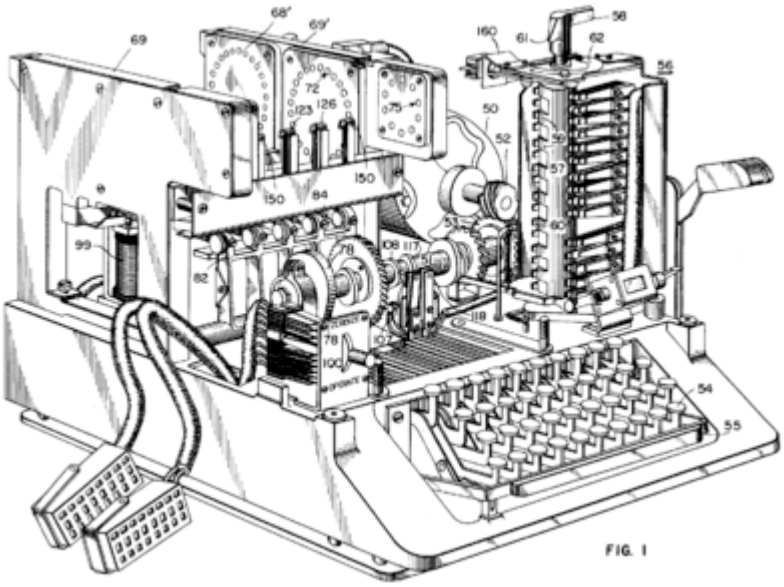
ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ



ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΟΝΟΜΑ:ΤΣΙΑΛΙΚΗ ΑΙΚΑΤΕΡΙΝΗ

Α.Μ : 09102184

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:

Α. ΠΑΠΑΪΩΑΝΝΟΥ

ΕΙΣΑΓΩΓΗ

Η εργασία αυτή έχει θέμα την κβαντική κρυπτογραφία. Η προσέγγιση του θέματος έγινε αρχικά μέσω την κβαντομηχανικής και στη συνέχεια μέσω της ιστορίας της κρυπτογραφίας για να καταλήξουμε στα επιτεύγματα της εποχής μας, τους κβαντικούς υπολογιστές.

Η εργασία είναι χωρισμένη σε 3 ενότητες, την «εισαγωγή στην κβαντομηχανική», την «κβαντική κρυπτογραφία» και τους «κβαντικούς υπολογιστές».

Στην πρώτη ενότητα γίνεται αρχικά αναφορά σε βασικές έννοιες της κβαντομηχανικής. Στη συνέχεια γίνεται ο χωρισμός της περιόδου σε προκβαντική και σε κβαντική. Ακολουθούν αναφορές σε σημαντικούς φυσικούς που έπαιξαν σημαντικό ρόλο στην ανάπτυξη και την θεμελίωση της κβαντομηχανικής. Μετά υπάρχουν θεματικές ενότητες με βασικές θεωρίες της κβαντομηχανικής όπως η ακτινοβολία μέλανος σώματος, το φωτοηλεκτρικό φαινόμενο, το φαινόμενο Compton και ο κυματοσωματιδιακός δυϊσμός. Στις θεματικές αυτές ενότητες γίνεται αναφορά προσπάθειες κλασσικής και κβαντικής ερμηνείας, σε βασικές αρχές και ιδιαίτερα χαρακτηριστικά, σε ιστορικές αναδρομές, σε παραδείγματα και σε πειράματα.

Η δεύτερη ενότητα ξεκινά με τον διαχωρισμό της κρυπτογραφίας σε 3 περιόδους, με αναφορά στα σημαντικότερα γεγονότα κάθε περιόδου. Μετά ακολουθεί μια μικρή λίστα με εξήγηση των βασικών όρων της εργασίας. Το μεγαλύτερο μέρος της ενότητας αφορά την ιστορία της εξέλιξης της επιστήμης της κρυπτογραφίας , από τον Β΄ Παγκόσμιο Πόλεμο μέχρι τις μέρες μας. Χαρακτηριστικό είναι το παράδειγμα επικοινωνίας της Αλίκης και του Μπομπ, με υποκλοπέα την Εύα. Στην πορεία δίνονται πληροφορίες για τις κβαντικές πύλες και τα qubits. Ακολουθεί ο Αλγόριθμος του Shor με το κβαντικό και το κλασικό κομμάτι καθώς και τα προβλήματα του. Τέλος γίνεται μια προσπάθεια να κατανοήσουμε αν η κβαντική κρυπτογραφία είναι ή όχι μια ασφαλής μέθοδος επικοινωνίας.

Η τρίτη ενότητα επεξεργάζεται τους κβαντικούς υπολογιστές. Ξεκινώντας από την υλοποίηση τους, και αφού γίνει αναφορά στα πλεονεκτήματα και στις εφαρμογές τους, στα προβλήματα που παρουσιάστηκαν κατά την υλοποίηση καθώς και στην κβαντική διόρθωση των σφαλμάτων, καταλήγουμε στις τεχνολογίες κατασκευής των κβαντικών υπολογιστών καθώς και στις προοπτικές και το μέλλον

τους. Η πρώτη πώληση κβαντικού υπολογιστή έχει ήδη πραγματοποιηθεί!

ΠΕΡΙΕΧΟΜΕΝΑ

❖ ΕΝΟΤΗΤΑ 1

- ΚΒΑΝΤΙΚΗ ΕΡΜΗΝΕΙΑ: Η ΥΠΟΘΕΣΗ ΤΩΝ ΦΩΤΟΝΙΩΝ
- ΚΑΙ ΜΕΤΑ ΤΙ;

4. ΦΑΙΝΟΜΕΝΟ COMPTON

- ΙΣΤΟΡΙΚΑ
- ΑΚΤΙΝΕΣ Χ
- ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ
- ΤΟ ΠΕΙΡΑΜΑ
- ΚΛΑΣΙΚΗ ΕΡΜΗΝΕΙΑ
- ΚΒΑΝΤΙΚΗ ΕΡΜΗΝΕΙΑ

5. ΚΥΜΑΤΟΣΩΜΑΤΙΔΙΑΚΟΣ ΔΥΙΣΜΟΣ

- ΓΕΝΙΚΑ
- ΚΛΑΣΙΚΗ ΦΥΣΙΚΗ

❖ ΕΝΟΤΗΤΑ 2

1. ΚΡΥΠΤΟΓΡΑΦΙΑ

- ΓΕΝΙΚΑ
- ΠΕΡΙΟΔΟΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ
- ΕΦΑΡΜΟΓΕΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

2. ΛΕΞΙΚΟ ΟΡΩΝ

3. ΚΩΔΙΚΕΣ ΚΑΙ ΜΥΣΤΙΚΑ

4. ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ

5. ΤΑ QUBITS

6. ΑΛΓΟΡΙΘΜΟΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΤΟΥ SHOR

7. ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΒΕΛΤΙΩΝΟΥΝ ΤΗΝ ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

- ΓΕΝΙΚΑ

8. ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΚΒΑΝΤΟΜΗΧΑΝΙΚΗ

- ΓΕΝΙΚΑ
- ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ
- ΠΡΟΒΛΗΜΑΤΑ
- ΠΟΙΕΣ ΕΤΑΙΡΙΕΣ ΠΟΥΛΟΥΝ ΗΔΗ ΚΒΑΝΤΙΚΑ ΚΛΕΙΔΙΑ

9. ΑΠΑΡΑΒΙΑΣΤΗ ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΟΚΙΜΑΣΤΗΚΕ ΣΕ ΔΙΚΤΥΟ ΥΠΟΛΟΓΙΣΤΩΝ

- ΕΙΣΑΓΩΓΗ
- Η ΜΥΣΤΙΚΗ ΔΥΝΑΜΗ ΤΩΝ ΦΩΤΟΝΙΩΝ
- ΕΙΝΑΙ ΟΜΩΣ ΑΠΑΡΑΒΙΑΣΤΗ;

❖ ΕΝΟΤΗΤΑ 3

1. ΕΙΣΑΓΩΓΗ ΣΤΟΥΣ ΚΒΑΝΤΙΚΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ

2. ΠΩΣ ΥΛΟΠΟΙΕΙΤΑΙ ΕΝΑΣ ΑΛΓΟΡΙΘΜΟΣ

3. ΠΡΟΒΛΗΜΑΤΑ ΣΤΗΝ ΥΛΟΠΟΙΗΣΗ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

4. ΚΒΑΝΤΙΚΗ ΔΙΟΡΘΩΣΗ ΣΦΑΛΜΑΤΩΝ

- ΔΥΑΔΙΚΗ ΑΝΑΣΤΡΟΦΗ
- ΑΠΟΣΥΣΧΕΤΙΣΜΟΣ
- ΔΙΟΡΘΩΣΗ ΣΦΑΛΜΑΤΩΝ

5. ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΤΑΣΚΕΥΗΣ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

- ΜΟΔΙΑΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ
- ΠΑΓΙΔΕΣ ΙΟΝΤΩΝ
- CAVITY QED
- ΤΕΧΝΟΛΟΓΙΑ NMR

6. Η ΠΡΟΟΠΤΙΚΗ ΚΑΙ ΤΟ ΜΕΛΛΟΝ ΤΩΝ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

7. Η ΠΡΩΤΗ ΠΩΛΗΣΗ ΚΒΑΝΤΙΚΟΥ ΥΠΟΛΟΓΙΣΤΗ

ΕΝΟΤΗΤΑ 1

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΒΑΝΤΟΜΗΧΑΝΙΚΗ

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΒΑΝΤΟΜΗΧΑΝΙΚΗ

➢ ΓΕΝΙΚΑ

Γενικά στη φυσική, ο όρος **κβάντο** ή **κβάντουμ** αναφέρεται σε μια αδιάστατη μονάδα ποσότητας, ένα "ποσό από κάτι". Για παράδειγμα ένα κβάντο φωτός είναι μία μονάδα φωτός (ή αλλιώς φωτόνιο). Έτσι ο όρος αυτός απαντάται με τρεις έννοιες:

1. ως μία ποσότητα (γενικά),
2. ως μια μονάδα φωτός, και
3. ως ελάχιστη ποσότητα στην οποία εκκρίνεται ένας νευροδιαβιβαστής, ειδικότερα.

Ένα εξ' ολοκλήρου νέο εννοιολογικό πλαίσιο αναπτύχθηκε γύρω από την έννοια "κβάντο", κατά τη διάρκεια του πρώτου μισού του 20ου αιώνα. Πρόκειται το εννοιολογικό πλαίσιο της Κβαντικής Μηχανικής. Ο όρος κβάντο (quantum, μικρή ποσότητα - προέρχεται από τη λέξη quantum που στα Λατινικά σημαίνει πόσο) αναφέρεται σε διακριτές μονάδες που χαρακτηρίζουν συγκεκριμένες φυσικές ποσότητες, όπως η ενέργεια ενός ατόμου ύλης σε κατάσταση ηρεμίας.

Η έννοια του κβάντου είναι συνυφασμένη με το γεγονός ότι ποσότητες που χαρακτηρίζουν ιδιότητες ενός φυσικού συστήματος (δηλ. φυσικά μεγέθη π.χ. ενέργεια, στροφορμή) μπορούν να παίρνουν διακριτές τιμές και όχι συνεχείς τιμές. Δηλαδή αντίθετα με αυτό που προβλέπει η κλασσική θεωρία, λέμε ότι ένα φυσικό μέγεθος έχει διακριτό φάσμα ιδιοτιμών αντί συνεχή φάσμα ιδιοτιμών. Σημειώνεται ότι δεν είναι όλα τα φυσικά μεγέθη ενός συστήματος που έχουν διακριτό φάσμα ιδιοτιμών, δηλ. είναι κβαντωμένα, υπάρχουν και μεγέθη που όπως και στην κλασσική μηχανική έχουν συνεχές φάσμα. Έτσι παρόλο που η λέξη κβάντο επινοήθηκε αρχικά για να περιγράψει τα "πακέτα" ενέργειας που λέγονται φωτόνια και από τα οποία αποτελείται το φως, τελικά ολόκληρη η θεωρία πήρε αυτό το όνομα, κβαντομηχανική. Αυτό δείχνει το πόσο ριζοσπαστική φαινόταν τότε η ιδέα ότι υπάρχουν φυσικά μεγέθη που παίρνουν μερικές μόνο τιμές από τις άπειρες διαθέσιμες.

Η **Κβαντομηχανική** ή **κβαντική μηχανική** ή **κβαντική φυσική** είναι μια θεωρία της φυσικής μηχανικής. Θεωρείται πιο θεμελιώδης από την κλασσική μηχανική, καθώς εξηγεί φαινόμενα που η κλασσική μηχανική και η κλασσική ηλεκτροδυναμική αδυνατούν να αναλύσουν.

Κεντρική σημασία στη θεωρία της κβαντικής μηχανικής κατέχει η έννοια της κβάντωσης: ένα φυσικό μέγεθος είναι δυνατόν να είναι "κβαντισμένο", πράγμα που σημαίνει ότι το μέγεθος αυτό δεν μπορεί να πάρει οποιαδήποτε τιμή, αλλά μόνο συγκεκριμένες τιμές. Για παράδειγμα, η κίνηση ενός ηλεκτρονίου σε κάποιο άτομο πραγματοποιείται μόνο σε συγκεκριμένες ενεργειακές τροχιές.

Η κβαντομηχανική σε έναν αιώνα πειραματισμού δεν έχει διαψευστεί. Κρύβεται πίσω από πολλά φυσικά φαινόμενα και ιδιαιτέρως τα χημικά φαινόμενα καθώς και τη φυσική της στερεάς κατάστασης.

➢ ΑΠΟ ΤΗΝ ΠΡΟΚΒΑΝΤΙΚΗ ΣΤΗΝ ΚΒΑΝΤΙΚΗ ΠΕΡΙΟΔΟ

Προς τα τέλη του 19ου αιώνα η κλασική φυσική – κλασική μηχανική, ηλεκτρομαγνητική θεωρία, στατιστική μηχανική – είχε φτάσει πια στην ιστορική της ολοκλήρωση. Ύστερα από μια μακραίωνη διαδικασία ενοποίησης και σύνθεσης, μια τεράστια ποικιλία εμπειρικών νόμων είχε πια συμπυκνωθεί σε ένα εκπληκτικά μικρό αριθμό θεμελιωδών εξισώσεων με βάση τις οποίες φαινόταν κατ΄ αρχήν δυνατόν να ερμηνευτούν όλα τα φυσικά φαινόμενα. Στους φυσικούς της εποχής κυριαρχεί η αντίληψη ότι ο οριακός στόχος της φυσικής να φτάσει σε μια έσχατη και τελική ερμηνεία του υλικού κόσμου είχε πραγματοποιηθεί.

Λίγους μήνες μετά την προαναγγελία του «τέλους της φυσικής» από τον Michelson, ο Planck στις 14 Δεκεμβρίου 1900 , θα ανακοινώσει στην Ακαδημία του Βερολίνου την εργασία του για το μέλαν σώμα, η οποία θα θέσει σε κίνηση μια χιονοστιβάδα εξελίξεων που θα οδηγήσουν το 1927 στην πλήρη ανατροπή της κλασικής φυσικής και την εγκαθίδρυση ενός νέου επιστημονικού καθεστώτος: της κβαντικής μηχανικής.

Η νέα θεωρία καλείται να εξηγήσει χωρίς αυθαιρεσίες

1. Τη σωματιδιακή υφή της ακτινοβολίας (φωτόνια – Einstein)
2. Την κυματική υφή των σωματιδίων (κυματόδεμα – de Broglie)
3. Την κβάντωση των τιμών των φυσικών μεγεθών

Η κβαντομηχανική αποτελεί τη βάση σχεδόν κάθε θεωρίας των συστημάτων του μικρόκοσμου. Αρχικά ήταν άμεσα συνδεδεμένη με την κλασσική Φυσική και κυρίως με τους κλάδους της κλασσικής μηχανικής ,της στατιστικής μηχανικής και της ηλεκτρομαγνητικής θεωρίας του Maxwell. Η κλασσική Φυσική ,όπως είναι γνωστό ,ασχολείται με μακροσκοπικά φαινόμενα ,τα οποία είναι παρατηρήσιμα είτε απ' ευθείας είτε με σχετικά απλά όργανα.

Από τις αρχές του 20ού αιώνα οι φυσικοί έστρεψαν την προσοχή τους και το ενδιαφέρον τους στη μελέτη των μοριακών ,ατομικών και πυρηνικών συστημάτων, στα οποία συμβαίνουν μικροσκοπικά φαινόμενα , δηλαδή φαινόμενα που δεν είναι δυνατόν να παρατηρηθούν απ' ευθείας. Υπάρχουν λόγοι για τους οποίους η ίδια η παρατήρηση διαταράσσει αυθαίρετα το υπό παρατήρηση σύστημα και έτσι το σφάλμα της μετρήσεως φυσικών μεγεθών ενός συστήματος δεν μπορεί να

ελαττωθεί απεριόριστα όπως στην κλασσική φυσική. Σύντομα έγινε αντιληπτό ότι οι νόμοι ,οι μέθοδοι και τα πρότυπα της κλασσικής φυσικής δεν ήταν αρκετά για να εξηγήσουν τα φαινόμενα της μοριακής ,ατομικής και πυρηνικής φυσικής.

Οι πρώτες προσπάθειες στην ατομική φυσική απέβλεψαν στην υπερνίκηση των δυσκολιών της κλασσικής θεωρίας με τροποποίηση νόμων ή με αλλαγή των προτύπων . Οι προσπάθειες αυτές οδήγησαν στην συνήθως καλούμενη παλαιά κβαντική θεωρία ,όπως διαμορφώθηκε με τις εργασίες των Planck, Bohr ,De Broglie και άλλων. Η πρώτη αυτή μορφή της κβαντικής θεωρίας άνοιξε ορίζοντες στην επιστήμη ,εξήγησε πολλά από τα τότε γνωστά φαινόμενα ,άφηνε όμως πολλά κενά στην κατανόηση άλλων. Οι προσπάθειες συνεχίστηκαν για να καταλήξουν σε επιτυχία την περίοδο 1925-1930, οπότε και διαμορφώθηκε και μια νέα μορφή κβαντικής θεωρίας με τις εργασίες των Schrödinger ,Heisenberg, Dirac και άλλων .

Η ανάπτυξη της κβαντομηχανικής χωρίζεται σε 2 περιόδους, γι αυτό και εμφανίζεται με δύο ονομασίες:

- 1900 – 1923 : Παλαιά κβαντική θεωρία

Η πρώτη φάση που αρχίζει περίπου το 1900 με την εισαγωγή της έννοιας του quantum από τον Planck, φτάνει στο ζενίθ της με το άτομο του Bohr το 1913 και τελειώνει το 1923, καλύπτει την ανάπτυξη της παλαιάς κβαντικής φυσικής θεωρίας. Αυτή η εποχή μπορεί να θεωρηθεί ως ένα μεταβατικό στάδιο μεταξύ της Κλασσικής Φυσικής και της σύγχρονης κβαντομηχανικής που θεμελιώθηκε μεταξύ 1924 και 1927 και αποτελεί τη δεύτερη φάση.

Η πρώτη φάση θεωρείται μεταβατικό στάδιο γιατί αποτελείται μεν από μη κλασσικές παραδοχές (π.χ. κβάντωση) αλλά σε ένα καθαρά κλασσικό εννοιολογικό πλαίσιο.

- 1923 κ έπειτα : Κβαντική μηχανική

Η θεωρία αυτή ξεκίνησε με την εισαγωγή πινάκων από τον Heisenberg στους μαθηματικούς υπολογισμούς. Ακολούθησε η κυματική μηχανική του Schrödinger καθώς και η αρχή της απροσδιοριστίας από τον Heisenberg.

Τα έξι κύρια σημεία που επεξηγεί η κβαντική θεωρία, υπερβαίνοντας τις δυνατότητες της κλασσικής, είναι:

1. Η διακριτότητα (κβάντωση) της ενέργειας
2. Η δυαδικότητα του φωτός και της ύλης

3. Ο Κβαντικός Εναγκαλισμός
4. Η Κβαντική Σήραγγα
5. Η Κβαντική Τηλεμεταφορά
6. Ο Κβαντικός Υπολογιστής

❖ ΔΙΑΚΡΙΤΟΤΗΤΑ ΕΝΕΡΓΕΙΑΣ

Τα ηλεκτρόνια υπάρχουν σε διακεκριμένες ενεργειακές στάθμες μέσα στο άτομο. Όταν κατά την αποδιέγερσή τους από μια υψηλή ενεργειακή στάθμη μεταπηδούν προς μια χαμηλότερη, εκπέμπουν ένα φωτόνιο το οποίο σύμφωνα με την αρχή διατήρησης της ενέργειας, έχει ενέργεια που αντιστοιχεί στη ενεργειακή διαφορά των δύο ενεργειακών σταθμών. Αυτό όμως προϋποθέτει ότι τα ηλεκτρόνια υπάρχουν μόνο σε συγκεκριμένες ενεργειακές στάθμες, αλλιώς σύμφωνα με την Κλασσική Φυσική θα κινούνταν με σπειροειδή πορεία προς τον πυρήνα.

Το γεγονός ότι υπάρχουν διακριτές τιμές για τα επίπεδα των ενεργειακών επιπέδων, μαζί με άλλες «κβαντισμένες» ατομικές ιδιότητες, αποτελούν και την κβάντωση της ενέργειας. Η κβάντωση είναι μια κεντρική υπόθεση για την κβαντική θεωρία καθώς με αυτήν επιλύεται το "αίνιγμα" της ατομικής σταθερότητας.

❖ ΔΥΑΔΙΚΟΤΗΤΑ ΑΚΤΙΝΟΒΟΛΙΑΣ

«Είναι ένα αναντίρρητο γεγονός ότι υπάρχει μια εκτεταμένη συλλογή δεδομένων για την ακτινοβολία που δείχνουν ότι, το φως έχει ορισμένες θεμελιώδεις ιδιότητες, που μπορούν να κατανοηθούν πολύ πιο εύκολα από τη σκοπιά της σωματιδιακής θεωρίας του Νεύτωνα παρά από τη σκοπιά της κυματικής θεωρίας. Επομένως, κατά τη γνώμη μου, η επόμενη φάση ανάπτυξης της Θεωρητικής Φυσικής θα μας οδηγήσει σε μια θεωρία για το φως, που θα μπορεί να ερμηνευθεί σαν ένα είδος συγκερασμού της κυματικής και σωματιδιακής εικόνας.» - A. Einstein (1909)

Ο Luis De Broglie το 1923 απέδειξε μαθηματικά πως ένα υλικό σωματίδιο θα μπορούσε να συμπεριφερθεί ως κύμα, κάτι που απέδειξαν και πειραματικά οι Davisson και Germer το 1927. Πώς γίνεται όμως κάτι να έχει τις ιδιότητες και τη συμπεριφορά ενός κύματος και ενός σωματιδίου ταυτόχρονα;

Αυτό το ερώτημα καλύπτει η δυαδικότητα που πρεσβεύει η Κβαντική Φυσική, αποδεχόμενη και τις δύο φύσεις του φωτός και των σωματιδίων. Αναφέρει δηλαδή πως η Ακτινοβολία και η Ύλη συντίθενται μεν από σωματίδια αλλά η πιθανότητα να βρεθεί αυτό το σωματίδιο σε διάφορες θέσεις διαθέτει κυματική συμπεριφορά. Το φως που εμφανίζεται μερικές φορές ως κύμα οφείλεται στο ότι παρατηρούμε

την συσσώρευση πολλών από τα σωματίδια του (κβάντα), κι έτσι διαμοιράζονται πάρα πολύ οι πιθανότητες για διαφορετικές θέσεις στις οποίες κάθε σωματίδιο θα μπορούσε να υπάρχει.

