένοι να σπάζουν με το χέρι τα μηνύματα που ήταν κρυπτογραφημένα με το κρυπτόγραμμα Λόρεντς, πράγμα που απαιτούσε επώδυνη προσπάθεια εβδομάδων, οπότε και τα μηνύματα έπαυαν πια να είναι επίκαιρα. Τελικά ο Μαξ Νιούμαν, ένας μαθηματικός του Μπλίτσλει, βρήκε ένα τρόπο για να μηχανοποιήσει την κρυπτανάλυση του κρυπτογράμματος Λόρεντς. Με βάση κυρίως τις ιδέες του Τιούρινγκ για την καθολική μηχανή, ο Νιούμαν σχεδίασε μια μηχανή ικανή να προσαρμόζεται από μόνη της στα διάφορα προβλήματα, αυτό που σήμερα θα αποκαλούσαμε προγραμματιζόμενο υπολογιστή. Η εφαρμογή του σχεδίου του Νιούμαν θεωρήθηκε ανέφικτη από τεχνική άποψη, και έτσι οι ανώτεροι αξιωματούχοι του Μπλίτσλει έβαλαν το σχέδιο στο αρχείο. Ευτυχώς ο Τόμι Φλάουερς, ένας μηχανικός που είχε λάβει μέρος στις συζητήσεις για το σχέδιο του Νιούμαν, αποφάσισε να αγνοήσει το σκεπτικισμό του Μπλίτσλει και προχώρησε στην κατασκευή της μηχανής. Στο ερευνητικό κέντρο του Ταχυδρομείου, στο Ντόλις Χιλ του βόρειου Λονδίνου, ο Φλάουερς πήρε ως βάση τα σχεδιαγράμματα του Νιούμαν και σε 10 μήνες κατασκεύασε τον Κολοσσό, τον οποίο παρέδωσε στο Μπλίτσλει στις 8 Δεκεμβρίου του 1943. Η μηχανή αποτελείτο από 1.500 ηλεκτρονικές λυχνίες, κατά πολύ ταχύτερες από τους αργοκίνητους ηλεκτρομηχανικούς διακόπτες που χρησιμοποιούσαν οι μπόμπες. Όμως το πιο σημαντικό και από την ταχύτητα του Κολοσσού ήταν το γεγονός ότι ήταν προγραμματιζόμενος, πράγμα που τον καθιστούσε πρόδρομο του σύγχρονου ψηφιακού υπολογιστή. Ο Κολοσσός καταστράφηκε μετά τον Πόλεμο, μαζί με όλα τα άλλα επιτεύγματα του Μπλίτσλει Παρκ και όσοι δούλευαν με αυτόν δεν επιτρεπόταν να μιλήσουν για το θέμα. Ο Τόμμυ Φλάουερς υπακούοντας στην εντολή να καταστρέψει τα σχεδιαγράμματα του Κολοσσού τα πήγε στο λεβητοστάσιο και τα έκαψε. Τα σχεδιαγράμματα για τον πρώτο υπολογιστή στον κόσμο χάθηκαν για πάντα. Η μυστικότητα αυτή είχε ως αποτέλεσμα να κερδίσουν άλλοι επιστήμονες τη δόξα της επινόησης του υπολογιστή. Επί δεκαετίες μητέρα όλων των υπολογιστών θεωρείτο ο ΕΝΙΑC, όχι ο Κολοσσός.

## ΚΕΦΑΛΑΙΟ 2

### *2.1. Ηλεκτρονικοί υπολογιστές και κλειδιά*

Αφού συνέβαλαν στη γέννηση του σύγχρονου υπολογιστή, οι κρυπταναλυτές συνέχισαν και μετά τον πόλεμο να αναπτύσσουν και να χρησιμοποιούν την τεχνολογία των υπολογιστών για να σπάζουν κάθε λογής κρυπτογράμματα. Τώρα μπορούσαν να εκμεταλλεύονται την ταχύτητα και την ευελιξία των προγραμματιζόμενων υπολογιστών για να ελέγχουν όλα τα πιθανά κλειδιά μέχρι να βρουν το σωστό. Οι κρυπτογράφοι δεν άργησαν να αντεπιτεθούν εκμεταλλευόμενοι την ισχύ των υπολογιστών για να δημιουργούν όλο και πιο περίπλοκα κρυπτογράμματα. Με δυο λόγια ο υπολογιστής έπαιξε καίριο ρόλο στη μεταπολεμική μάχη των κωδικοθραυστών με τους κωδικοπλάστες.

Υπάρχουν 3 μόνο σημαντικές διαφορές ανάμεσα στην κρυπτογράφηση μέσω υπολογιστή και τη μηχανική κρυπτογράφηση που αποτελούσε τη βάση των κρυπτογραμμάτων τύπου Αινίγματος. Η πρώτη διαφορά είναι ότι μια μηχανολογική κρυπτογραφική μηχανή υπόκειται στους περιορισμούς του πρακτικά κατασκευάσιμου, ενώ ένας υπολογιστής μπορεί να μιμηθεί μια απεριόριστα πολύπλοκη υποθετική κρυπτογραφική μηχανή. Για παράδειγμα ένας υπολογιστής μπορεί να προγραμματιστεί για να μιμηθεί τη δράση εκατό αναδιατακτών, που άλλοι θα περιστρέφονται κατά τη φορά των δεικτών του ρολογιού, άλλοι θα κινούνται προς τα πίσω, άλλοι θα εξαφανίζονται ύστερα από κάθε δέκατο γράμμα και άλλοι θα γυρνούν ολοένα και πιο γρήγορα όσο προχωράει η κρυπτογράφηση. Μια τέτοια μηχανική συσκευή είναι στην πράξη ανέφικτο να κατασκευαστεί, όμως το εικονικό αντίστοιχό της με μορφή υπολογιστή θα παρήγαγε ένα κρυπτόγραμμα υψηλής ασφάλειας.

Η δεύτερη διαφορά είναι απλώς θέμα ταχύτητας. Η ηλεκτρονική λειτουργεί πολύ πιο γρήγορα από ότι οι μηχανικοί αναδιατάκτες: ένας υπολογιστής προγραμματισμένος να μιμείται το κρυπτόγραμμα του Αινίγματος θα μπορούσε να αποκρυπτογραφήσει αυτοστιγμεί ένα εκτενές μήνυμα. Από την άλλη, ένας υπολογιστής προγραμματισμένος να εκτελεί μια απείρως πολυπλοκότερη μορφή κρυπτογράφησης, θα μπορούσε και πάλι να το κάνει μέσα σε λογικά χρονικά πλαίσια.

Η Τρίτη και ίσως η σημαντικότερη διαφορά, είναι ότι ένας υπολογιστής δεν αναδιατάσσει γράμματα του αλφαβήτου, αλλά αριθμούς ακολουθίες από μονάδες και μηδενικά γνωστά ως δυαδικά ψηφία, ή συντομογραφικά μπίτ. Συνεπώς οποιοδήποτε μήνυμα θα πρέπει πριν αποκρυπτογραφηθεί να μετατραπεί σε δυαδικά ψηφία. Η μετατροπή αυτή μπορεί να γίνει σύμφωνα με διάφορα πρωτόκολλα, όπως ο American Standard Code for Information Interchange (Αμερικανικός Καθιερωμένος Κώδικας για την Ανταλλαγή Πληροφοριών ), ευρύτερα γνωστός με το ακρωνύμιο ASCII.Ο ASCII αποδίδει σε κάθε γράμμα του αλφαβήτου έναν επταψήφιο δυαδικό αριθμό. Προς το παρόν αρκεί να σκεφτούμε ένα δυαδικό αριθμό απλώς σαν ένα σχήμα από μονάδες και μηδενικά που αποτελεί τη μοναδική ταυτότητα του κάθε γράμματος, όπως ακριβώς ο κώδικας Μορς αποδίδει σε κάθε γράμμα μια ταυτότητα αποτελούμενη από μια μοναδική σειρά από στιγμές και παύλες. Υπάρχουν 128 τρόποι διάταξης ενός συνδυασμού από 7 δυαδικά ψηφία και επομένως ο ASCII μπορεί να προσδιορίσει μέχρι και 128 χαρακτήρες. Αυτό παρέχει πλήρη ευχέρεια προσδιορισμού όλων των πεζών γραμμάτων (π.χ a=1100001), όλων των σημείων στίξης (π.χ !=0100001), καθώς και όλων των άλλων συμβόλων (π.χ &=0100110). Μόλις το μήνυμα μετατραπεί σε δυαδικό κώδικα, μπορεί να αρχίσει η κρυπτογράφηση.

Παρότι εδώ έχουμε να κάνουμε με υπολογιστές και αριθμούς και όχι με μηχανές και γράμματα, η κρυπτογράφηση εξακολουθεί να πραγματοποιείται με βάση τις παραδοσιακές αρχές της υποκατάστασης και της μετάθεσης, όπου κάποια στοιχεία του μηνύματος υποκαθιστούν κάποια άλλα, ή αλλάζουν αμοιβαία θέση και τα δύο. Κάθε κρυπτογράφηση, όσο πολύπλοκη κι αν είναι, μπορεί να αναλυθεί σε συνδυασμούς των δύο αυτών απλών διαδικασιών. Τα παρακάτω παραδείγματα καταδεικνύουν την ουσιώδη απλότητα της κρυπτογράφησης με υπολογιστή, δείχνοντας πώς ένας υπολογιστής μπορεί να εφαρμόσει ένα απλό κρυπτόγραμμα υποκατάστασης και ένα απλό κρυπτόγραμμα μετάθεσης.

Έστω ότι θέλουμε να κρυπτογραφήσουμε το μήνυμα **HELLO**, χρησιμοποιώντας μια απλή υπολογιστική εκδοχή ενός κρυπτογράμματος μετάθεσης. Πριν αρχίσει η κρυπτογράφηση θα πρέπει να μεταφράσουμε το μήνυμα σε ASCII, σύμφωνα με το δοσμένο πίνακα.

*Κανονικό κείμενο* = HELLO = 1001000 1000101 1001100 1001100 1001111

Μία από τις απλούστερες μορφές κρυπτογράμματος μετάθεσης θα ήταν να αντιμεταθέσουμε το πρώτο με το δεύτερο ψηφίο, το τρίτο με το τέταρτο κ.ο.κ. Στην περίπτωση αυτή, το τελικό ψηφίο θα παρέμενε αμετάβλητο, επειδή ο αριθμός των ψηφίων είναι περιττός. Για να φανεί καθαρότερα η διαδικασία αφαιρούμε τα διαστήματα ανάμεσα στα τμήματα ASCII του αρχικού κανονικού κειμένου ώστε να δημιουργηθεί μια συνεχής σειρά, και ακριβώς από κάτω παραθέτουμε το προκύπτον κρυπτογραφικό κείμενο, ώστε να γίνει η σύγκριση

*Κανονικό κείμενο* = 1001000100010110011001001100 1001111
*Κρυπτογραφικό κείμενο*= 0110001000101001100110001100 0110111

Μια ενδιαφέρουσα πτυχή της μετάθεσης στο επίπεδο των δυαδικών ψηφίων είναι ότι αυτή μπορεί να γίνει στο εσωτερικό του γράμματος. Επιπλέον τμήματα ενός γράμματος μπορούν να αλλάξουν αμοιβαία θέση με τμήματα του γειτονικού του. Για παράδειγμα κατά την αντιμετάθεση του έβδομου αριθμού με τον όγδοο, το τελικό Ο του Η παίρνει τη θέση του αρχικού 1 του Ε και ανάποδα. Το κρυπτογραφημένο μήνυμα είναι μια συνεχής σειρά από 35 δυαδικά ψηφία, η οποία μπορεί να διαβιβαστεί στον αποδέκτη, ο οποίος στη συνέχεια αντιστρέφει τη διαδικασία της αντιμετάθεσης ώστε να ανασυνθέσει την αρχική σειρά των δυαδικών ψηφίων. Τέλος ο αποδέκτης ερμηνεύει εκ νέου τα δυαδικά ψηφία, μέσω του ASCII και αναπαράγει το αρχικό μήνυμα HELLO.

Στη συνέχεια, έστω ότι θέλουμε να κρυπτογραφήσουμε το ίδιο μήνυμα, τη φορά αυτή χρησιμοποιώντας μια απλή υπολογιστική μορφή ενός κρυπτογράμματος υποκατάστασης. Και πάλι αρχίζουμε μετατρέποντας το μήνυμα σε ASCII πριν από την κρυτπογράφηση. Όπως συνήθως, η υποκατάσταση βασίζεται σε ένα κλειδί στο οποίο έχουν εκ των προτέρων συμφωνήσει ο αποστολέας και ο αποδέκτης. Στο συγκεκριμένο παράδειγμα, το κλειδί είναι η λέξη DAVID μεταφρασμένη σε ASCII, και χρησιμοποιείται ως εξής. Κάθε στοιχείο του κανονικού κειμένου προστίθεται στο αντίστοιχο στοιχείο του κλειδιού. Η πρόσθεση δύο στοιχείων μπορεί να νοηθεί με βάση δυο απλούς κανόνες. Αν τα στοιχεία του κανονικού μηνύματος και του κλειδιού είναι ταυτόσημα, τότε στη θέση του στοιχείου του κανονικού μηνύματος μπαίνει, στο κρυπτογραφημένο κείμενο, το 0. Αν αντίθετα, τα στοιχεία του κανονικού μηνύματος και του κλειδιού είναι διαφορετικά, τότε στο κρυπτογραφημένο κείμενο μπαίνει το 1.

*Μήνυμα* HELLO
*Μήνυμα σε ASCII* 1001000100010110011001001100 1001111
*Κλειδί=DAVID* 1000100100000110101101001001 1000100
*Κρυπτογραφικό κείμενο*= 0001100000010000110100000101 0001011

Το προκύπτον κρυπτογραφημένο μήνυμα είναι μια συνεχής σειρά από 35 δυαδικά ψηφία, η οποία μπορεί να διαβιβαστεί στον αποδέκτη. Εκείνος χρησιμοποιεί το ίδιο κλειδί για να αναστρέψει την υποκατάσταση, αναδημιουργώντας έτσι την αρχική σειρά δυαδικών ψηφίων. Τέλος, ο αποδέκτης ερμηνεύει εκ νέου τα δυαδικά ψηφία μέσω ASCII και αναπαράγει το αρχικό μήνυμα HELLO. Η κρυπτογράφηση μέσω υπολογιστή περιοριζόταν σε όσους διέθεταν υπολογιστές, δηλαδή, τα πρώτα χρόνια, στην κυβέρνηση και τους στρατιωτικούς. Ωστόσο μια σειρά επιστημονικά, τεχνολογικά και κατασκευαστικά επιτεύγματα έκαναν τους υπολογιστές προσιτούς σε ένα πολύ ευρύτερο κοινό.

Το 1947, η εταιρία AT& Bell Laboratories εφηύρε τον κρυσταλλικό πολλαπλασιαστή (τρανζίστορ), μια φθηνή εναλλακτική λύση αντί της ηλεκτρονικής λυχνίας. Η εμπορική χρήση των υπολογιστών έγινε πραγματικότητα το 1951 όταν εταιρίες σαν τη Φεράντι άρχισαν να κατασκευάζουν υπολογιστές κατά παραγγελία.

Το 1953 η IBM κυκλοφόρησε τον πρώτο της υπολογιστή, και τέσσερα χρόνια αργότερα παρουσίασε τη Fortran , μια προγραμματιστική γλώσσα που επέτρεπε στους συνηθισμένους ανθρώπους

να γράφουν υπολογιστικά προγράμματα. Στη συνέχεια, το 1959, η εφεύρεση του ολοκληρωμένου κυκλώματος σήμανε μια νέα αποχή στους υπολογιστές. Στη διάρκει της δεκαετίας του 1960, οι υπολογιστές έγιναν ισχυρότεροι και ταυτόχρονα φθηνότεροι. Οι επιχειρήσεις είχαν όλο και πιο πολύ τη δυνατότητα να τους παραγγείλουν, και μπορούσαν να τους χρησιμοποιούν για να κρυπτογραφούν σημαντικές επικοινωνίες, όπως μεταβιβάσεις χρημάτων ή λεπτές εμπορικές διαπραγματεύσεις. Ωστόσο καθώς όλο και περισσότερες επιχειρήσεις αγόραζαν υπολογιστές, και καθώς οι κρυπτογραφημένες επικοινωνίες ανάμεσα σε επιχειρήσεις εξαπλώνονταν, οι κρυπτογράφοι είχαν να αντιμετωπίσουν νέα προβλήματα. Ένα από τα σημαντικότερα προβλήματα ήταν το ζήτημα της τυποποίησης. Μια εταιρία μπορούσε να χρησιμοποιεί ένα συγκεκριμένο σύστημα κρυπτογράφησης για να διασφαλίζει τις εσωτερικές της επικοινωνίες αλλά δεν ήταν σε θέση να στείλει μυστικό μήνυμα σε μια εξωτερική οργάνωση, εκτός αν ο αποδέκτης χρησιμοποιούσε το ίδιο σύστημα κρυπτογράφησης. Τελικά, το Μάιο του 1973, το Εθνικό Γραφείο Μέτρων και Σταθμών των ΗΠΑ αποφάσισε να λύσει το πρόβλημα, και ζήτησε επίσημα την υποβολή αιτήσεων για ένα ενιαίο κρυπτογραφικό σύστημα που θα επέτρεπε στις επιχειρήσεις να επικοινωνούν μυστικά μεταξύ τους. Ένας από τους πιο καθιερωμένους κρυπτογραφικούς αλγορίθμους και υποψήφιος για το ενιαίο σύστημα, ήταν ο λεγόμενος Εωσφόρος, προιόν της IBM. Τον είχε αναπτύξει ο Χορστ Φάιστελ ένας γερμανός μετανάστης που είχε έρθει στην Αμερική. Όταν άρχισε έρευνα πάνω στα κρυπτογράμματα, στο Ερευνητικό Κέντρο Κέμπριτζ της Πολεμικής Αεροπορίας, παρενέβη στην εργασία του η NSA, Η Εθνική Υπηρεσία Ασφαλείας των ΗΠΑ, που έχει τη γενική ευθύνη για την ασφάλεια των στρατιωτικών και κυβερνητικών επικοινωνιών. Και παράλληλα ασχολείται με την υποκλοπή και την αποκρυπτογράφηση των επικοινωνιών των ξένων δυνάμεων.

Η NSA απασχολεί περισσότερους μαθηματικούς, αγοράζει περισσότερους υπολογιστές και υποκλέπτει περισσότερα μηνύματα από κάθε άλλη οργάνωση στον κόσμο. Είναι η παγκόσμια πρωταθλήτρια της κατασκοπίας. Η NSA δεν προέβαλε ενστάσεις σχετικά με το παρελθόν του Φάιστελ. Το μόνο που ήθελε ήταν να έχει το μονοπώλιο της κρυπτογραφικής έρευνας και όπως φαίνεται φρόντισε να ακυρώσει το ερευνητικό πρόγραμμά του. Τη δεκαετία του 1960 ο Φάιστελ μεταπήδησε στη Mitre Corporation αλλά η NSA εξακολουθούσε να ασκεί πιέσεις και τον ανάγκασε να εγκαταλείψει την εργασία του για δεύτερη φορά. Τελικά, ο Φάιστελ κατέληξε στο εργαστήριο Τόμας Τζ. Ουότσον της IBM στη ΝέΑ Υόρκη, όπου μπόρεσε να συβεχίσει την έρευνά του. Εκεί στις αρχές του 1970, ανέπτυξε το σύστημα Εωσφόρος.

Ο Εωσφόρος κρυπτογραφεί μηνύματα σύμφωνα με την ακόλουθη αναδιατακτική διαδικασία. Πρώτον, το μήνυμα μεταφράζεται σε μία επιμήκη σειρά δυαδικών ψηφίων.

Δεύτερον, η σειρά διασπάται σε ομάδες των 64 ψηφίων, και η κρυπτογράφηση διενεργείται χωριστά για την κάθε ομάδα.

Τρίτον, τα 64 ψηφία της κάθε ομάδας αναδιατάσσονται και μετά διασπόνται σε δυο υποομάδες των 32 ψηφίων, που χαρακτηρίζονται Αριστερή και Δεξιά.

Στη συνέχεια τα ψηφία στη Δεξιά περνούν από μια λειτουργία ανακατέματος η οποία αλλάζει τα ψηφία σύμφωνα με μια πολύπλοκη υποκατάσταση. Κατόπιν, η ανακατεμένη Δεξιά προστίθεται στην Αριστερή, ώστε να δημιουργηθεί μια νέα υποομάδα από 32 ψηφία, η οποία χαρακτηρίζεται Δεξιά. Η αρχική Δεξιά αλλάζει όνομα και γίνεται Αριστερή. Αυτή η σειρά ενεργειών αποκαλείται γύρος. Η όλη διαδικασία επαναλαμβάνεται μέχρις ότου συμπληρωθούν 16 συνολικά γύροι. Οι επιμέρους λεπτομέρειες της λειτουργίας ανακατέματος μπορούν να αλλάζουν, και καθορίζονται από ένα κλειδί στο οποίο έχουν συμφωνήσει αποστολέας και αποδέκτης. Με άλλα λόγια το ίδιο μήνυμα μπορεί να κρυπτογραφηθεί με άπειρους διαφορετικούς τρόπους, ανάλογα με ποιο κλειδί επιλέγεται. Τα κλειδιά που χρησιμοποιούνται στην κρυπτογραφία μέσω υπολογιστή είναι απλοί αριθμοί. Κατά συνέπεια ο αποστολέας και ο αποδέκτης δεν έχουν παρά να συμφωνήσουν σε έναν αριθμό, καθορίζοντας έτσι το κλειδί. Για να γίνει η κρυπτογράφηση πρέπει ο αποστολέας να εισαγάγει τον αριθμό κλειδί και το μήνυμα στον Εωσφόρο ο οποίος στη συνέχεια παράγει το αρχικό μήνυμα. Ο Εωσφόρος γενικά θεωρείτο ένα από τα ισχυρότερα κρυπτογραφικά προιόντα που κυκλοφόρησαν στο εμπόριο με αποτέλεσμα να τον χρησιμοποιούν πολλές και διάφορες οργανώσεις. Φαινόταν αναπόφευκτο ότι το συγκεκριμένο προιόν θα υιοθετείτο ως το επίσημο αμερικανικό σύστημα κρυπτογράφησης, όμως για μια ακόμη φορά παρενέβη στο έργο του Φάιστελ η NSA. Ο Εωσφόρος ήταν τόσο ισχυρός, ώστε παρείχε τη δυνατότητα υιοθέτησης μιας τυποποιημένης διαδικασίας κρυπτογράφησης η οποία πιθανότατα ξεπερνούσε τις κωδικοθραυστικές ικανότητες της NSA. Ο αριθμός των πιθανών κλειδιών

είναι ένας από τους κρίσιμους παράγοντες που καθορίζουν την ισχύ οποιουδήποτε κρυπτογράμματος. Ένας κρυπταναλυτής που προσπαθεί να αποκρυπτογραφήσει ένα κρυπτογραφημένο μήνυμα θα μπορούσε να επιχειρήσει να ελέγξει όλα τα πιθανά κλειδιά, και όσο περισσότερα είναι αυτά, τόσο περισσότερο χρόνο θα χρειαστεί για να βρει το σωστό. Αν υπάρχουν μόνο 1.000.000 πιθανά κλειδιά, ο κρυπταναλυτής μπορεί να χρησιμοποιήσει έναν ισχυρό υπολογιστή, να βρει το σωστό κλειδί μέσα σε λίγα λεπτά, και έτσι να αποκρυπτογραφήσει ένα υποκλαπέν μήνυμα. Αν όμως ο αριθμός των πιθανών κλειδιών είναι πολύ μεγαλύτερος, η ανεύρεση του σωστού δεν είναι πλέον πρακτική. Αν ο Εωσφόρος επρόκειτο να γίνει το επίσημο σύστημα κρυπτογράφησης, τότε η NSA ήθελε να διασφαλίσει ότι θα λειτουργούσε με περιορισμένο αριθμό κλειδιών. Η NSA υποστήριξε τον περιορισμό του αριθμού των κλειδιών σε περίπου 100.000.000.000.000.000(ο αριθμός αυτός στην τεχνική γλώσσα αποκαλείται 56 μπιτ, επειδή όταν γραφτεί σε δυαδική μορφή αποτελείται από 56 ψηφία). Φαίνεται πως η NSA πίστευε ότι ένα τέτοιο κλειδί θα παρείχε ασφάλεια στην πολιτική κοινότητα, εφόσον καμία μη στρατιωτική οργάνωση δεν διέθετε τόσο ισχυρό υπολογιστή ώστε να ελέγχει κάθε πιθανό κλειδί μέσα σε λογικό χρονικό διάστημα. Αντίθετα η ίδια η NSA, έχοντας πρόσβαση στο μεγαλύτερο δίκτυο υπολογιστών παγκοσμίως, θα μπορούσε να σπάζει τα μηνύματα. Έτσι ο Εωσφόρος υιοθετήθηκε επισήμως στην εκδοχή των 56 μπιτ και ονομάστηκε DES( Data Encryption Standard=τυποποιημένο σύστημα κρυπτογράφησης δεδομένων). Η υιοθέτηση του DES έλυσε το πρόβλημα της τυποποίησης ενθαρρύνοντας τις επιχειρήσεις να χρησιμοποιούν την κρυπτογραφία για λόγους ασφαλείας. Επιπλέον, το DES ήταν αρκετά ισχυρό ώστε να τις διασφαλίσει από τις επιθέσεις των εμπορικών τους ανταγωνιστών. Πράγματι, μια επιχείρηση με μη στρατιωτικό υπολογιστή ήταν ουσιαστικά αδύνατον να σπάσει ένα μήνυμα κρυπτογραφημένο με DES, επειδή ο αριθμός των πιθανών κλειδιών ήταν επαρκώς μεγάλος. Δυστυχώς, παρά την τυποποίηση και παρά την ισχύ του DES , οι επιχειρήσεις είχαν να αντιμετωπίσουν ένα άλλο μεγάλο ζήτημα, το λεγόμενο πρόβλημα της *διανομής των κλειδιών*.

Έστω ότι μια τράπεζα θέλει να στείλει κάποια εμπιστευτικά δεδομένα σε ένα πελάτη μέσω μιας τηλεφωνικής γραμμής, αλλά ανησυχεί μήπως κάποιος την έχει παγιδεύσει. Η τράπεζα επιλέγει ένα κλειδί και χρησιμοποιεί το DES για να κρυπτογραφήσει το μήνυμα που περιέχει τα δεδομένα. Για να κρυπτογραφήσει το μήνυμα, ο πελάτης πρέπει όχι μόνο να έχει εγκατεστημένο στον υπολογιστή του ένα αντίγραφο του DES αλλά και να γνωρίζει ποιο κλειδί έχει χρησιμοποιηθεί για την κρυπτογράφηση του μηνύματος. Η τράπεζα δεν μπορεί να στείλει στον πελάτη το κλειδί μέσω τηλεφωνικής γραμμής, γιατί υποψιάζεται ότι υπάρχει ωτακουστής. Ο μόνος πραγματικά ασφαλής τρόπος για να στείλει το κλειδί είναι να το παραδώσει στον παραλήπτη αυτοπροσώπως, πράγμα εμφανώς χρονοβόρο. Μια λιγότερο ασφαλής αλλά πι πρακτική λύση είναι να στείλει το κλειδί με έναν ταχυδρόμο. Τη δεκαετία του 1970, οι τράπεζες επιχείρησαν να στέλνουν τα κλειδιά χρησιμοποιώντας ειδικούς διανομείς, οι οποίοι είχαν υποστεί εξονυχιστικό έλεγχο και ανήκαν στους πιο έμπιστους υπαλλήλους της εταιρίας. Οι διανομείς αυτοί περιόδευαν ανά τον κόσμο με χαρτοφύλακες κλειδωμένους με λουκέτο και διένεμαν αυτοπροσώπως τα κλειδιά σε όλους όσοι επρόκειτο να λάβουν μηνύματα από την τράπεζα την επόμενη βδομάδα. Καθώς όμως τα δίκτυα των επιχειρήσεων επεκτείνονταν, στέλνονταν όλο και περισσότερα μηνύματα και έπρεπε να διανέμονται όλο και περισσότερα κλειδιά, με αποτέλεσμα οι τράπεζες να διαπιστώσουν ότι το κόστος της συγκεκριμένης διαδικασίας διανομής είχε γίνει απαγορευτικό. Το πρόβλημα της διανομής των κλειδιών υπήρξε η μάστιγα των κρυπτογράφων σε όλη την ιστορία. Όσο ασφαλές και να είναι ένα κρυπτόγραμμα στη θεωρία, στην πράξη μπορεί να υπονομευθεί από το πρόβλημα της διανομής των κλειδιών. Η διανομή των κλειδιών μπορεί να φαίνεται ευτελές ζήτημα, όμως αναδείχτηκε σε κυρίαρχο πρόβλημα για τους κρυπτογράφους της μεταπολεμικής περιόδου. Αν δυο πλευρές ήθελαν να επικοινωνήσουν με ασφάλεια, έπρεπε να βασιστούν σε μια Τρίτη πλευρά για την παράδοση του κλειδιού, κι αυτό έγινε ο ασθενέστερος κρίκος στην αλυσίδα της ασφάλειας. Το δίλλημα για τις επιχειρήσεις ήταν το εξής: αν οι κυβερνήσεις με όλα τα χρήματα που διέθεταν αγωνίζονταν για να εγγυηθούν την ασφαλή διανομή των κλειδιών, πώς θα μπορούσαν οι πολιτικές εταιρίες έστω και να ελπίζουν ότι θα πετύχαιναν το ίδιο πράγμα χωρίς να χρεοκοπήσουν; Παρά τους ισχυρισμούς ότι το πρόβλημα της διανομής των κλειδιών ήταν άλυτο, μια ομάδα μεγιστάνων διέψευσε όλες τις αρνητικές προβλέψεις και επινόησε ένα σύστημα κρυπτογράφησης που έμοιαζε να αψηφά κάθε λογική. Παρότι οι υπολογιστές άλλαξαν ριζικά την εφαρμογή των κρυπτογραμμάτων, η μεγαλύτερη επανάσταση στην κρυπτογραφία του εικοστού αιώνα υπήρξε η ανάπτυξη τεχνικών για την υπέρβαση του προβλήματος της διανομής των κλειδιών.