Χονδρικά, αναφερόμενοι στη διπλή υπόσταση του φωτός, μπορούμε πλέον να θεωρούμε ότι το φως είναι κύμα όσο δεν ανιχνεύεται (δηλαδή όταν δεν αποτελεί αντικείμενο μελέτης), ενώ όταν ανιχνεύεται, παύει να είναι κύμα και συμπεριφέρεται ως σωματίδιο.

Σε αυτό το σημείο κρίνεται σκόπιμο να αναφερθεί η Αρχή Αβεβαιότητας του Heisenberg. Αυτή η αρχή δηλώνει την αδυναμία ταυτόχρονης μέτρησης της θέσης και της ορμής ενός σωματιδίου σε μια δεδομένη στιγμή. Είναι βέβαια δυνατόν να γνωρίζουμε το ένα από τα δύο μεγέθη (δηλ. την ορμή ή τη θέση) αλλά όχι και τα δύο.

Αυτή η αρχή μάλιστα, πέρα από το ότι είναι ένα από τα σημαντικότερα «εργαλεία» της Κβαντικής Φυσικής, συνδέεται άμεσα και με την υπόθεση της συμπληρωματικότητας του Bohr, κατά την οποία η μέτρηση μιας μεταβλητής καθιστά αυτομάτως μη μετρήσιμη κάποια άλλη.

❖ ΚΒΑΝΤΙΚΟΣ ΕΝΑΓΚΑΛΙΣΜΟΣ

Αρχικά, πριν μιλήσουμε για τον κβαντικό εναγκαλισμό θα πρέπει να αναφέρουμε κάποιες άλλες πληροφορίες όπως το ότι ένα σωμάτιο είναι δυνατόν να βρίσκεται ταυτόχρονα σε περισσότερες από μια κβαντικές καταστάσεις (ή ιδιοσυναρτήσεις) που αντιστοιχούν στις συγκεκριμένες τιμές (ιδιοτιμές) ενός μεγέθους (π.χ. της ορμής). Αυτό λέγεται υπέρθεση ή επαλληλία καταστάσεων. Στην προσπάθεια μέτρησης μιας ποσότητας, το πείραμα θα εξάγει μια συγκεκριμένη τιμή καθώς θα προκληθεί κατάρρευση της κυματοσυνάρτησης κατά την ορθόδοξη ερμηνεία της κβαντικής.

Ο Schrodinger διαφώνησε με την ορθόδοξη αυτή ερμηνεία διατυπώνοντας το περίφημο πείραμα σκέψης (θεωρητικό πείραμα) της «γάτας του Schrodinger», το οποίο και αποτελεί ένα πολύ καλό παράδειγμα για να κατανοηθεί το φαινόμενο της επαλληλίας καταστάσεων.

Αυτό το πείραμα αναφέρεται στην περίπτωση μίας γάτας μέσα σε ένα κυτίο μαζί με πηγή εκπομπής ακτινοβολίας. Όταν η πηγή εκπέμπει ακτινοβολία, τότε λόγω κάποιας σύνδεσης σπάει μια φιάλη με δηλητηριώδες αέριο που αυτομάτως σκοτώνει τη γάτα. Η πηγή όμως είναι ένα Κβαντικό Σύστημα το οποίο βρίσκεται στην επαλληλία καταστάσεων εκπομπής και μη εκπομπής (δηλ. 50-50 οι πιθανότητες να εκπέμψει ή όχι ακτινοβολία).

Αν δώσουμε ένα χρονικό περιθώριο (π.χ. μια ώρα) για την ενεργοποίηση της πηγής, μετά το πέρας αυτής της ώρας, αν δεν ανοίξουμε το κυτίο, η γάτα θα είναι και ζωντανή και νεκρή, πράγμα φυσικά αδύνατον. Όταν ανοίξουμε το κυτίο (και καταρρεύσει η κυματοσυνάρτηση εξαιτίας της μέτρησης ή με άλλα λόγια, «καταστραφεί» η υπέρθεση), η γάτα θα είναι ή μόνο ζωντανή ή μόνο νεκρή, όχι όμως και τα δύο.

Στην Κβαντική Φυσική, αυτή η υπόθεση δεν είναι καθόλου παράλογη καθώς το σύστημα πριν τη μέτρηση (πριν ανοίξουμε το κυτίο) μπορεί να βρίσκεται στην υπέρθεση δύο μικροκαταστάσεων. Μόνο μετά τη μέτρηση περιγράφεται αποκλειστικά με την μία από τις δύο καταστάσεις.

Κάπως έτσι καταλήγουμε στον κβαντικό εναγκαλισμό, ο οποίος θεωρεί ότι σε ένα σύστημα το οποίο αποτελείται από ένα ή περισσότερα υποσυστήματα, δεν μπορούμε να αποδώσουμε μια συγκεκριμένη Κβαντική Κατάσταση στο κάθε υποσύστημα τη στιγμή που τα αντίστοιχα σωμάτια δεν έχουν δικές τους ιδιότητες. Αν επιχειρήσουμε να κάνουμε μέτρηση του ενός, επιφέρεται αυτομάτως η αλλαγή των ιδιοτήτων του άλλου, όσο μακριά και αν είναι το ένα από το άλλο.

Το παραπάνω οδήγησε στο παράδοξο EPR φαινόμενο, ένα πείραμα σκέψης που πήρε το όνομά του από τους δημιουργούς του Einstein, Podolsky και Rozen το 1935 και το οποίο αναφερόταν σε αυτή τη δράση εξ αποστάσεως μεταξύ των εναγκαλισμένων σωμάτιων. Βέβαια, αυτό το φαινόμενο δεν αμφισβητεί την πληρότητα της κβαντομηχανικής, όπως πίστευε ο Αϊνστάιν, αλλά την επεκτείνει (όπως αποδείχθηκε πειραματικά κατά τη δεκαετία του ’80).

❖ ΚΒΑΝΤΙΚΗ ΣΗΡΑΓΓΑ

Ένα σημαντικό φαινόμενο είναι η κβαντική σήραγγα. Χωρίς αυτήν, όχι μόνο θα ήταν αδύνατη η λειτουργία των κινητών τηλεφώνων, αλλά δε θα υπήρχαν και τα σημερινά chips που απαρτίζουν έναν σημερινό ηλεκτρονικό υπολογιστή, έτσι όπως τα ξέρουμε τουλάχιστον. Ένα κύμα καθορίζει την πιθανότητα της θέσης ενός σωματιδίου. Όταν αυτό το κύμα αντιμετωπίσει ένα ενεργειακό φράγμα, η κβαντική σήραγγα μας λέει ότι το μεγαλύτερο μέρος του θα ανακλαστεί, ωστόσο, ένα μικρό μέρος του θα διαρρεύσει μέσα στο φράγμα. Το κύμα που διέρρευσε από αυτό το φράγμα θα συνεχίσει τη διάδοσή του στην άλλη πλευρά του φράγματος. Το ενδιαφέρον εδώ είναι πως ακόμη κι αν το σωματίδιο έχει πολύ μικρή ενέργεια για να ξεπεράσει το φράγμα, είναι πιθανό (μικρή πιθανότητα βέβαια) να δημιουργήσει μια σήραγγα μέσα σε αυτό. Αυτό το φαινόμενο βέβαια είναι αρκετά σπάνιο να συναντηθεί στο Μακρόκοσμο (π.χ. μια μπάλα δε μπορεί να διαπεράσει έναν τοίχο χωρίς να του προκαλέσει φθορά), αλλά

στο Μικρόκοσμο (π.χ. με τη μορφή ενός ηλεκτρονίου) είναι μια συνήθης διαδικασία.

❖ ΤΗΛΕΜΕΤΑΦΟΡΑ

Μπορεί η τηλεμεταφορά γενικά ως θέμα να απασχολεί πολλούς συγγραφείς επιστημονικής φαντασίας, ωστόσο, κάτι τέτοιο δεν μπορεί να εφαρμοστεί σε μακροσκοπικό επίπεδο. Παρ' όλα αυτά, σε υποατομικό επίπεδο, η κβαντική τηλεμεταφορά είναι κάτι το οποίο έχει επιτευχθεί.

Ας θεωρήσουμε μια μηχανή fax (πομπός) που στέλνει ακριβή αντίγραφα τρισδιάστατων πληροφοριών σε μια άλλη μηχανή (δέκτης), αφού καταστρέψει το πρωτότυπο αντικείμενο κατά τη συλλογή των πληροφοριών που το διέπουν. Κατόπιν, ο δέκτης θα αναδιατάξει αυτές τις πληροφορίες ακριβώς στην ίδια θέση με το πρωτότυπο χρησιμοποιώντας κατά προτίμηση το ίδιο υλικό ή έστω άτομα του ίδιου είδους.

Μέχρι τη δεκαετία του ’90, αυτή η σκέψη «φόβιζε» τους επιστήμονες λόγω του ότι ένα τέτοιο εγχείρημα θα παραβίαζε την αρχή της αβεβαιότητας που προαναφέρθηκε. Πώς μπορείς να έχεις ακριβείς πληροφορίες για ένα αντικείμενο (ή σωματίδιο) τη στιγμή που η αρχή της αβεβαιότητας στο απαγορεύει; Κι όμως υπάρχει τρόπος: η περιπλοκή.

Η περιπλοκή είναι ένα «τέχνασμα», ένας θεωρητικός τρόπος χρησιμοποίησης της κβαντικής μηχανικής για να παρακαμφθούν οι περιορισμοί της αρχής της αβεβαιότητας, χωρίς όμως να παραβιαστεί η ίδια.

Η ομάδα που «βρήκε» την αρχή της περιπλοκής αποτελούνταν από τους Charles H. Bennett από την IBM , τους Gilles Brassard, Claude Crepeau και Richard Josza από το πανεπιστήμιο του Montreal, από τους Asher Peres από το τεχνολογικό ινστιτούτο του Israel και τον William K. Wootters από το Williams College.

Για να γίνει κατανοητή η περιπλοκή, παίρνουμε το «γνωστό» παράδειγμα των ζαριών: Έχουμε μπροστά μας πολλά ζεύγη ζαριών. Ρίχνουμε το πρώτο ζεύγος και έρχονται και τα δύο 4, ρίχνουμε το επόμενο ζεύγος και έρχονται και τα δύο 1 κ.ο.κ. Αυτό συμβαίνει σε κάθε ζεύγος ζαριών που ρίχνουμε. Το ένα ζάρι είναι τυχαίο, το άλλο όμως δίνει πάντα το ίδιο αποτέλεσμα με το συζευκτικό του.

Όσο περίεργη και αν ακούγεται αυτή η συμπεριφορά των ζαριών στο μακρόκοσμο, έχει αποδειχθεί πειραματικά ότι υφίσταται μεταξύ σωματιδίων. Σε αντιστοιχία με τους αριθμούς των ζαριών, ζεύγη σωματιδίων είναι δυνατόν να παίρνουν στοιχεία, όπως φυσικές ιδιότητες (π.χ. πολικότητα) το ένα από το άλλο. Φυσικά, αυτό συνδέεται

άμεσα με το παράδοξο φαινόμενο EPR της κβαντομηχανικής που προαναφέρθηκε.

Με την περιπλοκή ή τη «συσχέτιση» (όρος που έθεσε ο Schrodinger για το παράδοξο EPR) ως κύρια εφόδια, οι επιστήμονες διεξήγαγαν τρία -επίσημα- πειράματα κατά τη διάρκεια της δεκαετίας του '90. Εκτός από αυτά τα τρία άλλες έρευνες πάνω στην Κβαντική Τηλεμεταφορά έγιναν τον Δεκέμβριο του 1997, όπου δύο ερευνητικές ομάδες, μια στην Αυστρία και μια στη Ρώμη, εξέθεσαν τα επιτυχή πειράματα τηλεμεταφοράς.

❖ Κβαντικός Υπολογιστής

«Μόνο ένας κβαντικός υπολογιστής μπορεί να προσομοιώσει αποτελεσματικά τα κβαντικά συστήματα» - R. Feynman Η παραπάνω πρόταση του Feynman ήταν η πρώτη αναφορά στους κβαντικούς υπολογιστές το 1982, ενώ λίγο αργότερα, το 1985, ο Deutsch διατύπωσε τους κανόνες με τους οποίους θα λειτουργούσε μια υπολογιστική μηχανή βασισμένη στην Κβαντική Φυσική.

Επειδή στην Σύγχρονη Εποχή παρατηρείται μια ραγδαία αύξηση των τηλεπικοινωνιακών συστημάτων λόγω της ανάγκης για γρήγορη επεξεργασία και διακίνηση των πληροφοριών, η δημιουργία ενός κβαντικού υπολογιστή (Quantum computing) αποτελεί μια πολύ ενδιαφέρουσα πρόκληση.

Η Κβαντική Τηλεμεταφορά είναι απαραίτητη προϋπόθεση για τη δημιουργία των κβαντικών Λογικών Πυλών μέσα στους κβαντικούς υπολογιστές, στις οποίες θα γίνεται η επεξεργασία των πληροφοριών.

Υπολογίζεται ότι με τα qubits, έννοια αντίστοιχη με τα σημερινά bits, οι υπολογιστικές μηχανές θα μπορούν να κάνουν μέσα σε λίγα δευτερόλεπτα τεράστιους υπολογισμούς που με τους σημερινούς υπολογιστές θα χρειάζονταν δισεκατομμύρια ημέρες.

Αυτό οφείλεται στο ότι η τιμή ενός qubit μπορεί να είναι 0 και 1 ταυτόχρονα!

Το εμπόδιο, όμως, στη δημιουργία ενός κβαντικού υπολογιστή είναι το κριτήριο Rayleigh, μια βασική αρχή της Οπτικής σύμφωνα με την οποία δε μπορεί να κατασκευαστεί ένα microchip μικρότερο των 124 nanometers.

Θεωρητικά, αυτό το εμπόδιο στην πρόοδο γίνεται να υπερκερασθεί με τη χρήση πεπλεγμένων φωτονίων τα οποία θα μπορούν να συμπεριφέρονται ως ένα (κατά συνέπεια κάποιων κβαντικών νόμων που αναφέρουν ότι τα πεπλεγμένα φωτόνια έχουν ως σύστημα το μισό μήκος κύματος από ό,τι έχουν ως ατομικά σωματίδια)

και ως αποτέλεσμα, θα μπορούν να κατασκευαστούν chips μικρότερα των 64 nanometers.

Ακόμη κι αυτό να γίνει όμως, παρουσιάζονται και άλλα προβλήματα, με σημαντικότερο αυτό της αποσυσχέτισης, κατά την οποία μικρές αλληλεπιδράσεις με εξωτερικούς (ή και εσωτερικούς) περιβαλλοντικούς παράγοντες οδηγούν σε μη κβαντική συμπεριφορά χωρίς εναγκαλισμό, και συνεπώς δυσλειτουργία του κβαντικού υπολογιστή.

ΙΣΤΟΡΙΑ

Η κβαντομηχανική δεν είναι μια θεωρία που προέκυψε από τη φαντασία ενός φυσικού. Οι περισσότεροι φυσικοί την αποδέχτηκαν κάτω από την πίεση των πειραματικών δεδομένων, μια και ερχόταν σε σύγκρουση με τις καθιερωμένες τους αντιλήψεις. Μερικοί μάλιστα, όπως ο Αϊνστάιν, συνέχισαν να την αμφισβητούν μέχρι το τέλος της ζωής τους.

❖ Το 1900 ο **Μαξ Πλανκ (Max Karl Ernst Ludwig Planck)** ήταν ένας σημαντικός Γερμανός φυσικός και κάτοχος Βραβείου Νόμπελ. Γεννήθηκε στις 23 Απριλίου 1858 στο Κίελο της Γερμανίας και πέθανε στις 4 Οκτωβρίου 1947 στο Γκέτινγκεν. Θεωρείται ως ο πατέρας της Κβαντικής Θεωρίας.

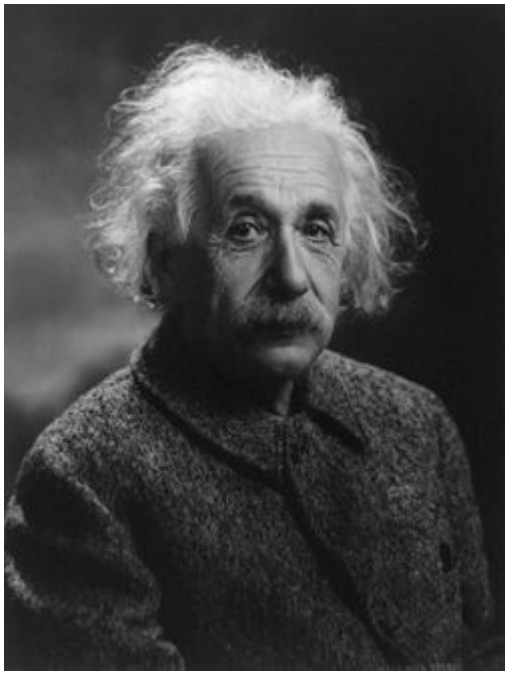
Ο Μαξ Πλανκ ήταν το έκτο παιδί του Johann Julius Wilhelm Planck και το τέταρτο της δεύτερης συζύγου του, Emma Patzig. Το 1867 η οικογένεια μετακόμισε στο Μόναχο και ο Μαξ εγγράφηκε στο περίφημο Königliches Maximilians gymnasium, όπου είχε ως διδάσκαλο τον μαθηματικό Hermann Müller, ο οποίος του δίδαξε επίσης Αστρονομία και Μηχανική. Ο Πλανκ τελείωσε τη μέση εκπαίδευση σε ηλικία 16 ετών, ενώ, όπως και ο Χάιζενμπεργκ, είχε εξαιρετικό ταλέντο στη Μουσική, σε βαθμό που θα μπορούσε να σταδιοδρομήσει και ως επαγγελματίας μουσικός: έπαιζε πιάνο, εκκλησιαστικό όργανο και βιολοντσέλο, τραγουδούσε και συνέθετε τραγούδια και όπερες. Παρόλα αυτά, αποφάσισε να σπουδάσει Φυσική.

Το 1877 πήγε στο Βερολίνο για ένα χρόνο μελέτης με τους διάσημους φυσικούς Hermann von Helmholtz και Gustav Kirchhoff. Επίσης μελέτησε κοντά στον μαθηματικό Καρλ Βάιερστρας. Βρήκε τις διαλέξεις των Χέλμχολτζ και Κίρκοφ μάλλον βαρετές, ωστόσο απέκτησε φιλία με τον πρώτο. Κυρίως, όμως, μελέτησε μόνος του τα έργα του φυσικού Ρούντολφ Κλαούζιους (R. Clausius), κάτι που τον οδήγησε να επιλέξει τη θεωρία της θερμότητας ως πεδίο για ειδίκευση.

Το 1907 προτάθηκε στον Πλανκ η θέση του Μπόλτζμαν στο Πανεπιστήμιο της Βιέννης, αλλά απέρριψε την προσφορά προκειμένου να παραμείνει στο Βερολίνο. Το 1909 δίδαξε ως επισκέπτης καθηγητής

της Θεωρητικής Φυσικής στο Πανεπιστήμιο Κολούμπια της Νέας Υόρκης. Συνταξιοδοτήθηκε από το Πανεπιστήμιο του Βερολίνου στις 10 Ιανουαρίου 1926. Τη θέση του κατέλαβε ο Έρβιν Σρέντινγκερ.

Ο Πλανκ μελετά την ακτινοβολία του μέλανος (μαύρου) σώματος. Προσπαθεί να βελτιώσει μια σχέση στην οποία είχε καταλήξει πριν από αυτόν ο Wien που αφορά την κατανομή της ακτινοβολούμενης ενέργειας στις διάφορες συχνότητες. Το πετυχαίνει χρησιμοποιώντας την υπόθεση πως το φως εκπέμπεται από ένα μέλαν σώμα μόνο σε συγκεκριμένα ποσά ενέργειας (κβάντα) ανάλογα με τη συχνότητά του, δηλαδή ακέραια πολλαπλάσια της ποσότητας $E = hv$ όπου v η συχνότητα και h μια σταθερά (που ονομάστηκε σταθερά του Πλανκ).



❖ Το 1905 ο **Αϊνστάιν** που από πολλούς θεωρείται ως ο μεγαλύτερος φυσικός του 20ού αιώνα, γεννήθηκε στην Ουλμ (Ulm) της Γερμανίας στις 14 Μαρτίου του 1879 και πέθανε στις 18 Απριλίου του 1955 στο Πρίνστον (Princeton) του Νιού Τζέρσεϋ (New Jersey) των ΗΠΑ σε ηλικία 75 ετών. Είναι ο θεμελιωτής της Θεωρίας της Σχετικότητας.

Το 1905 δημοσίευσε τέσσερα άρθρα στο επιστημονικό περιοδικό Annalen der Physik (τόμος 17). Στο πρώτο από αυτά έδωσε την εξήγηση του φωτοηλεκτρικού φαινομένου, για την οποία του απονεμήθηκε το βραβείο Νόμπελ το 1921.

Στηρίχθηκε στην υπόθεση της κβάντωσης η οποία είχε εισαχθεί μερικά χρόνια νωρίτερα από τον Πλανκ για ερμηνεία της ακτινοβολίας του μέλανος σώματος. Οι δύο αυτές εργασίες των Πλανκ και Άινσταϊν αποτέλεσαν την αρχή της κβαντικής μηχανικής. Αργότερα ο Άινσταϊν εναντιώθηκε στην θεωρία των κβάντα, γιατί δεν μπορούσε να πιστέψει ότι ο Θεός παίζει ζάρια.

Στο τρίτο από τα άρθρα που δημοσίευσε το 1905 ο Άινσταϊν διατύπωσε την ειδική θεωρία της σχετικότητας και στο τέταρτο έδειξε ότι από αυτήν συνάγεται ο διάσημος τύπος $E = mc^2$ (γενική θεωρία της σχετικότητας) που δηλώνει τη δυνατότητα και την ισοδυναμία

αλληλομετατροπής ενέργειας και μάζας, ορίζοντας έτσι, ως ενιαίο χώρο την υλοενέργεια. Αυτό σημαίνει πώς η ενέργεια που μπορεί να παράξει οτιδήποτε εξαρτάται από τη μάζα του. Τον Νοέμβριο του 1915, ο Αϊνστάιν παρουσίασε τη γενική θεωρία της σχετικότητας σε μία σειρά διαλέξεων ενώπιον της Πρωσικής Ακαδημίας Επιστημών. Το 1919 κατά τη διάρκεια μίας ηλιακής έκλειψης ο Σερ Άρθουρ Έντινγκτον (Eddington) παρακολούθησε το φως αστέρων καθώς αυτοί περνούσαν κοντά από τον ήλιο. Οι μετρήσεις του συμφωνούσαν με τη θεωρία της σχετικότητας και το γεγονός αυτό έκανε τον Άινσταϊν διάσημο.

❖ Το 1911 ο **Έρνεστ Ράδερφορντ** (**Ernest Rutherford**) προτείνει το πλανητικό μοντέλο για το άτομο, σύμφωνα με το οποίο τα ηλεκτρόνια κινούνται γύρω από ένα πυρήνα που συγκεντρώνει το μεγαλύτερο μέρος της μάζας του ατόμου. Το μοντέλο αυτό ήταν ασυμβίβαστο με την κλασική φυσική διότι σύμφωνα με αυτήν τα ηλεκτρόνια θα έπρεπε κατά την κίνησή τους να εκπέμπουν ακτινοβολία με αποτέλεσμα να χάνουν ενέργεια και έτσι τελικά να πέφτουν πάνω στον πυρήνα. Τα άτομα επομένως θα ήταν ασταθή.

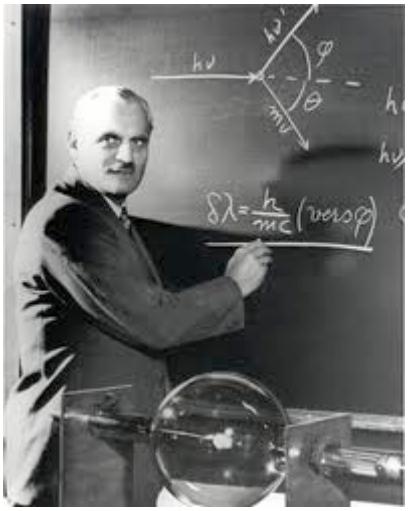
❖ Το 1913 ο **Μπορ** (Niels Bohr) Ο Νιλς Μπορ (Niels Henrik David Bohr 7 Οκτωβρίου 1885 - 18 Νοεμβρίου 1962) ήταν Δανός φυσικός. Σπούδασε στο Πανεπιστήμιο της Κοπεγχάγης και είχε θεμελιώδεις συνεισφορές στην κατανόηση της ατομικής δομής και της κβαντικής μηχανικής.

Το 1911 δούλεψε με τον Έρνεστ Ράδερφορντ και το 1913 σκέφθηκε να συνδυάσει το μοντέλο του τελευταίου για τη δομή του ατόμου (όπου τα αρνητικά φορτισμένα και ελαφρά ηλεκτρόνια περιφέρονται γύρω από τον θετικά φορτισμένο και βαρύ πυρήνα) με τη Κβαντική Θεωρία του Μαξ Πλανκ. Ο Μπορ υπέθεσε στη θεωρία του ότι (α) το ηλεκτρόνιο μπορεί να ακολουθεί μόνον ορισμένες τροχιές, και όχι οποιεσδήποτε, και (β) το ηλεκτρόνιο ακτινοβολεί όχι συνεχώς, όπως ήταν η ως τότε κρατούσα άποψη, αλλά μόνο όταν αλλάζει τροχιά.

Ερμήνευσε όλες τις φασματικές γραμμές που εκπέμπει το υδρογόνο με αυτή την θεωρία, και για τη θεωρητική του αυτή εργασία τιμήθηκε με το Βραβείο Νόμπελ Φυσικής το 1922.

❖ Στην περίοδο 1914 – 1919 οι **Φρανκ** και **Χερτζ** επιβεβαιώνουν πειραματικά την ύπαρξη σταθερών ενεργειακών καταστάσεων, μετρώντας την ενέργεια που χάνουν ηλεκτρόνια που έχουν επιταχυνθεί όταν συγκρούονται με άτομα.

❖ Ο **Ζόμερφιλντ** (**Sommerfeld**) επεξεργάζεται περαιτέρω τη θεωρία του Μπορ και το αποτέλεσμα είναι αυτό που ονομάζεται παλιά κβαντική θεωρία. Αν και πολλά πειραματικά δεδομένα εξηγούνται από αυτήν, υπάρχουν και άλλα που παραμένουν ανεξήγητα, όπως το φαινόμενο Ζέεμαν (Zeeman).



❖ Το 1923 ο **Κόμπτον** (**Arthur Compton**) δείχνει ότι οι ακτίνες Χ παρουσιάζουν χαρακτήρα κυματικό και σωματιδιακό (φαινόμενο Κόμπτον). Ο Λουί ντε Μπρολί (Louis De Broglie) προτείνει ότι και τα υλικά σωματίδια συμπεριφέρονται μερικές φορές σαν κύματα. Αυτό γίνεται γνωστό ως πρόβλημα του κυματοσωματιδιακού δυϊσμού, ενώ τα κύματα ύλης που προβλέπονται από αυτόν το συλλογισμό καθιερώθηκε να αποκαλούνται κύματα ντε Μπρολί.

❖ Το 1925 ο **Βόλφγκανγκ Πάουλι** (Wolfgang Pauli) εισάγει την απαγορευτική αρχή για τα ηλεκτρόνια, σύμφωνα με την οποία δύο ηλεκτρόνια δεν είναι δυνατόν να βρίσκονται στην ίδια κβαντική κατάσταση. Η αρχή αυτή, σε συνδυασμό με τη θεωρία του Μπορ, εξηγεί την σταθερότητα των ατόμων. Την ίδια χρονιά οι Uhlenbeck και Goudsmit εισάγουν την έννοια της ιδιοστροφορμής (σπιν) που δίνει ένα καινούργιο κβαντικό αριθμό, ο οποίος ήταν απαραίτητος για την εφαρμογή της αρχής του Πάουλι.

Ο όρος «κβαντική φυσική» χρησιμοποιήθηκε για πρώτη φορά στο έργο «Planck' s Universe in Light of Modern Physics» του Johnston.

Ως εκείνη την εποχή η κβαντική θεωρία του Πλανκ δεν ήταν πραγματικά μια γενικά αποδεκτή θεωρία αλλά κάτι που προκαλούσε αμηχανία.

Μέχρι την εποχή αυτή η κβαντική θεωρία δεν είχε κάποια γενική δομή και μαθηματικό υπόβαθρο. Ήταν ένα σύνολο από υποθέσεις, εμπειρικούς κανόνες, μεθόδους υπολογισμού και θεωρήματα και όχι μια συνεκτική θεωρία. Δεν υπήρχε σαφής αιτιολόγηση όλων αυτών και, έτσι, πολλοί θεωρούν αυτούς τους πρώτους νόμους φαινομενολογικούς. Η κατάσταση άλλαξε από δύο ανεξάρτητες προσπάθειες, του Χάιζενμπεργκ (Werner Heisenberg) και του Σρέντινγκερ (Erwin Schrodinger).

Ο όρος «Κβαντική Μηχανική» εμφανίζεται για πρώτη φορά σε μελέτη του Μπορν το 1924, με τίτλο "Περί της κβαντομηχανικής" (Zur Quantenmechanik) [1].

❖ Το 1925 ο **Χάιζενμπεργκ** αναπτύσσει μια μαθηματική δομή για την κβαντική θεωρία, βασισμένη στα μαθηματικά των πινάκων. Ο ίδιος, ωστόσο, αγνοεί αυτό το τμήμα των Μαθηματικών και αναγκάζεται να εφεύρει τον φορμαλισμό από την αρχή. Ο Χάιζενμπεργκ βασίζεται σε μια ιδέα της σχολής του Γκέτιγκεν, σύμφωνα με την οποία τα μεγέθη εκείνα που δεν μπορούν να παρατηρηθούν άμεσα πρέπει να απορριφθούν και να ασχολείται κανείς μόνο με παρατηρήσιμα μεγέθη.

❖ Το 1926 ο **Σρέντινγκερ**, ανεξάρτητα από τον Χάιζενμπεργκ και την σχολή του Γκέτιγκεν, προτείνει μια εξίσωση που περιγράφει τα κύματα ντε Μπρολί. Δεχόμενος ότι υπάρχει μια συνάρτηση κύματος Ψ(x,y,z,t) που αντιστοιχεί με ένα κινούμενο σωματίδιο, αναζητά την γενική διαφορική εξίσωση η οποία θα ικανοποιείται από την Ψ. Έτσι καταλήγει στην περίφημη εξίσωση Σρέντινγκερ. Η εξίσωση αυτή αποτέλεσε απαραίτητο εργαλείο για την μελέτη της κίνησης των σωματιδίων, ιδιαίτερα όταν αυτά βρίσκονται μέσα σε πεδίο δυνάμεων.

❖ Την ίδια περίοδο πέφτει στα χέρια του **Ντιράκ** (**Paul Dirac**) ένα αντίγραφο της εργασίας του Χάιζενμπεργκ. Ο Ντιράκ είχε αποφοιτήσει ως μηχανικός από το πανεπιστήμιο του Μπρίστολ και στη συνέχεια πήρε πτυχίο Μαθηματικών. Έτσι, ήταν ήδη

εξοικειωμένος με την άλγεβρα των πινάκων. Επεξεργάζεται, λοιπόν, την εργασία και στέλνει πίσω στον Χάιζενμπεργκ την δική του προσέγγιση.

❖ Το 1927 οι **Ντέιβισον** (**Davisson**) και **Γκέρμερ** (**Germer**) επιβεβαιώνουν πειραματικά την άποψη του ντε Μπρολί για την επέκταση του κυματοσωματιδιακού δυϊσμού στα σωματίδια ύλης, με την σκέδαση ηλεκτρονίων πάνω σε ένα κρύσταλλο. Το αποτέλεσμα της σκέδασης υποδεικνύει μια καθαρά κυματική συμπεριφορά.

❖ Παράλληλα, οι **Ντάργουιν** και **Πάουλι**, ανεξάρτητα ο ένας από τον άλλο, εισάγουν στον φορμαλισμό το σπιν του ηλεκτρονίου.

❖ Τον ίδιο χρόνο ο **φον Νόιμαν** αναπτύσσει μια ολοκληρωμένη και αυστηρή μαθηματική βάση για την κβαντομηχανική, κεντρικά στοιχεία της οποίας είναι οι γραμμικοί τελεστές που δρουν πάνω σε χώρους Χίλμπερτ (Hilbert).

❖ Ο **Μπορν** συσχετίζει τις κυματοσυναρτήσεις που προκύπτουν από την εξίσωση Σρέντινγκερ με την έννοια της πιθανότητας. Συγκεκριμένα, ερμηνεύει το τετράγωνο του μέτρου της κυματοσυνάρτησης $|\Psi(x,y,z,t)|^2$ ως την πυκνότητα πιθανότητας να βρεθεί το εξεταζόμενο σύστημα στις συντεταγμένες x,y,z,t. Η εξέλιξη αυτή θεωρείται ιδιαίτερα κρίσιμη, καθώς τα κβαντικά κύματα νοούνται πλέον σαν κύματα πιθανότητας και όχι ύλης, κάτι που λύνει και τις αντιφάσεις που δημιουργούσε η παλιά κβαντική θεωρία.

❖ Το 1928 ο **Ντιράκ** διατυπώνει την σχετικιστική του εξίσωση για το ηλεκτρόνιο και άλλα παρόμοια με αυτό σωματίδια (φερμιόνια), εξηγώντας ταυτόχρονα το σπιν και προβλέποντας την ύπαρξη του αντιηλεκτρονίου (ή ποζιτρονίου) και των αντισωματιδίων γενικότερα.

❖ Το 1932 ο **Άντερσον** ανακαλύπτει το ποζιτρόνιο μελετώντας κοσμικές ακτίνες.

Στο σημείο αυτό η κβαντομηχανική δεν τελειώνει, αλλά τίθενται οι βάσεις για την εκρηκτική εξέλιξη της επιστήμης και της τεχνολογίας που γνώρισε η ανθρωπότητα. Αναπτύσσεται η πυρηνική φυσική και η μελέτη των στοιχειωδών σωματιδίων, η κβαντική χημεία, εμβαθύνεται η

μελέτη των ημιαγωγών και εφευρίσκονται τα τρανζίστορ, οδηγώντας στην «ηλεκτρονική επανάσταση», ερμηνεύονται οι εσωτερικές διαδικασίες των άστρων, εφευρίσκονται τα λέιζερ, ανακαλύπτεται η υπεραγωγιμότητα κλπ. Σαν άμεση εξέλιξη της ίδιας της θεωρίας μπορούμε, πάντως, να ξεχωρίσουμε τα ακόλουθα:

Από το 1927 γίνονταν προσπάθειες να εφαρμοστεί η κβαντομηχανική σε πεδία αντί σε μεμονωμένα σωματίδια. Το αποτέλεσμα αυτών των προσπαθειών είναι οι λεγόμενες κβαντικές θεωρίες πεδίου. Μερικοί από τους πρώτους ερευνητές αυτού του τομέα είναι ο Ντιράκ, ο Παουλί, ο Weisskopf και ο Jordan. Το αποκορύφωμα της έρευνας αυτής είναι η κβαντική ηλεκτροδυναμική, που αναπτύχθηκε από τους Φάινμαν, Dyson, Schwinger και Tomonaga στα τέλη της δεκαετίας του 1940. Η κβαντική ηλεκτροδυναμική περιγράφει τις αλληλεπιδράσεις των ηλεκτρικά φορτισμένων σωματιδίων και τη φύση του ηλεκτρομαγνητικού πεδίου γενικότερα, ερμηνεύοντας τις ηλεκτρικές αλληλεπιδράσεις με ανταλλαγή φωτονίων. Χρησίμευσε ως πρότυπο για τις κβαντικές θεωρίες πεδίου που ακολούθησαν. Το επόμενο μεγάλο βήμα ήταν μια θεωρία που ενοποιεί τις ηλεκτρομαγνητικές δυνάμεις και την ασθενή πυρηνική δύναμη σε μια μοναδική δύναμη, την ηλεκτρασθενή. Στη συνέχεια αναπτύσσεται μια θεωρία για την ισχυρή πυρηνική δύναμη, η κβαντική χρωμοδυναμική, στις αρχές της δεκαετίας του 1960. Προσπάθειες για μια γενική θεωρία, που να περιλαμβάνει όλες τις θεμελιώδεις δυνάμεις (ηλεκτρομαγνητική, ασθενής πυρηνική, ισχυρή πυρηνική και βαρύτητα) δεν έχουν δώσει ακόμα ικανοποιητικό αποτέλεσμα, έχουν όμως δημιουργήσει νέους τομείς στην θεωρητική σκέψη όπως η θεωρία των υπερχορδών.

Το 1935, οι Αϊνστάιν, Ποντόλσκι (Podolsky) και Ρόζεν (Rosen), δημοσιεύουν το περίφημο παράδοξο που φέρει τα αρχικά των ονομάτων τους, EPR. Το ερώτημα με το οποίο καταπιάνεται το άρθρο τους είναι το κατά πόσον η κβαντομηχανική είναι ή όχι μια πλήρης θεωρία. Η συζήτηση αυτή παίρνει μεγάλες διαστάσεις και αποκαλύπτει νέες πτυχές της κβαντομηχανικής, όπως η μη τοπικότητα και η κβαντική πληροφορία. Οι τεχνολογικές εφαρμογές αυτού του νέου πεδίου, όπως η κβαντική τηλεμεταφορά, η κβαντική κρυπτογραφία και οι κβαντικοί υπολογιστές βρίσκονται σήμερα υπό εξέλιξη. Ως αποτέλεσμα αυτού του προβληματισμού προέκυψε και η ερμηνεία των πολλών κόσμων του Έβερετ (Everett), το 1956.

ΑΚΤΙΝΟΒΟΛΙΑ ΜΕΛΑΝΟΣ ΣΩΜΑΤΟΣ

➢ ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Η ακτινοβολία του μέλανος σώματος δεν είναι τίποτε άλλο από την θερμική ακτινοβολία που εκπέμπουν όλα τα σώματα όταν θερμανθούν. Στην πραγματικότητα, κάθε σώμα με θερμοκρασία έστω και ελάχιστα μεγαλύτερη του απολύτου μηδενός εκπέμπει θερμική ακτινοβολία, η οποία όμως δεν είναι άμεσα αισθητή από εμάς διότι έχει πολύ χαμηλή ένταση αλλά και μήκη κύματος που πέφτουν κυρίως στην περιοχή των ραδιοφωνικών κυμάτων. Αντίθετα, η θερμική ακτινοβολία των πυρακτωμένων σωμάτων γίνεται αισθητή όχι μόνο ως θερμότητα αλλά και ως πλούσιο ορατό φως με το χαρακτηριστικό κοκκινωπό ή κίτρινο χρώμα

Όλα ξεκίνησαν το 1792 όταν ο Thomas Wedgwood, συγγενής του Δαρβίνου και διάσημος κατασκευαστής πορσελάνης παρατήρησε ότι όλα τα αντικείμενα στους φούρνους του, ανεξάρτητα από την χημική τους σύσταση, το μέγεθος και το σχήμα γίνονται κόκκινα στην ίδια θερμοκρασία. Με άλλα λόγια το συμπέρασμα είναι σαφές: Όλα τα πυρακτωμένα αντικείμενα με την ίδια θερμοκρασία, εκπέμπουν την ίδια ακριβώς ηλεκτρομαγνητική ακτινοβολία, ανεξάρτητα από την χημική τους σύσταση και τις φυσικές τους ιδιότητες.

Με την πρόοδο της φασματοσκοπίας, αυτή η παρατήρηση αναπτύχθηκε, έτσι ώστε στα μέσα του $19^{ου}$ αιώνα ήταν γνωστό ότι τα πυρακτωμένα στερεά εκπέμπουν συνεχή φάσματα αντί για ζώνες ή γραμμές που εκπέμπουν τα θερμαινόμενα αέρια.

Το 1859 ο Gustav Kirchhoff όρισε ως μέλαν σώμα ένα αντικείμενο με συντελεστή απορρόφησης $A_F=1$ σε όλες τις συχνότητες. Ο όρος «μέλαν σώμα» προέρχεται από το γεγονός ότι ένα τέτοιο αντικείμενο απορροφά όλη την ηλεκτρομαγνητική ακτινοβολία που προσπίπτει πάνω του με αποτέλεσμα να φαίνεται μαύρο (όλες οι συχνότητες).

Η επόμενη σημαντική εξέλιξη στην προσπάθεια να κατανοηθεί ο καθολικός χαρακτήρας της ακτινοβολίας που εκπέμπεται από πυρακτωμένα στερεά οφείλεται στον Αυστριακό J. Stefan, ο οποίος το 1879 βρήκε πειραματικά ότι η ολική ένταση που εκπέμπει ένα θερμό

στερεό είναι ανάλογη προς τη τέταρτη δύναμη της απόλυτης θερμοκρασίας του.

Μόλις πέντε χρόνια αργότερα, πραγματοποιήθηκε άλλη μια εντυπωσιακή επιβεβαίωση της ηλεκτρομαγνητικής θεωρίας του φωτός του Maxwell, όταν ο Boltzmann εξήγαγε τον νόμο του Stefan συνδυάζοντας τη θερμοδυναμική με τις εξισώσεις του Maxwell.

Ο περίφημος νόμος της μετατόπισης του W. Wien είναι ότι καλύτερο μπορούσε να προκύψει από την χρήση των παραπάνω θεωριών.

Μέσα σε ένα έτος, ο Γερμανός φασματοσκόπος Friedrich Paschen τεκμηρίωσε την εικασία του Wien πειραματιζόμενος με την τότε δύσκολη υπέρυθρη περιοχή του φάσματος.

Το 1900 οι Lummer και Pringsheim επεξέτειναν την περιοχή των μετρήσεων στα 18 μικρόμετρα και οι Rubens και Kurlbaum προχώρησαν ακόμη περισσότερο από τα 18 μικρόμετρα. Αμφότερες οι ομάδες κατέληξαν ότι ο νόμος του Wien ήταν ανεπαρκής σε αυτή την περιοχή.

Μια Κυριακή βράδυ, στις αρχές Οκτωβρίου του 1900, ο Max Planck ανακάλυψε τον περίφημο νόμο για το μέλαν σώμα, ο οποίος οδήγησε στην κβαντική θεωρία. Η στενή σχέση που είχε ο Planck με τους πειραματιστές του Reichsanstalt ήταν πολύ σημαντική για την ανακάλυψη του καθώς νωρίς εκείνη την ημέρα είχε ακούσει από τον Rubens ότι οι τελευταίες του μετρήσεις κατέδειξαν ότι η φασματική πυκνότητα ενέργειας ήταν ανάλογη προς τη θερμοκρασία Τ για τα μεγάλα μήκη κύματος ή τις χαμηλές συχνότητες. Ο Planck ήξερε ότι ο νόμος του Wien ήταν σε πολύ καλή συμφωνία με τα πειραματικά δεδομένα στις υψηλές συχνότητες και εργαζόταν επίμονα επί αρκετά χρόνια, προκειμένου να εξαγάγει τον εκθετικό νόμο του Wien από τις αρχές της στατιστικής μηχανικής και από τους νόμους του Maxwell.

➢ ΓΙΑΤΙ ΟΜΩΣ ΑΚΤΙΝΟΒΟΛΙΑ ΜΕΛΑΝΟΣ ΣΩΜΑΤΟΣ;

Ο λόγος δεν είναι τετριμμένος και έχει να κάνει με την ουσία της ηλεκτρομαγνητικής ακτινοβολίας των θερμών σωμάτων, η οποία μπορεί να χαρακτηριστεί θερμική μόνο αν είναι πραγματικά θερμοποιημένη. Αν, δηλαδή, πριν εκπεμφθεί από το σώμα έχει αλληλεπιδράσει επανειλημμένα με την ύλη του ώστε να έχει έλθει σε θερμική ισορροπία μαζί της.

Στα περισσότερα πυκνά υλικά αυτή η διαδικασία θερμοποίησης είναι αυτονόητη διότι το φως που εκπέμπεται στο εσωτερικό του σώματος από τα άτομα του, πριν φτάσει στην επιφάνεια του και εκπεμφθεί, έχει αλληλεπιδράσει πολλές φορές με άλλα άτομα – αλλάζοντας κατεύθυνση ή συχνότητα κάθε φορά- οπότε η πλήρης θερμοποίηση είναι εξασφαλισμένη.

Σε ορισμένες περιοχές συχνοτήτων – πχ στα ραδιοκύματα ή σε συγκεκριμένες περιοχές του ορατού φάσματος – ένα σώμα μπορεί να είναι πρακτικά διαφανές, οπότε η θερμοποίηση της εκπεμπόμενης ακτινοβολίας θα είναι αδύνατη ή πολύ ατελής.

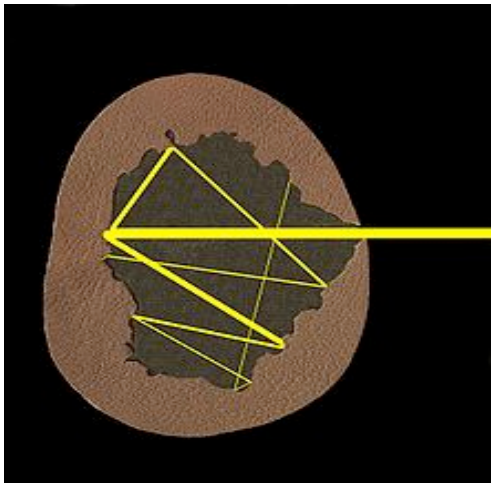
Η ιδέα του μέλανος σώματος ως μιας χρήσιμης εξιδανίκευσης γίνεται τώρα φυσιολογική από τα παραπάνω. Ένα μαύρο σώμα έχει , εξ ορισμού , την ιδιότητα να απορροφά έντονα όλες τις ορατές ακτινοβολίες που πέφτουν στην επιφάνεια του, άρα θα αλληλεπιδρά ισχυρά μαζί τους και όταν τις εκπέμπει και θα εξασφαλίζεται έτσι η πλήρης θερμοποίηση τους.