Με το πρόβλημα της διανομής των κλειδιών ασχολήθηκε ο Ουίτφιλντ Ντίφι, ένας από τους πιο λαμπρούς κρυπτογράφους της γενιάς του. Σπούδασε μαθηματικά στο Τεχνολογικό Ινστιτούτο της Μασαχουσέτης και στη συνέχεια ανέλαβε μια σειρά από εργασίες σχετικές με την ασφάλεια των υπολογιστών. Ενδιαφερόταν ιδιαιτέρως για το πρόβλημα τα διανομής των κλειδιών και συνειδητοποίησε ότι όποιος κατάφερνε να το λύσει θα έμενε στην ιστορία σαν ένας από τους μεγαλύτερους κρυπτογράφους όλων των εποχών. Το ενδιαφέρον του Ντίφι προερχόταν από το όραμά του για έναν καλωδιωμένο κόσμο. Ήδη από τη δεκαετία του 1960 το Υπουργείο Άμυνας των ΗΠΑ είχε αρχίσει να χρηματοδοτεί μια πρωτοποριακή οργάνωση με την επωνυμία ARPA, της οποίας τα σημαντικότερα σχέδια ήταν να βρει ένα τρόπο σύνδεσης των στρατιωτικών υπολογιστών διαμέσου μεγάλων αποστάσεων. Κάτι τέτοιο θα επέτρεπε σε έναν υπολογιστή που είχε υποστεί βλάβη να μεταφέρει τις λειτουργίες του σε έναν άλλον υπολογιστή τοθ δικτύου. Ο κύριος στόχο ήταν να ισχυροποιηθεί η υποδομή των υπολογιστών του Πενταγώνου για το ενδεχόμενο πυρηνικής επίθεσης, όμως το δίκτυο θα επέτρεπε επίσης στους επιστήμονες να ανταλλάσουν μηνύματα και να εκτελούν υπολογισμούς εκμεταλλευόμενοι τις εφεδρικές δυνατότητες μακρινών υπολογιστών. Έτσι το 1969 γεννήθηκε το ARPANET, και ως το τέλος της ίδιας χρονιάς υπήρχαν τέσσερις συνδεδεμένοι κόμβοι. Το ARPANET επεκτεινόταν σταθερά και το 1982 γεννήθηκε το Διαδίκτυο. Στα τέλη της δεκαετίας του 1980 επετράπη η πρόσβαση στο διαδίκτυο σε μη πανεπιστημιακούς και μη στρατιωτικούς χρήστες και έκτοτε ο αριθμός των χρηστών γνώρισε πραγματική έκρηξη. Ενώ το ARPANET βρισκόταν ακόμα στα σπάργανα, ο Ντίφι προέβλεψε την έλευση της πληροφορικής υπερλεωφόρου και την ψηφιακή επανάσταση. Ο ίδιος πίστευε ότι αν στο μέλλον οι άνθρωποι χρησιμοποιούσαν τους υπολογιστές τους για να ανταλλάσσουν ηλεκτρονικά μηνύματα, τότε είχαν το δικαίωμα να κρυπτογραφούν τα μηνύματά τους ώστε να διασφαλίζουν το απόρρητο της προσωπικής τους ζωής. Όμως η κρυπτογράφηση απαιτούσε την ασφαλή ανταλλαγή κλειδιών. Αν η κυβέρνηση και οι μεγάλες εταιρίες δυσκολεύονταν να αντιμετωπίσουν το πρόβλημα της διανομής των κλειδιών, το ευρύ κοινό θα το έβρισκε αδύνατον και ουσιαστικά θα έχανε το δικαίωμα προστασίας του απορρήτου. Ο Ντίφι φαντάστηκε δύο ξένους να συναντώνται μέσω του Διαδικτύου και διερωτήθηκε πώς θα μπορούσαν να ανταλλάσσουν κρυπτογραφημένα μηνύματα. Επίσης προβληματίστηκε πάνω στο σενάριο όπου κάποιος θέλει να αγοράσει μέσω του διαδικτύου ένα προιόν. Πώς θα μπορούσε το άτομο αυτό να στείλει ηλεκτρονικό ταχυδρομείο που να περιέχει κρυπτογραφημένα τα στοιχεία της πιστωτικής του κάρτας, ώστε μόνο ο πωλητής να μπορεί να αποκρυπτογραφήσει; Και στις δυο περιπτώσεις οι δυο πλευρές έπρεπε προφανώς να διαθέτουν ένα κοινό κλειδί, όμως πώς θα μπορούσαν να ανταλλάσσουν κλειδιά με ασφάλεια; Ο αριθμός των προσωπικών επαφών και των ηλεκτρονικών μηνυμάτων ανάμεσα στο κοινό θα ήταν τεράστιος και άρα η διανομή των κλειδιών ανεφάρμοστη. Ο Ντίφι φοβόταν ότι η ανάγκη για διανομή των κλειδιών θα απέκλειε το ευρύ κοινό από την πρόσβαση στην ψηφιακή ασφάλεια και του έγινε έμμονη ιδέα να βρει μια λύση στο πρόβλημα. Έτσι στη συνέχεια συνεργάστηκε με τον Μάρτιν Χέλμαν, καθηγητή στο πανεπιστήμιο της Καλιφόρνιας. Η συνεργασία αυτή εξελίχτηκε σε μια από τις δυναμικότερες συνεργασίες στον τομέα της κρυπτογραφίας. Οι δυο συνεργάτες άρχισαν να μελετούν το πρόβλημα της διανομής των κλειδιών, προσπαθώντας απελπισμένα να βρουν μια εναλλακτική λύση στο κοπιώδες έργο της μεταφοράς τους με φυσικά πρόσωπα διαμέσου τεράστιων αποστάσεων. Στην πορεία προσχώρησε στην ομάδα τους ο Ραλφ Μέρκλε ο οποίος είχε μεταναστεύσει από μια άλλη ερευνητική ομάδα. Το όλο πρόβλημα της διανομής των κλειδιών είναι μια κλασική περίπτωση φαύλου κύκλου. Αν δυο άτομα θέλουν να ανταλλάξουν ένα μυστικό μήνυμα από το τηλέφωνο, ο αποστολέας θα πρέπει να το αποκρυπτογραφήσει. Για να κρυπτογραφήσει το αρχικό μήνυμα, ο αποστολέας θα πρέπει να χρησιμοποιήσει ένα κλειδί , που είναι μυστικό το ίδιο οπότε υπάρχει το πρόβλημα διαβίβασης του μυστικού κλειδιού στον αποδέκτη ώστε να μεταδοθεί το μυστικό μήνυμα. Με δύο λόγια, προτού δυο άτομα ανταλλάξουν ένα μυστικό, θα πρέπει ήδη να μοιράζονται ένα μυστικό(το κλειδί). Ας φανταστούμε τρία υποθετικά πρόσωπα, την Αλίκη, τον Μπομπ, και την Εύα, που εμφανίζονται ως τυπικά παραδείγματα στις συζητήσεις με αντικείμενο την κρυπτογραφία. Σε μια τυπική κατάσταση, η Αλίκη θέλει να στείλει ένα μήνυμα στον Μομπ, ή το αντίστροφο, και η Εύα προσπαθεί να το υποκλέψει. Αν η Αλίκη στέλνει ιδιωτικά μηνύματα στον Μπομπ, θα κρυπτογραφεί το καθένα από αυτά πριν το στείλει, χρησιμοποιώντας κάθε φορά ένα ξεχωριστό κλειδί. Η Αλίκη αντιμετωπίζει συνεχώς το πρόβλημα της διανομής των κλειδιών επειδή είναι αναγκασμένη να μεταδίδει τα κλειδιά στον Μπομπ με ασφαλή τρόπο, διαφορετικά δεν μπορεί να κρυπτογραφήσει τα μηνύματα. Μια πιθανή λύση στο πρόβλημα είναι να συναντώνται η Αλίκη και ο Μπομπ μία φορά την εβδομάδα και να ανταλλάζουν όσα

κλειδιά χρειάζονται για να καλύψουν όλα τα μηνύματα που θα στέλνουν ο ένας στον άλλο τις επόμενες 7 ημέρες. Το να ανταλλάζουν τα κλειδιά αυτοπροσώπως είναι οπωσδήποτε ασφαλές αλλά άβολο, και αν ο ένας από τους δυο αρρωστήσει, το σύστημα καταρρέει. Εναλλακτικά η Αλίκη και ο Μπομπ μπορούν να μισθώνουν ταχυδρόμους πράγμα λιγότερο ασφαλές και πιο δαπανηρό, έτσι όμως τουλάχιστον μεταθέτουν σε άλλους ένα τμήμα της δουλειάς. Και στις δυο περιπτώσεις η ανταλλαγή κλειδιών φαίνεται αναπόφευκτη. Επί 2 χιλιάδες χρόνια αυτό θεωρείτο ως αξίωμα της κρυπτογραφίας. Υπάρχει ωστόσο ένα θεωρητικό πείραμα που μοιάζει να αντικρούσει το αξίωμα αυτό. Έστω ότι η Αλίκη και ο Μπομπ ζουν σε μια χώρα όπου το ταχυδρομικό σύστημα είναι εντελώς διεφθαρμένο. Μια μέρα η Αλίκη θέλει να στείλει ένα άκρως προσωπικό μήνυμα στον Μπομπ. Το τοποθετεί λοιπόν μέσα σε ένα σιδερένιο κουτί, το οποίο κλείνει και ασφαλίζει με λουκέτο και κλειδί. Παραδίδει το κλειδωμένο κουτί στο ταχυδρομείο και κρατάει το κλειδί. Όταν το κουτί φτάσει στον Μπομπ εκείνος δεν μπορεί να το ανοίξει γιατί δεν έχει το κλειδί. Ο μόνος τρόπος αντιμετώπισης του προβλήματος αποφεύγοντας την ανταλλαγή των κλειδιών, είναι ο εξής: Όταν ο Μπομπ παραλάβει το κουτί, προσθέτει σε αυτό το δικό του λουκέτο και το στέλνει πίσω στην Αλίκη. Τώρα το κουτί που παραλαμβάνει η Αλίκη είναι ασφαλισμένο με δυο λουκέτα. Αφαιρεί το δικό της λουκέτο, αφήνει μόνο το λουκέτο του Μπομπ και στέλνει πίσω στον Μπομπ το κουτί. Τώρα ο Μομπ μπορεί να ανοίξει το κουτί επειδή είναι σφαλισμένο με το δικό του λουκέτο για το οποίο μόνο αυτός έχει το κλειδί. Όλα τα παραπάνω αποδεικνύουν ότι ένα μυστικό μήνυμα μπορεί να ανταλλαγεί με ασφάλεια μεταξύ δυο ατόμων χωρίς να είναι απαραίτητη η ανταλλαγή κλειδιών. Για πρώτη φορά έχουμε μια υπόδειξη ότι η ανταλλαγή κλειδιών μπορεί να μην είναι αναπόφευκτο μέρος της κρυπτογραφίας. Μπορούμε να ερμηνεύσουμε εκ νέου την παραπάνω ιστορία με κρυπτογραφικούς όρους. Η Αλίκη χρησιμοποιεί το κλειδί της για να κρυπτογραφήσει ένα μήνυμα προς τον Μπομπ, ο οποίος το κρυπτογραφεί ξανά με δικό του κλειδί και της το επιστρέφει. Όταν η Αλίκη λάβει το διπλά κρυπτογραφημένο μήνυμα, αφαιρεί τη δική της κρυπτογράφηση και το ξαναστέλνει στον Μπομπ, ο οποίος πλέον μπορεί να αφαιρέσει τη δική του κρυπτογράφηση και να διαβάσει το μήνυμα. Το πρόβλημα της διανομής των κλειδιών φαίνεται να έχει λυθεί, εφόσον το σύστημα διπλής κρυπτογράφησης δεν απαιτεί ανταλλαγή κλειδιών. Υπάρχει ωστόσο ένα σοβαρό εμπόδιο στην εφαρμογή αυτού του συστήματος. Το πρόβλημα έγκειται στη σειρά με την οποία εκτελούνται οι κρυπτογραφήσεις και οι αποκρυπτογραφήσεις. Γενικά η σειρά της κρυπτογράφησης και της αποκρυπτογράφησης είναι θεμελιώδης και θα πρέπει να υπακούει στο πρόσταγμα «τελευταίο προστιθέμενο, πρώτο αφαιρούμενο». Με άλλα λόγια, το τελευταίο στάδιο της κρυπτογράφησης πρέπει να είναι το πρώτο που θα αποκρυπτογραφηθεί.

Στο παραπάνω σενάριο, ο Μπομπ διενήργησε το τελευταίο στάδιο της κρυπτογράφησης και επομένως αυτό θα έπρεπε να αποκρυπτογραφηθεί πρώτο, όμως ήταν η Αλίκη εκείνη που αφαίρεσε πρώτη την κρυπτογράφησή της.

Κάποια πολύ στοιχειώδη κρυπτογράμματα όπως αυτό του Καίσαρα, είναι τόσο απλά που δεν έχει σημασία η σειρά. Όμως στη δεκαετία του 1970, κάθε μορφή ισχυρής κρυπτογράφησης φαινόταν ότι έπρεπε να υπακούσει στον κανόνα που προαναφέρθηκε. Αν ένα μήνυμα έχει κρυπτογραφηθεί πρώτα με το κλειδί της Αλίκης και μετά με του Μπομπ, θα πρέπει να αποκρυπτογραφηθεί πρώτα με το κλειδί του Μπομπ και μετά με της Αλίκης. Η σειρά είναι θεμελιώδης ακόμα και σε ένα κρυπτόγραμμα μονοαλφαβητικής υποκατάστασης. Ας φανταστούμε ότι η Αλίκη και ο Μπομπ έχουν το δικό τους κλειδί ο καθένας, όπως φαίνεται παρακάτω, και ας δούμε τι συμβαίνει όταν η σειρά δεν είναι σωστή.

*Κλειδί της Αλίκης*

a b c d e f g h i j k l m n o p q r s t u v w x y z
H F S U G T A K V D E O Y J B P N X W C Q R I M Z L

*Κλειδί του Μπομπ*

a b c d e f g h i j k l m n o p q r s t u v w x y z
C P M G A T N O J E F W I Q B U R Y H X S D Z K L V

*Μήνυμα:* *m e e t me at noon*

| | |
|---|---|
| *Κρυπτογραφημένο με κλειδί Αλίκης:* | YGGC YG HC JBBJ |
| *Κρυπτογραφημένο με κλειδί Μπομπ:* | LNNM LN OM EPPE |
| *Αποκρυπτογραφημένο με κλειδί Αλίκης:* | ZQQX ZQ LX KPPK |
| *Αποκρυπτογραφημένο με κλειδί Μπομπ:* | w n n t w n y t x b b x |

Το αποτέλεσμα δεν βγάζει νόημα. Αντίθετα, αν η σειρά αποκρυπτογράφησης αναστραφεί, και ο Μπομπ αποκρυπτογραφήσει πριν την Αλίκη, το αποτέλεσμα θα είναι το αρχικό μήνυμα.

Παρότι το σύστημα του διπλά κλειδωμένου κουτιού δεν λειτουργεί για την κρυπτογραφία του πραγματικού κόσμου, ήταν αυτό που ενέπνευσε τους Ντίφι και Χέλμαν να αναζητήσουν μια πρακτική μέθοδο παράκαμψης ους προβλήματος σχετικά με τη διανομή των κλειδιών. Η έρευνά τους επικεντρώθηκε στην εξέταση διάφορων μαθηματικών συναρτήσεων. Συνάρτηση είναι οποιαδήποτε μαθηματική πράξη μετατρέπει ένας αριθμό σε έναν άλλο. Μπορούμε να θεωρήσουμε όλες τις μορφές κρυπτογράφησης μέσω υπολογιστή ως συναρτήσεις, εφόσον μετατρέπουν έναν αριθμό(το κανονικό κείμενο) σε έναν άλλο αριθμό(το κρυπτογραφημένο κείμενο). Οι περισσότερες μαθηματικές συναρτήσεις χαρακτηρίζονται ως αμφιμονοσήμαντες, επειδή εύκολα εκτελούνται και εύκολα αντιστρέφονται. Ωστόσο οι Ντίφι και Χέλμαν δεν ενδιαφέρονταν για τις αμφιμονοσήμαντες συναρτήσεις. Επικέντρωσαν την προσοχή τους στις μονοσήμαντες. Μία μονοσήμαντη συνάρτηση εύκολα εκτελείται, αλλά πολύ δύσκολα ακυρώνεται. Οι αμφιμονοσήμαντες συναρτήσεις είναι αναστρέψιμες ενώ οι μονοσήμαντες όχι. Ύστερα από δυο χρόνια εμμονής στη μοδιακή αριθμητική(τομές των μαθηματικών πλούσιος σε μονοσήμαντες συναρτήσεις), η τρέλα του Χέλμαν άρχισε να αποδίδει καρπούς.

Την άνοιξη του 1976 επινόησε μια στρατηγική για την επίλυση του προβλήματος της ανταλλαγής των κλειδιών. Απέδειξε ότι η Αλίκη και ο Μπομπ μπορούσαν να συμφωνήσουν σε ένα κλειδί χωρίς να συναντηθούν, καταρρίπτοντας έτσι ένα αξίωμα που είχε διαρκέσει αιώνες. Η ιδέα του Χέλμαν στηριζόταν σε μια μονοσήμαντη συνάρτηση του τύπου Y^X(modulo P). Αρχικά η Αλίκη και ο Μπομπ συμφωνούν στις τιμές των Y και P. Όλες σχεδόν οι τιμές είναι κατάλληλες, υπάρχουν όμως κάποιοι περιορισμοί, όπως ότι το Y πρέπει να είναι μικρότερο του P. Οι τιμές αυτές δεν είναι μυστικές και έτσι η Αλίκη μπορεί να τηλεφωνήσει στον Μπομπ και να του τις υποδείξει, ας πούμε ότι Y= 7 και P= 11. Ακόμη και αν η τηλεφωνική γραμμή δεν είναι ασφαλής, και η Εύα ακούσει αυτή τη συνομιλία, δεν έχει καμία σημασία όπως θα αποδειχθεί αργότερα. Τώρα η Αλίκη και ο Μπομπ έχουν συμφωνήσει στη μονοσήμαντη συνάρτηση 7^χ(modulo 11). Στο σημείο αυτό μπορούν να ξεκινήσουν τη διαδικασία της απόπειρας καθορισμού ενός μυστικού κλειδιού χωρίς να συναντηθούν. Επειδή εργάζονται παράλληλα, οι ενέργειές τους εξηγούνται στον πίνακα που ακολουθεί. Η Αλίκη και ο Μπομπ , χωρίς να συναντηθούν συμφώνησαν στο ίδιο κλειδί το οποίο μπορούν να χρησιμοποιήσουν για να κρυπτογραφήσουν ένα μήνυμα. Για παράδειγμα μπορούν να χρησιμοποιήσουν τον αριθμό τους, το 9, ως κλειδί για μια κρυπτογράφηση DES.

| | Αλίκη | Μπομπ |
|---|---|---|
| **Στάδιο 1** | Η Αλίκη επιλέγει<br>Έναν αριθμό π.χ. το 3<br>Και τον κρατά μυστικό.<br>Ονομάζουμε τον αριθμό της Α. | Ο Μπομπ επιλέγει έναν<br>Αριθμό π.χ το 6 και<br>Τον κρατά μυστικό.<br>Ονομάζουμε τον αριθμό του Β. |
| **Στάδιο 2** | Η Αλίκη εισάγει το 3 στη<br>Μονοσήμαντη συνάρτηση και<br>Βρίσκει το αποτέλεσμα της<br>πράξης<br>7^Α (modulo 11):7^3(mod11)=<br>=343(mod11)=2 | Ο Μπομπ εισάγει το 6 στη μονοσήμαντη<br>συνάρτηση και<br>Βρίσκει το αποτέλεσμα της πράξης<br>7^Β(modulo11):7^6(mod11)=<br>117.649(mod11)=4 |
| **Στάδιο 3** | Η Αλίκη ονομάζει το αποτέλεσμα αυτού του υπολογισμού a και στέλνει το αποτέλεσμά της, το 2, στον Μπομπ | Ο Μπομπ ονομάζει το αποτέλεσμα αυτού του υπολογισμού b και στέλνει το αποτέλεσμά του, το 4, στη Αλίκη. |
| **Η ανταλλαγή** | Η Αλίκη και ο Μπομπ ανταλλάσουν πληροφορίες και η Εύα έχει την ευκαιρία να κρυφακούει τις λεπτομέρειες της ανταλλαγής. Ωστόσο αποδεικνύεται ότι η Εύα μπορεί να κρυφακούσει χωρίς να επηρεάσει την τελική ασφάλεια του συστήματος. Η Αλίκη και ο Μπομπ χρησιμοποιούν την ίδια τηλεφωνική γραμμή στην οποία ανταλλάσουν τις αξίες των Υ και Ρ, και η Εύα υποκλέπτει τους δυο ανταλλασσόμενους αριθμούς, 2 και 4. Όμως οι αριθμοί αυτοί δεν είναι το κλειδί και επομένως δεν έχουν καμία αξία για την Εύα. | |
| **Στάδιο 4** | Η Αλίκη παίρνει το αποτέλεσμα του Μπομπ και βρίσκει το αποτέλεσμα της πράξης<br>b^Α(mod11):4^3(mod11)=64(mod11)=9 | Ο Μπομπ παίρνει το αποτέλεσμα της Αλίκης και βρίσκει το αποτέλεσμα της πράξης<br>a^Β(mod11):2^6(mod11)=64(mod11)=9 |
| **Το κλειδί** | Η Αλίκη και ο Μπομπ κατέληξαν στον ίδιο αριθμό, το 9. Αυτό είναι το κλειδί. | |

Η Αλίκη και ο Μπομπ κατόρθωσαν να συμφωνήσουν σε ένα κλειδί χωρίς να χρειαστεί να συναντηθούν. Το εκπληκτικό επίτευγμα είναι το το μυστικό κλειδί συμφωνήθηκε μέσω μια ανταλλαγής πληροφοριών σε μια τηλεφωνική κοινή γραμμή. Αν όμως η Εύα έχει παγιδεύσει τη γραμμή, ξέρει το κλειδί; Στην περίπτωση αυτή, η Εύα γνωρίζει μόνο τα εξής δεδομένα: ότι η συνάρτηση είναι 7^χ(modulo11), ότι η Αλίκη στέλνει a=2 και ότι ο Μπομπ στέλνει b=4. Για να βρει το κλειδί θα πρέπει να κάνει είτε ότι κάνει ο Μπομπ, δηλαδή να μετατρέψει το a στο κλειδί γνωρίζοντας το Β, ή να κάνει ότι κάνει η Αλίκη, δηλαδή να μετατρέψει το b στο κλειδί γνωρίζοντας το Α. Η Εύα όμως δεν γνωρίζει τις τιμές των Α και Β, επειδή η Αλίκη και ο Μπομπ δεν αντάλλαξαν αυτούς τους αριθμούς και τους κράτησαν μυστικούς. Η Εύα θεωρητικά θα μπορούσε να υπολογίσει το Α από το a επειδή το a προέκυψε από την εισαγωγή του Α σε μια συνάρτηση, και η Εύα γνωρίζει τη συνάρτηση . Ή θα μπορούσε να υπολογίσει το Β από το b, επειδή το b προέκυψε από την εισαγωγή του Β σε μια συνάρτηση την οποία η Εύα γνωρίζει. Η συνάρτηση όμως αυτή είναι μονοσήμαντη και έτσι ενώ είναι εύκολο για την Αλίκη να μετατρέψει το Α σε a και για τον Μπομπ να μετατρέψει το Β σε b, είναι πολύ δύσκολο για την Εύα να αντιστρέψει τη διαδικασία, ιδίως αν οι αριθμοί είναι πολύ μεγάλοι.

Το σύστημα ανταλλαγής κλειδιών Ντίφι-Χέλμαν-Μέρκλε, όπως είναι γνωστό, επιτρέπει στην Αλίκη και τον Μπομπ να καθορίσουν ένα μυστικό μέσω μιας δημόσιας συζήτησης, και υποχρέωσε το κρυπτογραφικό κατεστημένο να ξαναγράψει τους κανόνες κρυπτογράφησης. Στο εξής η Αλίκη και ο Μπομπ δεν χρειαζόταν να συναντηθούν για να ανταλλάξουν ένα κλειδί. Αντ' αυτού, η Αλίκη μπορούσε απλώς να τηλεφωνεί στον Μπομπ, να ανταλλάσσουν δυο αριθμούς, να καθορίσουν αμοιβαία ένα μυστικό κλειδί και στη συνέχεια να προχωρούν στην κρυπτογράφηση. Παρότι το σύστημα ανταλλαγής κλειδιών Ντίφι-Χέλμαν-Μέρκλε αποτελούσε ένα τεράστιο άλμα προς τα εμπρός δεν ήταν τέλειο επειδή από τη φύση του ήταν άβολο. Στη συνέχεια κάποιος έπρεπε απλώς να επινοήσει ένα πιο αποτελεσματικό σχήμα για να ξεπεραστεί το πρόβλημα της διανομής των κλειδιών.

Το διάστημα που ο Μάρτιν Χέλμαν ανέπτυσσε τη μέθοδό του για την ανταλλαγή των κλειδιών, ο Ουίτφιλντ Ντίφι επεξεργαζόταν μια εντελώς διαφορετική προσέγγιση για να επιλύσει το πρόβλημα της διανομής τους. Είχε επινοήσει ένα νέο τύπο κρυπτογράμματος, που περιλάμβανε το λεγόμενο ασύμμετρο κλειδί. Όλες οι κρυπτογραφικές τεχνικές που περιγράφηκαν ως τώρα ήταν συμμετρικές, που σημαίνει ότι η διαδικασία αναστροφής της αναδιάταξης δεν είναι παρά η αντίστροφή της. Για παράδειγμα το Αίνιγμα χρησιμοποιεί μια συγκεκριμένη ρύθμιση κλειδιού για να κρυπτογραφήσει ένα μήνυμα, και ο αποδέκτης χρησιμοποιεί μια ταυτόσημη μηχανή με την ίδια ρύθμιση κλειδιού για να το αποκρυπτογραφήσει. Με τον ίδιο τρόπο, η κρυπτογράφηση DES χρησιμοποιεί ένα κλειδί για να διενεργήσει 16 γύρους αναδιάταξης, και στη συνέχεια η αποκρυπτογράφηση DES χρησιμοποιεί το ίδιο κλειδί για τους 16 γύρους της αντίστροφης διαδικασίας. Αποστολέας και αποδέκτης έχουν ισοδύναμη γνώση, και χρησιμοποιούν και οι δυο τους το ίδιο κλειδί για να κρυπτογραφούν και να αποκρυπτογραφούν. Αντίθετα σε ένα ασύμμετρο σύστημα κλειδιών, όπως δείχνει η ίδια η λέξη, το κλειδί της κρυπτογράφησης δεν είναι ίδιο με το κλειδί της αποκρυπτογράφησης. Στην περίπτωση του ασύμμετρου κρυπτογράμματος, αν η Αλίκη γνωρίζει το κλειδί της κρυπτογράφησης, μπορεί να κρυπτογραφήσει το δικό της μήνυμα, αλλά δεν μπορεί να αποκρυπτογραφήσει το μήνυμα του άλλου. Για να το κάνει αυτό, θα πρέπει να έχει πρόσβαση στο κλειδί της αποκρυπτογράφησης. Αυτή ακριβώς η διάκριση ανάμεσα στα δυο κλειδιά, της κρυπτογράφησης και της αποκρυπτογράφησης, είναι που προσδίδει στο ασύμμετρο κρυπτόγραμμα τον ιδιαίτερο χαρακτήρα του.

Για να επανέλθουμε στην αναλογία των λουκέτων, η ασύμμετρη κρυπτογραφία μπορεί να περιγραφεί με τον ακόλουθο τρόπο. Οποιοσδήποτε μπορεί να κλειδώσει ένα λουκέτο απλώς κλείνοντάς το, αλλά το μόνο πρόσωπο που μπορεί να το ανοίξει είναι αυτό που έχει το κλειδί. Το κλείδωμα(η κρυπτογράφηση) είναι εύκολο, είναι κάτι που ο καθένας μπορεί να κάνει, όμως το ξεκλείδωμα (αποκρυπτογράφηση) μπορεί να γίνει μόνο από τον κάτοχο του κλειδιού. Η απλή γνώση του πώς να κλείσεις το λουκέτο δεν σου λέει πώς να το ξεκλειδώσεις. Επεκτείνοντας την αναλογία, έστω ότι η Αλίκη σχεδιάζει ένα λουκέτο και ένα κλειδί. Κρατάει για τον εαυτό της το κλειδί, αλλά κατασκευάζει χιλιάδες αντίγραφα του λουκέτου και τα διανέμει στα ταχυδρομεία όλου του κόσμου. Αν ο Μπομπ θέλει να στείλει ένα μήνυμα, το τοποθετεί σε ένα κουτί, παίρνει ένα τυχαίο λουκέτο «Αλίκης» και κλείνει με αυτό το κουτί. Τώρα δεν μπορεί να το ξεκλειδώσει, αλλά όταν το λάβει η Αλίκη μπορεί να το ανοίξει με το μοναδικό της κλειδί. Το λουκέτο και η διαδικασία του κλεισίματος ισοδυναμεί με το δημόσιο κλειδί της κρυπτογράφησης, επειδή όλοι έχουν πρόσβαση στα λουκέτα και ο καθένας μπορεί να χρησιμοποιήσει ένα λουκέτο για να σφραγίσει ένα μήνυμα μέσα σε ένα κουτί. Το κλειδί του λουκέτου ισοδυναμεί με το ιδιωτικό κλειδί της αποκρυπτογράφησης, επειδή μόνο η Αλίκη το έχει και άρα μόνο αυτή μπορεί να αποκτήσει πρόσβαση στο μήνυμα που βρίσκεται μέσα στο κουτί.

Στο ασύμμετρο σύστημα του Ντίφι, ο Μπομπ κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί αλλά δεν μπορεί να το αποκρυπτογραφήσει-πρόκειται ουσιαστικά για μια μονοσήμαντη συνάρτηση. Η Αλίκη αντίθετα είναι σε θέση να αποκρυπτογραφήσει το μήνυμα επειδή κατέχει το ιδιωτικό κλειδί, μια ειδική πληροφορία που της επιτρέπει να αντιστρέψει τη συνάρτηση. Και πάλι τα λουκέτα είναι μια καλή αναλογία-το κλείσιμο του λουκέτου είναι μονοσήμαντη συνάρτηση επειδή γενικά είναι δύσκολο να το ανοίξεις, εκτός αν διαθέτεις κάτι ειδικό (το κλειδί) οπότε η συνάρτηση αντιστρέφεται.

Στο τέλος το 1976 η ομάδα των Ντίφι, Χέλμαν και Μέρκλε είχε φέρει επανάσταση στον κόσμο της κρυπτογραφίας. Είχαν πείσει τον υπόλοιπο κόσμο ότι υπήρχε λύση στο πρόβλημα της διανομής των κλειδιών, το οποίο ήταν μεν εφαρμόσιμο αλλά ατελές, καθώς κανείς δεν μπορούσε να βρει μια κατάλληλη μονοσήμαντη συνάρτηση η οποία θα πληρούσε όλα τα κριτήρια που απαιτούνταν για ένα ασύμμετρο κρυπτόγραμμα.

Τις ιδέες των Ντίφι-Χέλμαν-Μερκλε, είχε πρώτος σκεφτεί ο Τζέιμς Έλις στα τέλη της δεκαετίας του 1960,όταν οι βρετανοί στρατιωτικοί είχαν αρχίσει να ανησυχούν για το πρόβλημα της διανομής των

κλειδιών. Την εποχή εκείνη η μόνη μορφή κρυπτογραφίας ήταν η συμμετρική, και έτσι κάθε κλειδί έπρεπε να μεταφέρεται με ασφάλεια σε κάθε μέλος του δικτύου επικοινωνιών. Στις αρχές του 1969, οι στρατιωτικοί ζήτησαν από τον Τζέιμς Έλις, έναν από τους πιο επιφανείς κυβερνητικούς κρυπτογράφους της Βρετανίας να αναζητήσει τρόπους αντιμετώπισης του προβλήματος διανομής των κλειδιών. Ο Έλις, σπούδασε φυσική στο αυτοκρατορικό κολέγιο και στη συνέχεια προσελήφθη στο ερευνητικό κέντρο της ταχυδρομικής υπηρεσίας στο Ντόλις Χιλ, εκεί που ο Ντόμις Φλάουερ είχε κατασκευάσει τον Κολοσσό. Την 1η Απριλίου του 1965 ο Έλις αποτέλεσε μέλος της νεοσύστατης ομάδας ασφάλειας των επικοινωνιών και της ηλεκτρονικής, ενός ειδικού τμήματος του GCHQ που είχε ως αντικείμενο την ασφάλεια των βρετανικών επικοινωνιών. Επειδή μπλεκόταν σε ζητήματα εθνικής ασφαλείας, είχε δώσει όρκο εχεμύθειας σε όλη τη διάρκεια της σταδιοδρομίας του.