Το ιδεατό μέλαν σώμα πρέπει να έχει αυτή την ιδιότητα όχι μόνο στην περιοχή του ορατού φωτός αλλά και σε όλη την έκταση του ηλεκτρομαγνητικού φάσματος. Γι αυτό είναι μια ιδεατή οντότητα χωρίς ακριβές αντίκρισμα στον πραγματικό κόσμο.

Όμως – όπως διαπιστώνεται και εμπειρικά με την ομοιοχρωμία όλων των πυρακτωμένων αντικειμένων – τα περισσότερα πυκνά υλικά συμπεριφέρονται με ικανοποιητική ακρίβεια τουλάχιστον σε εκείνο το μέρος του φάσματος – ορατό , υπέρυθρο, υπεριώδες – που έχει τη μεγαλύτερη σημασία για τις συνήθεις θερμοκρασίες των σωμάτων.

➢ ΑΚΤΙΝΟΒΟΛΙΑ ΚΟΙΛΟΤΗΤΑΣ

Ας εξετάσουμε πώς η κλασσική θεωρία προσπαθεί να εξηγήσει την ακτινοβολία του μέλανος σώματος. Για τις ανάγκες μιας πειραματικής μελέτης με μεγάλες απαιτήσεις ακριβείας, το ιδανικό πρότυπο μπορεί να προσεγγιστεί ακόμη καλύτερα με το «τέχνασμα της κοιλότητας». Δηλαδή τη δημιουργία ενός κενού στο εσωτερικό του σώματος με ένα μικρό άνοιγμα στη μια πλευρά του για την έξοδο της ακτινοβολίας που εγκλωβίζεται εκεί.



Το φώς που μπαίνει μέσα στην κοιλότητα από την οπή θα ανακλαστεί πολλές φορές πάνω στα τοιχώματα της κοιλότητας και κάθε φορά ένα μέρος του θα απορροφάται από αυτά. Η πιθανότητα για ένα τμήμα της ακτινοβολίας που μπήκε μέσα στην κοιλότητα από την οπή να ξαναβγεί από αυτήν είναι πολύ μικρή, αν η οπή είναι αρκετά μικρή σε σχέση με την κοιλότητα, πράγμα που σημαίνει ότι μόνο ένα πολύ μικρό μέρος από το προσπίπτον φως ανακλάται από την οπή, ενώ το υπόλοιπο έχει απορροφηθεί. Αυτό συμβαίνει ανεξάρτητα από το υλικό των τοιχωμάτων και το μήκος κύματος της προσπίπτουσας ακτινοβολίας, διότι, καθώς τα στερεά σώματα έχουν συνεχές φάσμα εκπομπής και απορρόφησης, όλα τα μήκη κύματος σταδιακά θα απορροφηθούν.

Δεδομένου ότι το φως που παίρνουμε πίσω είναι αμελητέο, η μόνη ακτινοβολία που θα παίρνουμε από την οπή είναι η θερμική ακτινοβολία που παράγεται στο εσωτερικό της κοιλότητας και εξαρτάται μόνο από την θερμοκρασία της, υπό την προϋπόθεση ότι αυτή βρίσκεται σε θερμική ισορροπία.

Το προσεγγιστικό αυτό μέλαν σώμα είναι μια παραλλαγή του μοντέλου που πρότεινε ο ίδιος ο Κίρχοφ.

➢ ΑΠΟΠΕΙΡΑ ΚΛΑΣΙΚΗΣ ΕΡΜΗΝΕΙΑΣ

Λόγω της θεμελιώδους σημασίας που της προσέδιδε η παγκοσμιότητα της, η φασματική κατανομή της ακτινοβολίας του μέλανος σώματος ήταν από την πρώτη στιγμή μια αυτονόητη πρόκληση για την κλασική φυσική και ειδικότερα για την κλασική ηλεκτροδυναμική και τη στατιστική μηχανική στο πλαίσιο των οποίων θα έπρεπε να είναι δυνατή η ερμηνεία της.

Το έργο αυτό ανέλαβαν οι Rayleigh και Jeans περί τα τέλη του 19ου αιώνα. Ο κλασικός τους τύπος συμφωνεί με τον τύπο του Planck μόνο στην περιοχή των χαμηλών συχνοτήτων, ενώ στις μεγάλες συχνότητες οδηγεί στο απαράδεκτο συμπέρασμα ότι η

ακτινοβολία αυξάνεται απεριόριστα. Η συμπεριφορά αυτή για μεγάλες συχνότητες – γνωστή ως υπεριώδης καταστροφή (δηλαδή την ακατάσχετη αύξηση της εκπεμπόμενης ακτινοβολίας στις υψηλές συχνότητες, η οποία οδηγεί και στο παράλογο συμπέρασμα ότι η ολική ενέργεια που εκπέμπεται από ένα θερμό σώμα ανα δευτερόλεπτο είναι .... άπειρη!!!) – συμπυκνώνει όχι απλώς την αδυναμία της κλασικής φυσικής να ερμηνεύσει τη θερμική ακτινοβολία των σωμάτων αλλά την πλήρη χρεωκοπία της σε αυτό το θέμα.

➢ ΚΒΑΝΤΙΚΗ ΕΡΜΗΝΕΙΑ – ΘΕΩΡΙΑ PLANCK

Έχοντας στη διάθεση του έναν ακριβή εμπειρικό τύπο για τη φασματική ένταση και γνωρίζοντας την πλήρη αδυναμία της κλασικής φυσικής να τον ερμηνεύσει, το αναγκαίο επόμενο βήμα για τον Planck ήταν να αναζητήσει ο ίδιος την κατάλληλη θεωρητική του ερμηνεία.

Το 1894 ο Planck έστρεψε την προσοχή του στο πρόβλημα της ακτινοβολίας μέλανος σώματος. Είχε αναλάβει να ανακαλύψει για λογαριασμό εταιρειών ηλεκτρισμού τον τρόπο παραγωγής του περισσότερου δυνατού φωτός με λαμπτήρες που θα κατανάλωναν την ελάχιστη ενέργεια. Με το πρόβλημα είχε ήδη ασχοληθεί ο Kirchhoff το 1859: πώς εξαρτάται η ένταση της ηλεκτρομαγνητικής ακτινοβολίας που εκπέμπει ένα μέλαν σώμα (ένας τέλειος απορροφητής της ξένης ακτινοβολίας, όπως μία κοιλότητα) από τη συχνότητα της ακτινοβολίας (π.χ. το χρώμα του φωτός) και τη θερμοκρασία του μέλανος σώματος; Το ζήτημα είχε ήδη μελετηθεί πειραματικά, αλλά ο νόμος Rayleigh – Jeans που εξαγόταν με τη βοήθεια της Κλασικής Φυσικής αποτύγχανε να εξηγήσει την παρατηρούμενη συμπεριφορά σε υψηλές συχνότητες, δίνοντας πυκνότητα ενέργειας αποκλίνουσα προς το άπειρο, από όπου και ο όρος «υπεριώδης καταστροφή». Ο Wilhelm Wien πρότεινε τον ομώνυμο νόμο (Νόμος του Wien), που προέβλεπε με ακρίβεια τη συμπεριφορά σε υψηλές συχνότητες, αλλά αποτύγχανε στις χαμηλές. Στην προσπάθειά του να συμφιλιώσει τη θεωρία με το πείραμα, ο Πλανκ ανακάλυψε τον περίφημο Νόμο του Πλανκ για την ακτινοβολία μέλανος σώματος, που θα συγκλόνιζε την επιστήμη της Φυσικής από τα θεμέλιά της. Ο νόμος πρωτοπαρουσιάσθηκε σε μία συνάντηση της Γερμανικής Φυσικής Εταιρείας, στις 19 Οκτωβρίου 1900, και δημοσιεύθηκε το 1901.

Μία πλήρης θεωρητική θεμελίωση του νόμου ήταν έτοιμη στις 14 Δεκεμβρίου 1900, και απαιτούσε ιδέες από τη Στατιστική Μηχανική. Μέχρι τότε ο Πλανκ απεχθανόταν τη στατιστική ερμηνεία του Δεύτερου

Νόμου της Θερμοδυναμικής, τον οποίο εκλάμβανε ως αξίωμα ή αρχή: «... μία πράξη απελπισίας... ήμουν έτοιμος να θυσιάσω οποιαδήποτε από τις προηγούμενες πεποιθήσεις μου σχετικά με τη Φυσική...».

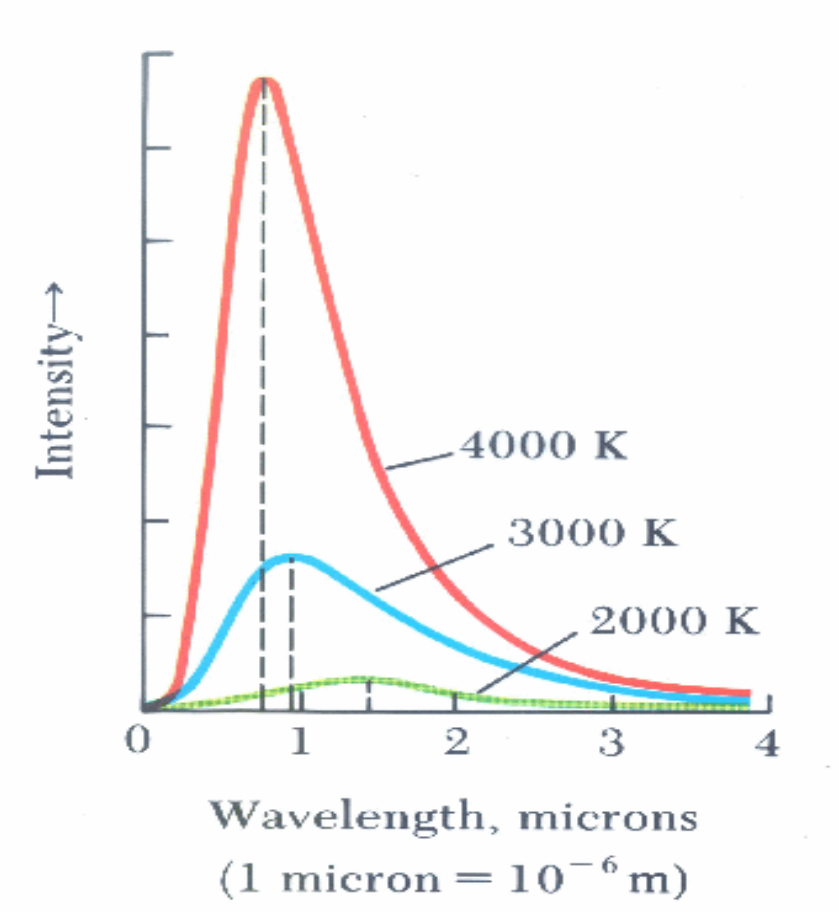
Η θεμελιώδης παραδοχή για να μπορεί να εξαχθεί ο Νόμος του Πλανκ είναι ότι η ηλεκτρομαγνητική ακτινοβολία μπορεί να εκπέμπεται μόνο σε κβαντισμένη μορφή, σε «κβάντα» ή «πακέτα», η ποσότητα της ενέργειας που περιείχε το καθένα από τα οποία ήταν υποχρεωτικώς ακέραιο πολλαπλάσιο μιας στοιχειώδους ποσότητας. Στην περίπτωση αυτή, η στοιχειώδης ποσότητα είναι ανάλογη της συχνότητας της ακτινοβολίας, E = h* ν, όπου h μία σταθερά που σήμερα ονομάζεται «σταθερά του Πλανκ» και είναι η θεμελιώδης σταθερά της Κβαντομηχανικής.

➢ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΚΤΙΝΟΒΟΛΙΑΣ ΜΕΛΑΝΟΣ ΣΩΜΑΤΟΣ.

Σύμφωνα με την κλασική φυσική η ακτινοβολία της κοιλότητας προέρχεται από τις ταλαντώσεις των φορτισμένων σωματιδίων στα τοιχώματα της κοιλότητας και η συχνότητά της είναι ίση με τη συχνότητα των ταλαντώσεων αυτών. Η ενέργεια της ακτινοβολίας μπορεί να πάρει οποιαδήποτε τιμή.

Η ακτινοβολία μέλανος σώματος, *I(λ,T)*, ως συνάρτηση του μήκους κύματος και της θερμοκρασίας έχει τη μορφή που φαίνεται στο σχήμα όπου:

- *I(λ, T)* είναι η εκπεμπόμενη ισχύς (ενέργεια/χρόνο) ανά μονάδα επιφάνειας και συχνότητας.
- *u(λ, T)* είναι η φασματική πυκνότητα ενέργειας, δηλαδή η ενέργεια ανά μονάδα συχνότητας και όγκου στην κοιλότητα που αναπαριστά το μέλαν σώμα. I(λ,T)=u(λ,T) c/4, όπου c η ταχύτητα του φωτός στο κενό.



Σχήμα : Ένταση της ακτινοβολίας που εκπέμπεται από μέλαν σώμα ως συνάρτηση της συχνότητας και της θερμοκρασίας.

ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

1. Το φάσμα (εκπεμπόμενη ακτινοβολία ως συνάρτηση της συχνότητας) του μέλανος σώματος είναι συνεχές με ένα ευρύ μέγιστο. Εξαρτάται μόνο από τη θερμοκρασία.
2. Η συνολική εκπεμπόμενη ισχύς ανά μονάδα επιφάνειας, *I(T)*, (*I(f,T)* ολοκληρωμένο ως προς συχνότητα) είναι ανάλογη προς την τέταρτη δύναμη της απόλυτης θερμοκρασίας: $I_{total} = \sigma T^4$. *Νόμος Stefan-Boltzmann.* ($\sigma = 5.67 \times 10^{-8}$ $Wm^{-2}K^{-4}$ είναι η σταθερά των Stefan -Boltzmann.)
3. Καθώς η θερμοκρασία αυξάνει το μέγιστο της καμπύλης εκπομπής μετακινείται προς υψηλότερες συχνότητες (μικρότερα μήκη κύματος). Η μετακίνηση αυτή περιγράφεται από τον *Νόμο μετατόπισης του Wien*: $\lambda_{max}\ T = 0.2898\ cm\ K$ (λ_{max} είναι το μήκος κύματος το οποίο η εκπομπή ακτινοβολίας γίνεται μέγιστη).

4. Για χαμηλές συχνότητες (μεγάλα μήκη κύματος) η εκπομπή μέλανος σώματος περιγράφεται από τον *νόμο των Rayleigh-Jeans*: $I(\lambda,T) = E_{av}\, 2\pi c/\lambda^4$, όπου $E_{av} = k_B T$ (σύμφωνα με τον Boltzmann) είναι η μέση ενέργεια (ανά ταλαντωτή) των ταλαντωτών που εκπέμπουν την ακτινοβολία. k_B είναι η σταθερά του Boltzmann.
5. Για υψηλές συχνότητες (μικρά μήκη κύματος) η εκπομπή μέλανος σώματος περιγράφεται από τον *εκθετικό νόμο του Wien* (πειραματικός νόμος): $I(\lambda,T) = (A/\lambda^5)e^{-B/\lambda T}$, *A, B* σταθερές.

➢ ΠΑΡΑΔΕΙΓΜΑΤΑ ΘΕΡΜΙΚΗΣ ΑΚΤΙΝΟΒΟΛΙΑΣ ΠΟΥ ΠΡΟΣΕΓΓΙΖΟΥΝ ΤΟ ΜΕΛΑΝ ΣΩΜΑ

❖ ΛΑΒΑ

Στην εικόνα φαίνεται μια ποσότητα λάβας pahoehoe, ενός είδους βαλσατικής λάβας. Η θερμοκρασία της μπορεί να υπολογιστεί από το χρώμα της. Το αποτέλεσμα του υπολογισμού συμφωνεί με τις πειραματικές μετρήσεις για λάβα θερμοκρασίας από 1000°C μέχρι 1200 °C.

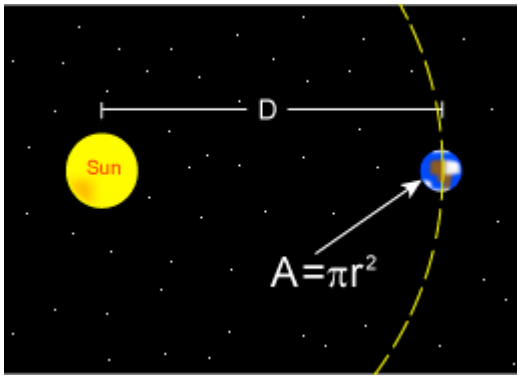
❖ ΑΚΤΙΝΟΒΟΛΙΑ ΑΝΘΡΩΠΙΝΟΥ ΣΩΜΑΤΟΣ

Όπως όλα τα υλικά σώματα, το ανθρώπινο σώμα εκπέμπει θερμική ακτινοβολία. Επειδή η θερμοκρασία του είναι χαμηλή, το μεγαλύτερο μέρος του φάσματος της ακτινοβολίας αυτής

βρίσκεται έξω από την περιοχή του ορατού, στην περιοχή της υπέρυθρης ακτινοβολίας. Ταυτόχρονα, το σώμα μας απορροφά θερμική ακτινοβολία από το περιβάλλον. Η διαφορά της ισχύς της απορροφούμενης ενέργειας από την εκπεμπόμενη μας δείχνει πόση ενέργεια απελευθερώνουμε στο περιβάλλον υπό την μορφή ηλεκτρομαγνητικής ακτινοβολίας.

Η θερμοκρασία της ελεύθερης επιδερμίδας είναι γύρω στους 32 °C, (90 °F, ή 305°K), αλλά τα ρούχα την μειώνουν κατά μερικούς βαθμούς. Έτσι, για τον υπολογισμό μας θα χρησιμοποιήσουμε την τιμή των 301 °K. Η θερμοκρασία του περιβάλλοντος κυμαίνεται πολύ. Αν θεωρήσουμε όμως ότι έχουμε θερμοκρασία δωματίου, 20 °C (68 °F, ή 293 °K), βρίσκουμε ότι η ισχύς της ακτινοβολούμενης ενέργειας από το ανθρώπινο σώμα είναι 95 watts. Βλέπουμε δηλαδή ότι το σώμα μας εκπέμπει ακτινοβολία περίπου ίση με ένα ηλεκτρικό λαμπτήρα των 100 watt, με την διαφορά ότι εκπέμπει στο υπέρυθρο ή και σε μεγαλύτερα μήκη κύματος.

Εφαρμόζοντας τον νόμο μετατόπισης του Wien βρίσκουμε ότι το μήκος κύματος για το οποίο η εκπομπή γίνεται μέγιστη είναι λ_{max}=9500nm. Γι' αυτό, οι συσκευές θερμικής απεικόνισης όπως οι διόπτρες υπερύθρου που είναι σχεδιασμένες για εντοπισμό ανθρώπων, ανταποκρίνονται συνήθως σε περιοχή φάσματος 7 ως 14μm.

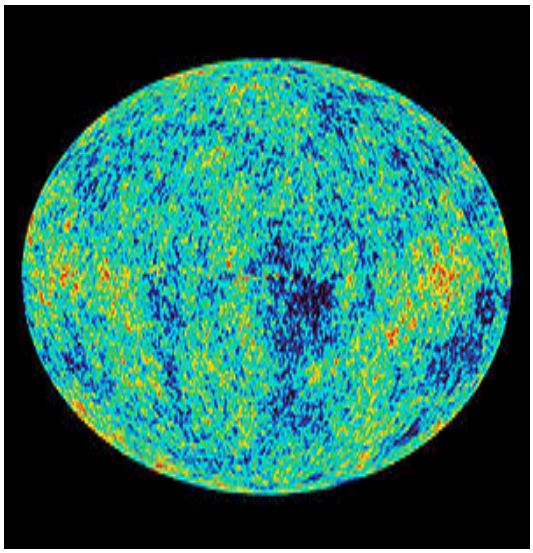


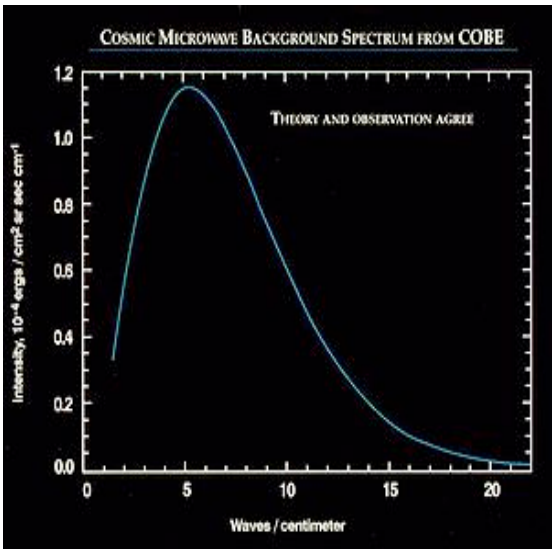
❖ ΣΧΕΣΗ ΘΕΡΜΟΚΡΑΣΙΑΣ ΜΕΤΑΞΥ ΕΝΟΣ ΠΛΑΝΗΤΗ ΚΑΙ ΤΟΥ ΑΣΤΡΟΥ ΤΟΥ

Θεωρώ ότι τόσο η Γη όσο και ο Ήλιος είναι σφαιρικά μελανά σώματα, το καθένα από τα οποία βρίσκεται σε κατάσταση θερμικής ισορροπίας. Για ένα πιο ακριβή υπολογισμό θα έπρεπε επιπλέον να ληφθούν υποψήν: το φαινόμενο albedo (η ανάκλαση μέρους της ακτινοβολίας από τον πλανήτη), το φαινόμενο του θερμοκηπίου (για πλανήτες με ατμόσφαιρα), η ενέργεια που παράγεται εσωτερικά από τον ίδιο τον πλανήτη (αυτό παίζει σημαντικότερο ρόλο σε πλανήτες όπως ο Δίας).

Μετά από υπολογισμούς βρίσκουμε την επιφανειακή θερμοκρασία του ήλιου ίση με 5960K. Η τιμή αυτή βρίσκεται μέσα στο 3% της συνήθους μέτρησης των 5780K. Έτσι πιο πάνω νόμος είναι έγκυρος για τις περισσότερες επιστημονικές και μηχανολογικές εφαρμογές.

❖ ΚΟΣΜΙΚΗ ΑΚΤΙΝΟΒΟΛΙΑ ΥΠΟΒΑΘΡΟΥ

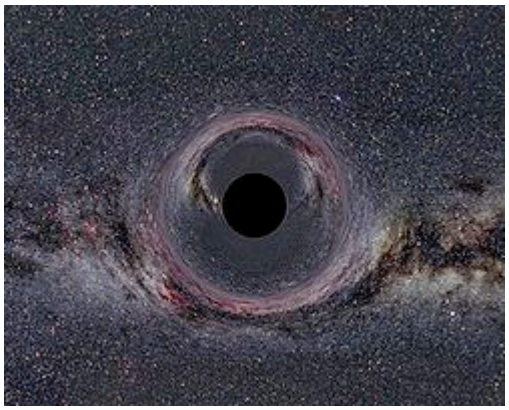




Στην πρώτη εικόνα βλέπουμε την σχηματοποιημένη καταγραφή δεδομένων από τον δορυφόρο WMAP (Wilkinson Microwave Anisotropy Probe) της NASA, ο οποίος μετρά προς διάφορες κατευθύνσεις την θερμοκρασία της θερμικής ακτινοβολίας που απελευθερώθηκε κατά την διάρκεια της μεγάλης έκρηξης που δημιούργησε το σύμπαν - γνωστής και ως κοσμική ακτινοβολία υποβάθρου. Σκοπός του WMAP είναι να ανιχνεύσει μικροσκοπικές διαφορές στην ακτινοβολία υποβάθρου ούτως ώστε να μπορούν να ελεγχθούν τα διάφορα μοντέλα που περιγράφουν την εξέλιξη του σύμπαντος. Αν και η ακτινοβολία αυτή είναι διάχυτη και δεν αφορά (πλέον) κανένα συγκεκριμένο σώμα, το φάσμα της παρουσιάζει εκπληκτική συμφωνία με τον νόμο της ακτινοβολίας του μέλανος σώματος. Πρόκειται για την πιο τέλεια προσέγγιση που έχει καταγραφεί ποτέ.

Η δεύτερη εικόνα προέρχεται από προηγούμενη αποστολή με παρόμοιο σκοπό, από τον δορυφόρο COBE (Cosmic Background Explorer). Είναι γραφική παράσταση της έντασης της ακτινοβολίας ως προς των αριθμό των κυμάτων ανά εκατοστό. Η συμφωνία των πειραματικών μετρήσεων με την θεωρία είναι τέτοια ώστε τα 34 σημεία που τοποθετήθηκαν για να σχηματίσουν την καμπύλη καλύφθηκαν ακριβώς από την καμπύλη που προβλέπει η θεωρία, και τα διαστήματα λάθους ήταν τόσο μικρά που δεν ξεπερνούν το πάχος της γραμμής. Τα δεδομένα δείχνουν ότι το 99,97% της ακτινοβολίας υποβάθρου απελευθερώθηκε μέσα στον πρώτο χρόνο από την στιγμή της μεγάλης έκρηξης, και αντιστοιχούν στο φάσμα μελανού σώματος θερμοκρασίας 2,7°K.

❖ ΜΑΥΡΕΣ ΤΡΥΠΕΣ



Μαύρη τρύπα ονομάζεται μια περιοχή του χώρου στην οποία το βαρυτικό πεδίο είναι τόσο ισχυρό, ώστε κανένα σώμα που βρίσκεται μέσα σ' αυτήν δεν μπορεί να διαφύγει. Η επιφάνεια της περιοχής αυτής ονομάζεται «ορίζοντας γεγονότων». Η δυνατότητα ύπαρξης μαύρων οπών προβλέπεται από την γενική θεωρία της σχετικότητας, όταν μια ποσότητα ύλης συγκεντρωθεί σε μια απειροελάχιστη περιοχή. Αναμένεται ότι κάτι τέτοιο συμβαίνει όταν ένα άστρο με αρκετά μεγάλη μάζα, τουλάχιστον 3-5 φορές μεγαλύτερη από την μάζα του Ήλιου, χρησιμοποιήσει όλα τα «καύσιμά» του και αρχίσει να ψύχεται. Τελικά η μάζα του άστρου καταρρέει λόγω της βαρυτικής έλξης των σωματιδίων που την αποτελούν, δημιουργώντας μια μαύρη τρύπα. Μέσα στα όρια της μαύρης τρύπας το βαρυτικό πεδίο είναι τόσο ισχυρό, που ούτε το φως δεν μπορεί να διαφύγει.

Εφόσον η μαύρη τρύπα απορροφά όλο το φως που πέφτει πάνω της (όπως και οτιδήποτε άλλο), αποτελεί, σύμφωνα με τον ορισμό, μέλαν σώμα. Όμως ο τρόπος με τον οποίο μια μαύρη τρύπα απορροφά φως, δεν έχει τίποτα να κάνει με τον τρόπο που ένα στερεό σώμα απορροφά φως. Επιπλέον, εφόσον τίποτα δεν είναι δυνατόν να διαφύγει από το βαρυτικό της πεδίο, δεν πρέπει ούτε και να εκπέμπει οποιαδήποτε ακτινοβολία.

Σύμφωνα με την θεωρία, μια μαύρη τρύπα χαρακτηρίζεται από μια θερμοκρασία αντιστρόφως ανάλογη από το μέγεθος του ορίζοντα γεγονότων της, και επομένως αντιστρόφως ανάλογη από την μάζα της. Με λίγα λόγια, όσο μικρότερη είναι μια μαύρη τρύπα, τόσο μεγαλύτερη είναι η θερμοκρασία της.

ΦΩΤΟΗΛΕΚΤΡΙΚΟ ΦΑΙΝΟΜΕΝΟ

➢ Η ΑΡΧΗ ΤΗΣ ΘΕΩΡΙΑΣ

Το 1887 ο Hertz παρατήρησε ηλεκτρονική εκπομπή, όταν η επιφάνεια ορισμένων μετάλλων, όπως ο ψευδάργυρος, το ρουβίδιο, το νάτριο κ.α. φωτιζόταν με υπεριώδη ακτινοβολία.

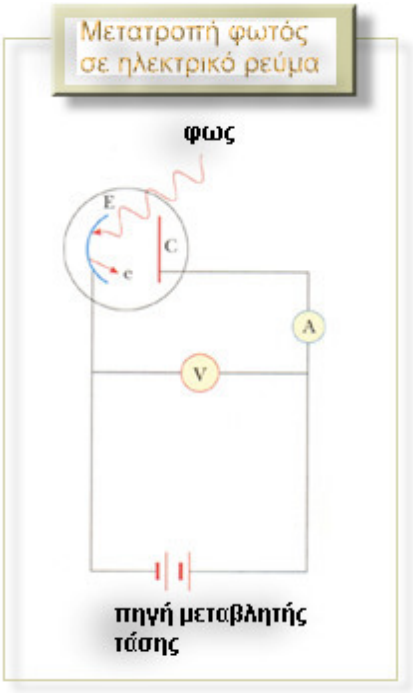
Το Μάρτιο του 1905 συνέβη μια σπουδαία εξέλιξη στην κβαντική θεωρία. Ο A. Einstein σε μία από τις τρεις του δημοσιεύσεις με τίτλο « μια ευρετική άποψη για την παραγωγή και τους μετασχηματισμούς του φωτός» διατύπωσε τη θεωρία των κβάντων φωτός και εξήγησε το φωτοηλεκτρικό φαινόμενο. Σύμφωνα με τον Einstein η ηλεκτρομαγνητική ακτινοβολία όχι μόνο απορροφάται και εκπέμπεται κατά κβάντα αλλά και διαδίδεται στο χώρο κατά κβάντα

Με αυτή του την δημοσίευση διασταύρωσε τα ξίφη του με τον Maxwell και αμφισβήτησε τη μέχρι τότε εντυπωσιακή επιτυχία της κυματικής θεωρίας του φωτός. Ο Einstein είχε διατυπώσει την ύπαρξη αντιφάσεων στους συλλογισμούς του Planck και, πιο συγκεκριμένα μεταξύ της κβάντωσης των ταλαντωτών, που βρίσκονται στα τοιχώματα του μέλανος σώματος και του ισχυρισμού του ότι η ακτινοβολία στην κοιλότητα απαρτιζόταν από κλασικά ηλεκτρομαγνητικά κύματα. Αποδεικνύοντας ότι η μεταβολή της εντροπίας της ακτινοβολίας μέλανος σώματος ήταν παρόμοια με την μεταβολή της εντροπίας του ιδανικού αερίου αποτελούμενου από ανεξάρτητα σωματίδια, ο Einstein κατέληξε στο συμπέρασμα ότι το φως αποτελείται από κόκκους ασυνεχών κβάντων ενέργειας. Επίσης, υποστήριξε ότι το φως, που αλληλεπιδρά με την ύλη, απαρτίζεται επίσης από κβάντα, και πραγματεύθηκε με έξοχο τρόπο τις συνέπειες που έχει αυτό το γεγονός στις φωτοηλεκτρικές και φωτοχημικές διεργασίες. Η εξήγηση που έδωσε για το φωτοηλεκτρικό φαινόμενο παρείχε πειστικά επιχειρήματα ότι το φως αποτελείται από κβάντα ενέργειας.

➢ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ

Με το όνομα «φωτοηλεκτρικό φαινόμενο» χαρακτηρίζουμε την εκπομπή ηλεκτρονίων από ένα μέταλλο η οποία προκαλείται από την πρόσπτωση ορατής ή υπεριώδους ακτινοβολίας στην επιφάνεια του. Στην πραγματικότητα ο όρος χρησιμοποιείται σήμερα με ένα πολύ

ευρύτερο περιεχόμενο. Δηλώνει την απόσπαση ηλεκτρονίων από οποιοδήποτε φυσικό σύστημα – άτομο, μόριο ή στερεό – στο οποίο τα ηλεκτρόνια αυτά είναι δέσμια.



Εφαρμογές του φωτοηλεκτρικού φαινομένου συναντάμε στα φωτοκύτταρα ή φωτοστοιχεία, τα φωτοβολταϊκά στοιχεία, τα ηλιακά στοιχεία κ.α.

Στην πειραματική διάταξη για την μελέτη του φαινομένου, οι παράμετροι που μπορούν να μετρηθούν είναι η συχνότητα και η ένταση της φωτεινής δέσμης και η τάση της πηγής. Το μέγεθος που μετράμε είναι η ένταση του φωτοηλεκτρικού ρεύματος.

Η φωτεινή δέσμη πέφτει σε μια φωτοευαίσθητη κάθοδο και τα αποσπώμενα ηλεκτρόνια συλλέγονται από την άνοδο και παράγουν το φωτοηλεκτρικό ρεύμα που διαρρέει το κύκλωμα.

Αντιστρέφοντας την πολικότητα της πηγής μέχρι την τιμή V_0 , όπου το φωτοηλεκτρικό ρεύμα σταματάει τελείως (τάση αποκοπής), μπορούμε να μετρήσουμε επίσης και την κινητική ενέργεια των αποσπώμενων από την κάθοδο ηλεκτρονίων.

Βασικά το φωτοηλεκτρικό φαινόμενο δεν είναι παρά ειδική περίπτωση μιας ευρύτατης κατηγορίας φαινομένων που αφορούν τη δράση του φωτός πάνω στην ύλη.

➢ ΠΕΙΡΑΜΑΤΙΚΟΙ ΝΟΜΟΙ

Με αφετηρία την πρώτη παρατήρηση από τον Hertz της εξαγωγής ηλεκτρονίων από μέταλλα με πρόσπτωση υπεριώδους φωτός, ακολούθησε μια εντατική μελέτη του φαινομένου – με καθολική τη συμβολή του Lenard στις αρχές του 1900 – που οδήγησε τελικά στη διατύπωση των ακολούθων πειραματικών νόμων:

1. Η ένταση του φωτοηλεκτρικού ρεύματος αυξάνεται ανάλογα με την ένταση της φωτεινής δέσμης.

2. Το φωτοηλεκτρικό φαινόμενο συμβαίνει μόνο όταν η προσπίπτουσα στη μεταλλική επιφάνεια ηλεκτρομαγνητική ακτινοβολία έχει συχνότητα μεγαλύτερη ή ίση από μια ορισμένη τιμή. Η τιμή αυτή ονομάζεται οριακή συχνότητα ή διαφορετικά συχνότητα κατωφλίου.
3. Η μέγιστη κινητική ενέργεια των φωτοηλεκτρονίων με την οποία εγκαταλείπουν το μέταλλο είναι γραμμική συνάρτηση της συχνότητας της προσπίπτουσας ακτινοβολίας, εξαρτάται από το έργο εξαγωγής του μετάλλου αλλά είναι ανεξάρτητη της έντασης της ακτινοβολίας.
4. Το φωτοηλεκτρικό ρεύμα εμφανίζεται σχεδόν ταυτόχρονα με την πρόσπτωση της φωτεινής δέσμης στη φωτοκάθοδο. Αν υπάρχει χρονική υστέρηση, αυτή θα είναι μικρότερη από ένα νανοδευτερόλεπτο (10^{-9} sec).

➢ ΑΠΟΠΕΙΡΑ ΚΛΑΣΙΚΗΣ ΕΡΜΗΝΕΙΑΣ

Η κλασσική φυσική υποστηρίζει ότι ένα σώμα απορροφά ή εκπέμπει ενέργεια κατά τρόπο συνεχή και έτσι αδυνατεί να ερμηνεύσει το φωτοηλεκτρικό φαινόμενο. Συγκεκριμένα:

❖ Η κλασσική φυσική δεν προβλέπει την ύπαρξη συχνότητας κατωφλίου. Αντίθετα προβλέπει ότι η εκπομπή ηλεκτρονίων είναι δυνατή για οποιαδήποτε συχνότητα εφόσον περνούσε αρκετός χρόνος φωτισμού του μετάλλου. Στην πραγματικότητα όμως αν η συχνότητα της προσπίπτουσας ακτινοβολίας είναι μικρότερη της συχνότητας κατωφλίου όσος χρόνος και να περάσει τα ηλεκτρόνια δεν μπορούν να απορροφήσουν αρκετή ενέργεια ώστε να διαφύγουν από το μέταλλο.

❖ Η κλασσική φυσική προβλέπει ότι η εκπομπή ηλεκτρονίων από το μέταλλο γίνεται μετά από την παρέλευση ορισμένου χρονικού διαστήματος από τη στιγμή φωτισμού του μέχρι να αποκτήσουν αρκετή κινητική ενέργεια. Στην πραγματικότητα όμως τα ηλεκτρόνια εκπέμπονται σχεδόν ταυτόχρονα με το φωτισμό του μετάλλου ακόμα και όταν η ένταση της ακτινοβολίας είναι μικρή.

❖ Η κλασσική φυσική προβλέπει ότι η μέγιστη κινητική ενέργεια των εκπεμπόμενων φωτοηλεκτρονίων αυξάνεται όσο αυξάνεται η ένταση της προσπίπτουσας ακτινοβολίας. Στην πραγματικότητα όμως η μέγιστη κινητική ενέργεια των εκπεμπόμενων φωτοηλεκτρονίων βρέθηκε να είναι ανεξάρτητη της έντασης. Βρέθηκε ότι εξαρτάται μόνο από τη συχνότητα της ακτινοβολίας.

Είναι φανερό ότι η αδυναμία της κλασικής φυσικής να εξηγήσει τους νόμους του φωτοηλεκτρικού φαινομένου είναι πλήρης και μάλλον αθεράπευτη.

➢ ΚΒΑΝΤΙΚΗ ΕΡΜΗΝΕΙΑ: Η ΥΠΟΘΕΣΗ ΤΩΝ ΦΩΤΟΝΙΩΝ

Το 1905 ο Albert Einstein σε μια δημοσίευση του αναφέρει: «η ενέργεια μιας φωτεινής ακτίνας που εκπέμπεται από μια σημειακή πηγή δεν είναι συνεχώς κατανεμημένη στον χώρο, αλλά αποτελείται από έναν πεπερασμένο αριθμό ενεργειακών κβάντων, που είναι τελείως εντοπισμένα στον χώρο χωρίς να διαιρούνται και τα οποία μπορούν να παραχθούν ή να απορροφηθούν μόνο ως ολόκληρες μονάδες.»

Το βασικό μήνυμα που μας μεταφέρουν οι πειραματικοί νόμοι μπορεί να συνοψιστεί στα ακόλουθα σημεία:

1. Το χαρακτηριστικό μέγεθος του κύματος που φαίνεται να παίζει κεντρικό ρόλο στον μηχανισμό της φωτοεκπομπής δεν είναι η ένταση αλλά η συχνότητα. Στην κλασική θεωρία του φωτός η συχνότητα είναι ένα καθαρά κυματικό χαρακτηριστικό, με τελείως δευτερεύοντα ρόλο στις ενεργειακές δοσοληψίες ύλης και ακτινοβολίας, οι οποίες ρυθμίζονται βασικά από την ένταση του ηλεκτρικού πεδίου. Τα πειραματικά αποτελέσματα μας λένε το αντίθετο ακριβώς. Η ενεργειακή δραστηριότητα του φωτός εξαρτάται κυρίως από την συχνότητα και δευτερευόντως από την ένταση.
2. Η απορρόφηση της ενέργειας γίνεται πρακτικώς ακαριαία. Το ηλεκτρόνιο παίρνει από το φως την ενέργεια εξαγωγής του σε μια μοναδική δόση και όχι βαθμιαία, όπως προβλέπει η κλασική ηλεκτρομαγνητική θεωρία.

Ενόψει των παραπάνω, ο Einstein δεν δίστασε να επεκτείνει τα όρια ισχύος της παραδοχής του Planck, θεωρώντας ότι η κβάντωση είναι μια εγγενής ιδιότητα του ηλεκτρομαγνητικού πεδίου και όχι απλώς μια ιδιομορφία του μηχανισμού αλληλεπίδρασης του με την ύλη , όπως πίστευε ο ίδιος ο Planck. Έτσι διατύπωσε την υπόθεση των φωτονίων : «το ηλεκτρομαγνητικό κύμα αποτελείται από φωτόνια ενέργειας $E=hf$ όπου h η σταθερά του Planck και f η συχνότητα του κύματος».

Με την φωτονιακή θεωρία ο μηχανισμός της εξαγωγής είναι πολύ απλός. Ένα φωτόνιο απορροφάται από ένα ηλεκτρόνιο μεταβιβάζοντας του όλη την ενέργεια. Ένα μέρος της αναλίσκεται ως

αντίτιμο του έργου εξαγωγής του μετάλλου και το υπόλοιπο μετατρέπεται σε κινητική ενέργεια του εξερχόμενου ηλεκτρονίου.

Και οι άλλοι πειραματικοί νόμοι εξηγούνται επίσης πολύ απλά. Αύξηση της φωτεινής έντασης στη φωτονιακή θεωρία σημαίνει αύξηση της ροής των φωτονίων, που με τη σειρά της συνεπάγεται αύξηση του ρυθμού των εξαγόμενων ηλεκτρονίων.

Είναι φανερό, επίσης, ότι η εξαγωγή γίνεται ακαριαία γιατί η μεταβίβαση της αναγκαίας ενέργειας από το φως στο ηλεκτρόνιο γίνεται στιγμιαία, με τη απορρόφηση ολόκληρης της ενέργειας ενός φωτονίου.

Τέλος, είναι φανερό ότι η κινητική ενέργεια των φωτοηλεκτρονίων συνδέεται γραμμικά με τη συχνότητα της προσπίπτουσας δέσμης, όπως είχε δείξει και το πείραμα. Μάλιστα η κλίση της πειραματικής ευθείας οφείλει να είναι ίση με τη σταθερά του Planck.

➢ ΚΑΙ ΜΕΤΑ ΤΙ;

Το 1914, οι James Franck και Gustav Hertz εκτέλεσαν ένα πείραμα στο οποίο κατέδειξαν το αντίστροφο του φωτοηλεκτρικού φαινομένου. Δηλαδή αποδείχθηκε ότι κατά την σύγκρουση ενός επιταχυνόμενου ηλεκτρονίου με ένα άτομο, για να αποσπαστεί ένα ηλεκτρόνιο από το άτομο, πρέπει η ενέργεια του ηλεκτρονίου να είναι πάνω από μία ορισμένη τιμή. Η ενέργεια αυτή που λέγεται ενέργεια ιοντισμού ποικίλλει από άτομο σε άτομο. Επίσης έδειξαν ότι για την εκπομπή φωτονίων από άτομα του υδραργύρου, τα οποία συγκρούονται με ηλεκτρόνια, απαιτείται η κινητική ενέργεια των ηλεκτρονίων να υπερβαίνει μια ορισμένη ενέργεια, που αντιστοιχεί στη μικρότερη συχνότητα του φάσματος εκπομπής του υδραργύρου.

Εμφάνισαν δηλαδή ότι είναι διακριτές - καθορισμένες - οι ενεργειακές στάθμες των ατόμων. Έτσι τα αποτελέσματα του πειράματος βοήθησαν να επιβεβαιωθεί η κβαντική θεωρία, που πρόβλεπε ότι τα ηλεκτρόνια καταλαμβάνουν μόνο καθορισμένες, κβαντικές ενεργειακές καταστάσεις. Για την συμβολή τους στην κατανόηση και επιβεβαίωση της κβαντικής θεωρίας πήραν το βραβείο Nobel φυσικής, το 1925.

ΦΑΙΝΟΜΕΝΟ COMPTON.

Το φαινόμενο Compton αφορά τη σκέδαση της ηλεκτρομαγνητικής ακτινοβολίας πάνω σε φορτισμένα σωματίδια και, ειδικότερα, πάνω σε ηλεκτρόνια.

Ήταν ένα από τα φαινόμενα που αδυνατούσε να εξηγήσει η κλασσική φυσική και μια από τις πρώτες επιτυχίες της κβαντικής θεωρίας. Ονομάστηκε έτσι προς τιμή του Αμερικάνου Arthur Compton, ο οποίος μελέτησε πειραματικά το πρόβλημα και κατάφερε να το εξηγήσει με την βοήθεια της κβαντικής θεωρίας. Ο Compton τιμήθηκε με το βραβείο Nobel το 1927 για την ανακάλυψη του

➢ ΙΣΤΟΡΙΚΑ

Αν και ο Einstein εισήγαγε το 1905 την αντίληψη ότι το φως αποτελείται από κβάντα ενέργειας σημειακής μορφής, δεν μελέτησε απευθείας την ορμή την οποία μεταφέρει το φως, μέχρι το 1919. Εκείνο το έτος, σε μια μελέτη του στην οποία πραγματευόταν το θέμα ενός μοριακού αερίου που βρίσκεται σε θερμική ισορροπία σε ηλεκτρομαγνητική ακτινοβολία, κατέληξε στο συμπέρασμα ότι ένα φωτόνιο μεταδίδεται προς μια κατεύθυνση (αντίθετα με ένα σφαιρικό κύμα) και ότι έχει ενέργεια E= h* f και μεταφέρει ορμή p= E/c. Όμως αυτή ήταν μόνο μια θεωρητική πρόβλεψη. Στις αρχές της δεκαετίας του '20, η σωματιδιακή φύση του φωτός, που δείχθηκε με τη βοήθεια του φωτοηλεκτρικού φαινομένου, ήταν ακόμη σε αμφισβήτηση.

Το 1923 ο Αμερικανός Arthur Holly Compton και ανεξάρτητα από αυτόν, ο Peter Debye, προχώρησαν ένα βήμα πιο πέρα από τον Einstein. Ερμήνευσαν τη σκέδαση των ακτίνων -Χ (φωτονίων μικρού μήκους κύματος) από ηλεκτρόνια, θεωρώντας ότι τα φωτόνια έχουν ενέργεια και ορμή σύμφωνα με το συμπέρασμα του Einstein.

Ήδη από το 1922 ο Compton είχε δείξει ότι η Κλασσική Φυσική δεν επαρκούσε να ερμηνεύσει τη σκέδαση των ακτίνων-Χ. Το 1923 δημοσίευσε τα αποτελέσματα πειραμάτων με ακτίνες Χ τα οποία επαληθεύουν την υπόθεση του σωματιδιακού χαρακτήρα της ακτινοβολίας.

➢ ΑΚΤΙΝΕΣ Χ

Οι ακτίνες Χ ανακαλύφθηκαν το 1895 από τον Γερμανό φυσικό Wilhelm Roentgen, ο οποίος διατύπωσε ότι, όταν μια δέσμη ηλεκτρονίων μεγάλης ταχύτητας προσπέσει σε έναν μεταλλικό στόχο παράγει μια νέα και πολύ διεισδυτική μορφή ακτινοβολίας.