Το κόστος της διανομής των κλειδιών ήταν ήδη υπέρογκο, και θα γινόταν ο παράγων που θα περιόριζε οποιαδήποτε επέκταση της κρυπτογράφησης. Ακόμη και αν κατόρθωναν να το μειώσουν κατά 10%, και πάλι θα έπρεπε να κάνουν σοβαρές περικοπές στον προυπολογισμό στρατιωτικής ασφάλειας. Όμως ο Έλις αντί για μια ήπια προσέγγιση του προβλήματος, άρχισε αμέσως να ψάχνει για μια πλήρη και ριζική λύση. Ανακάλυψε ότι η διανομή των κλειδιών δεν αποτελεί αναπόφευκτα μέρος της κρυπτογραφίας. Το γεγονός που άλλαξε την αντίληψη αυτή ήταν η ανακάλυψη μιας αναφοράς της Bell Telephone από την περίοδο του πολέμου. Ο άγνωστος συντάκτης της αναφοράς περιέγραψε μια μεγαλοφυή ιδέα για ασφαλείς τηλεφωνικές συνομιλίες. Πρότεινε ο δέκτης να καμουφλάρει τη φωνή του πομπού προσθέτοντας στη γραμμή θόρυβο. Αργότερα θα μπορούσε να αφαιρέσει τον θόρυβο, αφού ο ίδιος τον είχε προσθέσει και επομένως ήξερε τι ήταν. Η διαφορά του από τη συμβατική κρυπτογράφηση είναι ότι στην περίπτωση αυτή ο δέκτης παίρνει μέρος στη διαδικασία της κρυπτογράφησης.

Θόρυβος είναι ο τεχνικός όρος για οποιοδήποτε σήμα που προσβάλει την επικοινωνία. Συνήθως προκαλείται από φυσικά φαινόμενα, και το πιο εκνευριστικό χαρακτηριστικό του είναι η απόλυτη τυχαιότητά του, πράγμα που σημαίνει ότι είναι πολύ δύσκολο να αφαιρεθεί ο θόρυβος από ένα μήνυμα. Αν ένα σύστηνα ασύρματης επικοινωνίας είναι καλά σχεδιασμένο, τότε το επίπεδο θορύβου είναι χαμηλό και το μήνυμα ακούγεται καθαρά, αν όμως είναι υψηλό και υπερκαλύπτει το μήνυμα δεν υπάρχει τρόπος ανάκτησης του τελευταίου. Ο Έλις πρότεινε το εξής: ο δέκτης, η Αλίκη, να δημιουργεί εσκεμμένα θόρυβο, τον οποίο να έχει μετρήσει πριν τον προσθέσει στο δίαυλο επικοινωνιών που τη συνδέει με τον Μπομπ.

Ο Μπομπ τότε θα μπορούσε να στείλει το μήνυμα στην Αλίκη και αν η Εύα είχε παγιδεύσει τη γραμμή, δεν θα ήταν σε θέση να διαβιβάσει το μήνυμα, επειδή θα το έπνιγε ο θόρυβος. Η Εύα θα ήταν ανίκανη να διαχωρίσει το θόρυβο από το μήνυμα. Το μόνο άτομο που μπορεί να αφαιρέσει το θόρυβο και να διαβιβάσει το μήνυμα είναι η Αλίκη, επειδή είναι η μόνη που γνωρίζει τον ακριβή χαρακτήρα του θορύβου, αφού η ίδια τον έβαλε εκεί. Ο Έλις συνειδητοποίησε ότι με αυτόν τον τρόπο επιτυγχάνεται η ασφάλεια χωρίς να ανταλλαγεί κανένα κλειδί. Το κλειδί ήταν ο θόρυβος, και μόνο η Αλίκη χρειαζόταν να ξέρει τις λεπτομέρειες του θορύβου.

Είναι φανερό λοιπόν, ότι οι ιδέες του Έλις έμοιαζαν πολύ με τις αντίστοιχες των Ντίφι-Χέλμαν-Μέρκλε, με τη διαφορά ότι ο Έλις προηγείται αρκετά χρόνια. Ωστόσο κανείς δεν έμαθε ποτέ για τη δουλειά του, επειδή είχε δώσει όρκο εχεμύθειας. Στο τέλος του 1969, ο Έλις φαίνεται ότι είχε φτάσει στο αδιέξοδο που θα έφτανε η τριάδα του Στάνφορντ το 1975. Είχε αποδείξει στον εαυτό του ότι η κρυπτογραφία δημόσιου κλειδιού ήταν εφικτή, και είχε αναπτύξει την έννοια του διαχωρισμού δημόσιου και ιδιωτικού κλειδιού. Έπρεπε στη συνέχεια να βρει μια μονοσήμαντη συνάρτηση η οποία θα μπορούσε να αναστραφεί αν ο δέκτης είχε πρόσβαση σε μια ειδική πληροφορία. Δυστυχώς ο Έλις δεν ήταν μαθηματικός. Πειραματίστηκε με κάποιες μαθηματικές συναρτήσεις, γρήγορα όμως συνειδητοποίησε ότι δεν θα μπορούσε να προχωρήσει παραπέρα μόνος του.

Το Σεπτέμβριο του 1973, προστέθηκε ένας μαθηματικός, ο Κλίφορντ Κοκς. Ο Κοκς ανακάλυψε μια μαθηματική συνάρτηση που επέτρεπε την κρυπτογραφία δημόσιου κλειδιού αλλά παρέμενε η δυσκολία εφαρμογής του συστήματος. Η κρυπτογράφηση με τη μέθοδο αυτή απαιτεί πολύ μεγαλύτερη υπολογιστική ισχύ από ότι μέσω ενός συμμετρικού κρυπτογράμματος όπως το DES. Στις αρχές της δεκαετίας του 1970 οι υπολογιστές ήταν ακόμη σχετικά πρωτόγονοι και δεν μπορούσαν να εκτελέσουν τη διαδικασία της κρυπτογράφησης δημόσιου κλειδιού μέσα σε λογικά χρονικά πλαίσια. Κατά συνέπεια, το GCHQ δεν ήταν σε θέση να εκμεταλλευτεί την κρυπτογραφία δημόσιου κλειδιού.

Στα μέσα της δεκαετίας του 1980 το κλίμα στο GCHQ άρχισε να αλλάζει και η διοίκηση σκεφτόταν να ανακοινώσει τη συνεργασία των Έλις, Κοκς και Ουίλιαμσον. Τα μαθηματικά της κρυπτογραφίας δημόσιου κλειδιού είχαν ήδη καθιερωθεί στο δημόσιο τομέα και φαινόταν ότι δεν υπήρχε κανένας λόγος να

το κρατούν πλέον μυστικό και το 1987 ο Έλις συνέταξε ένα απόρρητο έγγραφο που κατέγραφε τη συμβολή του στην κρυπτογραφία δημόσιου κλειδιού και το οποίο περιλάμβανε τις σκέψεις του για τη μυστικότητα που τόσο συχνά περιβάλλει το κρυπτογραφικό έργο:

> *Η κρυπτογραφία είναι μια άκρως απόρρητη επιστήμη. Οι περισσότεροι επαγγελματίες επιστήμονες έχουν σα στόχο τους να είναι οι πρώτοι που θα δημοσιεύσουν την εργασία τους, γιατί το έργο τους αποκτά αξία μέσω της διάδοσης. Αντίθετα, κρυπτογραφία αποκτά τη μεγαλύτερη αξία όταν ελαχιστοποιούνται οι πληροφορίες που είναι διαθέσιμες στους πιθανούς εχθρούς. Έτσι οι επαγγελματίες κρυπτογράφοι συνήθως εργάζονται σε κλειστές κοινότητες, ώστε να διαθέτουν την επαγγελματική αλληλεπίδραση που είναι απαραίτητη για την ποιότητα του έργου τους, και παράλληλα να διατηρείται η μυστικότητα ως προς τα έξω. Η αποκάλυψη αυτών των μυστικών συνήθως επιτρέπεται, στο όνομα της ιστορικής ακρίβειας, μόνο όταν έχει αποδεχτεί ότι η συνέχιση της μυστικότητας δεν μπορεί πια να αποφέρει κανένα όφελος.*

## ΚΕΦΑΛΑΙΟ 3

### *3.1. Pretty good privacy (PGP)*

Στις αρχές της δεκαετίας του 1970, η ανταλλαγή ψηφιακών πληροφοριών είχε γίνει αναπόσπαστο μέρος της κοινωνίας μας. Το Διαδίκτυο, που ακόμη βρίσκεται στην παιδική του ηλικία, εξασφάλισε την υποδομή για την ανάπτυξη της ψηφιακής αγοράς και το ηλεκτρονικό εμπόριο ανθεί. Το χρήμα ρέει μέσω του κυβερνοχώρου και υπολογίζεται ότι καθημερινά το μισό Ακαθάριστο Εγχώριο Προιόν όλου του κόσμου ταξιδεύει μέσω του δικτύου SWIFT ( Society for Worldwide Interbank Financial Telecommunications = Εταιρία Παγκόσμιων Διατραπεζικών Οικονομικών Επικοινωνιών). Στο μέλλον, οι δημοκρατίες που ευνοούν τα δημοψηφίσματα θα αρχίσουν να εφαρμόζουν την ηλεκτρονική ψηφοφορία, και οι κυβερνήσεις θα χρησιμοποιούν το Διαδίκτυο για την καλύτερη διοίκηση ων χωρών τους, προσφέροντας υπηρεσίες όπως η ηλεκτρονική φορολογική δήλωση. Ωστόσο η επιτυχία της εποχής της πληροφορίας εξαρτάται από την ικανότητα προστασίας των πληροφοριών κατά την παγκόσμια ροή τους, και αυτό βασίζεται στην ισχύ της κρυπτογραφίας. Επί δυο χιλιάδες χρόνια, η κρυπτογράφηση ήταν σημαντική μόνο για τις κυβερνήσεις και τους στρατιωτικούς, σήμερα όμως έχει ένα νέο ρόλο να παίξει στη διευκόλυνση των επιχειρήσεων, και αύριο οι κοινοί άνθρωποι θα στηρίζονταν στην κρυπτογραφία για να προστατεύουν το ιδιωτικό τους απόρρητο. Η ανάπτυξη της κρυπτογραφίας δημόσιου κλειδιού, και ιδιαίτερα του κρυπτογράμματος RSA, έχει δώσει στους σημερινούς κρυπτογράφους σαφές πλεονέκτημα στον καθημερινό αγώνα τους με τους κρυπταναλυτές. Τα ο σημαντικότερο από όλα είναι το γεγονός ότι την κρυπτογραφία του δημόσιου κλειδιού δεν μπορεί να την εξασθενίσει κανένα πρόβλημα διανομής κλειδιών. Το RSA εγγυάται σχεδόν άθραυστες κλειδαριές για τις πιο πολύτιμες πληροφορίες.

Ωστόσο, όπως σε κάθε πτυχή της τεχνολογίας, έτσι και στην κρυπτογράφηση υπάρχει μια σκοτεινή πλευρά. Με τον ίδιο τρόπο που προστατεύει τις επικοινωνίες των νομοταγών πολιτών, η κρυπτογράφηση προστατεύει και τις επικοινωνίες των εγκληματιών και των τρομοκρατών. Σήμερα η αστυνομία χρησιμοποιεί παγίδευση των γραμμών ως μέσο συλλογής πληροφοριών σε σοβαρές περιπτώσεις, όπως το οργανωμένο έγκλημα και η τρομοκρατία, όμως αυτό θα ήταν αδύνατον αν οι κακοποιοί χρησιμοποιούσαν άθραυστα κρυπτογράμματα. Καθώς εισερχόμαστε στον εικοστό πρώτο αιώνα, το θεμελιώδες δίλλημα για την κρυπτογραφία είναι να βρει έναν τρόπο νε επιτρέπει στο κοινό και τους επιχειρηματίες να χρησιμοποιούν την κρυπτογράφηση ώστε να απολαμβάνουν τα οφέλη της Εποχής της πληροφορίας, χωρίς παράλληλα να επιτρέπει στους εγκληματίες να καταχωρούνται της κρυπτογράφησης και να διαφεύγουν τη σύλληψη. Σήμερα γίνεται μια έντονη συζήτηση για τον καλύτερο τρόπο επίλυσης του προβλήματος, και πηγή έμπνευσης αποτελεί σε μεγάλο βαθμό η ιστορία του Φιλ Ζίμερμαν, που επιχείρησε α ενθαρρύνει την ευρεία διάδοση της ισχυρής κρυπτογράφησης, σπέρνοντας τον πανικό στους ειδικούς των ΗΠΑ για θέματα ασφαλείας και απειλώντας την αποτελεσματικότητα της NSA με τον προυπολογισμό των δισεκατομμυρίων δολαρίων, με αποτέλεσμα να αποτελέσει αντικείμενο ομοσπονδιακής αστυνομικής και δικαστικής έρευνας. Κατά τον Ζίμερμαν υπάρχει μια θεμελιώδης διαφορά ανάμεσα στις ψηφιακές και τις παραδοσιακές επικοινωνίες, η οποία έχει σημαντικές επιπτώσεις για την ασφάλεια:

*Σήμερα το ηλεκτρονικό ταχυδρομείο βαθμιαία αντικαθιστά το συμβατικό και σύντομα θα είναι ο κανόνας για όλους, και όχι μια καινοτομία όπως είναι σήμερα. Αντίθετα με τις κλασικές επιστολές, τα ηλεκτρονικά μηνύματα είναι εξαιρετικά εύκολο να υποκλαπούν και σαρωθούν για ενδιαφέρουσες λέξεις-κλειδιά. Αυτό μπορεί να γίνει εύκολα, με διαδικασίες ρουτίνας, αυτόματα και χωρίς να εντοπιστεί σε ευρεία κλίμακα.*

Παρακάτω ακολουθεί ένα παράδειγμα για να γίνει κατανοητή παραστατικά η διαφορά ανάμεσα στο συμβατικό και το ηλεκτρονικό ταχυδρομείο.

Έστω ότι η Αλίκη θέλει να στείλει προσκλήσεις για το πάρτι γενεθλίων της, και ότι η Εύα που δεν έχει προσκληθεί, θέλει να μάθει το χρόνο και τον τόπο του πάρτι. Αν η Αλίκη χρησιμοποιήσει την παραδοσιακή μέθοδο ταχυδρόμησης των επιστολών, θα είναι πολύ δύσκολο για την Εύα να υποκλέψει μια από τις προσκλήσεις. Πρώτα πρώτα η Εύα δεν ξέρει σε ποιο σημείο εισήλθαν στο ταχυδρομικό

σύστημα οι προσκλήσεις, εφόσον η Αλίκη θα μπορούσε να χρησιμοποιήσει οποιοδήποτε ταχυδρομικό κουτί της πόλης. Η μόνη της ελπίδα να υποκλέψει μια πρόσκληση είναι να εντοπίσει με κάποιο τρόπο τη διεύθυνση ενός από τους φίλους της Αλίκης και να διεισδύσει στο τοπικό γραφείο διανομής. Στη συνέχεια θα πρέπει να ελέγξει μία προς μία όλες τις επιστολές με το χέρι. Αν κατορθώσει να βρει ένα γράμμα με αποστολέα την Αλίκη, θα πρέπει να το ανοίξει με τη μέθοδο του ατμού για να πάρει την πληροφορία που θέλει, και στη συνέχεια να το επαναφέρει στην αρχική του κατάσταση ώστε να αποφύγει οποιαδήποτε υποψία λαθροχειρίας.

Συγκριτικά, το έργο της Εύας γίνεται σαφώς ευκολότερο αν η Αλίκη στείλει τις επιστολές της με το ηλεκτρονικό ταχυδρομείο. Όταν τα μηνύματα θα φύγουν από τον υπολογιστή της Αλίκης θα πάνε σε ένα τοπικό σέρβερ, μια κεντρική πύλη εισόδου στο Διαδίκτυο. Αν η Εύα είναι αρκετά έξυπνη μπορεί να μπει στο στον τοπικό σέρβερ χωρίς να χρειαστεί να βγει από το σπίτι της. Οι προσκλήσεις θα έχουν γραμμένη την ηλεκτρονική διεύθυνση της Αλίκης και θα είναι πανεύκολο να ψάξει για ηλεκτρονικά μηνύματα με τη διεύθυνση αυτή. Από τη στιγμή που θα βρει μια πρόσκληση, εν χρειάζεται να βρει κανένα φάκελο, και έτσι μπορεί να τη διαβάσει χωρίς κανένα πρόβλημα. Επιπλέον, η πρόσκληση μπορεί να φτάσει στον προορισμό της χωρίς να δείχνει κανένα ίχνος υποκλοπής. Ωστόσο υπάρχει ένας τρόπος να εμποδιστεί η Εύα από το να διαβάσει τα μηνύματα της Αλίκης. Η κρυπτογράφηση.

Πάνω από εκατό εκατομμύρια ηλεκτρονικά μηνύματα στέλνονται καθημερινά σε όλο τον κόσμο, και όλα είναι ευάλωτα στην υποκλοπή. Η ψηφιακή τεχνολογία βοήθησε τις επικοινωνίες αλλά δημιούργησε και τη δυνατότητα παρακολούθησής τους. Κατά τον Ζίμερμαν, οι κρυπτογράφοι έχουν καθήκον να ενθαρρύνουν τν χρήση της κρυπτογράφησης και να προστατεύσουν με αυτόν τον τρόπο την ιδιωτική ζωή του κάθε ατόμου.

Θεωρητικά, όταν το 1977 επινοήθηκε το RSA πρόσφερε ένα αντίδοτο στο σενάριο του Μεγάλου Αδερφού, επειδή ο καθένας θα μπορούσε να δημιουργήσει το δικό του δημόσιο και ιδιωτικό κλειδί, και να στέλνει έτσι και να δέχεται απολύτως ασφαλή μηνύματα. Ωστόσο στην πράξη υπήρχε ένα μείζον πρόβλημα, επειδή η τότε διαδικασία κρυπτογράφησης με το RSA απαιτούσε μεγάλη υπολογιστική ισχύ σε σχέση με τις συμμετρικές μορφές κρυπτογράφησης όπως το DES. Κατά συνέπεια, τη δεκαετία του 1980 μόνο η κυβέρνηση ο στρατός και οι μεγάλες επιχειρήσεις διέθεταν ισχυρούς υπολογιστές ώστε να «τρέχουν» το RSA. Δεν είναι λοιπόν περίεργο που η RSA Data Security, Inc., η εταιρία που συστήθηκε για να διακινεί εμπορικά το RSA ,δημιουργούσε τα κρυπτογραφικά προιόντα της στοχεύοντας μόνο σε αυτές τις αγορές. Ο Ζίμερμαν αντίθετα πίστευε ότι όλοι έχουν το δικαίωμα της προστασίας του ιδιωτικού απορρήτου την οποί πρόσφερε η κρυπτογράφηση με το RSA, και διοχέτευε τον πολιτικό του ζήλο στη δημιουργία ενός προιόντος που θα βασιζόταν στο RSA αλλά θα απευθυνόταν στις μάζες. Ήθελε η δική του εκδοχή του RSA να διαθέτει χειρισμό ιδιαίτερα φιλικό προς το χρήστη, ώστε να μην χρειάζεται ο τελευταίος να έχει ειδικές κρυπτογραφικές γνώσεις. Το σχέδιό του το ονόμασε Pretty Good Privacy (Άριστη Προστασία Ιδιωτικού Απορρήτου), ή συντομογραφικά PGP. Στα τέλη της δεκαετίας του 1980, ολοκλήρωσε το κρυπτογραφικό του λογισμικό. Ο κύριος στόχος του ήταν να επιταχύνει την κρυπτογράφηση με το RSA. Κανονικά, όταν η Αλίκη θέλει να χρησιμοποιήσει το RSA για να κρυπτογραφήσει ένα μήνυμα προς τον Μπομπ, βρίσκει στον κατάλογο το δημόσιο κλειδί του και στη συνέχεια εφαρμόζει στο μήνυμα τη μονοσήμαντη συνάρτηση του RSA. Αντίστοιχα ο Μπομπ αποκρυπτογραφεί το κρυπτογραφικό κείμενο χρησιμοποιώντας το ιδιωτικό του κλειδί για να αναστρέψει τη μονοσήμαντη συνάρτηση του RSA. Και οι δυο διαδικασίες απαιτούν σημαντικούς υπολογισμούς, και αν το μήνυμα είναι εκτενές, κρυπτογράφηση και η αποκρυπτογράφησή του με έναν προσωπικό υπολογιστή μπορεί να πάρει αρκετά λεπτά. Για να επιταχύνει την κρυπτογράφηση και από κρυπτογράφηση, ο Ζίμερμαν κατέφυγε σε ένα προσφυές τέχνασμα, που χρησιμοποιούσε την ασύμμετρη κρυπτογράφηση RSA σε συνδυασμό με την παραδοσιακή συμμετρική κρυπτογράφηση. Η δεύτερη μπορεί να είναι εξίσου ασφαλής με την πρώτη, και γίνεται πολύ πιο γρήγορα, όμως πάσχει ως προς τη διανομή του κλειδιού, το οποίο μπορεί να διαβιβαστεί με ασφάλεια από τον αποστολέα στον παραλήπτη. Ο Ζίμερμαν φαντάστηκε το παρακάτω σενάριο. Αν η Αλίκη θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον Μπομπ, το πρώτο πράγμα που κάνει είναι να το κρυπτογραφήσει με ένα συμμετρικό κρυπτόγραμμα. Ο Ζίμερμαν πρότεινε τη χρήση του IDEA, ενός κρυπτογράμματος όμοιου με το DES. Για να κρυπτογραφήσει με το IDEA, η Αλίκη πρέπει να διαλέξει ένα κλειδί, αλλά για να μπορέσει ο Μπομπ να αποκρυπτογραφήσει το μήνυμα, θα πρέπει εκείνη να του στείλει με κάποιο τρόπο το κλειδί. Η Αλίκη βρίσκει στον κατάλογο το δημόσιο κλειδί RSA του Μπομπ και στη συνέχεια το χρησιμοποιεί για να κρυπτογραφήσει το κλειδί

IDEA. Έτσι τελικά η Αλίκη στέλνει στον Μπομπ το μήνυμα κρυπτογραφημένο με το συμμετρικό κρυπτόγραμμα IDEA και το κλειδί IDEA κρυπτογραφημένο με το ασύμμετρο κρυπτόγραμμα RSA. Ο Μπομπ χρησιμοποιεί το ιδιωτικό του κλειδί RSA για να αποκρυπτογραφήσει το κλειδί IDEA και στη συνέχεια χρησιμοποιεί το κλειδί IDEA για να αποκρυπτογραφήσει το μήνυμα. Όλο αυτό μπορεί να φαίνεται περίπλοκο, όμως το πλεονέκτημα είναι ότι το μήνυμα, που μπορεί να περιέχει μεγάλη ποσότητα πληροφοριών κρυπτογραφείται με ένα γρήγορο συμμετρικό κρυπτόγραμμα, και μόνο το συμμετρικό κλειδί IDEA, που αποτελείται από σχετικά μικρή ποσότητα πληροφοριών κρυπτογραφείται με ένα αργό ασύμμετρο κρυπτόγραμμα. Ο Ζίμερμαν ενσωμάτωσε στο PGP, μια σειρά από χρήσιμα χαρακτηριστικά. Για παράδειγμα η Αλίκη, πριν χρησιμοποιήσει τη συνιστώσα RSA του PGP, πρέπει να δημιουργήσει το δικό της δημόσιο και ιδιωτικό κλειδί. Η παραγωγή κλειδιών δεν είναι εύκολη, γιατί απαιτεί να βρεις δύο δυο τεράστιους πρώτους αριθμούς. Ωστόσο, η Αλίκη δεν έχει παρά να κουνήσει ακανόνιστα το ποντίκι του υπολογιστή της, και το πρόγραμμα PGP θα προχωρήσει στη δημιουργία των δυο κλειδιών της, του δημόσιου και του ιδιωτικού- οι κινήσεις του ποντικιού εισάγουν έναν τυχαίο παράγοντα τον οποίο χρησιμοποιεί το PGP για να εξασφαλίσει ότι κάθε χρήστης έχει το δικό του, ξεχωριστό ζευγάρι πρώτων αριθμών, και επομένως το δικό του δημόσιο και ιδιωτικό κλειδί. Μετά από αυτό, το μόνο που έχει να κάνει η Αλίκη είναι να ανακοινώσει το δημόσιο κλειδί της.

Μια άλλη χρήσιμη πτυχή του PGP είναι η δυνατότητα ψηφιακής υπογραφής των ηλεκτρονικών μηνυμάτων. Έστω για παράδειγμα ότι μια τράπεζα λαβαίνει ένα ηλεκτρονικό μήνυμα από έναν πελάτη, με την εντολή όλες του οι καταθέσεις να μεταφερθούν σε έναν ιδιωτικό τραπεζικό λογαριασμό σε μια άλλη χώρα. Σε αυτήν την περίπτωση, χωρίς ιδιόχειρη υπογραφή η τράπεζα δεν μπορεί να ξέρει ότι το ηλεκτρονικό μήνυμα είναι όντως από τον πελάτη. Κάλλιστα θα μπορούσε να το έχει γράψει ένας κακοποιός, επιχειρώντας να μεταφέρει τα χρήματα στο δικό του λογαριασμό. Για να εδραιωθεί η εμπιστοσύνη στο Διαδίκτυο, είναι απαραίτητο να υπάρχει κάποια αξιόπιστη μορφή ψηφιακής υπογραφής. Η ψηφιακή υπογραφή PGP βασίζεται σε μια αρχή που πρώτοι ανέπτυξαν οι Ουίτφιλντ και Μάρτιν Χέλμαν.

Το κρυπτόγραμμα IDEA χρησιμοποιείται για την κρυπτογράφηση του μηνύματος, το RSA χρησιμοποιείται για την κρυπτογράφηση του κλειδιού IDEA, και αν απαιτείται ψηφιακή υπογραφή, πρέπει να ενσωματωθεί ακόμα ένα στάδιο κρυπτογράφησης. Ωστόσο ο Ζίμερμαν σχεδίασε το προιόν του με τρόπο που να κάνει τα πάντα αυτόματα έτσι ώστε να μην απαιτείται γνώση ανώτατων μαθηματικών.

Για να στείλει κάποιος ένα μήνυμα δεν έχει παρά να γράψει το ηλεκτρονικό του γράμμα και να επιλέξει το PGP από ένα μενού επιλογών στην οθόνη του υπολογιστή του. Στη συνέχεια πληκτρολογεί το όνομα του παραλήπτη και το PGP βρίσκει το δημόσιο κλειδί του παραλήπτη και αυτόματα εκτελεί όλη τη διαδικασία της κρυπτογράφησης ενώ ταυτόχρονα κάνει όλα όσα χρειάζονται για την ψηφιακή υπογραφή του μηνύματος. Όταν λάβει το κρυπτογραφημένο μήνυμα ο παραλήπτης επιλέγει το PGP, και αυτό αποκρυπτογραφεί το μήνυμα και πιστοποιεί την ταυτότητα του συντάκτη. Στο PGP δεν υπήρχε τίποτα πρωτότυπο καθώς οι Ντίφι και Χέλμαν είχαν ήδη σκεφτεί για τις ψηφιακές υπογραφές και άλλοι κρυπτογράφοι είχαν χρησιμοποιήσει ένα συνδυασμό συμμετρικών και ασύμμετρων κρυπτογραμμάτων για να επιταχύνουν την κρυπτογράφηση, όμως ο Ζίμερμαν ήταν ο πρώτος που τα ενσωμάτωσε όλα αυτά σε ένα εύχρηστο πρόγραμμα κρυπτογράφησης το οποίο μπορούσε να «τρέξει» σε έναν μέτριας ισχύος προσωπικό υπολογιστή. Το καλοκαίρι του 1991 ο Ζίμερμαν ήταν έτοιμος να μετατρέψει το PGP σε ολοκληρωμένο εμπορικό προιόν. Τα μόνα προβλήματα που έμεναν ήταν το γεγονός ότι το RSA που αποτελούσε την καρδιά του PGP ήταν πατενταρισμένο προιόν, και ο νόμος περί ευρεσιτεχνίας υποχρέωνε τον Ζίμερμαν πριν κυκλοφορήσει το PGP να πάρει άδεια από την RSA Data Security, Inc., αλλά και το νομοσχέδιο κατά του εγκλήματος που είχε κατατεθεί στην αμερικανική Γερουσία το 1991. Λόγω της ανησυχίας της Γερουσίας μήπως οι εξελίξεις στην ψηφιακή τεχνολογία όπως καταλήξουν να εμποδίζουν τις δυνάμεις επιβολής του νόμου να πραγματοποιούν αποτελεσματικές παγιδεύσεις γραμμών, το νομοσχέδιο υποχρέωνε τις εταιρίες να εγγυώνται τη δυνατότητα παγίδευσης γραμμών αλλά και απειλούσε κάθε μορφή ασφαλούς κρυπτογράφησης. Η συντονισμένη δράση της RSA, της βιομηχανίας των επικοινωνιών και των ομάδων υπεράσπισης των ατομικών ελευθεριών, οδήγησε στην απάλειψη της επίμαχης ρήτρας, όμως όλοι συμφωνούσαν ότι επρόκειτο για μια πρόσκαιρη ανάπαυλα.

Αντί λοιπόν ο Ζίμερμαν να περιμένει, με κίνδυνο να απαγορευτεί το PGP από την κυβέρνηση, αποφάσισε ότι προείχε να γίνει το κρυπτόγραμμα προσιτό σε όλους πριν είναι πολύ αργά. Έτσι τον

Ιούνιο του 1991 ζήτησε από ένα φίλο του να «κολλήσει» το PGP στον ηλεκτρονικό πίνακα ανακοινώσεων του Usenet. Το PGP δεν είναι παρά ένα λογισμικό, και έτσι από τον πίνακα ανακοινώσεων θα μπορούσε ο οποιοσδήποτε να το κατεβάσει δωρεάν στο σύστημά του. Το PGP κυκλοφορούσε πλέον ελεύθερα στο Διαδίκτυο. Το PGP προκάλεσε αναταραχή μόνο στους φανατικούς της κρυπτογραφίας. Αργότερα άρχισαν να το κατεβάζουν και άτομα από ένα ευρύτερο φάσμα χρηστών του Διαδικτύου. Στη συνέχεια, τα περιοδικά των υπολογιστών δημοσίευαν σύντομες αναφορές, και μετά ολοσέλιδα άρθρα για το φαινόμενο PGP. Σταδιακά, το PGP άρχισε να διεισδύει στις πιο απομακρυσμένες γωνίες της ψηφιακής κοινότητας. Ενώ ο Ζίμερμαν κέρδιζε θαυμαστές σε όλο τον κόσμο, στην ίδια την Αμερική είχε γίνει στόχος κριτικής. Η RSA Data Security Inc., αποφάσισε να μην χορηγήσει στον Ζίμερμαν άδεια ελεύθερης χρήσης, και ήταν έξαλλη με την παραβίαση της ευρεσιτεχνίας της. Παρότι ο Ζίμερμαν κυκλοφόρησε το PGP ως ελεύθερο λογισμικό, αυτό περιείχε το σύστημα κρυπτογραφίας δημόσιου κλειδιού RSA, με συνέπεια η RSA να το χαρακτηρίσει «πειρατικό» λογισμικό ( banditware ). Ο Ζίμερμαν κατηγορείτο για παράνομο εμπόριο όπλων, εφόσον είχε εξαγάγει το PGP μέσω του Διαδικτύου. Στη διάρκεια των τριών επόμενων ετών, ο Ζίμερμαν υποβλήθηκε σε ομοσπονδιακή δικαστική έρευνα και βρέθηκε καταδιωκόμενος από το FBI.