Χονδρικές εκτιμήσεις που προέκυψαν από την περίθλαση των ακτίνων Χ σε λεπτή σχισμή κατέδειξαν ότι τα μήκη κύματος των ακτίνων Χ είναι περίπου 10^{-10}m, δηλαδή της ίδιας τάξης μεγέθους με τις διατομικές αποστάσεις στους κρυστάλλους.

Το ευρύ συνεχές φάσμα των ακτίνων Χ προκύπτει από την ανάκλαση ή έμμεση σκέδαση ηλεκτρονίων από μεταλλική επιφάνεια. Το ελάχιστο μήκος κύματος του συνεχούς φάσματος ακτίνων Χ, όπως διαπιστώνεται πειραματικά, είναι ανεξάρτητο από τη σύσταση του στόχου και εξαρτάται μόνο από την τάση της λυχνίας.

Οι στενές γραμμές στο φάσμα των ακτίνων Χ εξαρτώνται από τη σύσταση του στόχου και αποτελούν μαρτυρία για τις διακριτές ενεργειακές στάθμες των εσωτερικών ατομικών ηλεκτρονίων. Με απλά λόγια, μια δέσμη ακτίνων Χ μπορεί να θεωρηθεί ότι προκύπτει όταν ένα προσπίπτον ενεργητικό ηλεκτρόνιο απομακρύνει ένα ηλεκτρόνιο από ένα άτομο του στόχου, δημιουργώντας μια οπή σε κάποια εσωτερική στοιβάδα. Ένα ηλεκτρόνιο από μια εσωτερική στοιβάδα συμπληρώνει αμέσως την οπή αυτή και η περίσσεια ενέργειας του ηλεκτρονίου της εξωτερική στοιβάδας αποδίδεται ως ένα φωτόνιο ακτίνων Χ.

➢ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΦΑΙΝΟΜΕΝΟΥ

Ήδη από το 1922 ο Compton σε πειράματα που έκανε στο πανεπιστήμιο Washington του Saint Louis των ΗΠΑ και οι συνεργάτες του είχαν αποδείξει πως η σκέδαση ακτίνων Χ από ηλεκτρόνια δεν μπορούσαν να εξηγηθούν με τη βοήθεια της κλασικής φυσικής. Σύμφωνα με την κλασική ερμηνεία, οι ακτίνες Χ θέτουν σε ταλάντωση το ηλεκτρόνιο όταν προσπίπτουν πάνω του. Αυτό στη συνέχεια επιταχύνεται και εκπέμπει με τη σειρά του ηλεκτρομαγνητική ακτινοβολία. Η ακτινοβολία αυτή θα έχει συχνότητα που θα εξαρτάται από τον χρόνο έκθεσης του ηλεκτρονίου στην ακτινοβολία, καθώς και από την ένταση της τελευταίας. Το πείραμα, όμως, έδειχνε πως η συχνότητα της σκεδαζόμενης ακτινοβολίας εξαρτάται μόνο από τη γωνία σκέδασης. Η κλασική θεωρία ήταν κατά συνέπεια ανεπαρκής για την εξήγηση του φαινομένου.

➢ ΤΟ ΠΕΙΡΑΜΑ

Ως προς τη ακτινοβολία που θα χρησιμοποιήσουμε, είναι εύλογο ότι θα πρέπει να έχει αρκετά μικρό μήκος κύματος ώστε η ορμή των φωτονίων της, να είναι αρκετά μεγάλη και έτσι η σύγκρουση τους με τα ηλεκτρόνια να έχει μετρήσιμο αποτέλεσμα: μια μεγάλη μεταφορά ορμής και ενέργειας από τα φωτόνια στα ηλεκτρόνια. Η συνθήκη αυτή ικανοποιείται πολύ άνετα με την χρήση ακτίνων Χ, των οποίων τα φωτόνια έχουν ενέργεια μερικών keV και αντίστοιχο μήκος κύματος της τάξεως των μερικών angstrom.

Μετά την ακτινοβολία, το επόμενο ερώτημα για τη σωστή σχεδίαση του πειράματος Compton αφορά τα ηλεκτρόνια. Ποιος θα είναι ο στόχος; Θα είναι τα ελεύθερα ηλεκτρόνια ενός μετάλλου ή τα δέσμια ηλεκτρόνια των ατόμων ή μορίων ενός τυχόντος υλικού; Η απάντηση είναι ότι δεν έχει σημασία. Οι ενέργειες των φωτονίων των ακτίνων Χ είναι τόσο μεγάλες σε σύγκριση με τις ενέργειες δέσμευσης των εξωτερικών ηλεκτρονίων στα άτομα ή στα μόρια ώστε να είναι κυριολεκτικά αστείο να εκλαμβάνονται ως δέσμια αυτά τα ηλεκτρόνια.

Επιπλέον – ενόψει των τεράστιων ορμών που φέρουν τα προσπίπτοντα φωτόνια – δεν θα πρέπει να έχουν ιδιαίτερη σημασία ούτε οι ταχύτητες των ηλεκτρονίων του υλικού που θα χρησιμοποιηθεί σαν στόχος. Τα ηλεκτρόνια αυτά μπορεί να θεωρηθούν ακίνητα. Από πρακτικής πλευράς μπορούμε να επιλέξουμε ως στόχο οποιοδήποτε υλικό θέλουμε.

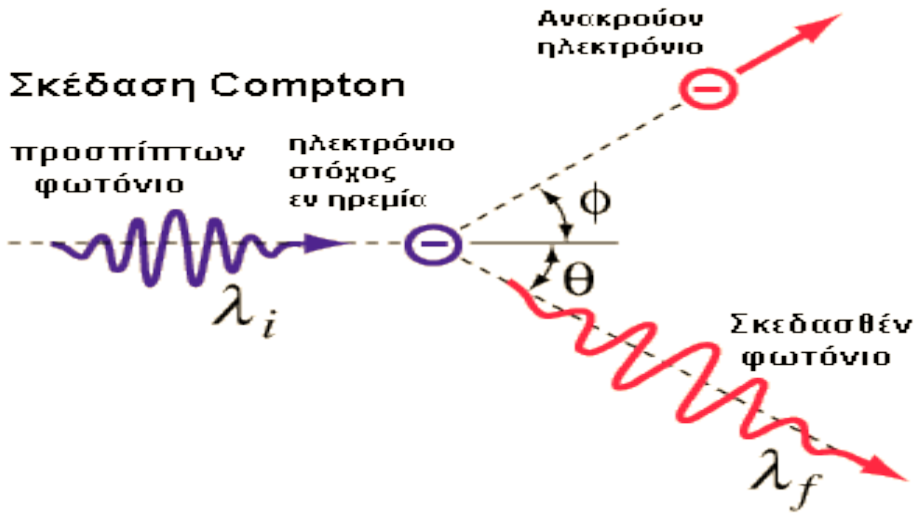
Μονοχρωματική δέσμη ακτίνων Χ , πέφτει πάνω σε κάποιο υλικό στόχο (γραφίτης στο αρχικό πείραμα) και σκεδάζεται προς διάφορες κατευθύνσεις της αρχικής δέσμης. Χρησιμοποιώντας κατάλληλο φασματογράφο μετρούμε, για δεδομένη γωνία σκέδασης , την ένταση του σκεδαζόμενου φωτός σαν συνάρτηση του μήκους κύματος .

Ο Compton εκτέλεσε το πείραμα για διάφορες γωνίες σκέδασης και μετρώντας τα μήκη κύματος και την ένταση των σκεδαζόμενων δεσμών, παρατήρησε ότι υπήρχαν δύο κορυφές στην γραφική παράσταση της έντασης, συναρτήσει του μήκους κύματος. Η πρώτη κορυφή αντιστοιχούσε σε μήκος κύματος λ, το οποίο ήταν το μήκος κύματος της αρχικής δέσμης. Η δεύτερη κορυφή αντιστοιχούσε σε μήκος κύματος λ’, του οποίου η σχέση με τη γωνία σκέδασης διδόταν από τον τύπο

$$\lambda_f - \lambda_i = \Delta\lambda = \frac{h}{m_e c}(1 - \cos\theta)$$

όπου h η σταθερά δράσεως του Planck , m_e η μάζα ηρεμίας του ηλεκτρονίου και c η ταχύτητα του φωτός. Η παραπάνω σχέση ονομάζεται μερικές φορές ως εξίσωση του φαινομένου Compton (ή απλά εξίσωση του Compton) και τα αποτελέσματα που έδινε ήταν πολύ κοντά στα αντίστοιχα πειραματικά του Compton

Με άλλα λόγια το φαινόμενο Compton μας λέει ότι η σκέδαση ηλεκτρομαγνητικής ακτινοβολίας μικρού μήκους κύματος πάνω σε ελεύθερα ή ασθενώς δέσμια ηλεκτρόνια συνοδεύεται με αύξηση του μήκους κύματος της. Η αύξηση είναι τόσο μεγαλύτερη όσο μεγαλύτερη είναι η γωνία σκέδασης θ.



Δύο βασικά χαρακτηριστικά που καλούμαστε να εξηγήσομε είναι (α) ότι για κάθε γωνία υπάρχει ένα τοπικό μέγιστο της έντασης , και (β) ότι για μη μηδενικές γωνίες σκέδασης εμφανίζεται ένα ακόμα μέγιστο σε τιμή του . Πώς εξηγούνται όλα αυτά;

Ένα απλό μοντέλο: Για να κατανοήσομε τα παραπάνω θα μελετήσουμε την σκέδαση ενός φωτονίου από ένα ακίνητο φορτίο. Χειριζόμαστε με άλλα λόγια το φως σαν μια δέσμη φωτονίων, καθένα από τα οποία θα σκεδαστεί με τον ίδιο τρόπο που θα σκεδαστεί αυτό που θα μελετήσομε. Τί είναι το φορτίο; Προφανώς, το φως σκεδάζεται από τα φορτία που βρίσκονται μέσα στην ύλη. Αυτά είναι ελεύθερα ηλεκτρόνια με μάζα m_e, ισχυρά δέσμια ηλεκτρόνια που συμπεριφέρονται σαν βαριά σωμάτια με μάζα ουσιαστικά ίση με την

μάζα ολόκληρου του ατόμου, και θετικά φορτισμένοι ατομικοί πυρήνες. Κανένα από αυτά φυσικά δεν είναι ακίνητο. Υπόκεινται τόσο σε κβαντομηχανικές όσο και σε θερμικές κινήσεις. Οι χαρακτηριστικές ταχύτητες αυτών των κινήσεων είναι πολύ μικρότερες από την ταχύτητα του φωτός και επομένως σε πρώτη προσέγγιση θα τις αγνοήσομε. Έστω, λοιπόν ότι φωτόνιο συχνότητας ν συγκρούεται με ακίνητο φορτίο μάζας m και σκεδάζεται στην κατεύθυνση με γωνία θ ως προς την αρχική. Αντίστοιχα, το φορτίο μετά τη σύγκρουση κινείται στην κατεύθυνση φ.

➢ ΚΛΑΣΙΚΗ ΕΡΜΗΝΕΙΑ

Ως προς τη δυνατότητα κλασικής ερμηνείας του φαινομένου Compton γίνεται γρήγορα φανερό ότι η παρατηρούμενη μεταβολή συχνότητας και μήκους κύματος είναι ακατανόητη μέσα στο πλαίσιο του κλασικού ηλεκτρομαγνητισμού. Στην Κλασσική Θεωρία, όταν ηλεκτρομαγνητική ακτινοβολία συχνότητας f_0 προσπίπτει σε ένα ελεύθερο ηλεκτρόνιο, τότε αυτό θα ταλαντωθεί με την ίδια συχνότητα f_0 του ηλεκτρικού πεδίου της Η/Μ ακτινοβολίας. Γνωρίζουμε όμως ότι ένα φορτίο που ταλαντώνεται αρμονικά εκπέμπει ακτινοβολία συχνότητας f_0, ίσης με την συχνότητα ταλάντωσης του ηλεκτρονίου. Έτσι η δευτερογενής ακτινοβολία που θα προέκυπτε κατά τη πρόσπτωση μιας ακτινοβολίας σε ελεύθερα ηλεκτρόνια, θα έπρεπε να είχε την ίδια συχνότητα f_0 με την πρωτογενή. Τέλος το μήκος κύματος της σκεδαζόμενης ακτινοβολίας θα εξαρτιόταν από τον χρόνο έκθεσης του δείγματος στην προσπίπτουσα ακτινοβολία και από την έντασή της.

Σύμφωνα όμως με την κλασική θεωρία, η μεταβολή συχνότητας κατά τη σκέδαση της ηλεκτρομαγνητικής ακτινοβολίας πάνω σε ελεύθερα ηλεκτρόνια είναι αδύνατη, δηλαδή το φαινόμενο Compton δεν υπάρχει!

➢ ΚΒΑΝΤΙΚΗ ΕΡΜΗΝΕΙΑ

Σύμφωνα με τη φωτονιακή θεωρία της ακτινοβολίας, το φαινόμενο Compton δεν είναι τίποτα άλλο παρά μια ελαστική κρούση ενός φωτονίου με ένα ηλεκτρόνιο. Ο λεπτομερειακός μηχανισμός του φαινομένου είναι ο ακόλουθος: το φωτόνιο απορροφάται προς στιγμήν από το ηλεκτρόνιο και αμέσως μετά επανεκπέμπεται σε μια διεύθυνση διαφορετική εν γένει από την αρχική.

Με την παρατήρηση του φαινομένου Compton και οι τελευταίες αντιρρήσεις για τον δυαδικό χαρακτήρα της ηλεκτρομαγνητικής ακτινοβολίας καταρρέουν. Η υπόθεση του κυματοσωματιδιακού δυϊσμού του φωτός αποκτά πια μια ακλόνητη πειραματική βάση.

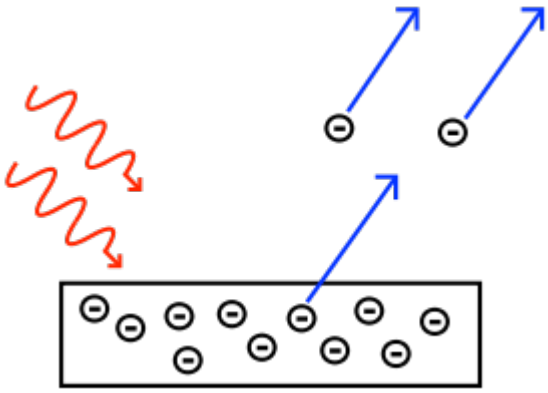
ΚΥΜΑΤΟΣΩΜΑΤΙΔΙΑΚΟΣ ΔΥΙΣΜΟΣ

➢ ΓΕΝΙΚΑ

Η ερμηνεία του φωτοηλεκτρικού φαινομένου έγινε το 1905 από τον Albert Einstein που πήρε το βραβείο Νόμπελ για αυτή του την εργασία. Για να ερμηνεύσει το φωτοηλεκτρικό φαινόμενο, ο Einstein υπέθεσε ότι η ενέργεια ενός ηλεκτρομαγνητικού κύματος δεν είναι ισοκατανεμημένη στο κυματικό μέτωπο αλλά μεταφέρεται σε διακριτές ποσότητες που ονομάζονται φωτόνια. Η διαπίστωση αυτή αποτέλεσε, μαζί με την ερμηνεία της ακτινοβολίας του μέλανος σώματος από τον Planck και την παρατήρηση του φαινομένου Compton, το θεμέλιο της θεωρίας για τον κυματοσωματιδιακό δυϊσμό του φωτός αλλά και της πρώιμης κβαντικής μηχανικής..

Η ηλεκτρομαγνητική ακτινοβολία δεν έχει τον καθαρά κυματικό χαρακτήρα που της αποδίδει η κλασική φυσική αλλά έχει ταυτόχρονα και σωματιδιακή υπόσταση με σωματιδιακό φορέα αυτό που αποκαλούμε σήμερα φωτόνιο, το σωματίδιο του φωτός. Όμως ο κυματοσωματιδιακός δυϊσμός του φωτός – δηλαδή η διαπίστωση ότι το φως είναι κύμα και σωματίδιο ταυτόχρονα- είναι απλώς μια όψη μιας γενικότερης αρχής. Διότι παράλληλα με τη διπλή φύση του φωτός ανακαλύφθηκε επίσης και το αντίθετο της. Ότι, δηλαδή, μια φυσική οντότητα όπως τα σωματίδια, π.χ τα ηλεκτρόνια, τα πρωτόνια, τα οποία μέσα στο κλασικό πλαίσιο θεωρούνται αποκλειστικά ως σωματίδια, εκδηλώνουν επίσης και κυματική συμπεριφορά. Είναι σωματίδια και κύματα ταυτόχρονα.

Αυτός ο περίφημος κυματοσωματιδιακός δυϊσμός της ύλης σε συνδυασμό με τον κυματοσωματιδιακό δυϊσμό του φωτός συγκροτούν δύο όψεις μιας ενιαίας φυσικής αρχής : του κυματοσωματιδιακού δυϊσμού.



➢ ΚΛΑΣΙΚΗ ΦΥΣΙΚΗ

Μέσα στο κλασικό πλαίσιο η συνύπαρξη σωματιδιακών και κυματικών ιδιοτήτων είναι όχι απλώς αδύνατη αλλά και λογικά αδιανόητη. Κατ΄ αρχάς ένα σωματίδιο δεν είναι παρά ένας αδιαίρετος κόκκος ύλης που κινείται πάνω σε μια καλά καθορισμένη τροχιά σύμφωνα με τους νόμους της νευτώνειας μηχανικής. Το κύριο χαρακτηριστικό τους είναι ότι είναι εντοπισμένα στο χώρο, δηλαδή μπορούμε με κάποια ακρίβεια να περιγράψουμε τις συντεταγμένες τους με 3 αριθμούς (στον τρισδιάστατο χώρο). Αντίθετα, ένα κύμα είναι μια εκτεταμένη φυσική διαταραχή που μπορεί κάλλιστα να διαιρεθεί και που διαδίδεται με κάποια ταχύτητα. Το πεδίο "απλώνεται" στο χώρο και για να το περιγράψουμε απαιτείται ένα ορισμένο πλήθος αριθμών (βαθμοί ελευθερίας)για κάθε σημείο του χώρου.

Από τα παραπάνω είναι κατανοητό ότι οι έννοιες σωματίδιο και κύμα είναι απολύτως ασυμβίβαστες και αμοιβαία αποκλειόμενες.

Η φύση όμως δεν ακολουθεί πάντα αυτό που σε μάς "φαίνεται" φυσιολογικό. Αρχικά αποδείχθηκε ότι το φως έχει και τις δύο ιδιότητες: είναι κύμα, αλλά και σωματίδιο (φωτόνιο, Planck 1900). Αργότερα με μία τολμηρή υπόθεση ο de Broglie απέδωσε κυματικές ιδιότητες στο ηλεκτρόνιο που περιστρέφεται γύρω από τον πυρήνα του υδρογόνου, με μήκος κύματος αντιστρόφως ανάλογο της ενέργειάς του.

Η ανάκριση της φύσης (πείραμα) έχει αποδείξει άπειρες φορές έκτοτε ότι αυτή η θεώρηση είναι σωστή. Τα σωματίδια έχουν και κυματικές ιδιότητες (παρουσιάζουν κυματική συμπεριφορά, για παράδειγμα συμβολή και περίθλαση) και τα κύματα έχουν και σωματιδιακές (συμπεριφέρονται σαν ρεύμα σωματιδίων, ιδίως κατά την εκπομπή και την απορρόφησή τους). Σε κάποια φαινόμενα εκδηλώνεται η κυματική φύση ενός σωματιδίου, ενώ σε κάποια άλλα εκδηλώνεται η σωματιδιακή του φύση. Η διαφορά με την κλασική θεώρηση του

κύματος, στην περίπτωση που ένα σωματίδιο εκδηλώνει την κυματική του φύση, είναι ότι δεν πρόκειται για υλικό κύμα αλλά για κύμα πιθανότητας.

Οι δύο φύσεις αυτές είναι συμπληρωματικές. Η μία δεν αναιρεί την άλλη.

ΕΝΟΤΗΤΑ 2

ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΚΡΥΠΤΟΓΡΑΦΙΑ

➢ ΓΕΝΙΚΑ

Η λέξη **κρυπτογραφία** προέρχεται από τα συνθετικά "κρυπτός" + "γράφω" και είναι ένας επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων.

Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με την 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 την λέξη "λόγος" και χωρίζεται σε δύο κλάδους: Την Κρυπτογραφία και την Κρυπτανάλυση με παρεμφερή κλάδο την Στεγανογραφία και αντίστοιχα την Στεγανοανάλυση.

Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες :

- *Εμπιστευτικότητα*: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία 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.

Το κβαντικό σύστημα κρυπτογραφίας είναι μια επέκταση της κβαντικής επικοινωνίας δεδομένου ότι στέλνει τα σωματίδια χρησιμοποιώντας την κβαντική τηλεμεταφορά. Τα σωματίδια κωδικοποιούνται σε κβαντικές καταστάσεις και στέλνονται στο δέκτη όπως στην κβαντική επικοινωνία. Οι καταστάσεις αντιπροσωπεύουν τις κωδικοποιημένες πληροφορίες που μπορούν να υποβληθούν σε επεξεργασία και να γίνουν κατανοητές μόνο από αυτόν που τις λαμβάνει στο τέλος. Εάν ένας άλλος παρατηρητής προσπαθήσει να

εξετάσει τις πληροφορίες που στέλνονται, πρέπει να ξέρει το σχέδιο κωδικοποίησης, επειδή η μετάδοση καταστρέφεται μόλις παρατηρηθεί.

➢ ΠΕΡΙΟΔΟΙ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

❖ Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. – 1900 μ.Χ.)

Κατά την διάρκεια αυτής της περιόδου αναπτύχθηκε μεγάλο πλήθος μεθόδων και αλγορίθμων κρυπτογράφησης, που βασίζονταν κυρίως σε απλές αντικαταστάσεις γραμμάτων. Όλες αυτές δεν απαιτούσαν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές, αλλά στηρίζονταν στην ευφυΐα και την ευρηματικότητα 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 μία μικρή σφηνοειδή επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη, οι πολιτισμοί που αναπτύχθηκαν στην Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη 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.

ΣΧΗΜΑ: Η Σπαρτιατική Σκυτάλη, μια πρώιμη συσκευή για την κρυπτογράφηση

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στην στεγανογραφία και όχι τόσο στην κρυπτογραφία. Οι Έλληνες συγγραφείς δεν αναφέρουν αν και πότε χρησιμοποιήθηκαν συστήματα γραπτής αντικατάστασης γραμμάτων, αλλά τα βρίσκουμε στους Ρωμαίους, κυρίως την εποχή του Ιουλίου 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. 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 ένα από τα πρώτα βιβλία κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και στους επόμενους αιώνες.