Η έρευνα σε σχέση με τον Ζίμερμαν πυροδότησε μια διαμάχη με αντικείμενο τις θετικές και τις αρνητικές συνέπειες της κρυπτογράφησης στην Εποχή της πληροφορίας. Από τη μία πλευρά ήταν αυτοί που πίστευαν ότι η διαδεδομένη χρήση της ασφαλούς κρυπτογράφησης θα ήταν ευλογία για την κοινωνία εφόσον θα διασφάλιζε στα άτομα το απόρρητο των ιδιωτικών τους ψηφιακών επικοινωνιών. Εναντίον τους τάσσονταν εκείνοι που θεωρούσαν την κρυπτογράφηση απειλή για την κοινωνία, επειδή οι εγκληματίες και οι τρομοκράτες θα μπορούσαν να επικοινωνούν μυστικά, ασφαλείς από την αστυνομική παρακολούθηση. Η διαμάχη συνεχίστηκε σε όλη τη διάρκεια της δεκαετίας του 1990, και σήμερα παραμένει εξίσου έντονη. Το θεμελιώδες ερώτημα είναι αν οι κυβερνήσεις θα πρέπει ή όχι να θεσπίσουν νόμους κατά της κρυπτογραφίας. Η κρυπτογραφική ελευθερία θα παρείχε στους πάντες, περιλαμβανομένων και των κακοποιών, τη βεβαιότητα ότι η ηλεκτρονική τους αλληλογραφία είναι ασφαλής. Από την άλλη ο περιορισμός της χρήσης της κρυπτογραφίας θα επέτρεπε στην αστυνομία να παρακολουθεί τους εγκληματίες, αλλά και το μέσο πολίτη.

Το παρακάτω κομμάτι είναι αφιερωμένο στη σκιαγράφηση των δύο πόλων της διαμάχης. Ένα μεγάλο μέρος θα έχει ως σημείο αναφοράς την πολιτική και τους πολιτικούς της Αμερικής, εν μέρει επειδή είναι πατρίδα του PGP, γύρω από το οποίο επικεντρώθηκε κυρίως η διαμάχη και εν μέρει επειδή όποια πολιτική υιοθετηθεί στην Αμερική θα έχει αντίκτυπο στις πολιτικές ανά τον κόσμο.

Τα επιχειρήματα που προβάλουν κατά της ευρείας διάδοσης της κρυπτογραφίας οι επιφορτισμένοι με την εφαρμογή του νόμου επικεντρώνονται στην επιθυμία διατήρησης της ισχύουσας ισορροπίας. Επί δεκαετίες η αστυνομία σε όλο τον κόσμο πραγματοποιούσε νόμιμες παγιδεύσεις τηλεφωνικών γραμμών για να συλλαμβάνει τους εγκληματίες. Η αντίληψη ότι οι τηλεφωνικές παγιδεύσεις αποτελούν απαραίτητο εργαλείο του νόμου εδραιώθηκε στα τέλη της δεκαετίας του 1960, όταν το FBI συνειδητοποίησε ότι το οργανωμένο έγκλημα απειλούσε όλο και περισσότερο το έθνος. Αυτοί που καλούνταν να επιβάλλουν το νόμο αντιμετώπιζαν μεγάλη δυσκολία στο να καταδικάσουν τους υπόπτους, επειδή η μαφία απειλούσε όλους τους εν δυνάμει μάρτυρες κατηγορίας, και επιπλέον υπήρχε ο κώδικας της σιωπής. Η αστυνομία θεώρησε ότι η μοναδική της ελπίδα ήταν η συγκέντρωση αποδείξεων μέσω των τηλεφωνικών παγιδεύσεων, και το Συμβούλιο της Επικρατείας έβλεπε με συμπάθεια αυτό το επιχείρημα. Το 1967 αποφάσισε ότι η αστυνομία μπορούσε να καταφεύγει σε τηλεφωνικές παγιδεύσεις, με τον όρο να έχει προηγουμένως εξασφαλίσει δικαστικό ένταλμα. Είκοσι χρόνια αργότερα, το εξακολουθεί να υποστηρίζει ότι η τηλεφωνική παγίδευση με δικαστική εντολή είναι η πιο αποτελεσματική τεχνική που διαθέτουν οι δυνάμεις του νόμου για την καταπολέμηση των παράνομων ναρκωτικών, της τρομοκρατίας, της εγκληματικής βίας, της κατασκοπείας κα του οργανωμένου εγκλήματος. Όμως οι τηλεφωνικές παγιδεύσεις της αστυνομίας θα ήταν άχρηστες αν οι κακοποιοί αποκτούσαν πρόσβαση στην κρυπτογράφηση. Μια τηλεφωνική κλήση σε ψηφιακή γραμμή δεν είναι παρά μια ροή αριθμών, και μπορεί να κρυπτογραφηθεί με τις ίδιες τεχνικές που χρησιμοποιούνται για την κρυπτογράφηση των ηλεκτρονικών μηνυμάτων. Το PGPfone, για παράδειγμα είναι από τα πολλά προιόντα τα οποία μπορούν να κρυπτογραφούν τις προφορικές επικοινωνίες που γίνονται μέσω Διαδικτύου. Οι επιφορτιζόμενοι με την εφαρμογή του νόμου υποστηρίζουν ότι οι αποτελεσματικές τηλεφωνικές παγιδεύσεις είναι απαραίτητες για τη διατήρηση του νόμου και της τάξης, και ότι θα πρέπει να τεθούν περιορισμοί στην κρυπτογράφηση, ώστε να συνεχίζουν οι

υποκλοπές τους. Η αστυνομία έχει ήδη συναντήσει κακοποιούς που χρησιμοποιούν ισχυρή κρυπτογράφηση για να προστατεύονται. Ένας αξιωματούχος του Λευκού Οίκου διαπίστωσε μια εξίσου ανησυχητική τάση στην Αμερική, αποκαλύπτοντας ότι τα μέλη του οργανωμένου εγκλήματος συγκαταλέγονται ανάμεσα στους πιο προχωρημένους χρήστες των συστημάτων υπολογιστών και της ισχυρής κρυπτογράφησης. Οι υπεύθυνοι για την εφαρμογή του νόμου φοβούνται ότι ο συνδυασμός Διαδικτύου και κρυπτογραφίας θα επιτρέπει στους κακοποιούς να επικοινωνούν και να συντονίζουν τις ενέργειές τους, ενώ ανησυχούν ιδιαίτερα για τους Τέσσερις Ιππότες της Πληροφορικής Αποκάλυψης, δηλαδή τις τέσσερις ομάδες που θα ωφεληθούν τα μέγιστα από την κρυπτογράφηση : έμποροι ναρκωτικών, οργανωμένο έγκλημα, τρομοκράτες και παιδόφιλοι. Κακοποιοί και τρομοκράτες δεν κρυπτογραφούν μόνο τις επικοινωνίες τους αλλά και τα σχέδια και τα αρχεία τους, παρεμποδίζοντας τη συλλογή αποδεικτικών στοιχείων.

Μια μελέτη την οποία ολοκλήρωσαν το 1997 οι Ντόροθι Ντένινγκ και Ουίλιαμ Μπόου, για λογαριασμό της Ομάδας Εργασίας για το οργανωμένο έγκλημα του Αμερικανικού Κέντρου Εθνικών Στρατηγικών πληροφοριών, κατέληξε στην εκτίμηση ότι σε πεντακόσιες εγκληματικές υποθέσεις παγκοσμίως υπεισέρχεται η κρυπτογράφηση, και προέβλεψε ότι ο αριθμός αυτός θα διπλασιάζεται κάθε χρόνο. Πέρα όμως από την εσωτερική αστυνόμευση, ανακύπτουν και ζητήματα εθνικής ασφάλειας. Η NSA είναι επιφορτισμένη με τη συλλογή πληροφοριών για τους εχθρούς του έθνους μέσω της αποκρυπτογράφησης των επικοινωνιών τους. Για το σκοπό αυτό διαθέτει ένα παγκόσμιο δίκτυο σταθμών ακρόασης, σε συνεργασία με τη Βρετανία την Αυστραλία, τον Καναδά και τη Νέα Ζηλανδία. Το δίκτυο περιλαμβάνει τοποθεσίες όπως η βάση παρακολούθησης σημάτων Μένγουιθ Χιλστο Γιορκσαιρ, που αποτελεί τον μεγαλύτερο κατασκοπευτικό σταθμό στον κόσμο. Ένα μέρος των δραστηριοτήτων αυτού τους σταθμού χρησιμοποιεί το σύστημα Έσελον, που έχει τη δυνατότητα να σαρώνει ηλεκτρονικά μηνύματα, φαξ, τηλέτυπα και τηλεφωνικές κλήσεις, αναζητώντας συγκεκριμένες λέξεις. Το Έσελον λειτουργεί με βάση ένα λεξικό ύποπτων λέξεων, και είναι αρκετά έξυπνο ώστε να τις αναγνωρίζει αμέσως. Το Έσελον θα ήτα ουσιαστικά άχρηστο αν όλα τα μηνύματα ήταν κρυπτογραφημένα με ισχυρή κρυπτογράφηση. Οι χώρες που μετέχουν στο Έσελν θα έχαναν πολύτιμες πληροφορίες για πολιτικές συνομωσίες και τρομοκρατικές επιθέσεις.

Στην αντιπέρα όχθη της διαμάχης βρίσκονται οι υπέρμαχοι των ατομικών ελευθεριών, που περιλαμβάνουν ομάδες όπως το κέντρο για τη Δημοκρατία και την Τεχνολογία και το Ίδρυμα Ηλεκτρονικών Συνόρων. Τα επιχειρήματα των υπερασπιστών της κρυπτογράφησης στηρίζονται στην πεποίθηση ότι το ιδιωτικό απόρρητο αποτελεί θεμελιώδες ανθρώπινο δικαίωμα, όπως αναγνωρίζεται από το Άρθρο 12 της Παγκόσμιας Διακήρυξης των Ανθρωπίνων Δικαιωμάτων. Οι υπέρμαχοι των ατομικών ελευθεριών υποστηρίζουν ότι η κρυπτογράφηση είναι απαραίτητη για τη διασφάλιση του δικαιώματος στο ιδιωτικό απόρρητο. Διαφορετικά φοβούνται ότι η έλευση της ψηφιακής τεχνολογίας, που διευκολύνει την παρακολούθηση, θα εγκαινιάσει μια νέα εποχή παγιδεύσεων των επικοινωνιών, με όλες τις καταχρήσεις που αναπόφευκτα συνεπάγεται κάτι τέτοιο. Μια από τις γνωστότερες υποθέσεις συνεχούς και αδικαιολόγητης τηλεφωνικής παγίδευσης αφορά στον Μάρτιν Λούθερ Κινγκ τον Νεότερο, του οποίου οι τηλεφωνικές συνδιαλέξεις παρακολουθούνταν επί σειρά ετών. Το FBI συγκέντρωνε πληροφορίες για την προσωπική του ζωή οι οπόίες χρησιμοποιούνταν για να τον μειώσουν ηθικά.

Και άλλες όμως κυβερνήσεις είναι εξίσου ένοχες για κατάχρηση των τηλεφωνικών παγιδεύσεων. Η γαλλική Εθνική Επιτροπή Ελέγχου των Υποκλοπών Ασφαλείας εκτιμά ότι στη Γαλλία διενεργούνται κάθε χρόνο περίπου 100.000 παράνομες τηλεφωνικές παγιδεύσεις. Η μεγαλύτερη ίσως παραβίαση του ιδιωτικού απορρήτου όλων των πολιτών είναι το διεθνές πρόγραμμα Έσελον. Το Έσελον δεν είναι υποχρεωμένο να δικαιολογεί τις υποκλοπές του, και δεν εστιάζεται σε συγκεκριμένα άτομα. Αντ' αυτού, συλλέγει πληροφορίες αδιακρίτως, χρησιμοποιώντας δέκτες που ανιχνεύουν τις επικοινωνίες μέσω δορυφόρων. Όταν οι υπεύθυνοι για την επιβολή του νόμου προβάλλουν το επιχείρημα ότι η ισχυρή κρυπτογράφηση θα μειώσει τις καταδίκες εγκληματιών, οι υπέρμαχοι των ατομικών ελευθεριών απαντούν ότι το ζήτημα του ιδιωτικού απορρήτου είναι πιο σημαντικό, και επιμένουν ότι ούτως ή άλλως, η κρυπτογράφηση δεν πρόκειται να αποτελέσει τεράστιο εμπόδιο για την επιβολή του νόμου, εφόσον στις περισσότερες περιπτώσεις οι τηλεφωνικές παγιδεύσεις δεν είναι καίριο στοιχείο. Για παράδειγμα, το 1994 σε όλη την Αμερική, επί συνόλου 250.000 ομοσπονδιακών διώξεων, μόνο σε χίλιες περίπου περιπτώσεις υπήρξαν τηλεφωνικές παγιδεύσεις με δικαστική εντολή. Μεταξύ των υποστηρικτών της κρυπτογραφικής ελευθερίας συγκαταλέγονται, όπως ήταν αναμενόμενο, και

κάποιοι από τους εφευρέτες της κρυπτογραφίας δημόσιου κλειδιού. Ο Ουίτφιλντ Ντίφι δηλώνει ότι στο μεγαλύτερο μέρος της Ιστορίας, τα άτομα απολάμβαναν πλήρους προστασίας του ιδιωτικού τους απορρήτου.

Οι μεγαλύτεροι ίσως σύμμαχοι της φιλελεύθερης πλευράς είναι οι μεγάλες εταιρίες. Τα εμπόριο μέσω Διαδικτύου βρίσκεται ακόμη στα σπάργανα, αλλά οι πωλήσεις αυξάνουν ταχύτατα, με τη βιομηχανία των βιβλίων, των μουσικών cd και του λογισμικού να ανοίγει το δρόμο, και τα σουπερμάρκετ, τα πρακτορεία ταξιδιών και άλλες επιχειρήσεις να ακολουθούν καταπόδας. Το 1998, ένα εκατομμύριο Βρετανοί χρησιμοποίησαν το Διαδίκτυο για να αγοράσουν προιόντα αξίας 400 εκατομμυρίων λιρών. Σε λίγα μόλις χρόνια από σήμερα, το εμπόριο μέσω του Διαδικτύου ίσως να κυριαρχεί στην αγορά, με την προυπόθεση όμως να μπορέσουν οι επιχειρήσεις να αντιμετωπίσουν το ζήτημα της ασφάλειας και της εμπιστοσύνης.

Μια επιχείρηση πρέπει να είναι σε θέση να εγγυάται τη μυστικότητα και την ασφάλεια των οικονομικών συναλλαγών, και ο μόνος τρόπος να γίνει αυτό είναι η χρήση ισχυρής κρυπτογράφησης. Προς το παρόν, μια αγορά στο Διαδίκτυο μπορεί να διασφαλιστεί με την κρυπτογραφία δημόσιου κλειδιού. Ως συνήθως η ασφάλεια της κρυπτογράφησης εξαρτάται από το μέγεθος του κλειδιού. Στην Αμερική δεν υπάρχουν περιορισμοί στο μέγεθος του κλειδιού, όμως οι αμερικανικές εταιρίες λογισμικού ακόμη απαγορεύεται να εξάγουν προϊόντα δικτύου που παρέχουν ασφαλή κρυπτογράφηση. Κατά συνέπεια, οι πλοηγοί δικτύου που εξάγονται στον υπόλοιπο κόσμο μπορούν να χειρίζονται μόνο μικρά κλειδιά, και έτσι παρέχουν μέτρια μόνο ασφάλεια. Ωστόσο όσο αυξάνει ο όγκος των χρημάτων που ρέουν μέσω του Διαδικτύου, κάποια στιγμή θα είναι επικερδές για τους κακοποιούς το να αποκρυπτογραφούν στοιχεία πιστωτικών καρτών. Με δύο λόγια, για να ανθίσει το εμπόριο μέσω του Διαδικτύου θα πρέπει οι καταναλωτές σε όλο τον κόσμο να διαθέτουν πραγματική ασφάλεια, και οι επιχειρήσεις δεν θα ανεχθούν κολοβωμένη κρυπτογράφηση. Οι επιχειρήσεις επιθυμούν ισχυρή κρυπτογράφηση και για έναν επιπρόσθετο λόγο. Οι εταιρίες αποθηκεύουν σε ηλεκτρονικές βάσεις δεδομένων τεράστιο όγκο πληροφοριών, όπου περιλαμβάνονται περιγραφές προϊόντων, στοιχεία των πελατών και τραπεζικοί λογαριασμοί. Όπως είναι φυσικό, οι εταιρίες θέλουν να προστατεύσουν τις πληροφορίες αυτές από τους χάκερς που θα μπορούσαν να παρεισφρήσουν στους υπολογιστές και να τις κλέψουν. Η προστασία αυτή μπορεί να επιτευχθεί με την κρυπτογράφηση των αποθηκευμένων πληροφοριών, ώστε να είναι προσιτές μόνο στους υπαλλήλους που κατέχουν το κλειδί της αποκρυπτογράφησης.

Συνοψίζοντας την κατάσταση, είναι σαφές ότι ο αγώνας διεξάγεται μεταξύ δύο στρατοπέδων: οι υπέρμαχοι των ατομικών ελευθεριών και οι επιχειρήσεις είναι υπέρ της ισχυρής κρυπτογράφησης, ενώ οι υπεύθυνοι για την επιβολή του νόμου υπέρ των αυστηρών περιορισμών. Γενικά η κοινή γνώμη φαίνεται να κλίνει υπέρ της φιλοκρυπτογραφικής συμμαχίας, την οποία ενίσχυσαν κάποια φιλικά μέσα ενημέρωσης.

Ενώ η φιλοκρυπτογραφική παράταξη μάχεται για την κρυπτογραφική ελευθερία και η αντικρυπτογραφική υπεραμύνεται των κρυπτογραφικών περιορισμών, υπάρχει και μια Τρίτη επιλογή που θα μπορούσε να οδηγήσει σε μια συμβατική λύση. Τη δεκαετία του 1980, οι κρυπτογράφοι και οι κυβερνητικές αρχές διερευνούσαν τα υπέρ και τα κατά ενός σχήματος γνωστού ως «παρακαταθήκη κλειδιού». Ο όρος παρακαταθήκη συνήθως αναφέρεται σε μια ρύθμιση όπου κάποιος εμπιστεύεται ένα χρηματικό ποσό σε μια Τρίτη πλευρά, η οποία στη συνέχεια μπορεί να το παραδώσει σε μια δεύτερη πλευρά κάτω από ορισμένες συνθήκες. Για παράδειγμα, ένας ενοικιαστής γης μπορεί να καταθέσει προς φύλαξη ένα ποσό σε έναν δημοσιογράφο, ο οποίος μπορεί να το παραδώσει στο γαιοκτήμονα σε περίπτωση βλάβης της ιδιοκτησίας του. Στο χώρο της κρυπτογραφίας, ο όρος σημαίνει ότι η Αλίκη καταθέτει ως παρακαταθήκη ένα αντίγραφο του ιδιωτικού κλειδιού της σε έναν ανεξάρτητο, αξιόπιστο μεσολαβητή, ο οποίος είναι εξουσιοδοτημένος να το παραδώσει στην αστυνομία, αν υπάρξουν επαρκή τεκμήρια ότι η Αλίκη ενεπλάκη σε εγκληματική ενέργεια. Η πιο διάσημη δοκιμή του κρυπτογραφικού συστήματος παρακαταθήκης κλειδιού ήταν το AEES (American Escrowed Encryption Standard (Αμερικανικό Μέτρο Κρυπτογράφησης Παρακαταθήκης), που υιοθετήθηκε το 1994. Στόχος ήταν να ενθαρρυνθεί η υιοθέτηση δύο συστημάτων κρυπτογράφησης στις τηλεφωνικές επικοινωνίες μέσω υπολογιστή, με τις ονομασίες, αντίστοιχα, clipper (ισοσταθμιστής) και capstone (επιστέγασμα). Για να χρησιμοποιήσει την κρυπτογραφία τύπου clipper, η Αλίκη θα έπρεπε να αγοράσει μια τηλεφωνική συσκευή με ένα προεγκατεστημένο κύκλωμα το οποίο θα περιείχε τα στοιχεία του μυστικού ιδιωτικού της κλειδιού. Την ίδια στιγμή που θα αγόραζε την ειδική αυτή συσκευή, ένα αντίγραφο του ιδιωτικού

κλειδιού θα χωριζόταν σε δυο ίσα μέρη, το καθένα από τα οποία θα διαβιβαζόταν σε δυο διαφορετικές ομοσπονδιακές αρχές για αποθήκευση. Η αμερικανική κυβέρνηση υποστήριζε ότι η Αλίκη θα είχε πρόσβαση σε ασφαλή κρυπτογράφηση, και το ιδιωτικό της απόρρητο θα παραβιαζόταν μόνο αν οι υπεύθυνοι για τν επιβολή του νόμου ήταν σε θέση να πείσουν και τις δυο ομοσπονδιακές αρχές ότι υπήρχε νομική βάση για να αποκτήσουν το υπό παρακαταθήκη ιδιωτικό της κλειδί. Η αμερικανική κυβέρνηση χρησιμοποιούσε τα συστήματα clipper και capstone για τις δικές της επικοινωνίες και υποχρέωσε τις εταιρίες που εμπλέκονταν σε κυβερνητικές επιχειρήσεις να υιοθετήσουν το AEES. Οι υπόλοιπες επιχειρήσεις και οι ιδιώτες ήταν ελεύθεροι να χρησιμοποιούν άλλες μορφές κρυπτογράφησης, όμως η κυβέρνηση πίστευε ότι το AEES θα γινόταν βαθμιαία ο αγαπημένος τύπος κρυπτογράφησης του έθνους. Ωστόσο, η πολιτική αυτή δεν τελεσφόρησε. Η ιδέα της παρακαταθήκης κλειδιού κέρδισε ελάχιστους υποστηρικτές εκτός της κυβέρνησης. Στους υπέρμαχους των ατομικών ελευθεριών δεν άρεσε η ιδέα του να κατέχουν οι ομοσπονδιακές αρχές τα κρυπτογραφικά κλειδιά του κάθε πολίτη. Οι ειδικοί της κρυπτογραφίας επισήμαιναν ότι αρκούσε ένας και μόνο διεφθαρμένος υπάλληλος για να υπονομεύσει όλο το σύστημα, πουλώντας τα υπό παρακαταθήκη κλειδιά στο μεγαλύτερο πλειοδότη. Τέλος, οι επιχειρήσεις ανησυχούσαν για το θέμα του απορρήτου. Για παράδειγμα, μια ευρωπαϊκή επιχείρηση στην Αμερική ίσως να φοβόταν ότι τα μηνύματά της θα μπορούσαν να υποκλέπτονται από αμερικανούς εμπορικούς αξιωματούχους, που θα επιχειρούσαν έτσι να αποκτήσουν μυστικά τα οποία θα έδιναν προβάδισμα στους αμερικανούς ανταγωνιστές της. Παρά την αποτυχία του AEES, πολλές κυβερνήσεις παραμένουν πεπεισμένες ότι η παρακαταθήκη κλειδιού μπορεί να λειτουργήσει αποτελεσματικά, υπό τον όρο να είναι τα κλειδιά επαρκώς προστατευμένα και να υπάρχουν εχέγγυα που θα καθησυχάζουν το κοινό ότι το σύστημα δεν είναι ανοιχτό σε κυβερνητικές καταχρήσεις. Παρότι η αμερικανική κυβέρνηση απέσυρε τις προτάσεις τα για την παρακαταθήκη κλειδιού, πολλοί υποπτεύονται ότι κάποια στιγμή στο μέλλον θα επιχειρήσει και πάλι να εισαγάγει μια εναλλακτική μορφή της. Ύστερα από την αποτυχία της προαιρετικής παρακαταθήκης, ίσως οι κυβερνήσεις να σκεφτούν να τη θεσπίσουν ως υποχρεωτική.

Υπάρχουν διάφορες άλλες εναλλακτικές λύσεις που θα μπορούσαν να επιλέξουν να εφαρμόσουν οι κυβερνήσεις, ώστε να εξισορροπήσουν τις ανησυχίες των φιλελεύθερων, των επιχειρηματιών και των υπευθύνων για την επιβολή του νόμου. Το ποια επιλογή τελικά θα προτιμήσουν δεν είναι καθόλου σαφές, επειδή αυτή τη στιγμή η κρυπτογραφική πολιτική είναι ιδιαίτερα ρευστή. Μια συνεχής ροή γεγονότων ανά τον κόσμο επηρεάζει διαρκώς τη διαμάχη για την κρυπτογράφηση. Το Νοέμβριο του 1998, ο Λόγος της Βασίλισσας ανήγγειλε επικείμενη βρετανική νομοθεσία σχετικά με την ψηφιακή αγορά. Το Δεκέμβριο της ίδιας χρονιάς, 33 έθνη υπέγραψαν τη Συμφωνία του Βάσεναρ, που περιορίζει τις εξαγωγές όπλων και επιπλέον καλύπτει ισχυρές τεχνολογίες κρυπτογράφησης. Τον Ιανουάριο του 1999, η Γαλλία ανακάλεσε τους αντικρυπτογραφικούς της νόμους, που ως τότε ήταν οι πιο περιοριστικοί σε όλη τη Δυτική Ευρώπη, πιθανότατα κατόπιν πιέσεων της επιχειρηματικής κοινότητας. Το Μάρτιο του 1999, η βρετανική κυβέρνηση κυκλοφόρησε ένα συμβουλευτικό έγγραφο για ένα προτεινόμενο Νομοσχέδιο περί Ηλεκτρονικού Εμπορίου. Θα έχουν μεσολαβήσει πολλές ακόμη μεταπτώσεις στη διαμάχη σχετικά με την κρυπτογραφική πολιτική. Μια πάντως πτυχή της μελλοντικής πολιτικής για την κρυπτογράφηση φαίνεται βέβαιη, και αυτή είναι η ανάγκη για πιστοποιητικές αρχές.

Το 1998, η πρώτη εταιρία στην αγορά, στο χώρο της πιστοποίησης, ήταν η Verisign, που μέσα σε τέσσερα μόλις χρόνια αύξησε το κεφάλαιό της σε 30 εκατομμύρια δολάρια. Οι πιστοποιητικές αρχές, πέραν του να διασφαλίζουν αξιόπιστη κρυπτογράφηση επιβεβαιώνοντας τα δημόσια κλειδιά, μπορούν επίσης να εγγυώνται τη γνησιότητα των ψηφιακών υπογραφών και δεν αποτελούν σε καμία περίπτωση κίνδυνο για την ασφάλεια. Υπάρχουν όμως κάποιες άλλες εταιρίες γνωστές ως TTP (Trusted Third Parties), οι οποίες παρέχουν μια πιο αμφιλεγόμενη υπηρεσία, τη λεγόμενη ανάκτηση κλειδιού. Οι εταιρίες αυτές κρατούν αντίγραφα όλων των κλειδιών. Σε αυτήν την περίπτωση, μια εταιρία που θα χάσει το ιδιωτικό κλειδί της μπορεί να το ανακτήσει ερχόμενη σε επαφή με την TTP της. Οι εταιρίες αυτές αποτελούν σημείο αμφιλεγόμενο, επειδή έχουν πρόσβαση στα ιδιωτικά κλειδιά των πελατών τους και επομένως μπορούν να διαβάζουν τα μηνύματά τους. Θα πρέπει να είναι αξιόπιστες, διαφορετικά είναι εύκολο να υπάρξουν καταχρήσεις. Ορισμένοι υποστηρίζουν ότι οι TTP είναι στην ουσία μια μετενσάρκωση της παρακαταθήκης κλειδιού, και ότι οι επιφορτισμένοι με την εφαρμογή του νόμου θα μπουν στον πειρασμό να πιέσουν αυτές τις εταιρίες να τους παραδώσουν τα κλειδιά ενός πελάτη στα πλαίσια μια αστυνομικής έρευνας. Άλλοι πάλι θεωρούν ότι οι TTP αποτελούν αναπόσπαστο μέρος της υποδομής του δημόσιου κλειδιού. Κανείς δεν μπορεί να προφητέψει ποιος θα είναι ο ρόλος των TTP

στο μέλλον ούτε τη μορφή της κρυπτογραφικής πολιτικής. Αν για παράδειγμα εκδηλωθεί μια σειρά από αποτρόπαιες τρομοκρατικές ενέργειες και οι υπεύθυνοι για την επιβολή του νόμου αποδείξουν ότι οι παγιδεύσεις τηλεφώνων θα μπορούσαν να τις είχαν αποτρέψει, τότε οι κυβερνήσεις θα κερδίσουν γρήγορα τη συμπάθεια του κοινού υπέρ μιας πολιτικής που θα στηρίζεται στην παρακαταθήκη κλειδιού. Όλοι οι χρήστες θα υποχρεωθούν να καταθέσουν τα κλειδιά τους σε έναν αντιπρόσωπο παρακαταθήκης κλειδιού και επομένως όποιος στείλει ένα μήνυμα κρυπτογραφημένο με μη κατατεθειμένο κλειδί θα παραβιάζει το νόμο. Αργότερα, αν οι κυβερνήσεις καταχραστούν την εμπιστοσύνη που συνδέεται με ένα σύστημα παρακαταθήκης κλειδιού, το κοινό θα απαιτήσει την επάνοδο στην κρυπτογραφική ελευθερία. Τίποτα λοιπόν δεν μας εμποδίζει να αλλάζουμε την πολιτική μας ανάλογα με το πολιτικό, οικονομικό και κοινωνικό κλίμα. Ο αποφασιστικός παράγων θα είναι το ποιον φοβούνται περισσότερο οι πολίτες, τους κακοποιούς ή την κυβέρνηση.

Το 1993 διατάχθηκε δικαστική έρευνα εναντίον του Φιλ Ζίμερμαν. Κατά το FBI , εξήγαγε εξοπλισμό, εφόσον εφοδίασε τις εχθρικές χώρες και τους τρομοκράτες με τα εργαλεία που χρειάζονταν για να διαφύγουν από τον έλεγχο της αμερικανικής κυβέρνησης. Ύστερα από 3 χρόνια η ομοσπονδιακή έρευνα δεν είχε ακόμη οδηγήσει σε δίκη τον Ζίμερμαν. Την υπόθεση περιέπλεκε η φύση του PGP και ο τρόπος διανομής του καθώς ο Ζίμερμαν δεν είχε εγκαταστήσει το PGP σε έναν υπολογιστή τον οποίο στη συνέχεια θα έστελνε σε εχθρικό καθεστώς, αλλά έδωσε ένα αντίγραφο σε έναν φίλο του ο οποίος απλώς το εγκατέστησε σε έναν αμερικανικό υπολογιστή που έτυχε να είναι συνδεδεμένος με το διαδίκτυο. Το 1996, ύστερα από 3 χρόνια έρευνας το γραφείο του Υπουργού Δικαιοσύνης των ΗΠΑ απέσυρε τις κατηγορίες καθώς το FBI συνειδητοποίησε πως ήταν πλέον πολύ αργά αφού το PGP είχε διαδοθεί στο διαδίκτυο. Ο Ζίμερμαν στη συνέχεια προχώρησε σε διακανονισμό με το RSA και πήρε την άδεια που έλυσε το θέμα της ευρεσιτεχνίας. Έτσι το PGP ήταν πια νόμιμο και ο Ζίμερμαν ελεύθερος.

### *3.2. Κρυπτογραφία και ψηφιακές υπογραφές*

Η μετάδοση πληροφοριών χωρίς να γίνεται αντιληπτή από τρίτους, η εξασφάλιση της δυνατότητας να μην μπορεί να ερμηνευθεί το μήνυμα στην περίπτωση που η μετάδοση γίνει αντιληπτή καθώς και η απόδειξη της ιδιοκτησίας, κυριότητος ενός μηνύματος απασχόλησαν από το μακρινό παρελθόν και εξακολουθούν να απασχολούν έως σήμερα τον άνθρωπο. Τα προβλήματα αυτά, θα εξακολουθούν να υπάρχουν, όσο θα υπάρχουν άνθρωποι που θα προσπαθούν να προστατέψουν τα δικαιώματά τους και κάποιοι που θα προσπαθούν να τα παραβιάσουν. Στη σύγχρονη εποχή, η διαμάχη αυτή διεξάγεται στο χώρο των ψηφιακών δεδομένων. Σύγχρονες υπολογιστικές μηχανές, με υψηλές δυνατότητες επεξεργασίας και αποθήκευσης πληροφοριών, χρησιμοποιούνται τόσο για να εξασφαλίζουν τη νομιμότητα όσο και για να την παρακάμπτουν. Ειδικότερα, η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο, οι συναλλαγές και η μετάδοση εμπιστευτικών δεδομένων, μέσω ανοιχτών δικτύων έχει γίνει κοινός τόπος σήμερα. Η σημερινή πραγματικότητα επιβάλλει μεταξύ των παραπάνω και την ύπαρξη μηχανισμών προστασίας του απαραβίαστου του προσωπικού και του επαγγελματικού απορρήτου των συναλλασσόμενων χρηστών. Επιβάλλει μηχανισμούς ασφάλειας στις συναλλαγές, ασφάλειας η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, την ταυτότητα δηλαδή των συναλλασσόμενων. Λόγοι, οι οποίοι καθιστούν την ασφάλεια στην ηλεκτρονική επικοινωνία επιτακτική, είναι η ευκολία που παρέχεται μέσω ενός ανοικτού δικτύου, όπως είναι το Internet στην:

α) παρακολούθηση της επικοινωνίας από τρίτους

β) αλλοίωση του περιεχομένου του μεταφερόμενου μηνύματος

γ) αδυναμία να εξακριβωθεί η ταυτότητα των επικοινωνούντων μερών (πλαστοπροσωπία με τη χρήση πλαστής ηλεκτρονικής διεύθυνσης).

Μια από τις μεθόδους που χρησιμοποιούνται για την ασφαλή διακίνηση των πληροφοριών στο σύγχρονο περιβάλλον, είναι η κρυπτογραφία. Η κρυπτογραφία αποτέλεσε πανάρχαια μέθοδο εξασφάλισης της εμπιστευτικότητας των συναλλαγών, όπως προκύπτει από την παρακάτω συνοπτική ιστορική διαδρομή. Εξακολουθεί επίσης, έως και σήμερα να συμβάλλει στον παραπάνω στόχο, καθώς η ίδια αποτελεί μια
πολύ βασική τεχνολογία στον τομέα της ασφάλειας του Internet.

Τα Σχήματα Υπογραφών ή Σχήματα Ψηφιακών Υπογραφών (Digital Signature Schemes) όπως αλλιώς ονομάζονται, έρχεται κατ' αρχήν σαν απόρροια της μεγάλης ποσότητας πληροφορίας που διακινείται πλέον μέσω του διαδικτύου. Ένα σχήμα ψηφιακής υπογραφής είναι μια μέθοδος υπογραφής

ενός μηνύματος σε ηλεκτρονική μορφή και έχει παρόμοιες ιδιότητες με αυτές της χειρόγραφης υπογραφής. Ο παραλήπτης ενός υπογεγραμμένου ηλεκτρονικού μηνύματος μπορεί να διαπιστώσει τη γνησιότητά του και σ' αυτή την περίπτωση είναι βέβαιος για την προέλευση, την ακεραιότητα και την μη αποκήρυξη του από τον αποστολέα. Για παράδειγμα, ας υποθέσουμε ότι θέλουμε να υπογράψουμε ένα ηλεκτρονικό έγγραφο. Γιατί δεν μπορούμε απλά να ψηφιοποιήσουμε την υπογραφή μας και να την επισυνάψουμε στο έγγραφο; Πολύ απλά γιατί οποιοσδήποτε έχει πρόσβαση σε αυτό μπορεί να αφαιρέσει ή να αντιγράψει την υπογραφή μας και να την τοποθετήσει κάπου αλλού όπως σε μια επιταγή για ένα υπέρογκο ποσό. Με τις χειρόγραφες υπογραφές αυτό θα απαιτούσε την αποκοπή ή ένα φωτοαντίγραφο της υπογραφής και την επικόλλησή της στην επιταγή κάτι που σπανίως θα μπορούσε να θεωρηθεί ως γνήσια υπογραφή. Παρ' όλα αυτά μια τέτοια απάτη είναι σχετικά εύκολη και είναι κάπως δύσκολο να γίνει η διάκριση μεταξύ της γνήσιας και της πλαστογραφημένης υπογραφής. Επομένως, απαιτούμε οι ψηφιακές υπογραφές να μην μπορούν να διαχωριστούν από το μήνυμά μας και να μεταβούν οπουδήποτε αλλού. Αυτό σημαίνει, η υπογραφή να είναι άμεσα συνυφασμένη με τον υπογράφον αλλά και το μήνυμα στο οποίο προσαρτάται. Επίσης, η ψηφιακή υπογραφή πρέπει εύκολα να αναγνωρίζεται από άλλους συμβαλλόμενους. Τα σχήματα των ψηφιακών υπογραφών, λοιπόν, αποτελούνται από δυο διακριτά βήματα τη διαδικασία της υπογραφής και της επαλήθευσής της.

Σύγκριση ψηφιακών – χειρόγραφων υπογραφών

Προτού προχωρήσουμε στον ορισμό της ψηφιακής υπογραφής, θα συγκρίνουμε τις ψηφιακές υπογραφές με τις χειρόγραφες υπογραφές για να κατανοήσουμε και τις τεχνικές απαιτήσεις που μας οδηγούν στις ψηφιακές υπογραφές.

Μια σύντομη σύγκριση της χειρόγραφης με την ψηφιακή υπογραφή κάνει εμφανείς τις παρακάτω διαφορές:

- Η χειρόγραφη επισυνάπτεται φυσικά σε ένα μήνυμα έτσι που κάθε γνήσιο αντίγραφό του την περιέχει, ενώ η ψηφιακή είναι δυνατό να αφαιρεθεί από το αρχικό μήνυμα. Για να αντιμετωπιστεί το πρόβλημα αυτό είναι απαραίτητο ο αλγόριθμος υπογραφής να «συνδέει» με κάποιο τρόπο το μήνυμα με την υπογραφή. Ένας τρόπος για να γίνει αυτό είναι να κρυπτογραφήσουμε πρώτα το υπογεγραμμένο μήνυμα και έπειτα να το στείλουμε σε εκείνον που θέλουμε (Εδώ θέλει προσοχή αφού πρέπει η διαδικασία να γίνει με τη σειρά Υπογραφή → κρυπτογράφηση διότι σε αντίθετη περίπτωση, αν ο Ο καταφέρει να κλέψει το υπογεγραμμένο μήνυμα του Α προς τον Β, μπορεί να αφαιρέσει την υπογραφή του Α και να προσθέσει τη δική του. Έτσι ο Ο θα μπορεί να υποδύεται τον Α στις υπόλοιπες επικοινωνίες του με τον Β).

- Από την άλλη μεριά η χρήση μίας ασφαλούς ψηφιακής υπογραφής είναι πολύ βολική, αφού η επαλήθευσή της (verification), γίνεται μ' έναν δημόσιο (public) αλγόριθμο επαλήθευσης, σε αντίθεση με την περίπτωση της χειρόγραφης μόνο που ο γραφολόγος μπορεί να την επιβεβαιώσει με ανάλογη ασφάλεια.

Στον παρακάτω πίνακα φαίνονται συγκεντρωτικά οι αναλογίες μεταξύ χειρόγραφων και ψηφιακών υπογραφών.

| ΧΕΙΡΟΓΡΑΦΕΣ ΥΠΟΓΡΑΦΕΣ | ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ |
|---|---|
| Ενσωματωμένη στο μήνυμα | Εξωτερικό «αντικείμενο» το οποίο συνδέεται με το μήνυμα |
| Αναγνώριση της ταυτότητας του υπογεγραμμένου | Αυθεντικοποίηση της ταυτότητας του υπογεγραμμένου:<br>- Η ψηφιακή υπογραφή θα πρέπει να συνδέει την ταυτότητα ενός μέλους με κάποια πληροφορία με τέτοιον τρόπο ώστε να είναι αναμφισβήτητη η αναγνώριση του μέλους |
| Αναγνώριση της αυθεντικότητας του υπογεγραμμένου κειμένου | Αυθεντικοποίηση του μηνύματος προορισμού:<br>- Η ψηφιακή υπογραφή θα πρέπει να αντιστοιχεί σε πληροφορία η οποία να εξαρτάται από το υπογεγραμμένο μήνυμα και τον υπογεγραμμένο |
| Δυνατότητα επαλήθευσης της υπογραφής από τρίτους | Δυνατότητα επαλήθευσης της ψηφιακής υπογραφής από τρίτους:<br>- Η επαλήθευση της ψηφιακής υπογραφής θα πρέπει να είναι εύκολη διαδικασία και θα πρέπει να μπορεί να εκτελεσθεί από οποιονδήποτε |
| Δυνατή η πλαστογράφηση | Σχεδόν αδύνατη η «πλαστογράφηση» |
| Απευθείας ορατή | Απαιτείται ειδικό λογισμικό για να δημιουργηθεί και κατά συνέπεια για να είναι ορατή |

*Σύγκριση χειρόγραφης και ψηφιακής υπογραφής*

Άλλα χαρακτηριστικά των χειρόγραφων υπογραφών είναι η δήλωση της ημερομηνίας που πραγματοποιείται η υπογραφή και πολλές φορές η δήλωση της τοποθεσίας. Το μειονέκτημα της χειρόγραφης υπογραφής είναι η επαλήθευσή της, δηλαδή ο έλεγχος γνησιότητας της υπογραφής. Στις ψηφιακές υπογραφές η διαδικασία ελέγχου είναι υποχρεωτική, ενώ στις χειρόγραφες υπογραφές η διαδικασία ελέγχου παραλείπεται και εκτελείται μόνο σε περίπτωση διαφωνίας.

Κρυπτογραφία

Ιστορικά στοιχεία

Η Κρυπτογραφία έχει μια μακρά και συναρπαστική ιστορία. Η κρυπτογραφία είχε αρχικά την μορφή τέχνης που τα μυστικά της γνώριζαν λίγοι και εκλεκτοί. Η ιστορία της κρυπτογραφίας ξεκινά περίπου το 4000 π.Χ. στην αρχαία Αίγυπτο περνά στην αρχαία Ελλάδα που έχουμε αναφορές της στο ιστορικό Πολύβιο και συνεχίζεται στον Ιούλιο Καίσαρα. Ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς

τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί π.χ. 3. Δηλαδή, η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο. Θα μπορούσε το κλειδί να ήταν ο αριθμός 6, οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό. Έτσι, διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα. Ο πίνακας αντιστοίχισης των γραμμάτων, έχοντας ως κλειδί το 3, φαίνεται παρακάτω:

Το γράμμα a b c d e f g h i j k v m n o p q r s t u v w x y z
Αντικαθίσταται από το γράμμα d e f g h i j k l m n o p q r s t u v w x y z a b c

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη secret, θα προκύψει το κρυπτογράφημα wigvix. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερότερά του στο αλφάβητο. Προφανώς, δεν αρκεί να ξέρει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά πρέπει να γνωρίζει και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει να γνωρίζει το κλειδί, που σε αυτήν την περίπτωση είναι ο αριθμός 3.

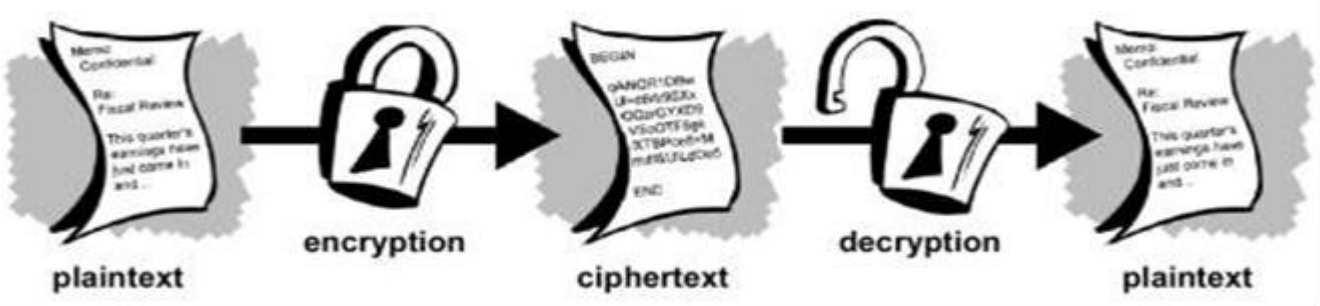
Από την στιγμή που η κρυπτογραφία άρχισε να χρησιμοποιείται για στρατιωτικούς σκοπούς και για απόκρυψη ζωτικής σημασίας πληροφοριών, έπαψε να είναι απόκρυφη τέχνη και έτυχε της μελέτης τόσο αυτών που ήθελαν να αποκρύψουν τα μυστικά τους όσο και από αυτούς που ήθελαν να βρουν τρόπο να αποκαλύψουν τα μυστικά των αντιπάλων τους. Έτσι η κρυπτογραφία πέρασε στο πεδίο της επιστήμης. Κρυπτογράφοι και κρυπταναλυτές επιδόθηκαν σε έναν ανελέητο συναγωνισμό. Κάθε πρόοδος της κρυπτογραφίας συνοδευόταν από μια αντίστοιχη πρόοδο της κρυπτανάλυσης. Η κρυπτογραφία έγινε χρήσιμο εργαλείο στα χέρια του στρατού των διπλωματών και του κράτους με σκοπό την διαφύλαξη εθνικών μυστικών και στρατηγικών. Όσο πιο πολύτιμα τα μυστικά τόσο πιο μεγάλη αξία αποκτούσε η ασφαλής φύλαξή τους. Στον 20ό αιώνα τα παραδείγματα εκτεταμένης χρήσης κρυπτογραφικών τεχνικών είναι πολλά. Την περίοδο της ποτοαπαγόρευσης στην Αμερική (δεκαετία του 20-30) το νεοσύστατο τότε σώμα FBI χρησιμοποίησε τεχνικές κρυπτογραφίας για να αποκρύπτει από τη μαφία τους τόπους παράδοσης μεγάλων φορτίων ποτών. Δεν θα ήταν υπερβολή να πούμε ότι η έκβαση του δευτέρου Παγκοσμίου Πολέμου κρίθηκε υπέρ των συμμάχων εξαιτίας της ικανότητας τους να αποκρυπτογραφούν τα γερμανικά μηνύματα και της ανικανότητας των Γερμανών να πράξουν κάτι ανάλογο με τα συμμαχικά μηνύματα. Είναι γνωστή άλλωστε η ιστορία της μηχανής ENIGMA (αναφέρθηκε στο πρώτο μέρος της εργασίας) που χρησιμοποίησαν οι Άγγλοι για να αποκρυπτογραφούν τα μηνύματα του Γερμανικού επιτελείου προς τις αγέλες των υποβρυχίων τους στη Μεσόγειο αλλά και τον Ατλαντικό ωκεανό.

Η πιο ολοκληρωμένη και χωρίς τεχνικούς όρους περιγραφή του θέματος είναι το βιβλίο The Codebreakers του Kahn. Το βιβλίο αυτό ακολουθεί τα ίχνη της κρυπτογραφίας από την αρχική και περιορισμένη χρήση της από τους Αιγύπτιους περίπου 4000 χρόνια πριν, μέχρι τον εικοστό αιώνα όπου έπαιξε κρίσιμο ρόλο στην έκβαση και των δύο παγκόσμιων πολέμων. Ολοκληρωμένο το 1963, το βιβλίο του Kahn καλύπτει εκείνες τις πλευρές της ιστορίας, οι οποίες ήταν οι πιο σημαντικές (μέχρι τότε) στην εξέλιξη του θέματος. Αυτοί που ασκούσαν κυρίως την τέχνη ήταν όσοι σχετίζονταν με τον στρατό, τη διπλωματική υπηρεσία και την κυβέρνηση γενικότερα. Η κρυπτογραφία χρησιμοποιούνταν σαν εργαλείο για την προστασία των εθνικών μυστικών και στρατηγικών. Η εξάπλωση των υπολογιστών και των συστημάτων επικοινωνίας τη δεκαετία του ’60 έφερε μαζί της μια απαίτηση από τον ιδιωτικό τομέα για την ύπαρξη μέσων προστασίας των πληροφοριών σε ψηφιακή μορφή και για την παροχή υπηρεσιών ασφάλειας. Αρχίζοντας με την έρευνα του Feistel στην IBM στις αρχές της δεκαετίας του ’70 και μεσουρανώντας στα 1977, με την υιοθεσία του ως Πρότυπο Επεξεργασίας Ομοσπονδιακών Πληροφοριών των Η.Π.Α για την κρυπτογράφηση μη απόρρητων πληροφοριών, το DES, το Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard), είναι ο πιο γνωστός κρυπτογραφικός μηχανισμός στην ιστορία. Παραμένει το καθιερωμένο μέσο για την ασφαλή προστασία του ηλεκτρονικού εμπορίου για πολλά οικονομικά ιδρύματα ανά τον κόσμο. Η πιο αξιοσημείωτη εξέλιξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν οι Diffie και Hellman δημοσίευσαν το άρθρο τους New Directions in Cryptography (Νέες Κατευθύνσεις στην Κρυπτογραφία). Αυτή η εργασία εισήγαγε την επαναστατική ιδέα της κρυπτογραφίας δημόσιου κλειδιού και επίσης παρείχε μια νέα και ευφυή μέθοδο για την ανταλλαγή κλειδιών, η ασφάλεια της οποίας βασίζεται στη

δυσεπιλυσιμότητα του προβλήματος διακριτού λογαρίθμου. Παρ' όλο που οι συγγραφείς δεν είχαν τότε να προτείνουν μια πρακτική υλοποίηση ενός σχήματος κρυπτογράφησης δημόσιου κλειδιού, η ιδέα ήταν ξεκάθαρη και δημιούργησε έντονο ενδιαφέρον και εκτεταμένη δραστηριότητα στην κρυπτογραφική κοινότητα. Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν το πρώτο πρακτικό σχήμα κρυπτογράφησης και υπογραφής δημόσιου κλειδιού, το οποίο αναφέρεται τώρα ως RSA. Το σχήμα RSA βασίζεται σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, τη δυσεπιλυσιμότητα της παραγοντοποίησης μεγάλων ακεραίων. Αυτή η εφαρμογή ενός δύσκολου μαθηματικού προβλήματος στην κρυπτογραφία αναζωογόνησε τις προσπάθειες για την εύρεση περισσότερο αποδοτικών μεθόδων παραγοντοποίησης.
Στη δεκαετία του 80 σημειώθηκαν σημαντικές πρόοδοι σ' αυτόν τον τομέα, αλλά καμία που να καθιστά το σύστημα RSA ανασφαλές. Μια άλλη κλάση ισχυρών και πρακτικών σχημάτων δημόσιου κλειδιού ανακαλύφθηκε από τον ElGamal το 1985. Τα σχήματα αυτά βασίζονται επίσης στο πρόβλημα διακριτού λογαρίθμου. Μια από τις πιο σημαντικές συνεισφορές που παρείχε η κρυπτογραφία δημόσιου κλειδιού είναι η ψηφιακή υπογραφή. Το 1991 υιοθετήθηκε το πρώτο διεθνές πρότυπο για ψηφιακές υπογραφές (ISO/IEC 9796). Είναι βασισμένο στο σχήμα δημόσιου κλειδιού RSA. Το 1994 η Κυβέρνηση των Η.Π.Α υιοθέτησε το Πρότυπο Ψηφιακών Υπογραφών (Digital Signature Standard – DSA), έναν μηχανισμό βασισμένο στο σχήμα δημόσιου κλειδιού ElGamal.

Η ανάγκη για εμπιστευτικότητα στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία. Ο αποστολέας χρησιμοποιώντας κάποια μαθηματική συνάρτηση μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, μέχρι να αποκρυπτογραφηθεί. Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν αλγόριθμους και κλειδιά (σειρά από bits συγκεκριμένου μήκους) για να διατηρήσουν την πληροφορία ασφαλή. Μία παραδοσιακή μέθοδος κρυπτογράφησης είναι η συμμετρική κρυπτογραφία η οποία χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αποστολέας κρυπτογραφεί και ο παραλήπτης αποκρυπτογραφεί με το ίδιο κλειδί. Το κλειδί θα πρέπει να παραμένει μυστικό και να είναι γνωστό μόνο στους συναλλασσόμενους. Η μέθοδος αυτή παρουσιάζει μειονεκτήματα όσον αφορά την εφαρμογή της σε ανοιχτά δίκτυα με πολλούς χρήστες και τις αυξημένες απαιτήσεις της για την ασφάλεια (π.χ. αποθήκευση των κλειδιών κλπ). Η ασύμμετρη κρυπτογραφία (ή κρυπτογραφία δημοσίου κλειδιού- public key cryptography) χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Κάθε χρήστης έχει στη διάθεσή του δύο κλειδιά. Το δημόσιο κλειδί είναι αυτό που ο χρήστης μπορεί να το γνωστοποιήσει σε τρίτους ενώ το ιδιωτικό είναι εκείνο που το φυλάσσει με ασφάλεια και μόνο αυτός θα πρέπει να το γνωρίζει και κατέχει. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη. Έτσι, το μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη (που είναι ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού εκτός και αν η μυστικότητα του ιδιωτικού κλειδιού έχει παραβιαστεί).

Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext).
Στο σχήμα που ακολουθεί φαίνεται η κρυπτογράφηση ενός απλού κειμένου.



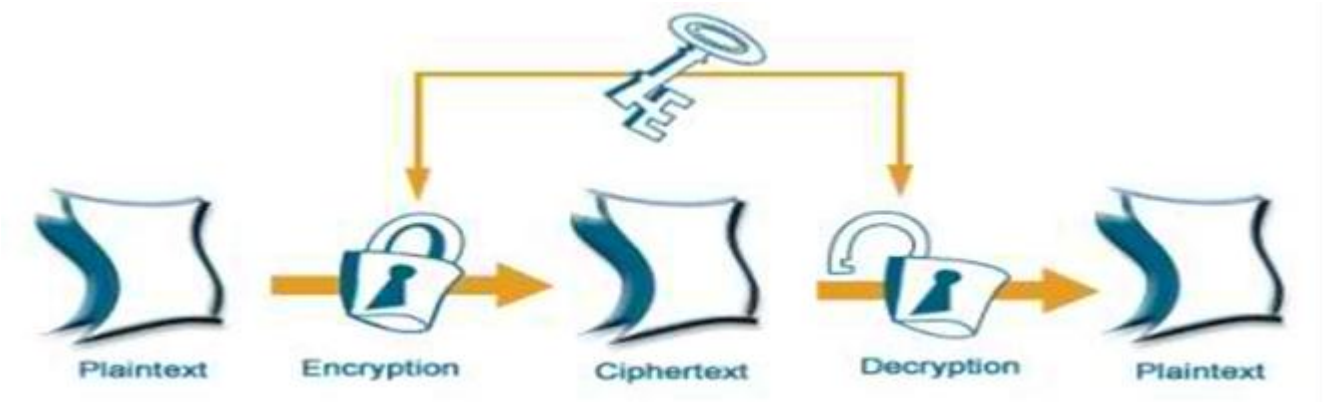

*Κρυπτογράφηση απλού κειμένου*

Συμμετρική και ασύμμετρη κρυπτογραφία

Οι δύο βασικές τεχνικές κρυπτογράφησης είναι η συμμετρική και η μη- συμμετρική. Στη συμμετρική κρυπτογράφηση περιλαμβάνεται μόνο ένα κλειδί, το οποίο χρησιμοποιείται τόσο από τον αποστολέα για την κρυπτογράφηση, όσο και στον παραλήπτη για την αποκρυπτογράφηση. Κάποιοι από τους αλγόριθμους συμμετρική κρυπτογράφησης που χρησιμοποιούνται είναι οι blowfish, Triple-DES, CAST, IDEA. Οι αλγόριθμοι IDEA και RSA είναι νομικά περιορισμένοι, αλλά οι υπόλοιποι ελεύθεροι. Το προφανές πρόβλημα με τη συμμετρική κρυπτογράφηση είναι το μέσο για τη διανομή του κλειδιού. Η ασύμμετρη κρυπτογράφηση λύνει αυτό το πρόβλημα με τη χρήση δύο κλειδιών, ενός δημόσιου και ενός ιδιωτικού. Ένα μήνυμα κωδικοποιείται προτού σταλεί σε κάποιον παραλήπτη χρησιμοποιώντας το δημόσιο κλειδί του, αλλά στη συνέχεια αποκρυπτογραφείται μόνο με το αντίστοιχο ιδιωτικό κλειδί του παραλήπτη. Αυτό σημαίνει ότι δεν μπορείτε να διαβάσετε ένα μήνυμα που εσείς κωδικοποιήσατε ( εκτός και αν το έχετε ταυτόχρονα κρυπτογραφήσει με το δικό σας δημόσιο κλειδί). Εξ ου και το δημόσιο κλειδί μπορεί να διανέμεται ελεύθερα σε όλους χωρίς να θέτει σε κίνδυνο την ασφάλεια ενώ το ιδιωτικό κλειδί, βέβαια, θα πρέπει να φυλάσσεται προσεκτικά. Οι αλγόριθμοι δημόσιου κλειδιού αναπτύχθηκαν στη δεκαετία του 1970 σε δύο κύρια «στρατόπεδα». Ο πρώτος, RSA (Rivest, Shamir και Adleman), είχε κατοχυρωθεί με δίπλωμα ευρεσιτεχνίας στις ΗΠΑ, περιορίζοντας την εφαρμογή της από νομική άποψη (μέχρι το Σεπτέμβριο του 2000). Ο δεύτερος, DH (Diffie- Hellman), είναι ελεύθερο προς χρήση. Ένα κλειδί μεγέθους 2048 bits είναι αρκετά ασφαλές. Η συμμετρική κρυπτογράφηση με κλειδί μήκους 128 bits είναι περίπου το ίδιο ασφαλής με την ασύμμετρη κρυπτογράφηση με κλειδί μήκους 2048 bits. Ο Zimmermann επέλεξε να χρησιμοποιήσει ένα «υβριδικό» δημόσιο κλειδί, ενσωματώνοντας τόσο συμμετρικές όσο και ασύμμετρες μεθόδους κρυπτογράφησης. Το ηλεκτρονικό μήνυμα είναι κρυπτογραφημένο με έναν αλγόριθμο συμμετρικής κρυπτογράφησης με ένα κλειδί μήκους, έστω, 128 bit. Στη συνέχεια αυτό το κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη, έστω μήκους 2048 bits, και ολόκληρο το μήνυμα (συμμετρικά κρυπτογραφημένο σώμα και ασύμμετρα κρυπτογραφημένο κλειδί) αποστέλλεται. Το μήνυμα μπορεί επιπροσθέτως να έχει και ψηφιακή υπογραφή.

Συμμετρική κρυπτογραφία ή κρυπτογραφία συμμετρικού ή μυστικού κλειδιού

Στη συμμετρική κρυπτογραφία, χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση. Επομένως, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.



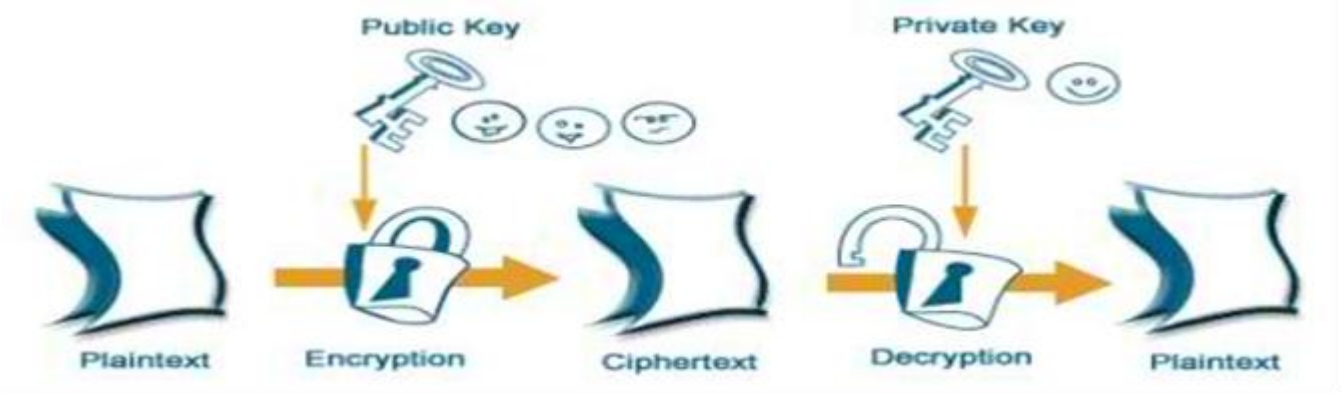

*Συμμετρική Κρυπτογραφία*

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με περισσότερο γνωστό το Data Encryption Standard (DES), ο οποίος όπως προαναφέρθηκε υιοθετήθηκε από την κυβέρνηση των Η.Π.Α., ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών. Το πρόβλημα που παρουσιάζει όμως αυτή η τεχνική είναι η διανομή των κλειδιών, η εξασφάλιση δηλαδή ότι τα κλειδιά που αποστέλλονται στους παραλήπτες που θα τα χρησιμοποιήσουν δεν θα πέσουν σε λάθος χέρια. Κατά αυτόν τον τρόπο τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών

μέσα από δημόσια δίκτυα έχουν αναπτυχθεί και χρησιμοποιούνται, με περισσότερο διαδεδομένο το σύστημα Kerberos που έχει αναπτυχθεί στο MIT.

Ασύμμετρη Κρυπτογραφία ή κρυπτογραφία ασυμμετρικού ή δημόσιου κλειδιού

Στην ασύμμετρη κρυπτογραφία, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση, το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά παράγονται έτσι ώστε να έχουν τις εξής ιδιότητες: Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα. Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.




*Ασύμμετρη κρυπτογραφία*

Ευνόητο επίσης είναι, ότι όσο ο αριθμός των χρηστών αυτού του συστήματος ασφαλείας μεγαλώνει, μεγαλώνουν και τα προβλήματα της δημιουργίας, της διανομής, της ασφάλειας αλλά και της καταγραφής και αντιστοιχίας των μυστικών κλειδιών. Άρα τα σχήματα αυτά δεν είναι εύκολο να επεκταθούν για την εξυπηρέτηση μεγάλων πληθυσμών και απαιτούν επίσης πρόσθετες διαδικασίες ασφάλειας, όπως την αποθήκευση των κλειδιών σε ένα κεντρικό ασφαλή εξυπηρετητή.