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. Στο γνωστό μυθιστόρημα «Χίλιες και μία νύχτες» κυριαρχούν οι λέξεις-αινίγματα, οι γρίφοι, τα λογοπαίγνια και οι αναγραμματισμοί. Έτσι, εμφανίστηκαν βιβλία που περιείχαν κρυπταλφάβητα, όπως το αλφάβητο «Dawoudi» που πήρε το όνομα του από τον βασιλιά Δαυίδ. Οι Άραβες είναι οι πρώτοι που επινόησαν αλλά και χρησιμοποίησαν μεθόδους κρυπτανάλυσης. Το κυριότερο εργαλείο στην κρυπτανάλυση, η χρησιμοποίηση των συχνοτήτων των γραμμάτων κειμένου, σε συνδυασμό με τις συχνότητες εμφάνισης στα κείμενα των γραμμάτων της γλώσσας, επινοήθηκε από αυτούς γύρω στον 14ο αιώνα.

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.

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 Αθανάσιος Κίρχερ 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 επιδαψιλεύσουν 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 σς ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και κυρίως ο Σαμπολιόν, μοιράστηκαν την δόξα της ερμηνείας τους.

Οι προϊστορικοί πληθυσμοί χρησιμοποίησαν τρεις γραφές μέχρι να επινοήσουν αλφάβητο, γύρω στο 850 π.Χ. Χρονολογικά, οι γραφές αυτές κατατάσσονται ως εξής

- 3000 1600 π.Χ. : Εικονογραφική (Ιερογλυφική) γραφή
- 1850 1450 π.Χ.: Γραμμική γραφή Α
- 1450 1200 π.Χ.: Γραμμική Γραφή Β

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 (Σχήμα 2.2), 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 χειροποίητα, αλλά έχουν χαραχθεί 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.

Σχήμα : Ο Δίσκος της Φαιστού

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. 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. 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. 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, που συνέβη την ίδια ακριβώς εποχή. Για αυτό και έγινε γνωστή σαν το «Έβερεστ της Ελληνικής αρχαιολογίας».

- **Δεύτερη Περίοδος Κρυπτογραφίας (1900 μ.Χ. – 1950 μ.Χ.)**

Η δεύτερη περίοδος της κρυπτογραφίας όπως προαναφέρθηκε τοποθετείται στις αρχές του 20ου αιώνα και φτάνει μέχρι το 1950. Καλύπτει, επομένως, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων (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. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma.

Εικόνα: Η μηχανή Αίνιγμα χρησιμοποιήθηκε ευρέως από την Γερμανία

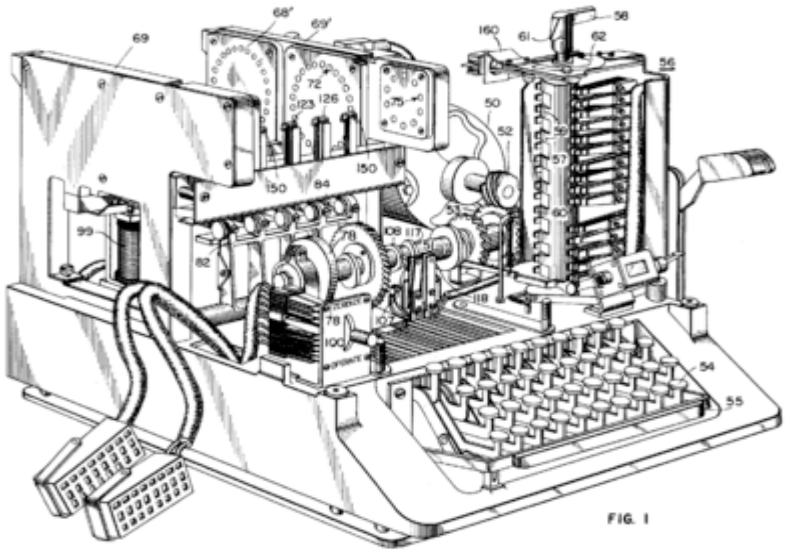
Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασιζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Ακόμη και ο Rejewski και οι μαθηματικοί και κρυπτογράφοι του Biuro Szyfrow, κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τούρινγκ (Alan Turing), τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Παρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με την βοήθεια και ενός υπολογιστή, που κατασκεύασαν οι Βρετανοί επιστήμονες, ο οποίος ονομάσθηκε Colossus και, δυστυχώς, καταστράφηκε με το τέλος του Πολέμου. Οι κρυπτογράφοι του αμερικανικού ναυτικού (σε συνεργασία με Βρετανούς και Ολλανδούς κρυπτογράφους μετά από το 1940) έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στην Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά αναπτυγμένο κρυπτογραφικό σύστημα, (που καλείται Purple), και χρησιμοποίησε, επίσης, διάφορες παρόμοιες μηχανές για τις συνδέσεις μερικών ιαπωνικών πρεσβειών. Μία από αυτές αποκλήθηκε "Μηχανή-Μ" από τις ΗΠΑ, ενώ μια άλλη αναφέρθηκε ως «Red» (Κόκκινη). Μια ομάδα του αμερικανικού στρατού, η αποκαλούμενη SIS, κατάφερε να σπάσει το ασφαλέστερο ιαπωνικό διπλωματικό σύστημα κρυπτογράφησης (μια ηλεκτρομηχανική συσκευή, η οποία αποκλήθηκε "Purple" από τους Αμερικανούς) πριν καν ακόμη αρχίσει ο Β΄ Παγκόσμιος Πόλεμος. Οι Αμερικανοί αναφέρονται στο αποτέλεσμα της κρυπτανάλυσης, ειδικότερα της μηχανής Purple, αποκαλώντας το ως Magic (Μαγεία).

Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA (Σχήμα 2.4). Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια

κρυπτομηχανών M-94. Οι Βρετανοί πράκτορες της Υπηρεσίας "SOE" χρησιμοποίησαν αρχικά ένα τύπο κρυπτογραφίας που βασιζόταν σε ποιήματα (τα απομνημονευμένα ποιήματα ήταν τα κλειδιά). Οι Γερμανοί, ώρες πριν την Απόβαση της Νορμανδίας συνέλαβαν ένα μήνυμα - ποίημα του Πολ Βερλέν, για το οποίο, χωρίς να το έχουν αποκρυπτογραφήσει, ήταν βέβαιοι πως προανάγγελε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτή την προειδοποίηση.

Οι Πολωνοί είχαν προετοιμαστεί για την εμπόλεμη περίοδο κατασκευάζοντας την κρυπτομηχανή LCD Lacida, η οποία κρατήθηκε μυστική ακόμη και από τον Rejewski. Όταν. τον Ιούλιο του 1941 ελέγχθηκε από τον Rejewski η ασφάλειά της, του χρειάστηκαν μερικές μόνον ώρες για να την "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, εντούτοις, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.



Σχήμα : Κρυπτό-μηχανή SIGABA

❖ Τρίτη Περίοδος Κρυπτογραφίας (1950 μ.Χ. - Σήμερα)

Αυτή η περίοδος 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. Το 1949 δημοσίευσε την εργασία «Θεωρία επικοινωνίας των συστημάτων μυστικότητας» (*Communication Theory of Secrecy Systems*) στο τεχνικό περιοδικό Bell System και λίγο αργότερα στο βιβλίο του, «Μαθηματική Θεωρία της Επικοινωνίας» (*Mathematical Theory of Communication*), μαζί με τον Warren Weaver. Αυτά, εκτός από

τις άλλες εργασίες του επάνω στην θεωρία δεδομένων και επικοινωνίας καθιέρωσε μια στερεά θεωρητική βάση για την κρυπτογραφία και την κρυπτανάλυση. Εκείνη την εποχή η κρυπτογραφία εξαφανίζεται και φυλάσσεται από τις μυστικές υπηρεσίες κυβερνητικών επικοινωνιών όπως η NSA. Πολύ λίγες εξελίξεις δημοσιοποιήθηκαν ξανά μέχρι τα μέσα της δεκαετίας του '70, όταν όλα άλλαξαν.

Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες (δηλ. μη-μυστικές) πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard) στον ομοσπονδιακό κατάλογο της Αμερικής στις 17 Μαρτίου 1975. Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου των Προτύπων (τώρα γνωστό ως NIST), σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις. Μετά από τις συμβουλές και την τροποποίηση από την NSA, αυτό το πρότυπο υιοθετήθηκε και δημοσιεύθηκε ως ένα ομοσπονδιακή τυποποιημένο πρότυπο επεξεργασίας πληροφοριών το 1977 (αυτήν την περίοδο αναφέρεται σαν FIPS 46-3). Ο DES ήταν ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης που εγκρίνεται από μια εθνική αντιπροσωπεία όπως η NSA. Η απελευθέρωση της προδιαγραφής της από την NBS υποκίνησε μια έκρηξη δημόσιου και ακαδημαϊκού ενδιαφέροντος για τα συστήματα κρυπτογραφίας.

Ο DES αντικαταστάθηκε επίσημα από τον AES το 2001 όταν ανήγγειλε ο NIST το FIPS 197. Μετά από έναν ανοικτό διαγωνισμό, ο NIST επέλεξε τον αλγόριθμο Rijndael, που υποβλήθηκε από δύο Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του όπως ο 3DES ή TDES χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένος σε πολλά εθνικά και οργανωτικά πρότυπα. Εντούτοις, το βασικό μέγεθος των 56-bit έχει αποδειχθεί ότι είναι ανεπαρκές να αντισταθεί στις επιθέσεις ωμής βίας (μια τέτοια επίθεση πέτυχε να σπάσει τον DES σε 56 ώρες ενώ το άρθρο που αναφέρεται ως το σπάσιμο του DES δημοσιεύτηκε από τον O'Reilly and Associates). Κατά συνέπεια, η χρήση απλής κρυπτογράφησης με τον DES είναι τώρα χωρίς την αμφιβολία επισφαλής για χρήση στα νέα σχέδια των κρυπτογραφικών συστημάτων και μηνύματα που προστατεύονται από τα παλαιότερα κρυπτογραφικά συστήματα που χρησιμοποιούν DES, και όλα τα μηνύματα που έχουν αποσταλεί από το 1976 με την χρήση DES, διατρέχουν επίσης σοβαρό κίνδυνο αποκρυπτογράφησης. Ανεξάρτητα από την έμφυτη ποιότητά του, το βασικό μέγεθος του DES (56-bit) ήταν πιθανά πάρα πολύ μικρό ακόμη και το 1976, πράγμα που είχε επισημάνει ο Whitfield Diffie. Υπήρξε επίσης η υποψία ότι κυβερνητικές οργανώσεις είχαν ακόμα και τότε ικανοποιητική υπολογιστική δύναμη ώστε να σπάσουν μηνύματα που είχαν κρυπτογραφηθεί με τον DES.

➢ 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 x_o 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)

ΛΕΞΙΚΟ ΟΡΩΝ

- **Αλγόριθμος κρυπτογράφησης.** Οποιαδήποτε γενική διαδικασία κρυπτογράφησης η οποία μπορεί να εξειδικευτεί με ακρίβεια μέσω της επιλογής ενός κλειδιού.
- **Αποκρυπτογραφώ.** Μετατρέπω ένα κρυπτογραφημένο μήνυμα στο αρχικό. Τυπικά ο όρος αναφέρεται μόνο στον παραλήπτη του μηνύματος, που γνωρίζει το κλειδί για να βρει το κανονικό κείμενο, άτυπα όμως αναφέρεται και στη διαδικασία της κρυπτανάλυσης, όπου η αποκρυπτογράφηση διενεργείται από έναν υποκλοπέα εχθρό.
- **Αποκωδικοποιώ.** Μετατρέπω ένα κωδικοποιημένο μήνυμα στο αρχικό.
- **ASCII** (American Standard Code for Information Interchange – Αμερικανικός Καθιερωμένος Κώδικας για την Ανταλλαγή Πληροφοριών). Επίσημα καθιερωμένο σύστημα μετατροπής αλφαβητικών και λοιπών χαρακτήρων σε αριθμούς.
- **DES** (Data Encryption Standard – Καθιερωμένο Σύστημα Κρυπτογράφησης Δεδομένων). Αναπτύχθηκε από την IBM και υιοθετήθηκε επίσημα το 1976.
- **Δημόσιο κλειδί.** Το κλειδί που χρησιμοποιεί ο αποστολέας για να κρυπτογραφεί μηνύματα σε ένα σύστημα δημόσιας κρυπτογραφίας. Το δημόσιο κλειδί είναι προσιτό στο κοινό.
- **Διανομή κλειδιών.** Η διαδικασία που διασφαλίζει ότι τόσο ο αποστολέας όσο και ο παραλήπτης έχουν πρόσβαση στο κλειδί το οποίο απαιτείται για την αποκρυπτογράφηση ενός μηνύματος, και ταυτόχρονα ότι το κλειδί δεν θα πέσει σε εχθρικά χέρια. Η διανομή κλειδιών αποτελούσε μείζον πρόβλημα λογιστικής και ασφάλειας πριν από την επινόηση της κρυπτογραφίας δημοσίου κλειδιού.
- **Ιδιωτικό κλειδί.** Το κλειδί που χρησιμοποιεί ο παραλήπτης για να αποκρυπτογραφήσει μηνύματα σε ένα σύστημα δημόσιας κρυπτογραφίας. Το ιδιωτικό κλειδί πρέπει να είναι μυστικό.
- **Κανονικό κείμενο.** Το αρχικό μήνυμα πριν από την κρυπτογράφηση.
- **Κβαντική κρυπτογραφία.** Μια άθραυστη μορφή κρυπτογραφίας που εκμεταλλεύεται την κβαντική θεωρία, και ιδιαίτερα την αρχή της απροσδιοριστίας – η οποία ορίζει ότι είναι αδύνατον να μετρήσουμε όλες τις πτυχές ενός αντικειμένου με απόλυτη βεβαιότητα. Η κβαντική κρυπτογραφία εγγυάται την ασφαλή ανταλλαγή μιας τυχαίας σειράς μπιτ (δυαδικών ψηφίων), η οποία στη συνέχεια χρησιμοποιείται ως βάση για ένα κρυπτόγραμμα του τύπου μπλοκ μιας χρήσης.

- **Κβαντικός υπολογιστής.** Ένας υπολογιστής τεράστιας ισχύος που εκμεταλλεύεται την κβαντική θεωρία, και ιδιαίτερα τη θεωρία ότι ένα αντικείμενο μπορεί να βρίσκεται ταυτόχρονα σε πολλές καταστάσεις (υπέρθεση), ή τη θεωρία ότι ένα αντικείμενο μπορεί να βρίσκεται ταυτόχρονα σε πολλά σύμπαντα. Αν ποτέ οι επιστήμονες κατορθώσουν να κατασκευάσουν έναν κβαντικό υπολογιστή σε οποιαδήποτε λογική κλίμακα, αυτός θα έθετε σε κίνδυνο την ασφάλεια όλων των σημερινών κρυπτογραμμάτων, με εξαίρεση το κρυπτόγραμμα του μπλοκ μιας χρήσης.
- **Κλειδί.** Το στοιχείο που μετατρέπει το γενικό αλγόριθμο της κρυπτογράφησης σε μια συγκεκριμένη μέθοδο κρυπτογράφησης. Γενικά, ο εχθρός μπορεί να γνωρίζει τον αλγόριθμο της κρυπτογράφησης τον οποίο χρησιμοποιούν αποστολέας και παραλήπτης, όμως δεν επιτρέπεται να γνωρίζει το κλειδί.
- **Κρυπανάλυση.** Η επιστήμη του να συναρμολογείς το κανονικό κείμενο από ένα κρυπτογραφημένο κείμενο χωρίς να γνωρίζεις το κλειδί.
- **Κρυπτόγραμμα.** Οποιοδήποτε γενικό σύστημα απόκρυψης του νοήματος ενός μηνύματος με τη μέθοδο της αντικατάστασης κάθε γράμματος του αρχικού μηνύματος με ένα άλλο γράμμα. Το σύστημα θα πρέπει να έχει κάποια εγγενή ευκαμψία, γνωστή ως κλειδί.
- **Κρυπτογραφία.** Η επιστήμη της κρυπτογράφησης ενός μηνύματος ή η επιστήμη της απόκρυψης του νοήματος ενός μηνύματος. Ενίοτε, ο όρος χρησιμοποιείται με γενικότερη έννοια, δηλώνοντας την επιστήμη που έχει ως αντικείμενο οτιδήποτε σχετίζεται με τα κρυπτογράμματα, οπότε αποτελεί συνώνυμο του όρου κρυπτολογία.
- **Κρυπτογραφία ασύμμετρου κλειδιού.** Μορφή κρυπτογραφίας όπου το κλειδί που απαιτείται για την κρυπτογράφηση δεν είναι το ίδιο με το κλειδί που απαιτείται για την αποκρυπτογράφηση. Περιγράφει τα συστήματα κρυπτογραφίας δημοσίου κλειδιού, όπως το RSA.
- **Κρυπτογραφία δημοσίου κλειδιού.** Σύστημα κρυπτογραφίας το οποίο ξεπερνά το πρόβλημα της διανομής κλειδιών. Η κρυπτογραφία δημοσίου κλειδιού απαιτεί ένα ασύμμετρο κρυπτόγραμμα, ώστε ο κάθε χρήστης να μπορεί να δημιουργεί ένα δημόσιο κλειδί κρυπτογράφησης και ένα ιδιωτικό κλειδί αποκρυπτογράφησης.
- **Κρυπτογραφία συμμετρικού κλειδιού.** Μορφή κρυπτογραφίας όπου το κλειδί που απαιτείται για την κρυπτογράφηση είναι το ίδιο με το κλειδί που απαιτείται για την αποκρυπτογράφηση. Ο όρος περιγράφει όλα τα παραδοσιακά συστήματα κρυπτογράφησης, δηλαδή εκείνα που χρησιμοποιούνται πριν από την δεκαετία του 1970.
- **Κρυπτογραφικό κείμενο.** Το μήνυμα ή κανονικό κείμενο μετά την κρυπτογράφηση.

- **Κρυπτογραφώ.** Μετατρέπω το αρχικό μήνυμα σε κρυπτογραφημένο.
- **Κρυπτολογία.** Η επιστήμη της μυστικής γραφής σε όλες τις μορφές της. Καλύπτει τόσο την κρυπτογραφία όσο και την κρυπτανάλυση
- **Κώδικας.** Σύστημα απόκρυψης του νοήματος ενός μηνύματος με τη μέθοδο της αντικατάστασης κάθε λέξης ή φράσης του αρχικού μηνύματος με έναν άλλο χαρακτήρα ή σειρά χαρακτήρων.
- **Κωδικοποιώ.** Μετατρέπω το αρχικό μήνυμα σε κωδικοποιημένο.
- **Μήκος κλειδιού.** Η κρυπτογράφηση μέσω υπολογιστή εμπεριέχει κλειδιά που είναι αριθμοί. Το μήκος κλειδιού αναφέρεται στον αριθμό των ψηφίων ή των μπιτ (δυαδικών ψηφίων) που περιλαμβάνει το κλειδί, και έτσι υποδεικνύει το μεγαλύτερο αριθμό που μπορεί να χρησιμοποιηθεί ως κλειδί, προσδιορίζοντας με αυτόν τον τρόπο τον αριθμό των πιθανών κλειδιών. Όσο μεγαλύτερο είναι το μήκος του κλειδιού (ή όσο μεγαλύτερος είναι ο αριθμός των πιθανών κλειδιών), τόσο περισσότερο χρόνο χρειάζονται οι κρυπταναλυτές για να ελέγξουν όλα τα κλειδιά.
- **Μπλοκ μιας χρήσης.** Η μόνη γνωστή μορφή κρυπτογράφησης που είναι άθραυστη. Βασίζεται σε ένα τυχαίο κλειδί που το μήκος του είναι ίσο με το μήκος του μηνύματος. Κάθε κλειδί μπορεί να χρησιμοποιηθεί μόνο μια φορά.
- **NSA** (National Security Agency – Εθνική Υπηρεσία Ασφάλειας). Κλάδος του Υπουργείου Αμύνης των ΗΠΑ, υπεύθυνος για την ασφάλεια των αμερικανικών επικοινωνιών και για την παρείσφρηση στις επικοινωνίες των άλλων χωρών.
- **PGP** (Pretty Good Privacy – Άριστη Προστασία Ιδιωτικού Απορρήτου). Αλγόριθμος κρυπτογράφησης μέσω υπολογιστή. Τον ανέπτυξε ο Φιλ Ζίμερμαν με βάση το σύστημα RSA.
- **RSA.** Το πρώτο σύστημα που ανταποκρίθηκε στις απαιτήσεις της κρυπτογραφίας δημοσίου κλειδιού. Το επινόησαν το 1977 οι Ρον Ρίβεστ, Άντι Σαμίρ και Λέοναρντ Άντλεμαν.
- **Σύστημα ανταλλαγής κλειδιών Ντίφι – Χέλμαν – Μέρκλε.** Διαδικασία μέσω της οποίας ένας αποστολέας και ένας παραλήπτης μπορούν να καθορίσουν ένα μυστικό κλειδί μέσω μιας δημόσιας συζήτησης. Από τη στιγμή που θα συμφωνηθεί το κλειδί, ο αποστολέας μπορεί να χρησιμοποιήσει ένα κρυπτόγραμμα όπως το DES για να κρυπτογραφήσει ένα μήνυμα.
- **Ψηφιακή υπογραφή.** Μέθοδος για την πιστοποίηση της ταυτότητας του συντάκτη ενός ηλεκτρονικού μηνύματος. Συχνά παράγεται από το/τη συγγραφέα που κρυπτογραφεί ένα μήνυμα με το ιδιωτικό κλειδί του/της.

ΚΩΔΙΚΕΣ ΚΑΙ ΜΥΣΤΙΚΑ

Στην διάρκεια του Δευτέρου Παγκοσμίου Πολέμου, οι βρετανοί κωδικοθραύστες είχαν το πάνω χέρι στη μάχη τους με τους γερμανούς κωδικοπλάστες, κυρίως επειδή οι γυναίκες και οι άντρες του Μπλίτσλεϊ Παρκ, 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 άλλην κωδικοθραυστική μηχανή, τον Κολοσσό, προκειμένου να αντιμετωπίσουν μια ακόμη πιο ισχυρή μορφή κρυπτογράφησης, το γερμανικό κρυπτόγραμμα Λόρεντς. Από τις δύο 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 κρυπτογράφηση 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 κρυπτοαναλυτές του Μπλίτσλεϊ. 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 Μπλίτσλεϊ 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 κρυπτοαναλυτές του Μπλίτσλεϊ ήταν αναγκασμένοι να σπάζουν με το χέρι τα μηνύματα που ήταν κρυπτογραφημένα με το κρυπτόγραμμα Λόρεντς, πράγμα που απαιτούσε επώδυνη προσπάθεια εβδομάδων, οπότε τα μηνύματα έπαβαν πια να είναι επίκαιρα. Τελικά, ο Μαξ Νιούμαν, ένας μαθηματικός του Μπλίτσλεϊ, βρήκε έναν 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 σε

διάφορα προβλήματα, αυτό που σήμερα αποκαλούμε «προγραμματιζόμενο υπολογιστή».