Για να αποκατασταθεί επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Αναλυτικότερα, ένα μήνυμα ή και ένα αρχείο που έχει κρυπτογραφηθεί με το δημόσιο κλειδί ενός κατόχου, μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί του ίδιου κατόχου, πράγμα που σημαίνει ότι μόνο ο κάτοχος ενός δημόσιου κλειδιού μπορεί να διαβάσει τα μηνύματα που έχουν κρυπτογραφηθεί με το κλειδί αυτό, καθώς μόνο αυτός γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Η διαδικασία αυτή εξασφαλίζει ότι το μήνυμα ή το αρχείο δεν μπορεί να παρακολουθείται ή και να αλλοιώνεται από κάποιον τρίτο που δεν κατέχει το αντίστοιχο ιδιωτικό κλειδί του δημοσίου κλειδιού με το οποίο κρυπτογραφήθηκε το μήνυμα ή το αρχείο. Στην περίπτωση αυτή λέμε ότι το μήνυμα είναι κρυπτογραφημένο.

Συμπερασματικά, το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δε μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα. Η ασύμμετρη κρυπτογραφία προσφέρει μεγαλύτερη ασφάλεια από τη συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογράφησης.

Εφαρμογές κρυπτογραφίας

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)

3. Σταθερή τηλεφωνία (cryptophones)
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα (VPN)
15. Word Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

Ψηφιακή υπογραφή

Η «νομιμοποίηση» ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που έφερε. Καθώς τα ηλεκτρονικά έγγραφα κάθε είδους τείνουν να αντικαταστήσουν τα «παραδοσιακά» χειρόγραφα, αντίστοιχα και η υπογραφή του συντάκτη γίνεται «εικονική», ηλεκτρονική. Κρίνεται απαραίτητη η διευκρίνιση του όρου της «ψηφιακής υπογραφής», πριν την ανάλυση των εννοιών που σχετίζονται με τη
δημιουργία, την επαλήθευσης της κλπ.
Ορισμοί

• Μια «κλειδωμένη» σύντμηση ενός ηλεκτρονικού κειμένου, η οποία παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσής του
• Είναι μια συμβολοσειρά από δεδομένα τα οποία σχετίζουν ένα μήνυμα (στην ψηφιακή του μορφή) με την οντότητα που το δημιούργησε.
• Οι ψηφιακές υπογραφές είναι δεδομένα που έχουν ενσωματωθεί σε άλλα δεδομένα για λόγους ταυτοποίησης και εξακρίβωσης στοιχείων.
• Οι ψηφιακές υπογραφές είναι ηλεκτρονικές υπογραφές που συνδέονται με τα υπογεγραμμένα δεδομένα με τέτοιο τρόπο ώστε οποιαδήποτε επέμβαση να μπορεί να γίνει αντιληπτή, αλλά και να μπορεί επίσης να αναγνωριστεί ο αποστολέας πέρα από κάθε αμφιβολία
• Η ψηφιακή υπογραφή είναι μία ακολουθία χαρακτήρων άμεσα συσχετισμένη με το περιεχόμενο του μηνύματος και την ταυτότητα αυτού που το υπογράφει. Αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί, ελέγχοντας την υπογραφή, να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι
• «Η ψηφιακής μορφής υπογραφή σε δεδομένα ή λογικά συνεχιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη υπογραφής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή:
α) συνδέεται μονοσήμαντα με τον υπογράφοντα,
β) ταυτοποιεί τον υπογράφοντα,
γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του και
δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε αλλοίωση των εν λόγω δεδομένων» (Π.Δ. 150/2001 Προσαρμογή στην Οδηγία 99/93/ΕΚ)

Προκύπτει από τους παραπάνω ενδεικτικούς ορισμούς πως η ψηφιακή υπογραφή παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσης του περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά. Επιπλέον, έχει επιβεβαιωτική λειτουργία, καθώς εξασφαλίζει ότι το μήνυμα που λαμβάνει

ο παραλήπτης ανήκει όντως στον αποστολέα και ότι είναι ακέραιο, αλλά και εμπιστευτική λειτουργία, καθώς μόνο ο
παραλήπτης είναι σε θέση να διαβάσει το μήνυμα και κανένας άλλος.

Συνοψίζοντας λοιπόν, θα λέγαμε ότι η Ψηφιακή Υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού (hash function) για δημιουργία της σύνοψης (hash) σε συνδυασμό με ασυμμετρική κρυπτογραφία για κρυπτογράφηση/αποκρυπτογράφηση σύνοψης (ο συνδυασμός σύνοψης και κρυπτογράφησης με ασυμμετρική κρυπτογραφία αποδεικνύει την ακεραιότητας του εγγράφου αλλά και την απόδειξη ταυτότητας του αποστολέα). Σε μερικές χώρες όπως τις ΗΠΑ και κάποιες χώρες της Ευρωπαϊκής ένωσης, οι ψηφιακές υπογραφές έχουν και νομική υπόσταση. Οι ψηφιακές υπογραφές σε ψηφιακά έγγραφα είναι παρόμοιες με τις αντίστοιχες χειρόγραφες υπογραφές σε έντυπα έγγραφα. Όταν οι ψηφιακές υπογραφές υλοποιούνται - εφαρμόζονται σωστά (με χρήση ασφαλών κρυπτογραφικών αλγορίθμων), είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις αντίστοιχες χειρόγραφες. Επίσης το φυσικό πρόσωπο που ψηφιακά υπογράφει το ψηφιακό έγγραφο δεν μπορεί να ισχυριστεί ότι δεν το υπόγραψε (όσο το ιδιωτικό κλειδί που χρησιμοποίησε δεν υποκλάπηκε). Κάποιες υλοποιήσεις των ψηφιακών υπογραφών προσθέτουν και την ημερομηνία υπογραφής του εγγράφου, ώστε και τον ιδιωτικό κλειδί να υποκλαπεί, η ψηφιακή υπογραφή να είναι έγκυρη. Η ψηφιακή υπογραφή μπορεί να προστεθεί σε οποιαδήποτε σειρά από bits (δηλαδή δεδομένα): παραδείγματα χρήσης είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, μηνύματα που στέλνονται στο Διαδίκτυο κλπ. Πολλοί οργανισμοί υιοθετούν την χρήση των ψηφιακών υπογραφών ώστε να αποφεύγεται η αποστολή τυπωμένων εγγράφων (επικυρωμένα με χρήση σφραγίδων και υπογραφών). Τα σχήματα ψηφιακών υπογραφών χρησιμοποιούνται σήμερα σε ηλεκτρονικές τραπεζικές συναλλαγές, ηλεκτρονικό εμπόριο, σε ανταλλαγή κλειδιών για συμμετρικά κρυπτοσυστήματα κ.τ.λ. Σημαντικό είναι πάντως, να τονίσουμε ότι όλο και περισσότερες χώρες (μετά τις ΗΠΑ) αρχίζουν να αναγνωρίζουν νομικά την ισχύ της Ψηφιακής Υπογραφής.

Το 1976 ο Whitfield Diffie και ο Martin Hellman για πρώτη φορά παρουσίασαν την ιδέα των ψηφιακών υπογραφών, αν και η κεντρική ιδέα των τέτοιων συστημάτων προϋπήρχε. Λίγο αργότερα ο Ronald Rivest, ο Adi Shamir και ο Len Adleman παρουσίασαν τον αλγόριθμο RSA ο οποίος χρησιμοποιήθηκε στις πρώτες ψηφιακές υπογραφές. Οι πρώτες ψηφιακές υπογραφές με τον αλγόριθμο RSA αποδείχθηκαν ότι δεν ήταν ασφαλείς. Το πρώτο, ευρέος γνωστό στην αγορά, λογισμικό που χρησιμοποίησε τέτοιες ψηφιακές υπογραφές ήταν τον Lotus Notes 1.0, το οποίο κυκλοφόρησε το 1989. Η χρήση της συνάρτησης κατατεμαχισμού στις ψηφιακές προστέθηκε αργότερα για λόγους ασφάλειας. Η ιδέα είναι ότι υπολογίζεται η σύνοψη (hash) του μηνύματος/εγγράφου και η ψηφιακή υπογραφή υπολογίζεται πάνω στην σύνοψη (hash) και όχι στο μήνυμα/έγγραφο. Άλλοι αλγόριθμοι που αναπτύχθηκαν μετά το RSA ήταν οι ψηφιακές υπογραφές Lamport, οι ψηφιακές υπογραφές Merkle (γνωστές ως δένδρα Merkle ή απλούστερα "δένδρα συνόψεων/hash") και οι ψηφιακές υπογραφές Rabin. Το 1988 ο Shafi Goldwasser, ο Silvio Micali και ο Ronald Rivest ήταν οι πρώτοι που δημοσίευσαν ολοκληρωμένη μελέτη για τις απαιτήσεις ασφάλειας των ψηφιακών υπογραφών. Παρουσίασαν με ποιους τρόπους κάποιος μπορεί να παραβιάσει τις υπάρχουσες υλοποιήσεις ψηφιακών υπογραφών και παρουσίασαν το μοντέλο ψηφιακών υπογραφών GMR.

Οι πρόσφατες υλοποιήσεις ψηφιακών υπογραφών είναι παρόμοιας τεχνικής: χρησιμοποιούν μια συνάρτηση της οποίας η έξοδος δεν είναι προβλέψιμη από την είσοδο (trapdoor function), όπως η συνάρτηση RSA. Η κύρια τεχνική είναι ότι η ψηφιακή υπογραφή είναι η σύνοψη (hash) του μηνύματος κρυπτογραφημένη με το ιδιωτικό κλειδί (χρησιμοποιώντας ασυμμετρική κρυπτογραφία). Υπάρχουν διάφοροι λόγοι που ουσιαστικά εφαρμόζεται η ψηφιακή υπογραφή στην σύνοψη του μηνύματος (hash) και όχι σε ολόκληρο το μήνυμα/έγγραφο:

- Αποτελεσματικότητα (efficiency): Η ψηφιακή υπογραφή είναι πολύ μικρότερη σε μέγεθος και χρειάζεται λιγότερο χρόνος για να εφαρμοστεί η ψηφιακή υπογραφή (η σύνοψη (hash)) έχει πολύ μικρότερο μέγεθος από ότι ολόκληρο το μήνυμα/έγγραφο).

- Συμβατότητα (compartibility): Τα μηνύματα/έγγραφα είναι ουσιαστικά μεταβλητές δέσμες bits. Ο αλγόριθμος κατατεμαχισμού μπορεί να μετατρέψει μεταβλητού μεγέθους δέσμες bits σε συγκεκριμένο αριθμό bits (σύνοψη - hash).
- Ακεραιότητα (integrity): Αν δεν εφαρμοστεί η συνάρτηση κατατεμαχισμού το αρχικό μήνυμα/έγγραφο θα πρέπει να διαιρεθεί σε μικρότερα μεγέθη bits (πακέτα bits) ώστε ο αλγόριθμος ψηφιακών υπογραφών να εφαρμοστεί σε αυτά. Ο αποδέκτης των πακέτων bits δεν είναι σε θέση να αναγνωρίσει αν όλα τα πακέτα έχουν έρθει και αν βρίσκονται στη σωστή σειρά.

Η ψηφιακή υπογραφή αποτελείται από τρεις αλγόριθμους:

- Ο αλγόριθμος δημιουργίας δημόσιου και ιδιωτικού κλειδιού: Ο αλγόριθμος αυτός χρησιμοποιεί μια γεννήτρια τυχαίων αριθμών και με βάση αυτόν τον τυχαίο αριθμό δημιουργεί το δημόσιο και ιδιωτικό κλειδί (με το ιδιωτικό κλειδί δημιουργείται η ψηφιακή υπογραφή και με το δημόσιο κλειδί ελέγχεται η ψηφιακή υπογραφή).
- Ο αλγόριθμος προσθήκης ψηφιακής υπογραφής σε μηνύματα ή έγγραφα: Χρησιμοποιώντας το μήνυμα/έγγραφο και το ιδιωτικό κλειδί (το οποίο ανήκει μόνο σε αυτόν που υπογράφει το έγγραφο), δημιουργεί την ψηφιακή υπογραφή.
- Ο αλγόριθμος έλεγχου ψηφιακής υπογραφής μηνύματος ή εγγράφου: Χρησιμοποιώντας το μήνυμα/έγγραφο και το δημόσιο κλειδί (το δημόσιο κλειδί είναι διαθέσιμο σε όλους, και συσχετίζεται με το ιδιωτικό κλειδί και ανήκει αυτόν που υπέγραψε ψηφιακά το μήνυμα/έγγραφο), ελέγχει την αυθεντικότητα (ποιος το υπέγραψε) αλλά και ακεραιότητα (ότι το μήνυμα δεν παραποιήθηκε) του μηνύματος/εγγράφου.

Σύμφωνα με την ασυμμετρική κρυπτογράφηση κάποιος που γνωρίζει το δημόσιο κλειδί δεν μπορεί να δημιουργήσει (είναι υπολογιστικά ανέφικτο) το αντίστοιχο ιδιωτικό κλειδί. Επίσης κάποιος ο οποίος έχει το δημόσιο κλειδί μπορεί να ελέγξει την αυθεντικότητα και ακεραιότητα ενός μηνύματος/εγγράφου το οποίο είναι ψηφιακά υπογεγραμμένο.

Ένα πρόβλημα με τις ψηφιακές υπογραφές είναι ότι δεν γνωρίζουμε αν το δημόσιο κλειδί (κατά την διάρκεια ελέγχου της υπογραφής) που έχουμε ανήκει σε αυτόν που ισχυρίζεται ότι είναι. Για αυτό ακριβώς τον λόγο υπάρχει ο Πάροχος Υπηρεσιών Πιστοποίησης ο οποίος είναι ένας οργανισμός-οντότητα ο οποίος πιστοποιεί την σχέση ενός ανθρώπου με το δημόσιο κλειδί του. Ο Πάροχος Υπηρεσιών Πιστοποίησης θα πρέπει να εμπνέει εμπιστοσύνη γιατί είναι η αρχή η οποία εκδίδει ψηφιακά πιστοποιητικά. Τα ψηφιακά πιστοποιητικά ταυτοποιούν ένα δημόσιο κλειδί με τον δικαιούχο του. Πολλές φορές αυτός που υπογράφει ψηφιακά ένα ηλεκτρονικό έγγραφο, ενδέχεται να επισυνάψει στο έγγραφο μαζί με την ψηφιακή υπογραφή και το ψηφιακό πιστοποιητικό του δημόσιου κλειδιού.

Οι ψηφιακές υπογραφές λοιπόν, χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει. Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα).

Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης. Η ηλεκτρονική υπογραφή, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα!! Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος. Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες όπως προαναφέραμε: τη δημιουργία της υπογραφής και την επαλήθευσή της. Παρακάτω, θα αναφέρουμε βήμα προς βήμα τις ενέργειες του αποστολέα και του παραλήπτη ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής.

Αποστολέας

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.

2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.

3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).

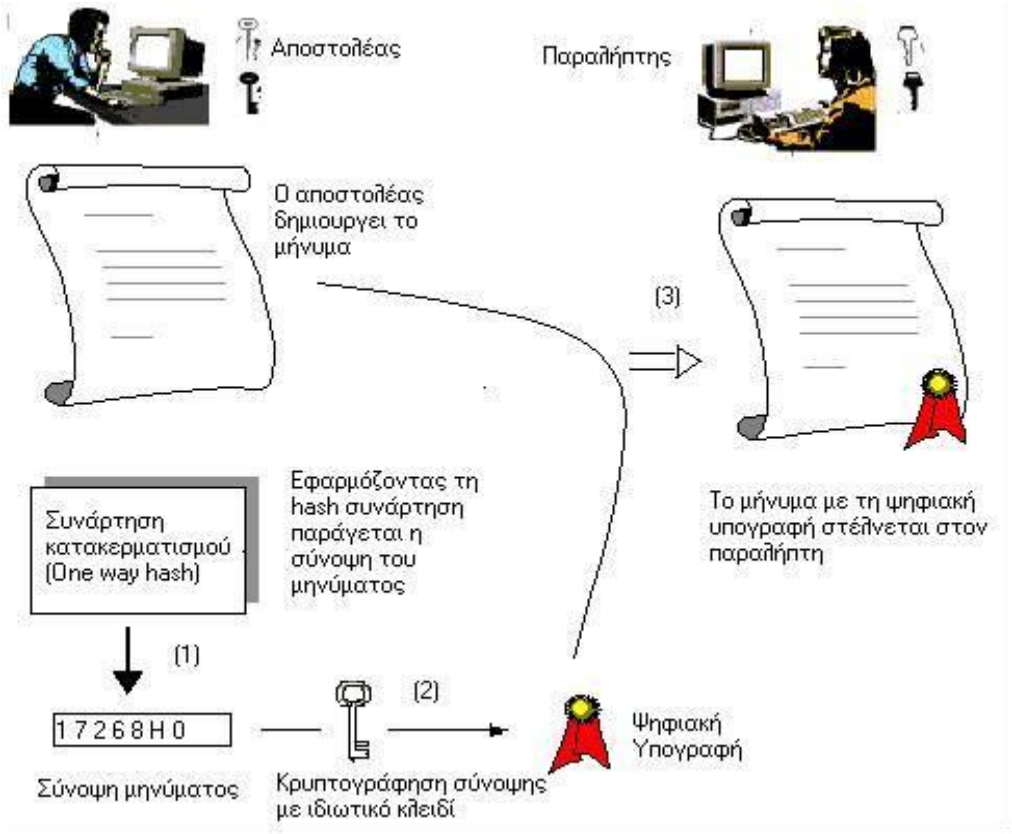
Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).

2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος ( ψηφιακή υπογραφή).

4. Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.




### *3.3. <u>Δημιουργία ψηφιακής υπογραφής</u>*

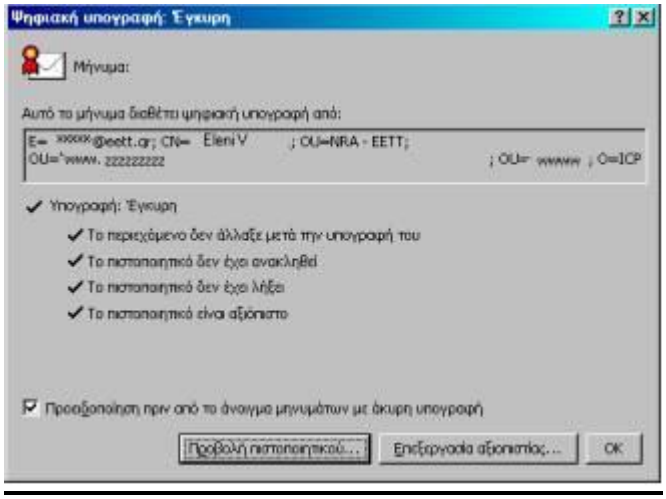
Οι παραπάνω διεργασίες γίνονται από το ανάλογο λογισμικό στον υπολογιστή του χρήστη.

Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι (και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί) ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε (μη αποποίηση). Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί. Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι η οντότητα που παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ένα ηλεκτρονικό αρχείο) στο οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του. Από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών είναι το πιστοποιητικό δημοσίου κλειδιού ( public key certificate). Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το

υπογράφει. Το ψηφιακό πιστοποιητικό, είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Παρόχου Υπηρεσιών Πιστοποίησης, όπου ο Πάροχος με την ψηφιακή του υπογραφή, υπογράφει το πιστοποιητικό του δικαιούχου. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο Πάροχος εκδίδει. Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο χρήστης δεν γνωρίζει έναν Πάροχο και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει, και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο που ο χρήστης εμπιστεύεται, τότε ο χρήστης μπορεί να εμπιστευθεί τον πρώτο Πάροχο. Ο χρήστης, μπορεί να επαληθεύσει τη ψηφιακή υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που έχει εκδώσει ένα ψηφιακό πιστοποιητικό, χρησιμοποιώντας το δημόσιο κλειδί του Παρόχου, για το οποίο (δημόσιο κλειδί) ένας άλλος Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει εκδώσει πιστοποιητικό κ.λπ.

Παράδειγμα προβολής πιστοποιητικού


### *3.4. Ένδειξη ψηφιακής υπογραφής σε μήνυμα με πιστοποιητικό*




Ένα πιστοποιητικό εφόσον διαπιστωθεί ή υπάρχει υπόνοια ότι για κάποιους λόγους δεν είναι έγκυρο (π.χ. αν το ιδιωτικό κλειδί του δικαιούχου έχει γίνει γνωστό σε τρίτους ή το πρόσωπο εξαπάτησε τον Πάροχο Υπηρεσιών Πιστοποίησης ως προς τα στοιχεία της ταυτότητάς του κ.λπ.), τότε ο Πάροχος Υπηρεσιών Πιστοποίησης προβαίνει στην ανάκλησή του, όπως ρυθμίζεται από τη νομοθεσία.

Για την εγκυρότητα μιας καθημερινής συναλλαγής απαιτείται η υπογραφή του συναλλασσόμενου. Η υπογραφή σε ένα κείμενο, αποτελεί απόδειξη ότι το υπογράφον το περιεχόμενο του κειμένου πρόσωπο γνωρίζει, αναγνωρίζει, αποδέχεται το κείμενο αυτό. Ο υπογράφων δεν μπορεί να αρνηθεί το από αυτόν υπογεγραμμένο περιεχόμενο, εκτός από συγκεκριμένες περιπτώσεις εκδήλωσης παραβατικής συμπεριφοράς (πλαστογραφία, απάτη κ.λπ.). Ένα υπογεγραμμένο κείμενο έχει νομική υπόσταση και επικυρώνει τη συναλλαγή.

Το Π.Δ. 150/2000 που εναρμόνισε την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, καθόρισε το πλαίσιο εκείνο μέσα στο οποίο μία ψηφιακή υπογραφή αναγνωρίζεται νομικά ως ιδιόχειρη. Αυτό σημαίνει ότι υπό συγκεκριμένες προϋποθέσεις, τα πρόσωπα που συμβάλλονται σε μία ηλεκτρονική συναλλαγή, και υπογράφουν ηλεκτρονικά, δεν μπορεί να την αρνηθούν.

Επιπλέον, το προεδρικό Διάταγμα, εκτός των άλλων,

- καθόρισε τους όρους που πρέπει να ισχύουν σε ψηφιακά πιστοποιητικά για να θεωρούνται αναγνωρισμένα πιστοποιητικά και τους όρους που πρέπει να πληρούν οι Πάροχοι Υπηρεσιών Πιστοποίησης για να παρέχουν αναγνωρισμένα πιστοποιητικά.
- έθεσε τις αρχές λειτουργίας της εσωτερικής αγοράς όσον αφορά την παροχή υπηρεσιών πιστοποίησης
- έθεσε τις προϋποθέσεις νομικής αναγνώρισης εντός ΕΕ των αναγνωρισμένων πιστοποιητικών που εκδίδονται από Παρόχους Υπηρεσιών Πιστοποίησης εγκατεστημένους σε χώρες εκτός ΕΕ, και άλλες σχετικές προβλέψεις που αφορούν διεθνείς πτυχές.
- έθεσε το πλαίσιο της ευθύνης των Παρόχων Υπηρεσιών Πιστοποίησης
- ανέθεσε στην ΕΕΤΤ συγκεκριμένες αρμοδιότητες.

Οι αρμοδιότητες της ΕΕΤΤ όπως απορρέουν από το ΠΔ 150/2001, είναι επιγραμματικά οι εξής:

- Η παροχή Εθελοντικής Διαπίστευσης, ύστερα από έγγραφη αίτηση του ενδιαφερόμενου Παρόχου Υπηρεσιών Πιστοποίησης, προκειμένου να επιτευχθεί βελτιωμένο επίπεδο παροχής υπηρεσιών πιστοποίησης. (άρθρο 4 παρ. 5 εδ.α) ή η ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού. Με την Εθελοντική Διαπίστευση απονέμονται δικαιώματα και επιβάλλονται υποχρεώσεις, συμπεριλαμβανομένων τελών, στον Πάροχο Υπηρεσιών Πιστοποίησης.
- Η εποπτεία και ο έλεγχος των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και των φορέων διαπίστευσης και ελέγχου της συμμόρφωσης των υπογραφών προς το Παράρτημα ΙΙΙ του πδ. 150/2001 (εφόσον η ΕΕΤΤ αναθέσει τέτοια καθήκοντα σε άλλους φορείς) (άρθρο 4 παρ. 8).

- Η διαπίστωση της συμμόρφωσης των διατάξεων δημιουργίας υπογραφής (υλικού ή λογισμικού που χρησιμοποιείται για την εφαρμογή του ιδιωτικού κλειδιού για τη δημιουργία της ηλεκτρονικής υπογραφής) προς το Παράρτημα ΙΙΙ του Προεδρικού Διατάγματος 150/2001 (άρθρο 4 παρ. 2, εδ.α) ή ανάθεση σε δημόσιους ή ιδιωτικούς φορείς του έργου αυτού.
- Η επιβολή προστίμων σε Παρόχους Υπηρεσιών Πιστοποίησης, οι οποίοι ενεργούν ως διαπιστευμένοι, χωρίς να είναι (άρθρο 4 παρ.9)
- Η ενημέρωση της Ευρωπαϊκής Επιτροπής για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων εθνικών Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και για τυχόν αλλαγές στις παραπάνω πληροφορίες (άρθρα 8 παρ. 2 και 3).

Η ΕΕΤΤ με την υπ. αρ. 248/71 Απόφασή της «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (ΦΕΚ 603/Β/16-5-2002) ρυθμίζει ζητήματα των αναγνωρισμένων πιστοποιητικών και θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης

Η Κρυπτογραφία έχει μια μακρά και συναρπαστική ιστορία. Η πιο ολοκληρωμένη και χωρίς τεχνικούς όρους περιγραφή του θέματος είναι το βιβλίο The Codebreakers του Kahn. Το βιβλίο αυτό ακολουθεί τα ίχνη της κρυπτογραφίας από την αρχική και περιορισμένη χρήση της από τους Αιγύπτιους περίπου 4000 χρόνια πριν, μέχρι τον εικοστό αιώνα όπου έπαιξε κρίσιμο ρόλο στην έκβαση και των δύο παγκόσμιων πολέμων. Ολοκληρωμένο το 1963, το βιβλίο του Kahn καλύπτει εκείνες τις πλευρές της ιστορίας, οι οποίες ήταν οι πιο σημαντικές (μέχρι τότε) στην εξέλιξη του θέματος. Αυτοί που ασκούσαν κυρίως την τέχνη ήταν όσοι σχετίζονταν με τον στρατό, τη διπλωματική υπηρεσία και την κυβέρνηση γενικότερα. Η κρυπτογραφία χρησιμοποιούνταν σαν εργαλείο για την προστασία των εθνικών μυστικών και στρατηγικών. Η εξάπλωση των υπολογιστών και των συστημάτων επικοινωνίας τη δεκαετία του ’60 έφερε μαζί της μια απαίτηση από τον ιδιωτικό τομέα για την ύπαρξη μέσων προστασίας των πληροφοριών σε ψηφιακή μορφή και για την παροχή υπηρεσιών ασφάλειας. Αρχίζοντας με την έρευνα του Feistel στην IBM στις αρχές της δεκαετίας του ’70 και μεσουρανώντας στα 1977, με την υιοθεσία του ως Πρότυπο Επεξεργασίας Ομοσπονδιακών Πληροφοριών των Η.Π.Α για την κρυπτογράφηση μη απόρρητων πληροφοριών, το DES, το Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard), είναι ο πιο γνωστός κρυπτογραφικός μηχανισμός στην ιστορία. Παραμένει το καθιερωμένο μέσο για την ασφαλή προστασία του ηλεκτρονικού εμπορίου για πολλά οικονομικά ιδρύματα ανά τον κόσμο.

Η πιο αξιοσημείωτη εξέλιξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν οι Diffie και Hellman δημοσίευσαν το άρθρο τους New Directions in Cryptography (Νέες Κατευθύνσεις στην Κρυπτογραφία). Αυτή η εργασία εισήγαγε την επαναστατική ιδέα της κρυπτογραφίας δημόσιου κλειδιού και επίσης παρείχε μια νέα και ευφυή μέθοδο για την ανταλλαγή κλειδιών, η ασφάλεια της οποίας βασίζεται στη δυσεπιλυσιμότητα του προβλήματος διακριτού λογαρίθμου. Παρ’ όλο που οι συγγραφείς δεν είχαν τότε να προτείνουν μια πρακτική υλοποίηση ενός σχήματος κρυπτογράφησης δημόσιου κλειδιού, η ιδέα ήταν ξεκάθαρη και δημιούργησε έντονο ενδιαφέρον και εκτεταμένη δραστηριότητα στην κρυπτογραφική κοινότητα.

Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν το πρώτο πρακτικό σχήμα κρυπτογράφησης και υπογραφής δημόσιου κλειδιού, το οποίο αναφέρεται τώρα ως RSA. Το σχήμα RSA βασίζεται σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, τη δυσεπιλυσιμότητα της παραγοντοποίησης μεγάλων ακεραίων. Αυτή η εφαρμογή ενός δύσκολου μαθηματικού προβλήματος στην κρυπτογραφία αναζωογόνησε τις προσπάθειες για την εύρεση περισσότερο αποδοτικών μεθόδων παραγοντοποίησης. Στη δεκαετία του 80 σημειώθηκαν σημαντικές πρόοδοι σ’ αυτόν τον τομέα, αλλά καμία που να καθιστά το σύστημα RSA ανασφαλές.

Μια άλλη κλάση ισχυρών και πρακτικών σχημάτων δημόσιου κλειδιού ανακαλύφθηκε από τον ElGamal το 1985. Τα σχήματα αυτά βασίζονται επίσης στο πρόβλημα διακριτού λογαρίθμου. Μια από τις πιο σημαντικές συνεισφορές που παρείχε η κρυπτογραφία δημόσιου κλειδιού είναι η ψηφιακή υπογραφή. Το 1991 υιοθετήθηκε το πρώτο διεθνές πρότυπο για ψηφιακές υπογραφές (ISO/IEC 9796). Είναι βασισμένο στο σχήμα δημόσιου κλειδιού RSA. Το 1994 η Κυβέρνηση των Η.Π.Α υιοθέτησε το Πρότυπο Ψηφιακών Υπογραφών (Digital Signature Standard – DSA), έναν μηχανισμό βασισμένο στο σχήμα δημόσιου κλειδιού ElGamal.

Η έρευνα για νέα σχήματα δημόσιου κλειδιού, βελτιώσεις στους υπάρχοντες κρυπτογραφικούς μηχανισμούς και αποδείξεις της ασφάλειας, συνεχίζονται με ταχύτατα βήματα. Εμφανίζονται διαρκώς διάφορα πρότυπα και υποδομές που εμπλέκουν την κρυπτογραφία. Αναπτύσσονται προϊόντα ασφάλειας προκειμένου να ανταποκριθούν στις ανάγκες προστασίας μιας αναπτυσσόμενης κοινωνίας της πληροφορίας. Η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι αυτό άτομα (εμπιστευτικότητα). Τα δεδομένα, δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά την μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (ακεραιότητα). Επιπλέον, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (αυθεντικότητα). Δηλαδή, να γνωρίζει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ. Χ, είναι όντως από τον κ. Χ και όχι από κάποιον που παριστάνει τον Χ. Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή (π.χ. ηλεκτρονικό εμπόριο) θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (μη αποποίηση ευθύνης). Οι παραπάνω ιδιότητες, (εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση) στον ηλεκτρονικό κόσμο, αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών. Διάφοροι μηχανισμοί, τεχνικές και τεχνολογίες έχουν αναπτυχθεί αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή.

Η ανάγκη για εμπιστευτικότητα στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία. Ο αποστολέας χρησιμοποιώντας κάποια μαθηματική συνάρτηση μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, μέχρι να αποκρυπτογραφηθεί. Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν αλγόριθμους και κλειδιά (σειρά από bits συγκεκριμένου μήκους) για να διατηρήσουν την πληροφορία ασφαλή.

Μία παραδοσιακή μέθοδος κρυπτογράφησης είναι η συμμετρική κρυπτογραφία η οποία χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αποστολέας κρυπτογραφεί και ο παραλήπτης αποκρυπτογραφεί με το ίδιο κλειδί. Το κλειδί θα πρέπει να παραμένει μυστικό και να είναι γνωστό μόνο στους συναλλασσόμενους.

Η μέθοδος αυτή παρουσιάζει μειονεκτήματα όσον αφορά την εφαρμογή της σε ανοιχτά δίκτυα με πολλούς χρήστες και τις αυξημένες απαιτήσεις της για την ασφάλεια (π.χ. αποθήκευση των κλειδιών κ.λπ.). Η ασύμμετρη κρυπτογραφία (ή κρυπτογραφία δημοσίου κλειδιού- public key cryptography) χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Κάθε χρήστης έχει στη διάθεσή του δύο κλειδιά. Το δημόσιο κλειδί είναι αυτό που ο χρήστης μπορεί να το γνωστοποιήσει σε τρίτους ενώ το ιδιωτικό είναι εκείνο που το φυλάσσει με ασφάλεια και μόνο αυτός θα πρέπει να το γνωρίζει και κατέχει. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη. Έτσι, το μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη (που είναι ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού εκτός και αν η μυστικότητα του ιδιωτικού κλειδιού έχει παραβιαστεί).

### *3.5. Συναρτήσεις κατακερματισμού και ψηφιακές υπογραφές*

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού (ή κατατεμαχισμού) είναι μηχανισμοί ύψιστης σημασίας στον τομέα της κρυπτογραφίας. Σε μεγαλύτερο βαθμό από τους αλγόριθμους κρυπτογράφησης, οι μονόδρομες λειτουργίες των συναρτήσεων τύπου hash αποτελούν την κινητήριο δύναμη της σύγχρονης κρυπτογραφίας. Χρησιμοποιούνται σε συνδυασμό με αλγορίθμους δημόσιων κλειδιών τόσο για κρυπτογράφηση, όσο και για ψηφιακές υπογραφές, ενώ εφαρμόζονται ευρέως και στην ακεραιότητα των δεδομένων, στη διαχείριση αρχείων και στα πρωτόκολλα αναγνώρισης (identification protocols).

Οι συναρτήσεις κατακερματισμού είναι υπολογιστικά εφικτές συναρτήσεις της μορφής h: D→R όπου το σύνολο R είναι πεπερασμένο και |D| > |R|, ενώ δεν αποκλείεται |D| = ∞. Δέχονται στην είσοδό τους ένα οσοδήποτε μεγάλο μήνυμα x (όρισμα) και στην έξοδο δίνουν ένα αλφαριθμητικό σταθερού μήκους, ίσου ή μικρότερου του μεγέθους εισόδου. Συγκεκριμένα, μια συνάρτηση κατακερματισμού h αντιστοιχίζει σειρές bit μεταβλητού μεγέθους σε ακολουθία συγκεκριμένου μεγέθους. Η ακολουθία αυτή συμβολίζεται με h(x) και αναφέρεται ως «σύνοψη» του μηνύματος (message digest), αποτύπωμα (fingerprint) ή τιμή κατακερματισμού (hash value). Είναι μια ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού είναι συναρτήσεις μονής κατεύθυνσης (one-way functions) διότι από τη σύνοψη που δημιουργούν είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Είναι δηλαδή εξαιρετικά απίθανη η αντιστροφή μιας συνάρτησης hash.

Επιπλέον, η πιθανότητα δύο διαφορετικά μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά τη μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

Αυτό ακριβώς είναι και το ενδιαφέρον με τις συναρτήσεις τύπου hash: η εξαιρετική «ευαισθησία» που έχουν στο περιεχόμενο του μηνύματος εισόδου. Εάν αυτό μεταβληθεί στο παραμικρό, τότε το αλφαριθμητικό εξόδου διαφέρει πολύ από το προηγούμενο. Εφαρμόζοντας για παράδειγμα, μια γνωστή υλοποίηση συνάρτησης hash στο αλφαριθμητικό “RAM”, παίρνουμε ως αποτέλεσμα το αλφαριθμητικό “8d8bea89388715ee7c01183a0667e892”. Δίνοντας όμως στην ίδια συνάρτηση το αλφαριθμητικό “RaM” (πεζό a αντί για κεφαλαίο) παίρνουμε στην έξοδο το αλφαριθμητικό “73ac38c363394f66211f67f0a92b480a”, ουδεμία ομοιότητα.

*Ορισμός:* Η συνάρτηση κατακερματισμού h: D→R καλείται μοναδικής κατεύθυνσης αν υπάρχει αλγόριθμος πολυωνυμικού χρόνου ο οποίος για κάθε x ε D υπολογίζει την τιμή h(x), ενώ σχεδόν για κάθε y ε h(D) είναι υπολογιστικά ανέφικτη η εύρεση x ε D με h(x) = y.

Σημείωση: σημειώνουμε ότι δεν είναι γνωστό αν υπάρχουν συναρτήσεις μοναδικής κατεύθυνσης. Υπάρχουν όμως συναρτήσεις των οποίων οι τιμές υπολογίζονται εύκολα και συγχρόνως δε γνωρίζουμε έναν αποδοτικό αλγόριθμο (πολυωνυμικού χρόνου) αντιστροφής τους. Τέτοιες συναρτήσεις θεωρούνται μοναδικής κατεύθυνσης και χρησιμοποιούνται στην κρυπτογραφία. Οι όροι μονόδρομη, μη αντιστρέψιμη, μονής κατεύθυνσης (ή μίας ή μοναδικής) και αντίσταση 1ου ορίσματος συμπίπτουν.

Με βάση τα παραπάνω, η μονόδρομη συνάρτηση κατακερματισμού h είναι ένας μετασχηματισμός με τις εξής ιδιότητες:

- **Συμπίεση (compression):** η είσοδος είναι οποιουδήποτε μήκους ενώ η έξοδος έχει περιορισμένο, σταθερό μήκος.

- **Ευκολία στον υπολογισμό:** δεδομένης της συνάρτησης h και ενός ορίσματος x είναι εύκολος ο υπολογισμός του h(x).

- **Αντίσταση 1ου ορίσματος (preimage resistance) – μη αντιστρεψιμότητα:** δεδομένης της συνάρτησης h και ενός στοιχείου y του πεδίου τιμών της, είναι υπολογιστικά ανέφικτο να βρεθεί x στο πεδίο ορισμού τέτοιο ώστε h(x) = y.

- **Αντίσταση 2ου ορίσματος (2nd preimage resistance):** για δοθέν όρισμα x1 είναι υπολογιστικά ανέφικτο να βρεθεί όρισμα x2 τέτοιο ώστε x1 ≠ x2 και h(x1) ≠ h(x2).

Επιπρόσθετες ιδιότητες των μονόδρομων συναρτήσεων κατακερματισμού:

- **Μη-συσχέτιση (non-correlation):** τα bit εισόδου και εξόδου δεν πρέπει να είναι συσχετισμένα.

- **Αντίσταση κοντινής σύγκρουσης (near-collision resistance):** θα πρέπει να είναι δύσκολο να βρεθεί ζεύγος εισόδων (x1, x2) ώστε οι αντίστοιχες h(x1), h(x2) να διαφέρουν σε ένα μικρό πλήθος bits.

- **Αντίσταση μερικού ορίσματος (partial preimage resistance) – τοπική μονοδρομικότητα (local one-wayness):**θα πρέπει να είναι το ίδιο δύσκολο να ανακτήσουμε οποιαδήποτε υποακολουθία χαρακτήρων, όσο και μια ολόκληρη είσοδο.

Οι συναρτήσεις κατακερματισμού μονής κατεύθυνσης εμπλέκονται άμεσα στις διαδικασίες δημιουργίας και επαλήθευσης ψηφιακών υπογραφών: Διευκολύνουν τα συμβαλλόμενα μέρη (οι κρυπτογραφικές διαδικασίες εφαρμόζονται στο message digest που έχει παραχθεί, το οποίο είναι πιο μικρό και εύκολο στη διαχείριση από το αρχικό μήνυμα) και ενισχύουν τόσο την αποδοτικότητα των αντίστοιχων αλγορίθμων όσο και την ασφάλεια των σχημάτων ψηφιακής υπογραφής (ένα message digest μπορεί να δημοσιοποιηθεί ή να υποκλαπεί χωρίς να αποκαλύπτεται το περιεχόμενο του αυθεντικού κειμένου). Έτσι, θεωρούμε τη χρήση τους σκόπιμη, σχεδόν σε κάθε σχήμα ψηφιακής υπογραφής.

Λόγω των λειτουργιών που προαναφέρθηκαν, οι συναρτήσεις hash εμποδίζουν τυχόν πλαστογραφήσεις. Εντούτοις, αφότου τα message digests είναι καθορισμένου μήκους, δεν είναι τόσο απεριόριστα στο πλήθος, όσο είναι όλα τα δυνατά μηνύματα. Αυτό οδηγεί σε άλλες επιθέσεις εναντίων σχημάτων ψηφιακής υπογραφής που χρησιμοποιούν συναρτήσεις τύπου hash.

### *3.6. Επίθεση γενεθλίων*

Είναι σημαντικό να σημειωθεί ότι η δυνατότητα παραγωγής δύο εγγράφων με την ίδια σύνοψη μπορεί να είναι χρήσιμη για κάποιον κακόβουλο και μάλιστα είναι σαφώς ευκολότερο από την παραγωγή ενός εγγράφου με συγκεκριμένη σύνοψη.

Η μέθοδος για να πραγματοποιηθεί αυτό είναι γνωστή ως «επίθεση γενεθλίων» (birthday attack) και ονομάζεται έτσι επειδή αν ερωτηθεί μια ομάδα ατόμων άνω των 25 ετών για τα γενέθλιά τους, υπάρχει μεγάλη πιθανότητα δύο από αυτούς να έχουν την ίδια ημέρα γενέθλια, γεγονός που εκπλήσσει τους περισσότερους καθώς θεωρούν ότι θα χρειαζόταν ένας μεγαλύτερος αριθμός ατόμων για να παραχθεί αυτό το αποτέλεσμα. Αυτό είναι γενικά αληθές για οποιαδήποτε τυχαία λίστα επιλεγμένη από ένα πεπερασμένο σύνολο.

Για να εφαρμοστεί αυτή η επίθεση στις συνόψεις αντικειμένων, πρέπει να πραγματοποιηθούν μια σειρά από ανακόλουθες αλλαγές σε δύο αντικείμενα και κάθε φορά να παράγεται μια σύνοψή τους, ώστε να παραχθεί μια λίστα από συνόψεις για το κάθε αντικείμενο. Μετά από ένα πλήθος προσπαθειών, περίπου ίσο με την τετραγωνική ρίζα του πλήθους των πιθανών τιμών σύνοψης, υπάρχει μεγάλη πιθανότητα ότι κάποια εκδοχή των δύο αντικειμένων που παράγουν την ίδια σύνοψη θα έχει κατασκευαστεί.

Στόχος αυτής της επίθεσης συνήθως είναι να υπογραφεί από το θύμα το ένα έγγραφο και στη συνέχεια να χρησιμοποιηθεί η υπογραφή του σαν να υπέγραψε το άλλο. Για την αποφυγή της παραπάνω επίθεσης, οι συναρτήσεις κατακερματισμού θα πρέπει να παράγουν αρκούντως μεγάλες συνόψεις. Συγκεκριμένα, επειδή αυτή η επίθεση ελαττώνει αποτελεσματικά τη δυσκολία μιας επίθεσης στο περίπου μισό του πλήθος των bits της σύνοψης, οι συναρτήσεις κατακερματισμού πρέπει να παράγουν διπλάσια σύνοψη για να είναι ασφαλείς.

Οι συνεχώς αυξανόμενες απαιτήσεις στον τομέα της κρυπτογράφησης και της ασφαλούς ηλεκτρονικής επικοινωνίας οδήγησαν στην ανάπτυξη μιας σειράς συναρτήσεων κατακερματισμού και σχετικών τεχνολογιών, με σημαντικότερες τις πιο κάτω:

- **HMAC:** είναι μία τεχνική που χρησιμοποιείται για να ελέγχεται αν κάποιο αρχείο έχει τροποποιηθεί. Χρησιμοποιεί μια συνάρτηση κατακερματισμού και ένα ιδιωτικό κλειδί. Η συνάρτηση εφαρμόζεται στο κείμενο, η σύνοψη κρυπτογραφείται και αποστέλλεται τελικά με το αυθεντικό κείμενο. Ο παραλήπτης αποκρυπτογραφεί τη σύνοψη, κατακερματίζει το μήνυμα (εφαρμόζοντας την δημόσια γνωστή συνάρτηση κατακερματισμού) και συγκρίνει τα δύο αποτελέσματα. Αν συμφωνούν, τότε το μήνυμα έφτασε «ασφαλές».

- **Η σειρά MD (Message Digest):** είναι μια σειρά συναρτήσεων κατακερματισμού που αναπτύχθηκε από τον Ron Rivest. Όλες παράγουν ως αποτέλεσμα έναν αριθμό των 128 bits. Διαφέρουν μεταξύ τους όσον αφορά την ταχύτητα με την οποία μπορούν να υπολογιστούν και την ισχύ τους (αντίσταση σε συγκρούσεις).

- **Η σειρά SHA (Secure Hash Algorithm):** το 1993 το National Institute of Standards and Technology (NIST) εξέδωσε τη συνάρτηση SHA και το 1995 εντοπίζοντας μια νέα αδυναμία έκανε μια αλλαγή στον αλγόριθμό της. Ο νέος αλγόριθμος ονομάστηκε SHA-1 και είναι σήμερα η πιο δημοφιλής συνάρτηση τύπου hash. Δέχεται στην είσοδο μήνυμα μικρότερο από 264 bits και δίνει στην έξοδο κρυπτογράφημα μήκους 160 bits.

Οι πρόσφατες υλοποιήσεις ψηφιακών υπογραφών είναι παρόμοιας τεχνικής: χρησιμοποιούν μια συνάρτηση της οποίας η έξοδος δεν είναι προβλέψιμη από την είσοδο (trapdoor function), όπως η συνάρτηση RSA. Η κύρια τεχνική είναι ότι η ψηφιακή υπογραφή είναι η σύνοψη (hash) του μηνύματος κρυπτογραφημένη με το ιδιωτικό κλειδί (χρησιμοποιώντας ασυμμετρική κρυπτογραφία). Υπάρχουν διάφοροι λόγοι που ουσιαστικά εφαρμόζεται η ψηφιακή υπογραφή στην σύνοψη του μηνύματος (hash) και όχι σε ολόκληρο το μήνυμα/έγγραφο:

- Αποτελεσματικότητα (efficiency): Η ψηφιακή υπογραφή είναι πολύ μικρότερη σε μέγεθος και χρειάζεται λιγότερο χρόνος για να εφαρμοστεί η ψηφιακή υπογραφή (η σύνοψη (hash)) έχει πολύ μικρότερο μέγεθος από ότι ολόκληρο το μήνυμα/έγγραφο).
- Συμβατότητα (compartibility): Τα μηνύματα/έγγραφα είναι ουσιαστικά μεταβλητές δέσμες bits. Ο αλγόριθμος κατατεμαχισμού μπορεί να μετατρέψει μεταβλητού μεγέθους δέσμες bits σε συγκεκριμένο αριθμό bits (σύνοψη - hash).
- Ακεραιότητα (integrity): Αν δεν εφαρμοστεί η συνάρτηση κατατεμαχισμού το αρχικό μήνυμα/έγγραφο θα πρέπει να διαιρεθεί σε μικρότερα μεγέθη bits (πακέτα bits) ώστε ο αλγόριθμος ψηφιακών υπογραφών να εφαρμοστεί σε αυτά. Ο αποδέκτης των πακέτων bits δεν είναι σε θέση να αναγνωρίσει αν όλα τα πακέτα έχουν έρθει και αν βρίσκονται στη σωστή σειρά.

**Διάγραμμα χρήσης ψηφιακής υπογραφής:** Η ψηφιακή υπογραφή είναι η σύνοψη του μηνύματος κωδικοποιημένη με το ιδιωτικό κλειδί του αποστολέα. Μαζί με την ψηφιακή υπογραφή μπορεί να επισυνάπτει και το πιστοποιητικό (από έμπιστη/ο αρχή-οργανισμό) το οποίο πιστοποιεί τον ιδιοκτήτη του δημόσιου κλειδιού (το πιστοποιητικό μπορεί να χρησιμοποιηθεί αργότερα στον έλεγχο της υπογραφής).

**Ασυμμετρική Κρυπτογραφία:** Μεγάλος τυχαίος αριθμός (έξοδος γεννήτριας τυχαίων αριθμών), γεννήτρια ιδιωτικού και δημόσιου κλειδιού.

**Δημιουργία σύνοψης/digest με την συνάρτηση κατατεμαχισμού (hash function):** Μικρές αλλαγές στην είσοδο δημιουργούν εντελώς διαφορετικές νέες συνόψεις.

*Άλλες μορφές ηλεκτρονικής υπογραφής*
Ψηφιακές υπογραφές - υδατογραφήματα (watermarks)

Όπως έχει αναφερθεί παραπάνω, η ραγδαία εξάπλωση και ευρύτατη διείσδυση του Διαδικτύου (Internet) σε ποικίλους χώρους της κοινωνικής δραστηριότητας είχε σαν αποτέλεσμα την ανάπτυξη συνόλου μηχανισμών προστασίας για τη διαφύλαξη της ασφάλειας των συναλλαγών, της κατοχύρωσης των πνευματικών δικαιωμάτων στα διακινούμενα ψηφιακά αντικείμενα. Εκτός από τις ψηφιακές υπογραφές και την κρυπτογραφία έννοιες όπως η στεγανογραφία, η υδατογράφηση αναφέρονται στη βιβλιογραφία ως μέθοδοι

προστασίας των πνευματικών δικαιωμάτων στον ψηφιακό κόσμο. Κρίθηκε λοιπόν απαραίτητη, για την αποφυγή συγχύσεων η συνοπτική παράθεση των τεχνικών αυτών, και η αποσαφήνιση πιθανών μεταξύ τους διαφορών. Η στεγανογραφία επιτρέπει την κρυφή επικοινωνία, συνήθως κρύβοντας τις πληροφορίες σε άλλα δεδομένα υπεράνω υποψίας. Βασίζεται στην υπόθεση ότι η ύπαρξη κρυφής επικοινωνίας είναι άγνωστη σε τρίτους και χρησιμοποιείται κυρίως στην κρυφή σημείο-προς-σημείο επικοινωνία ανάμεσα σε έμπιστα μέρη. Ως εκ τούτου, οι κρυφές πληροφορίες δε μπορούν να ανακτηθούν μετά από παραποίηση των δεδομένων. Σε αντίθεση με την κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει την πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη "αθώα" πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της. Συμπερασματικά, θα μπορούσαμε να αναφέρουμε ότι η στεγανογραφία επιδιώκει την απόκρυψη της πληροφορίας χωρίς να λαμβάνει υπόψη το ενδεχόμενο επίθεσης σε αυτήν, προφυλάσσοντάς την μέσα σε κάποιο "στεγανό". Η κρυπτογραφία εξασφαλίζει ότι η πληροφορία που θα διαβαστεί από μη εξουσιοδοτημένους χρήστες θα είναι άχρηστη και ακατανόητη ή παραπλανητική. Η κρυπτογραφία επίσης, προστατεύει ένα προϊόν υπό μεταφορά, αλλά μόλις αποκρυπτογραφηθεί, το περιεχόμενο είναι ευάλωτο.
Η υδατογράφηση (watermarking) έχει την ιδιότητα προστασίας του περιεχομένου και μετά την αποκρυπτογράφηση του, τοποθετώντας την πληροφορία μέσα στο περιεχόμενο, απ' όπου δεν αφαιρείται ποτέ κατά την κανονική χρήση. Ακόμα κι αν η ύπαρξη κρυφών πληροφοριών είναι γνωστή, είναι δύσκολο - ιδανικά αδύνατο- να καταστραφεί το ένθετο υδατογράφημα.
Συμπληρωματικά με ότι προαναφέρθηκε, θα μπορούσαμε να πούμε ότι σε τεχνικό επίπεδο προτείνονται και διάφορες άλλες μέθοδοι διακρίβωσης της γνησιότητας της προέλευσης δεδομένων ηλεκτρονικού υπολογιστή. Χαρακτηριστικό παράδειγμα αποτελούν οι βιομετρικές μέθοδοι, οι οποίες συσχετίζουν στα προς διαβίβαση δεδομένα που συνδέονται μονοσήμαντα με το χρήστη («υπογράφοντα»), όπως π.χ. το δακτυλικό αποτύπωμα ή την απεικόνιση της ίριδας του ματιού, βιολογικά στοιχεία που θεωρούνται μοναδικά σε κάθε άνθρωπο. Ωστόσο, οι συγκεκριμένες μέθοδοι δε χρησιμοποιούνται ευρέως στις συναλλαγές μέχρι σήμερα. Στο ζήτημα που γεννάται κατά πόσο η διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail address) αποτελεί ή όχι μορφή ηλεκτρονικής υπογραφής, η απάντηση είναι καταφατική σύμφωνα με την νομολογία και το Μονομελές Πρωτοδικείο Αθηνών. Να διευκρινιστεί ότι και οι δύο παραπάνω μέθοδοι (βιομετρικά χαρακτηριστικά, διεύθυνση ηλεκτρονικού ταχυδρομείου) αποτελούν απλά μορφές ηλεκτρονικής υπογραφής, έννοια που αντιδιαστέλλεται με αυτήν της προηγμένης ηλεκτρονικής ή ψηφιακής υπογραφής.

## ΣΤΑΤΙΣΤΙΚΕΣ ΜΕΛΕΤΕΣ ΚΑΙ ΧΡΗΣΙΜΕΣ ΣΥΜΒΟΥΛΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Έλλειψη προφύλαξης των προσωπικών δεδομένων των ανηλίκων.

Ανυποψίαστοι και αδύναμοι είναι το 57% των ανηλίκων όσον αφορά την προστασία των προσωπικών τους δεδομένων μέσα από το Διαδίκτυο. Αυτό έδειξε έρευνα του Πανευρωπαϊκού Δικτύου Εθνικών Κόμβων Ασφαλούς Διαδικτύου «Insafe» (τελεί υπό την αιγίδα της Κομισιόν) που έγινε (6-7/2/07) σε 37 χώρες με συμμετοχή 21.825 παιδιών και εφήβων - τα 322 ήταν Ελληνόπουλα. Ειδικότερα, τα παιδιά κάτω των 10 ετών δεν γνωρίζουν τους κινδύνους που εγκυμονούν οι συναντήσεις με άτομα που γνώρισαν μέσα από τα chat rooms, αφού περισσότερα από το 1/3 δήλωσαν ότι θα συναντούσαν τους άγνωστους αυτούς χωρίς να ενημερώσουν τους γονείς τους, ενώ τα Ελληνόπουλα είναι πιο υποψιασμένα. Στις ηλικίες μεταξύ 14-17 χρόνων η έκθεση στους κινδύνους του Διαδικτύου είναι μεγαλύτερη με το 22% των 17χρονων να δηλώνει ότι θα ξεχνούσαν να αναφέρουν μια συνάντηση με αγνώστους στους γονείς τους και το 24% των 18χρονων ότι θα πήγαιναν μόνοι τους. Από τα 322 Ελληνόπουλα, 8 στα 10 δηλώνουν ότι έχουν δικό τους υπολογιστή (82,30%). 6 στα 10 (62,73%) ότι «σερφάρουν» έως 5 ώρες εβδομαδιαίως, 2 στα 10 πως είναι online πάνω από 10 ώρες (22,98%) και 7 στα 10 ότι δεν συνομιλούν με αγνώστους στο Διαδίκτυο και δεν θα τους συναντούσαν.
Επίσης 1 στα 2 δηλώνουν ότι δίνουν πολλές προσωπικές πληροφορίες και για τη ζωή τους μέσα από τους ιστοχώρους κοινωνικής δικτύωσης, τα social networking sites, όπως το MySpace ή το Bebo. Ωστόσο, 1 στα 4 παιδιά θα έδινε τα στοιχεία του τραπεζικού λογαριασμού του πατέρα του μέσα από το Διαδίκτυο, ενώ 4,5 στα 10 θα συμπλήρωναν μόνο βασικά στοιχεία (τηλέφωνο, διεύθυνση κ.λπ.) σε φόρμες ιστοχώρων. Στα

δύο μόνο το ένα θα έλεγε στους γονείς ή στον δάσκαλο ότι έλαβε διαδικτυακά από φίλο φωτογραφία πορνογραφικού περιεχομένου, 8 στα 10 παιδιά (80,43%) θα ζητούσαν από τη μητέρα τους να τους αγοράσει με πιστωτική κάρτα κάτι από το Διαδίκτυο, δύο (6,52%) θα «δανείζονταν» την πιστωτική κάρτα του γονιού τους ή θα χρησιμοποιούσαν στοιχεία κάρτας που θα τους έδινε φίλος τους (13,04%). Τέλος, 8 στα 10 Ελληνόπουλα ότι θα άκουγαν προσεκτικά τις συμβουλές των δασκάλων τους για ασφαλή χρήση του Διαδικτύου.
Τέλος, η περιφρούρηση του Διαδικτύου είναι πολύ σημαντική αν σκεφτεί κανείς πως 1 στους 5 ανηλίκους δέχεται σεξουαλική προσέγγιση ή παρενόχληση στο Διαδίκτυο, μόνο το 17% το αναφέρει στους γονείς του, ενώ ελάχιστες απ' αυτές τις περιπτώσεις έκθεσης σε σεξουαλικού περιεχομένου ιστοσελίδες (περίπου το 3%) έχει αναφερθεί στις Αρχές. Η ΕΛ.ΑΣ έχει εξαπολύσει από το 2001 σαρωτικές επιχειρήσεις και έχει ασχοληθεί με 50 υποθέσεις στις οποίες σχηματίστηκαν δικογραφίες εις βάρος 120 δραστών. Αξιοσημείωτο είναι πως αν πληκτρολογήσει κάποιος τη λέξη «σεξ» σε μια μηχανή αναζήτησης μέσα σε λίγα δευτερόλεπτα εμφανίζονται πάνω από 2,764,667 sites. Παρακάτω παρουσιάζονται τα συνολικά ευρωπαϊκά στοιχεία:

- 50% των εφήβων παραδέχονται ότι έχουν επισκεφτεί τουλάχιστον μία φορά ιστοσελίδες με πορνογραφικό περιεχόμενο.
- Από αυτούς το 79% χρησιμοποίησε υπολογιστή του σχολείου του ή της δημόσιας βιβλιοθήκης, ενώ το 67% μπαίνει στο διαδίκτυο και από το σπίτι του.
- Σημαντικό είναι το γεγονός ότι οι γονείς αυτών των παιδιών σε ποσοστό που ξεπερνούσε το 75% πίστευαν ότι γνώριζαν τι αναζητούσαν τα παιδιά τους στο διαδίκτυο ενώ στην πραγματικότητα δεν είχαν την παραμικρή ιδέα για το σκληρό πορνογραφικό περιεχόμενο στο οποίο είχαν πρόσβαση.
- Τα παιδιά χρήστες του διαδικτύου έχουν την πρώτη τους «πορνογραφική εμπειρία» κατά μέσο όρο στα 12 τους χρόνια. Το 71% παραδέχεται ότι το διαδίκτυο είναι η κύρια πηγή τους για πορνογραφικό υλικό.
- Οι έφηβοι χρησιμοποιούν το διαδίκτυο κατά μέσο όρο 8,5 ώρες την εβδομάδα για επικοινωνήσουν στις ανοιχτές αίθουσες συζητήσεων (chat rooms) και για ηλεκτρονικό ταχυδρομείο. Αντίθετα χρησιμοποιούν το διαδίκτυο για τις σχολικές εργασίες τους μόνο 1,8 ώρες εβδομαδιαίως.
- Υπολογίζεται ότι 18,8 εκατομμύρια παιδιά και έφηβοι κάτω των 18 ετών έχουν σήμερα πρόσβαση στο διαδίκτυο από το σπίτι τους. Το γνωστό αντρικό περιοδικό Playboy προσφέρει μέσα από τις ιστοσελίδες του δωρεάν προκλητικές φωτογραφίες από τις playmates και δέχεται 5 εκατομμύρια επισκέψεις καθημερινά.
- Οι σελίδες με πορνογραφικό περιεχόμενο υπολογίζεται ότι είναι ο πιο αναπτυγμένος τομέας πωλήσεων μέσα από το διαδίκτυο. Περίπου 266 νέες ιστοσελίδες προστίθενται καθημερινά στον ήδη μεγάλο όγκο πορνογραφικού υλικού που διατίθεται.

Τέλος εξίσου σημαντικό είναι οι ίδιοι οι γονείς να μάθουν στα παιδιά τους να σερφάρουν με ασφάλεια στον καταπληκτικό αλλά αχανή κόσμο του διαδικτύου, να χρησιμοποιούν την πλειάδα των πληροφοριών που παρέχει σωστά, και να αποφεύγουν τους πιθανούς κινδύνους. Σύμφωνα με την τελευταία έρευνα του Ευρωβαρόμετρου “Safer Internet”, Μάιος 2006 γύρω από την Ασφάλεια του Διαδικτύου:

♦ 3 στους 4 Έλληνες γονείς δεν κάθονται ποτέ με τα παιδιά τους, όταν αυτά σερφάρουν στο διαδίκτυο. Η Ελλάδα τοποθετείτε στην τελευταία θέση μεταξύ των υπολοίπων χωρών της Ευρωπαϊκής Ένωσης .
♦ Μόνο 1 στους 9 γονείς κάνει χρήση φίλτρων στο σπίτι, για να μπλοκάρει κάποιες ιστοσελίδες, που δεν θα ήθελε να δουν τα παιδιά του.
♦ Μόνο 1 στους 12 γονείς θέτει κανόνες χρήσης του διαδικτύου. Εδώ η Ελλάδα βρίσκεται στην προτελευταία θέση στην Ευρωπαϊκή Ένωση.
♦ Μόνο 1 στους 5 γονείς θέτει κανόνες χρήσης του κινητού τηλεφώνου, ποσοστό που είναι όμως διπλάσιο από το αντίστοιχο για το διαδίκτυο.
♦ 1 στους 4 γονείς δεν επιτρέπει στα παιδιά του να πηγαίνουν σε δωμάτια ανοιχτής επικοινωνίας chat και να δίνουν προσωπικά τους στοιχεία.
♦ 1 στους 8 γονείς πιστεύει ότι τα παιδιά του έχουν συναντήσει επιβλαβές περιεχόμενο στο διαδίκτυο, ενώ 7 στους 10 γονείς πιστεύουν ότι τα παιδιά τους δεν έχουν συναντήσει ποτέ επιβλαβές περιεχόμενο στο διαδίκτυο.

♦ Μόνο 1 στους 8 γονείς δεν επιτρέπει την αντιγραφή μουσικής και ταινιών από το διαδίκτυο, ποσοστό που μας προβληματίζει ιδιαίτερα, σε σχέση με το μείζον θέμα της προστασίας της πνευματικής ιδιοκτησίας στο διαδίκτυο.
♦ Από την άλλη μεριά, 1 στους 2 γονείς δηλώνουν ότι δεν ξέρουν πού να αναφέρουν παράνομο περιεχόμενο, ενώ 1 στους 2 γονείς δεν ξέρει αν ή δεν πιστεύει ότι τα παιδιά του μπορούν να αντιμετωπίσουν άβολες καταστάσεις στο διαδίκτυο.
♦ 9 στους 10 Έλληνες γονείς δηλώνουν την ανάγκη να πάρουν περισσότερες πληροφορίες γύρω από τους τρόπους που μπορούν να προστατεύσουν τα παιδιά τους, τοποθετώντας για άλλη μια φορά την Ελλάδα στην πρώτη, αλλά όχι τόσο ευχάριστη θέση στην Ευρωπαϊκή Ένωση των 25 κρατών-μελών.

Η νομοθεσία από την Ευρωπαϊκή Ένωση για ασφαλή πλοήγηση των νέων

Στις 25 Ιανουαρίου 1999, η Επιτροπή υιοθέτησε ένα πολυετές κοινοτικό πρόγραμμα δράσης που αποσκοπεί στην προώθηση της ασφαλέστερης χρήσης του Διαδικτύου για την καταπολέμηση του παράνομου και επιβλαβούς περιεχομένου στα παγκόσμια δίκτυα. Το πρόγραμμα δράσης για ένα ασφαλέστερο Διαδίκτυο διαρθρώνεται γύρω από τους παρακάτω τομείς δράσης :

- Δημιουργία ενός ασφαλέστερου περιβάλλοντος.
- Δημιουργία ενός ευρωπαϊκού δικτύου «θερμών γραμμών» για να αναφέρουν οι καταναλωτές τις υποψίες τους για παιδική πορνογραφία.
- Ενθάρρυνση της αυτορρύθμισης και των κωδίκων συμπεριφοράς.
- Ανάπτυξη συστημάτων φιλτραρίσματος και κατάταξης.
- Επίδειξη των οφελών των εθελοντικών συστημάτων φιλτραρίσματος και κατάταξης όπως, π.χ., το ICRA.
- Διευκόλυνση της διεθνούς συμφωνίας για τα συστήματα κατάταξης.
- Ενθάρρυνση δράσεων ευαισθητοποίησης.
- Προετοιμασία του πεδίου για δράσεις ευαισθητοποίησης.
- Ενθάρρυνση της εκτέλεσης δράσεων ευαισθητοποίησης ευρείας κλίμακας.
- Δράσεις στήριξης.
- Εκτίμηση των νομικών συνεπειών.
- Συντονισμός με συναφείς διεθνείς δράσεις.
- Αξιολόγηση του αντίκτυπου των κοινοτικών μέτρων.

Το 2005, η Ευρωπαϊκή Επιτροπή καθιέρωσε το Πρόγραμμα «Safer Internet Plus», ένα 4ετές πρόγραμμα που έχει σκοπό να καταστήσει ασφαλέστερο το Διαδίκτυο για τα παιδιά της Ευρώπης. Το πρόγραμμα αποτελεί συνέχεια των δράσεων που αναλαμβάνει η Ευρωπαϊκή Ένωση για την προαγωγή της ασφαλέστερης χρήσης του Διαδικτύου και την καταπολέμηση του παράνομου και επιβλαβούς περιεχομένου από το 1996. Καλύπτει τις νέες επιγραμμικές τεχνολογίες συμπεριλαμβανομένων του κινητού και ευρυζωνικού περιεχομένου, των επιγραμμικών παιχνιδιών, και κάθε μορφής επικοινωνίας πραγματικού χρόνου όπως δικτυακοί χώροι συζήτησης (chat rooms) και άμεσα μηνύματα (instant messages), με βασικό στόχο τη βελτίωση της προστασίας των παιδιών και των ανηλίκων.

Οδηγίες για ασφαλές σερφάρισμα.

**<u>ΟΔΗΓΙΕΣ ΓΙΑ ΠΑΙΔΙΑ</u>**

- Μη συνδέεστε για πολύ ώρα στο διαδίκτυο.
- Μη δίνετε το όνομά σας, το πού μένετε ή το σχολείο στο οποίο πηγαίνετε σε ιστοσελίδες ή σε άτομα που γνωρίζετε στο διαδίκτυο.
- Σε περίπτωση που νιώσετε άβολα είτε διαβάζοντας κάποιο μήνυμα είτε συνομιλώντας στο διαδίκτυο, κλείστε τη σύνδεση και αμέσως ενημερώστε τους γονείς σας για ό,τι είδατε ή διαβάσατε.

• Μην ανοίγετε τα παράθυρα με διαφημίσεις παιχνιδιών ή νέων ταινιών που εμφανίζονται στην οθόνη του Η/Υ σας. Πολλές φορές επιλέγοντάς τα, συνδέεστε χωρίς να το γνωρίζετε με σελίδες που έχουν βλαβερό για εσάς περιεχόμενο.
• Να είστε πολύ προσεκτικοί όταν κάποιος «φίλος» που γνωρίσατε μέσω διαδικτύου σας ζητήσει να συναντηθείτε. Ενημερώστε τους γονείς σας ή κάποιον μεγαλύτερό σας ώστε να είναι μαζί σας στη συνάντηση.
• Μην πιστεύετε εύκολα αυτά που σας λένε ή διαβάζετε στο διαδίκτυο. Δεν είναι πάντα αλήθεια.
• Έχετε πάντα υπόψη σας ότι οι ιοί βρίσκονται παντού: σε e-mails, σε δισκέτες, σε αρχεία που «κατεβάζετε» από το διαδίκτυο.

## ΟΔΗΓΙΕΣ ΓΙΑ ΝΕΟΥΣ/ΕΦΗΒΟΥΣ

• Αποφεύγετε να διαχέετε τα προσωπικά σας στοιχεία (όνομα, διεύθυνση, αριθμό ταυτότητας, διαβατηρίου κτλ) στο διαδίκτυο.
• Κρατήστε μυστικό τον κωδικό σύνδεσής σας στο διαδίκτυο
• Διαβάστε προσεκτικά κάθε μήνυμα και παράθυρο που εμφανίζεται στην οθόνη του υπολογιστή σας.
• Μην ανοίγετε τα παράθυρα που εμφανίζονται στην οθόνη του Η/Υ (pop-up windows)σας μιας και μπορεί να κρύβουν κινδύνους τόσο για τη λειτουργία του Η/Υ σας όσο και για τα προσωπικά σας στοιχεία, αφού έχουν αναπτυχθεί τρόποι για την καταστρατήγησή τους.
• Δώστε προσοχή στα δωμάτια άμεσης συνομιλίας (chatrooms). Να διαβάζετε πάντα την πολιτική που εφαρμόζουν όσον αφορά την ασφάλεια των προσωπικών σας δεδομένων.
• Μην αποκαλύπτετε τα πραγματικά σας στοιχεία και μην είστε ευκολόπιστοι σε όσα σας λένε.
• Να διατηρείτε πάντα μία κριτική άποψη και συμπεριφορά απέναντι σε αυτά που βλέπετε, ακούτε και διαβάζετε στο διαδίκτυο και πολύ περισσότερο σε αυτά που ενδεχομένως κάποιοι να σας περιγράφουν .
• Σε περίπτωση που το άτομο με το οποίο συνομιλείτε σας κάνει να νιώσετε άβολα, διακόψτε τη συνομιλία και αναφέρετε το συμβάν σε κάποιον που εμπιστεύεστε (π.χ. γονείς, κηδεμόνας, φίλοι)
• Σε περίπτωση που θα συναντήσετε το άτομο με το οποίο συνομιλείτε μέσω διαδικτύου, ενημερώστε κάποιον για τη συνάντηση αυτή και πηγαίνετε συνοδευόμενοι από τους φίλους σας. Προτιμήστε η συνάντηση να γίνει σε κάποιο δημόσιο χώρο όπου θα υπάρχει κόσμος.

## E-MAILS

• Μη δίνετε ποτέ το e-mail σας σε ανθρώπους που δε γνωρίζετε.
• Μην ανοίγετε ποτέ άγνωστα e-mails. Ο ηλεκτρονικός σας υπολογιστής μπορεί να χρησιμοποιηθεί από απατεώνες του ίντερνετ με βλαβερά αποτελέσματα, όπως ιούς, κλοπή κωδικού σύνδεσης στο ίντερνετ και υπέρογκους λογαριασμούς τηλεφώνου.
• Μην ανοίγετε e-mails που σας υπόσχονται ότι κερδίσατε κάποιο βραβείο ή χρήματα.

## ΟΔΗΓΙΕΣ ΓΙΑ ΕΝΗΛΙΚΕΣ/ΓΟΝΕΙΣ

• Να είστε ιδιαίτερα προσεκτικοί στις συναλλαγές μέσω διαδικτύου, όταν αυτές θα γίνουν με την πιστωτική σας κάρτα.
• Μην παρασύρεστε από παράθυρα διαφημίσεων που σχετίζονται με τυχερά παιχνίδια τζόγου.
• Μη γνωστοποιείτε τα προσωπικά σας στοιχεία στο διαδίκτυο, π.χ. το όνομα σας, τη διεύθυνσή σας, τον αριθμό της ταυτότητάς σας ή της πιστωτικής σας κάρτας.
• Στην περίπτωση που είστε γονείς και έχετε παιδιά που χρησιμοποιούν το διαδίκτυο, τοποθετήστε τον υπολογιστή σε έναν κεντρικό κοινόχρηστο χώρο του σπιτιού σας ώστε να τα επιβλέπετε.
• Εγκαταστήστε ειδικά λογισμικά φίλτρα τα οποία «μπλοκάρουν» την πρόσβαση σε σελίδες απαγορευμένου και βλαβερού περιεχομένου για τα παιδιά και παράλληλα φτιάξτε μία λίστα με ιστοσελίδες που εσείς εγκρίνετε για τα παιδιά σας.

• Συμβουλέψτε τα παιδιά σας να μην είναι ευκολόπιστα και να μην δίνουν σε αγνώστους τα προσωπικά τους στοιχεία. Μιλήστε τους για τους κινδύνους που μία τέτοια πράξη συνεπάγεται.

**Συμπεράσματα**

Η ευρύτατη διείσδυση της τεχνολογίας σε όλους τους τομείς του κοινωνικού γίγνεσθαι, κάνει επιτακτική περισσότερο από ποτέ την ανάπτυξη μηχανισμών και μεθόδων προστασίας για την ασφαλή διακίνηση των ψηφιακών «αντικειμένων». Η ανάγκη προστασίας του απαραβίαστου του απορρήτου, στο σύγχρονο ψηφιακό περιβάλλον προκύπτει περισσότερο καθοριστική από ποτέ. Ειδικότερα, καθώς το Διαδίκτυο αποτελεί σήμερα το σημαντικότερο εκφραστικό μέσο της ελευθερίας στην επικοινωνία των ανθρώπων, θα πρέπει να αναπτυχθούν μηχανισμοί προστασίας και ασφάλειας, από εκείνους που επιβουλεύονται την ελευθερία αυτή. Η δημιουργία των ψηφιακών υπογραφών, βασιζόμενη στη τεχνολογία της κρυπτογραφίας, αποτελεί μια διαδεδομένη μέθοδο, προστασίας και ασφαλείας στη διακίνηση των ηλεκτρονικών εγγράφων. Συμπερασματικά, κρίνεται σκόπιμο να αναφερθεί ότι η ψηφιακή υπογραφή, παρέχει εγγύηση της αυθεντικότητας, της ακεραιότητας, της μη αλλοίωσης του περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά. Ωστόσο, όπως προαναφέρθηκε, η ψηφιακή υπογραφή προστατεύει ένα προϊόν υπό μεταφορά, αλλά μόλις αποκρυπτογραφηθεί, το περιεχόμενο είναι ευάλωτο. Κατά συνέπεια, προκύπτει πως η ιδανικότερη λύση για την ασφαλή διακίνηση αλλά και χρήση των ψηφιακών αντικειμένων είναι ο συνδυασμός των αναπτυγμένων μεθόδων προστασίας. Η προσθήκη δηλαδή ψηφιακής υπογραφής και υδατογραφήματος στα διακινούμενα ηλεκτρονικά έγγραφα, αποτελούν ενδεδειγμένο τρόπο, για την προστασία του εγγράφου τόσο κατά την μεταφορά του, όσο και κατά τη χρήση του.

## ΚΕΦΑΛΑΙΟ 4

### *4.1. ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ*

Η εξέλιξη της χρησιμοποίησης της κρυπτογραφίας ολοένα αυξάνεται καθιστώντας πλέον αξιόπιστη την μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς

1. Ασφάλεια συναλλαγών σε τράπεζες δίκτυα - ATM
2. Κινητή τηλεφωνία (ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM)
3. Σταθερή τηλεφωνία (cryptophones)
4. Διασφάλιση Εταιρικών πληροφοριών
5. Στρατιωτικά δίκτυα (Τακτικά συστήματα επικοινωνιών μάχης)
6. Διπλωματικά δίκτυα (Τηλεγραφήματα)
7. Ηλεκτρονικές επιχειρήσεις (πιστωτικές κάρτες, πληρωμές)
8. Ηλεκτρονική ψηφοφορία
9. Ηλεκτρονική δημοπρασία
10. Ηλεκτρονικό γραμματοκιβώτιο
11. Συστήματα συναγερμών
12. Συστήματα βιομετρικής αναγνώρισης
13. Έξυπνες κάρτες
14. Ιδιωτικά δίκτυα (VPN)
15. Word Wide Web
16. Δορυφορικές εφαρμογές (δορυφορική τηλεόραση)
17. Ασύρματα δίκτυα (Hipperlan, bluetooth, 802.11x)
18. Συστήματα ιατρικών δεδομένων και άλλων βάσεων δεδομένων
19. Τηλεσυνδιάσκεψη - Τηλεφωνία μέσω διαδικτύου (VOIP)

### *4.2. Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΤΟΥ ΜΕΛΛΟΝΤΟΣ*

Παρά την τεράστια ισχύ του RSA και των άλλων σύγχρονων κρυπτογραμμάτων, οι κρυπταναλυτές εξακολουθούν να παίζουν σημαντικό ρόλο στη συλλογή πληροφοριών. Η επιτυχία τους φαίνεται από το γεγονός ότι η ζήτηση κρυπταναλυτών είναι μεγαλύτερη από ποτέ. Μόνο ένα μικρό ποσοστό των πληροφοριών που ρέουν ανά τον κόσμο είναι κρυπτογραφημένο με ασφαλή τρόπο ενώ οι υπόλοιπες είναι κρυπτογραφημένες ανεπαρκώς ή και καθόλου. Αυτό συμβαίνει επειδή ο αριθμός των χρηστών του διαδικτύου αυξάνει ραγδαία, και ελάχιστοι είναι εκείνοι που παίρνουν τις κατάλληλες προφυλάξεις ως προς την προστασία των προσωπικών τους δεδομένων. Αυτό με τη σειρά του σημαίνει ότι οι οργανώσεις εθνικής ασφαλείας, οι υπεύθυνοι για την επιβολή του νόμου αλλά και οποιοσδήποτε περίεργος μπορεί να έχει πρόσβαση σε περισσότερες πληροφορίες από όσες είναι σε θέση να διαχειριστεί. Ακόμη και αν οι χρήστες χρησιμοποιούν σωστά το κρυπτόγραμμα RSA και πάλι οι κωδικοθραύστες διαθέτουν πολλές μεθόδους για να σταχυολογούν τα μηνύματα που υποκλέπτουν. Κατ' αρχάς εξακολουθούν να χρησιμοποιούν τις παραδοσιακές τεχνικές όπως η ανάλυση πληροφορίας που ακόμα κι αν δεν είναι σε θέση να υποκλέψουν το περιεχόμενο του μηνύματος μπορούν να εντοπίσουν τον αποστολέα και τον παραλήπτη, πράγμα που από μόνο του μπορεί να είναι αποκαλυπτικό. Μια πιο πρόσφατη εξέλιξη είναι η λεγόμενη *επίθεση θυέλλης*, που έχει στόχο να ανιχνεύει τα ηλεκτρομαγνητικά σήματα τα οποία εκπέμπονται από τα ηλεκτρονικά κυκλώματα της οθόνης ενός υπολογιστή. Για να προστατεύσουν τους χρήστες από τις επιθέσεις θυέλλης, οι εταιρίες τους εφοδιάζουν με μονωτικό υλικό το οποίο μπορούν να επενδύσουν στους τοίχους των δωματίων τους ώστε να εμποδίζουν την έξοδο των ηλεκτρομαγνητικών σημάτων. Κάποιες άλλες μορφές επίθεσης περιλαμβάνουν τη χρήση ιών και δούρειων ίππων. Η Εύα θα μπορούσε να σχεδιάσει έναν ιό που να

προσβάλει το λογισμικό PGP, παραμένοντας ήσυχος μέσα στον υπολογιστή της Αλίκης. Όταν η Αλίκη χρησιμοποιήσει το ιδιωτικό της κλειδί για να αποκρυπτογραφήσει ένα μήνυμα ο ιός θα ξυπνήσει και θα το καταστρέψει. Την επόμενη φορά που θα συνδεθεί η Αλίκη με το διαδίκτυο ο ιός θα στείλει το ιδιωτικό της κλειδί στην Εύα επιτρέποντάς της να αποκρυπτογραφεί όλα τα μηνύματα που θα στέλνονται στο εξής στην Αλίκη. Ο δούρειος ίππος, ένα άλλο λογισμικό τέχνασμα, συνίσταται στο σχεδιασμό από την Εύα ενός προγράμματος που εμφανίζεται να ενεργεί ως γνήσιο κρυπτογραφικό προιόν, αλλά στην πραγματικότητα προδίδει το χρήστη του. Για παράδειγμα, η Αλίκη μπορεί να πιστεύει ότι κατεβάζει από το διαδίκτυο ένα γνήσιο αντίγραφο του PGP, ενώ στην πραγματικότητα πρόκειται για μια έκδοση δούρειο ίππο η οποία μοιάζει ακριβώς με το αυθεντικό πρόγραμμα, αλλά περιέχει οδηγίες να στέλνει στην Εύα μη κρυπτογραφημένα αντίγραφα όλης της αλληλογραφίας της Αλίκης. Μια παραλλαγή του δούρειου ίππου είναι ένα εντελώς καινούργιο λογισμικό κρυπτογράφησης που μοιάζει ασφαλές αλλά στην πραγματικότητα περιέχει μια πίσω πόρτα, κάτι που επιτρέπει στους σχεδιαστές του να αποκρυπτογραφούν τα μηνύματα όλων των χρηστών.

Παρότι οι επιθέσεις θυέλλης, οι ιοί και οι δούρειοι ίπποι αποτελούν χρήσιμες τεχνικές για τη συλλογή πληροφοριών, οι κρυπταναλυτές συνειδητοποιούν ότι ο πραγματικός στόχος τους είναι να βρουν ένα τρόπο για να σπάσουν το κρυπτόγραμμα RSA. Το RSA χρησιμοποιείται για να προστατεύει τις πιο σημαντικές στρατιωτικές, διπλωματικές, εμπορικές και εγκληματικές επικοινωνίες, ακριβώς δηλαδή εκείνα τα μηνύματα που επιδιώκουν να αποκρυπτογραφούν οι οργανώσεις συλλογής πληροφοριών. Αν λοιπόν οι κρυπταναλυτές θέλουν να απειλήσουν την ισχυρή κρυπτογράφηση RSA θα πρέπει να πραγματοποιήσουν λενα μείζον θεωρητικό ή τεχνολογικό επίτευγμα. Ένα θεωρητικό επίτευγμα θα ήταν ένας ριζικά νέος τρόπος ανεύρεσης του ιδιωτικού κλειδιού της Αλίκης. Το κλειδί αυτό αποτελείται από τους αριθμούς p και q, οι οποίοι μπορούν να ευρεθούν από την παραγοντοποίηση του N του δημόσιου κλειδιού. Οι κρυπταναλυτές προσπάθησαν να βρουν ένα σύντομο δρόμο για την παραγοντοποίηση, μια μέθοδο που να μειώνει δραστικά τα βήματα που χρειάζονται για να βρεθούν τα p και q, όμως μέχρι τώρα όλες οι απόπειρες έχουν καταλήξει σε αποτυχία. Οι μαθηματικοί μελετούν την παραγοντοποίηση εδώ και αιώνες, και οι σύγχρονες τεχνικές στον τομέα αυτό δεν είναι σημαντικά καλύτερες από τις παλιές. Ίσως μάλιστα οι νόμοι των μαθηματικών να αποκλείουν την ύπαρξη ενός ριζικά σύντομου δρόμου για την παραγοντοποίηση. Αν δεν υπάρχει ένας προφανής τρόπος μείωσης αριθμού των βημάτων που απαιτούνται τότε οι κρυπταναλυτές χρειάζονται μια τεχνολογία που θα εκτελεί αυτά τα βήματα ταχύτερα και η οποία θα είναι δισεκατομμύρια φορές γρηγορότερη από τους σημερινούς υπολογιστές. Επομένως αναζητούν μια ριζικά νέα μορφή υπολογιστή, τον ***κβαντικό υπολογιστή.***

Σήμερα γνωρίζουμε ότι το φως συμπεριφέρεται σαν κύμα και ξέρουμε ότι μπορεί να συμπεριφέρεται και σαν σωματίδιο. Το αν αντιλαμβανόμαστε το φως σαν κύμα ή σαν σωματίδιο εξαρτάται από τις συνθήκες και αυτή η διττή φύση του φωτός είναι γνωστή ως δυισμός κύματος – σωματιδίου. Η σύγχρονη φυσική θεωρεί μια ακτίνα φωτός ως αποτελούμενη από αμέτρητα μεμονωμένα σωματίδια, γνωστά ως φωτόνια, τα οποία εμφανίζουν κυματικές ιδιότητες. Η κλασική Φυσική μπορεί να εξηγήσει τις περιφορές πλανητών ή την τροχιά ενός βλήματος, όμως δεν μπορεί να περιγράψει πλήρως τον κόσμο του πραγματικά μικρού, όπως την τροχιά ενός φωτονίου. Για να εξηγήσουν τέτοιου είδους φωτονικά φαινόμενα, οι φυσικοί καταφεύγουν στην κβαντική θεωρία, μια ερμηνεία του πώς να συμπεριφέρονται τα αντικείμενα στο μικροσκοπικό επίπεδο.

Η κβαντική θεωρία είναι μια φιλοσοφία που θέτει πολλά ερωτήματα. Ωστόσο απέδειξε ότι είναι η πιο επιτυχημένη και πρακτική επιστημονική θεωρία που επινοήθηκε ποτέ. Επιτρέπει στους φυσικούς να υπολογίζουν τις συνέπειες των πυρηνικών αντιδράσεων στους σταθμούς παραγωγής ενέργειας, μπορεί να εξηγήσει τα θαύματα του DNA, μπορεί να εξηγήσει το πώς λάμπει ο ήλιος, μπορεί να χρησιμοποιηθεί για το σχεδιασμό της ακτίνας λέιζερ που διαβάζει τα cd. Από τις συνέπειες της κβαντικής θεωρίας η πιο σημαντική από τεχνολογική άποψη είναι ο κβαντικός υπολογιστής καθώς πέραν του ότι θα κατέστρεφε την ασφάλεια όλων των σύγχρονων κρυπτογραμμάτων, ο κβαντικός υπολογιστής θα εγκαινίαζε μια νέ αποχή υπολογιστικής ισχύος.

Ένας από τους σκαπανείς της κβαντικής υπολογιστικής ήταν ο Ντέιβιντ Ντόις ένας βρετανός φυσικός ο οποίος υποστήριζε ότι οι υπολογιστές θα πρέπει να υπακούοθν στους νόμους της κβαντικής Φυσικής, επειδή οι κβαντικοί νόμοι είναι πιο θεμελιώδεις.

Για να πάρουμε μια ιδέα της ισχύος ενός κβαντικού υπολογιστή ας υποθέσουμε ότι έχουμε δύο εκδοχές μιας ερώτησης. Για να απαντήσουμε και στις δύο ερωτήσεις χρησιμοποιώντας έναν

συνηθισμένο υπολογιστή, θα πρέπει να υποβάλουμε την πρώτη εκδοχή και να περιμένουμε την απάντηση, και στη συνέχεια να υποβάλουμε τη δεύτερη εκδοχή και πάλι να περιμένουμε την απάντηση. Με άλλα λόγια ένας κοινός υπολογιστής μπορεί να επεξεργαστεί μόνο μια ερώτηση τη φορά, και αν υπάρχουν πολλές ερωτήσεις, πρέπει να τις επεξεργάζεται διαδοχικά. Αντίθετα με έναν κβαντικό υπολογιστή οι δύο ερωτήσεις θα μπορούσαν να συνδυαστούν ως υπέρθεση δύο καταστάσεων και να υποβήθούν ταυτόχρονα.

Δυστυχώς όταν ο Ντόιτς συνέλαβε το όραμα ενός κβαντικού υπολογιστή, στα μέσα της δεκαετίας του ’80 κανείς δεν μπορούσε να σκεφτεί πώς θα ήταν δυνατό στην πράξη να κατασκευαστεί μια τέτοια μηχανή. Οι επιστήμονες δεν μπορούσαν να βρουν τρόπο να προγραμματίσουν έναν κβαντικό υπολογιστή και επομένως δεν ήταν σίγουροι τι είδους υπολογισμούς θα ήταν σε θέση να κάνει. Το 1994 ο Πίτερ Σορ όρισε μια σειρά βημάτων τα οποία θα μπορούσε να εκτελέσει ένας κβαντικός υπολογιστής για να παραγοντοποιήσει έναν τεράστιο αριθμό, ότι ακριβώς χρειαζόταν δηλαδή για να σπάσει το κρυπτόγραμμα RSA. Ο Σορ όμως δεν μπορούσε να επιδείξει το παραγοντοποιητικό του πρόγραμμα επειδή ακόμα δεν υπήρχε κβαντικός υπολογιστής. Το 1996 ο Λοβ Γκρόβερ επίσης από τα Bell Labs, ανακάλυψε ένα άλλο ισχυρό πρόγραμμα το οποίο ήταν ένας τρόπος να ερευνάται ένας κατάλογος με εκπληκτικά υψηλή ταχύτητα, ακριβώς αυτό δηλαδή που απαιτείται για το σπάσιμο ενός κρυπτογράμματος DES. Παρότι τα προγράμματα των Σορ και Γκρόβερ προκάλεσαν τρομερή αισιοδοξία στις τάξεις των κωδικοθραυστών, μεγάλη ήταν και η απογοήτευση, επειδή ακόμα δεν υπήρχε ένας λειτουργικός κβαντικός υπολογιστής που θα μπορούσε να «τρέξει» με αποτέλεσμα η τεχνολογία να παραμένει ουσιαστικά πρωτόγονη.

Από τη δεκαετία του 1970, οι κωδικοπλάστες απέκτησαν σαφές προβάδισμα στον αγώνα κατά των κωδικοθραυστών, χάρη σε κρυπτογράμματα όπως το RSA και το DES. Καθώς η πληροφορία γίνεται το πιο πολύτιμο αγαθό στον κόσμο, η οικονομική, πολιτική και στρατιωτική μοίρα των εθνών θα εξαρτάται από την ισχύ των κρυπτογραμμάτων. Κατά συνέπεια, η ανάπτυξη ενός πλήρους λειτουργικού κβαντικού υπολογιστή θα απειλούσε την παγκόσμια σταθερότητα. Όποια χώρα φτάσει πρώτη εκεί, θα έχει τη δυνατότητα να παρακολουθεί τις επικοινωνίες των πολιτών της, να διαβάζει τις σκέψεις των εμπορικών της ανταγωνιστών και να υποκλέπτει τα σχέδια των εχθρών της. Η κβαντική υπολογιστική, παρότι βρίσκεται ακόμη στα σπάργανα, συνίσταται εν δυνάμει απειλή για το άτομο, τις διεθνείς επιχειρήσεις και την παγκόσμια ασφάλεια.

## ***ΕΠΙΛΟΓΟΣ***

Επί δύο χιλιάδες χρόνια, οι κωδικοπλάστες αγωνίζονταν να προστατεύσουν μυστικά, ενώ οι κωδικοθραύστες έβαζαν τα δυνατά τους για να τα αποκαλύψουν. Η επινόηση της κρυπτογραφίας δημόσιου κλειδιού και η πολιτική διαμάχη που περιβάλλει τη χρήση ισχυρής κρυπτογραφίας μας φέρνει στο σήμερα, και είναι σαφές ότι οι κρυπτογράφοι κερδίζουν τον πόλεμο της πληροφορίας. Η εμπειρία ωστόσο του παρελθόντος μας διδάσκει ότι όλα τα υποτιθέμενα άθραυστα κρυπτογράμματα αργά ή γρήγορα υπέκυψαν στην κρυπτανάλυση.

Το κρυπτόγραμμα Βινεζέρ αποκαλείτο le chiffre indechiffrable, όμως ο Μπάμπατζ το έσπασε. Παρομοίως, το Αίνιγμα θεωρείτο άτρωτο, μέχρις ότου οι Πολωνοί αποκάλυψαν τα τρωτά του σημεία. Η ιστορία του James Elis και του GCHQ μας προειδοποιεί ότι μπορεί να υπάρχουν ήδη σημαντικά επιτεύγματα κρυμμένα κάτω από το πέπλο της κυβερνητικής μυστικότητας.

Η συνεχής ανάπτυξη της τεχνολογίας των υπολογιστικών συστημάτων και της ασφάλειας τόσο των στρατιωτικών μυστικών όσο και των συναλλαγών έχει τοποθετήσει την επιστήμη της κρυπτογραφίας και κρυπτανάλησης σε εξέχουσα θέση.

Οι άνθρωποι από αιώνες προσπαθούν να μεταδώσουν τα μηνύματα τους και τα κρυμμένα τους μυστικά με διάφορους τρόπους. Η ανθρωπότητα έχει προοδεύσει και με αυτή την προσπάθεια. Εκατομμύρια ζωές έχουν σωθεί από πληροφορίες που μεταδόθηκαν με ασφάλεια και εκατοντάδες μυστικά που έπρεπε καμιά φορά να μείνουν θαμμένα για πάντα παρέμειναν, χάρις στην κρυπτογραφία.

Οι άνθρωποι από τη φύση τους πάντα θα προσπαθούν να μεταδίδουν μυστικά και πληροφορίες στους άλλους με τον τρόπο αυτό.

Είναι κάτι σαν το παιδικό παιχνίδι του χαμένου θησαυρού.

Μόνο που πρέπει να διαβάσεις πρώτα και τον μυστικό χάρτη.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

## Ελληνική

1) 2)Χ.Κουκουβίνος-Αλ.Παπαιωάννου, Εισαγωγή στην Κρυπτογραφία
3)http://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1

**Ξενόγλωσση**


1) SIMON SINGH, The Code Book, The secret history of Codes and Code breaking, μετάφραση Νάσος Κυριαζόπουλος, Δ.Φ.
2) Trappe W. , Washington L. (2002) Introduction to Cryptography with Coding Theory, Prentice Hall
3) Stallings W. (2003) Cryptography and Network Security, Prentice Hall
4) Mao W. (2004) Modern Cryptography- Theory and Practice, Prentice Hall
5) A.Menezes,P.Van Oorschot, S.Vanstone Εγχειρίδιο Εφαρμοσμένης Κρυπτογραφίας , μεταφρ.Γ.Χ.Στεφανίδης
6) http://www.saferinternet.gr
7) http://en.wikipedia.org/wiki/Pretty_Good_Privacy