Η εφαρμογή του σχεδίου του Νιούμαν θεωρήθηκε ανέφικτη από τεχνική άποψη, και έτσι οι ανώτεροι αξιωματούχοι του Μπλίτσλεϊ 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 Μπλίτσλεϊ 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 δέκα μήνες κατασκεύασε τον Κολοσσό, τον οποίο παρέδωσε στο Μπλίτσλεϊ Παρκ 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 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 Μπλίτσλεϊ Παρκ, και όσοι δούλευαν με αυτόν δεν επιτρεπόταν να μιλήσουν για το θέμα. Ο Τόμι Φλάουερς, υπακούοντας στην διαταγή να καταστρέψει τα σχεδιαγράμματα του Κολοσσού, τα πήγε στο λεβητοστάσιο και τα έκαψε. Τα σχέδια για τον πρώτο υπολογιστή στον κόσμο χάθηκαν για πάντα. Η μυστικότητα αυτή είχε σαν αποτέλεσμα να κερδίσουν άλλοι την δόξα της επινόησης του υπολογιστή. Το 1945, οι Τζ. Πρέσπερ Έκερτ και Τζον Ου. Μόλτσι από το πανεπιστήμιο της Πενσιλβάνιας, ολοκλήρωσαν την κατασκευή του ENIAC (Electronic Numerical Integrator And Calculator - Ηλεκτρονικός Αριθμητικός Ολοκληρωτής και Υπολογιστής), που αποτελείτο από 18.000 ηλεκτρονικές λυχνίες και μπορούσε να εκτελεί 5.000 υπολογισμούς ανά δευτερόλεπτο. Επί δεκαετίες, μητέρα όλων των υπολογιστών θεωρείτο ο ENIAC, όχι ο Κολοσσός.

Αφού συνέβαλαν στην γέννηση του σύγχρονου υπολογιστή, οι κρυπτοαναλυτές, συνέχισαν και μετά τον πόλεμο να αναπτύσσουν και να χρησιμοποιούν την τεχνολογία των υπολογιστών και 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 και να δημιουργούν όλο και πιο περίπλοκα

κρυπτογράμματα. Με δυο λόγια, ο υπολογιστής έπαιξε καίριο ρόλο στην μεταπολεμική μάχη των κωδικοθραυστών με τους κωδικοπλάστες.

Η χρήση υπολογιστή για την κρυπτογράφηση ενός μηνύματος μοιάζει σε μεγάλο βαθμό με τις παραδοσιακές μορφές κρυπτογράφησης. Πράγματι, υπάρχουν μόνο τρεις 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» αντίστοιχο της με μορφή υπολογιστή θα παρήγαγε ένα κρυπτόγραμμα υψηλής ασφάλειας.

Η δεύτερη διαφορά είναι απλά θέμα ταχύτητας. Η ηλεκτρονική λειτουργεί πολύ πιο γρήγορα απ' ό,τι 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 επιτελεί 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 μπιτ (bit, από το binary digit). Συνεπώς, οποιοδήποτε μήνυμα θα πρέπει, πριν κρυπτογραφηθεί, να μετατραπεί σε δυαδικά ψηφία. Η μετατροπή αυτή μπορεί να γίνει σύμφωνα με διάφορα πρωτόκολλα, όπως το 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 (2^7) τρόποι διάταξης ενός συνδυασμού από 7 δυαδικά ψηφία, και επομένως ο ASCII μπορεί να προσδιορίσει έως και 128 χαρακτήρες. Αυτό παρέχει πλήρη ευχέρεια προσδιορισμού όλων των πεζών γραμμάτων (π.χ. a=1100001) , όλων των απαραίτητων σημείων στίξης (π.χ. !=0100001) καθώς και όλων των 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 ή και τα δύο. Κάθε κρυπτογράφηση, όσο πολύπλοκη και αν είναι, μπορεί να αναλυθεί σε συνδυασμούς των δύο αυτών απλών διαδικασιών.

Τα δύο παραδείγματα που ακολουθούν καταδεικνύουν την ουσιώδη απλότητα της κρυπτογράφησης με υπολογιστή, δείχνοντας πως ένας υπολογιστής μπορεί να εφαρμόσει ένα κρυπτόγραμμα υποκατάστασης και ένα απλό κρυπτόγραμμα μετάθεσης.

Κατ' αρχάς ας φανταστούμε 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:

ΚΑΝΟΝΙΚΟ ΚΕΙΜΕΝΟ: HELLO= 1001000 1000101 1001100 1001100 1001111

Μια 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, αφαιρέσαμε τα διαστήματα ανάμεσα στα τμήματα ASCII του αρχικού κανονικού κειμένου ώστε να δημιουργηθεί μια συνεχής σειρά, και στη συνέχεια, ακριβώς από κάτω, παραθέσαμε το προκύπτον κρυπτογραφικό κείμενο ώστε να γίνει η σύγκριση:

ΚΑΝΟΝΙΚΟ ΚΕΙΜΕΝΟ: 10010001000101100110010011001001111

ΚΡΥΠΤΟΓΡΑΦΙΚΟ ΚΕΙΜΕΝΟ: 01100010001010011001100011000110111

Μια ενδιαφέρουσα πτυχή της μετάθεσης στο επίπεδο των δυαδικών ψηφίων είναι ότι αυτή μπορεί να γίνει στο εσωτερικό του γράμματος. Επιπλέον, τμήματα ενός γράμματος μπορεί να αλλάξουν

αμοιβαία θέση με τμήματα του γειτονικού του. Για παράδειγμα, κατά την αντιμετάθεση του έβδομου αριθμού με τον όγδοο, το τελικό 0 του Η παίρνει τη θέση του 1 του Ε και τανάπαλιν. 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, ας φανταστούμε ότι θέλουμε να κρυπτογραφήσουμε το ίδιο μήνυμα, HELLO, τη φορά αυτή χρησιμοποιώντας μια απλή υπολογιστική μορφή ενός κρυπτογράμματος υποκατάστασης. Και πάλι αρχίζουμε μετατρέποντας το μήνυμα σε ASCII πριν την κρυπτογράφηση. 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 δυαδικών ψηφίων μπορεί να νοηθεί με βάση δύο 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.

ΜΗΝΥΜΑ: HELLO

ΜΗΝΥΜΑ ΣΕ ASCII : 10010001000101100110010011001001111

ΚΛΕΙΔΙ = DAVID : 10001001000001101011010010011000100

ΚΡΥΠΤΟΓΡΑΦΙΚΟ ΚΕΙΜΕΝΟ : 00011000000100001101000001010001011

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 τη 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

πολύ ευρύτερο κοινό. Το 1947, η εταιρία AT&T Bell Laboratories εφηύρε τον κρυσταλλικό πολλαπλασιαστή (τρανζίστορ), μια φτηνή εναλλακτική λύση αντί της ηλεκτρονικής λυχνίας. Η εμπορική χρήση των υπολογιστών έγινε πραγματικότητα το 1951, όταν εταιρίες σαν την Φεράντι άρχισαν να κατασκευάζουν υπολογιστές κατά παραγγελία. Το 1953 η IBM κυκλοφόρησε τον πρώτο της υπολογιστή και τέσσερα χρόνια αργότερα παρουσίασε την FORTRAN, μια προγραμματιστική γλώσσα που επέτρεπε στους συνηθισμένους ανθρώπους να γράφουν υπολογιστικά προγράμματα. Στη συνέχεια, το 1959, η εφεύρεση του ολοκληρωμένου κυκλώματος σήμαινε μια νέα εποχή στους υπολογιστές.

Στη διάρκεια της δεκαετίας του 1960, οι υπολογιστές έγιναν ισχυρότεροι, και ταυτόχρονα φθηνότεροι. Οι επιχειρήσεις είχαν όλο και πιο πολύ την δυνατότητα να τους παραγγέλνουν, και μπορούσαν να τους χρησιμοποιούν για να κρυπτογραφούν σημαντικές επικοινωνίες, όπως διαβιβάσεις χρημάτων ή λεπτές εμπορικές διαπραγματεύσεις. Ωστόσο, καθώς όλο και περισσότερες επιχειρήσεις αγόραζαν υπολογιστές και καθώς οι κρυπτογραφημένες επικοινωνίες ανάμεσα στις επιχειρήσεις εξαπλώνονταν, οι κρυπτογράφοι είχαν να αντιμετωπίσουν νέα προβλήματα, δυσκολίες που δεν υπήρχαν όταν η κρυπτογραφία ήταν αναγνωρισμένη ως αποκλειστικό δικαίωμα των κυβερνήσεων και των στρατιωτικών. Ένα από τα σημαντικότερα προβλήματα ήταν το ζήτημα της τυποποίησης. Μια εταιρεία, 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, στις 15 Μαΐου 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 (Lucifer) , προϊόν της IBM. Τον είχε αναπτύξει ο Χορστ Φάιστελ, ένας γερμανός μετανάστης που είχε έλθει στην Αμερική το 1934. Και ενώ επρόκειτο να αποκτήσει την Αμερικανική υπηκοότητα, η Αμερική μπήκε στον πόλεμο, με αποτέλεσμα ο Φάιστελ να τεθεί σε κατ' οίκον περιορισμό μέχρι το 1944. Τα πρώτα μεταπολεμικά χρόνια, κατέπνιξε το ενδιαφέρον του για την κρυπτογραφία για να μην εγείρει υποψίες εκ μέρους των αμερικανικών αρχών. Όταν τελικά άρχισε έρευνα πάνω στα κρυπτογράμματα, στο Ερευνητικό Κέντρο Κέμπριτζ

της Πολεμικής Αεροπορίας, παρενέβη στην εργασία του η NSA, η Εθνική Υπηρεσία Ασφάλειας 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 επί σειράν ετών να συνεχίσει την έρευνα του χωρίς παρενοχλήσεις. Εκεί, στις αρχές της δεκαετίας του 1970, ανέπτυξε το σύστημα Εωσφόρος.

Ο Εωσφόρος κρυπτογραφεί μηνύματα σύμφωνα με την ακόλουθη αναδιατακτική διαδικασία. Πρώτον, το μήνυμα μεταφράζεται σε μια 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 διασπώνται σε δύο υποομάδες των 32 ψηφίων, που χαρακτηρίζονται Αριστερή^0 και Δεξιά^0. Στη συνέχεια τα ψηφία στη Δεξιά^0 περνούν από μια «λειτουργία ανακατέματος», η οποία αλλάζει τα ψηφία σύμφωνα με μια πολύπλοκη υποκατάσταση. Κατόπιν η ανακατεμένη Δεξιά^0 προστίθεται στην Αριστερή^0, ώστε να δημιουργηθεί μια νέα υποομάδα από 32 ψηφία, η οποία χαρακτηρίζεται Δεξιά^1. Η αρχική Δεξιά^0 αλλάζει όνομα και γίνεται Αριστερή^1. Αυτή η σειρά ενεργειών αποκαλείται «γύρος». Η όλη διαδικασία επαναλαμβάνεται μέχρις ότου συμπληρωθούν 16 συνολικά γύροι. Η κρυπτογράφηση με αυτή τη μέθοδο μοιάζε λίγο με το ζύμωμα μιας φέτας λουκουμά. Φαντασθείτε μια μακριά φέτα λουκουμά με ένα μήνυμα κρυμμένο πάνω της. Πρώτον, χωρίζουμε τη μακριά φέτα σε δύο κομμάτια, που το καθένα τους έχει μήκος 64 εκατοστά. Στη συνέχεια παίρνουμε το μισό του ενός από τα δύο κομμάτια, το ζυμώνουμε, το διπλώνουμε, το προσθέτουμε στο άλλο μισό και το απλώνουμε ώστε να δημιουργηθεί ένα νέο κομμάτι. Η διαδικασία επαναλαμβάνεται ξανά και ξανά, έως ότου το μήνυμα ανακατευτεί καλά. Ύστερα από 16 γύρους ζυμώματος,

στέλνουμε το κρυπτογραφικό κείμενο, και ο παραλήπτης το αποκρυπτογραφεί αναστρέφοντας τη διαδικασία.

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 πιο 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 ένα 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 κρυπτογραφημένο κείμενο. Για την αποκρυπτογράφηση, ο παραλήπτης πρέπει να εισαγάγει τον ίδιο αριθμό – κλειδί και το κρυπτογραφικό κείμενο στον Εωσφόρο, ο οποίος στη συνέχεια παράγει το αρχικό μήνυμα.

Ο Εωσφόρος γενικά θεωρείτο ως ένα από τα ισχυρότερα κρυπτογραφικά προϊόντα που κυκλοφορούσαν στο εμπόριο, με αποτέλεσμα να τον χρησιμοποιούν πολλές και διάφορες οργανώσεις. Φαινόταν αναπόφευκτο ότι το συγκεκριμένο προϊόν θα υιοθετείτο ως το επίσημο αμερικανικό σύστημα κρυπτογράφησης, όμως για ακόμη μια φορά παρενέβη στο έργο του Φάιστελ η NSA. Ο Εωσφόρος ήταν τόσο ισχυρός, ώστε παρείχε την δυνατότητα υιοθέτησης μιας τυποποιημένης διαδικασίας κρυπτογράφησης η οποία πιθανότατα ξεπερνούσε τις κωδικοθραυστικές ικανότητες της NSA. Δεν είναι λοιπόν περίεργο που η NSA δεν ήθελε να δει να υιοθετείται ένα επίσημο κρυπτογραφικό σύστημα το οποίο η ίδια δεν μπορούσε να σπάσει. Λέγεται λοιπόν ότι η NSA άσκησε όλη την επιρροή της ώστε να εξασθενίσει μια πτυχή του Εωσφόρου, τον αριθμό των πιθανών κλειδιών, πριν επιτρέψουν την επίσημη υιοθέτηση του.

Ο αριθμός των πιθανών κλειδιών είναι ένας από τους κρίσιμους παράγοντες που καθορίζουν την ισχύ οποιουδήποτε κρυπτογράμματος. Ένας κρυπτοαναλυτής που προσπαθεί να αποκρυπτογραφήσει ένα κρυπτογραφημένο μήνυμα θα μπορούσε να επιχειρήσει να ελέγξει όλα τα πιθανά κλειδιά, και όσο περισσότερα είναι αυτά, τόσο πιο πολύ χρόνο θα χρειαστεί για να βρει το σωστό. Αν υπάρχουν μόνο 1.000.000 πιθανά κλειδιά, ο κρυπτοαναλυτής 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 σπάσει τα μηνύματα. Έτσι το κρυπτόγραμμα του Φάιστελ, ο Εωσφόρος, υιοθετήθηκε επισήμως στην εκδοχή του των 56 μπιτ στις 23 Νοεμβρίου 1976, και ονομάστηκε DES (Data Encryption Standard – Τυποποιημένο σύστημα Κρυπτογράφησης Δεδομένων). Ύστερα από ένα τέταρτο του αιώνα, το DES παραμένει το επίσημο σύστημα κρυπτογράφησης των ΗΠΑ.

Η υιοθέτηση του DES έλυσε το πρόβλημα της τυποποίησης, ενθαρρύνοντας τις επιχειρήσεις να χρησιμοποιούν την κρυπτογραφία για λόγους ασφάλειας. 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 το DES, επειδή ο αριθμός των πιθανών κλειδιών ήταν επαρκώς μεγάλος. Δυστυχώς, παρά την τυποποίηση και παρά την ισχύ του DES, οι επιχειρήσεις είχαν ακόμη να αντιμετωπίσουν ένα άλλο μεγάλο ζήτημα, το λεγόμενο πρόβλημα της «διανομής των κλειδιών».

Φαντασθείτε ότι μια τράπεζα θέλει να στείλει κάποια εμπιστευτικά δεδομένα σε έναν 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 αποκρυπτογραφήσει 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. Πώς πληροφορεί η τράπεζα τον πελάτη για το κλειδί; Δεν μπορεί να του το στείλει μέσω μιας 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 πιο 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 άνηκαν 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 κλειδιά, με αποτέλεσμα οι τράπεζες να διαπιστώσουν ότι η συγκεκριμένη διαδικασία διανομής είχε μετατραπεί σε φρικτό λογιστικό εφιάλτη, και το συνολικό κόστος της είχε γίνει απαγορευτικό.

Το πρόβλημα της διανομής των κλειδιών υπήρξε η μάστιγα των κρυπτογράφων σε όλη την ιστορία. Για παράδειγμα, στη διάρκεια του Δευτέρου Παγκοσμίου Πολέμου, η Γερμανική Ανώτατη Διοίκηση έπρεπε να διανέμει το μηνιαίο βιβλίο των ημερήσιων κλειδιών σε όλους τους χειριστές του Αινίγματος, πράγμα που αποτελούσε τεράστιο λογιστικό πρόβλημα. Επίσης, τα υποβρύχια, που συχνά έμεναν για μεγάλες περιόδους μακριά από τη βάση τους, έπρεπε με κάποιον τρόπο να εφοδιάζονται τακτικά με τα κλειδιά. Σε προηγούμενες εποχές, οι χρήστες του κρυπτογράμματος Βιζενέρ έπρεπε να βρίσκουν τρόπους μεταβίβασης της λέξης – κλειδιού από τον αποστολέα στον αποδέκτη. Όσο ασφαλές και να είναι ένα κρυπτόγραμμα στη θεωρία, στην πράξη μπορεί να υπονομευθεί από το πρόβλημα της διανομής των κλειδιών.

Η κυβέρνηση και οι στρατιωτικοί κατάφεραν, ως ένα βαθμό, να αντιμετωπίσουν το πρόβλημα, διαθέτοντας για την επίλυση του χρήματα και πόρους. Τα μηνύματα τους είναι τόσο σημαντικά, ώστε είναι διατεθειμένοι να κάνουν οτιδήποτε για να εγγυηθούν την ασφαλή διανομή των κλειδιών. Τα κλειδιά της κυβέρνησης των ΗΠΑ τα διαχειρίζεται και τα διανέμει η COMSEC (Communications Security – Ασφάλεια Επικοινωνιών). Στη δεκαετία του 1970, η COMSEC εισερχόταν στο λιμάνι, ανέβαιναν σε αυτά κρυπτοσυνοδοί, συνέλεγαν σωρούς από χαρτιά, ταινίες, δισκέτες ή οποιοδήποτε άλλο μέσον όπου ήταν αποθηκευμένα τα κλειδιά, και στη συνέχεια τα παρέδιδαν στους παραλήπτες τους.

Η διανομή κλειδιών μπορεί να φαίνεται ευτελές ζήτημα, όμως αναδείχθηκε σε κυρίαρχο πρόβλημα για τους κρυπτογράφους της μεταπολεμικής περιόδου. Αν δύο πλευρές ήθελαν να επικοινωνήσουν με ασφάλεια, έπρεπε να βασιστούν σε μια τρίτη πλευρά για την παράδοση του κλειδιού, και αυτό έγινε ο ασθενέστερος κρίκος στην αλυσίδα της ασφάλειας. Το δίλημμα για τις επιχειρήσεις ήταν ξεκάθαρο:

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 πανηγυρικά όλες τις αρνητικές προβλέψεις και βρήκε μια λαμπρή λύση στα μέσα της δεκαετίας του 1970, επινοώντας 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. Πράγματι, η επιτυχία αυτή θεωρείται ως το μεγαλύτερο κρυπτογραφικό επίτευγμα μετά την επινόηση του μονοαλφαβητικού κρυπτογράμματος πριν από δύο χιλιάδες και πλέον χρόνια.

➢ Ο ΘΕΟΣ ΑΝΤΑΜΕΙΒΕΙ ΤΟΥΣ ΤΡΕΛΟΥΣ

Ο Ουίτφιλντ Ντίφι είναι ένας από τους πιο λαμπρούς κρυπτογράφους της γενιάς του. Και μόνο η εξωτερική του εμφάνιση εκπέμπει μια εντυπωσιακή και κάπως αντιφατική εικόνα. Το άψογο κουστούμι του αντικατοπτρίζει το γεγονός ότι κατά το μεγαλύτερο μέρος της δεκαετίας του 1990 υπήρξε στέλεχος μιας από τις μεγαλύτερες αμερικανικές εταιρίες υπολογιστών – σήμερα η επίσημη εργασία του είναι Διακεκριμένος Μηχανικός στη Sun Microsystems. Ωστόσο, τα μακριά ως τους ώμους μαλλιά του και η λευκή γενειάδα μαρτυρούν ότι η καρδιά του βρισκόταν ακόμη στη δεκαετία του 1960. Τον περισσότερο χρόνο του τον περνάει μπροστά στην οθόνη ενός υπολογιστή, όμως δείχνει ότι θα μπορούσε να νιώθει το ίδιο άνετα σε ένα ινδουιστικό μοναστήρι στην Βομβάη. Ο Ντίφι έχει επίγνωση ότι η αμφίεση και η προσωπικότητα του εντυπωσιάζουν, και το σχολιάζει ως εξής: «ο κόσμος πάντα νομίζει ότι είμαι ψηλότερος από ό,τι στην πραγματικότητα, και όπως μου λένε πρόκειται για το φαινόμενο Τίγκερ».

Ο Ντίφι γεννήθηκε το 1944 και πέρασε τα πρώτα χρόνια του κυρίως στο Κουίνς της Νέας Υόρκης. Παιδί ακόμη τον συνάρπαζαν τα μαθηματικά, και διάβαζε όποιο βιβλίο έπεφτα στα χέρια του, από το Εγχειρίδιο μαθηματικών πινάκων της εταιρίας Χημικών ελαστικών ως τα Μαθήματα καθαρών μαθηματικών του Τζ. Χ. Χάρντι. Σπούδασε

μαθηματικά στο Τεχνολογικό Ινστιτούτο της Μασαχουσέτης, από όπου και αποφοίτησε το 1965. Στη συνέχεια ανέλαβε μια σειρά από εργασίες σχετικές με την ασφάλεια των υπολογιστών, και ως τις αρχές της δεκαετίας του 1970 είχε εξελιχθεί σε έναν από τους ελάχιστους πραγματικά ανεξάρτητους ειδικούς σε αυτόν τον τομέα, ένας ελεύθερος στοχαστής της κρυπτογραφίας, που δεν δούλευε ούτε για την κυβέρνηση ούτε για καμιά από τις μεγάλες εταιρίες.

Ο Ντίφι ενδιαφερόταν ιδιαίτερα για το πρόβλημα της διανομής κλειδιών, και συνειδητοποίησε ότι όποιος κατόρθωνε να το λύσει, θα έμενε στην ιστορία σαν ένας από τους μεγαλύτερους κρυπτογράφους όλων των εποχών. Τόσο πολύ τον είχε συναρπάσει το πρόβλημα αυτό, που αποτέλεσε το σημαντικότερο λήμμα στο ειδικό του βιβλίο σημειώσεων με τον τίτλο «Προβλήματα για μια φιλόδοξη θεωρία της κρυπτογραφίας». Το ενδιαφέρον του Ντίφι προερχόταν εν μέρει από το όραμα του για έναν καλωδιωμένο κόσμο. Ήδη από τη δεκαετία του 1960, το Υπουργείο Άμυνας των ΗΠΑ είχε αρχίσει να χρηματοδοτεί μια πρωτοποριακή ερευνητική οργάνωση με την επωνυμία ARPA (Advanced Research Projects Agency – Γραφείο Προωθημένων Ερευνητικών Προγραμμάτων), της οποίας ένα από τα σημαντικότερα σχέδια ήταν το να βρει έναν 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 άλλο υπολογιστή του δικτύου. Ο κύριος στόχος 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 (INTERNET). 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. Σήμερα, πάνω από εκατό εκατομμύρια άνθρωποι χρησιμοποιούν το Διαδίκτυο για να ανταλλάσουν πληροφορίες και να στέλνουν με το ηλεκτρονικό ταχυδρομείο (e- mail).

Ενώ το ARPANet βρισκόταν ακόμη στα σπάργανα, ο Ντίφι διέθετε αρκετή διορατικότητα ώστε να προβλέψει την έλευση της πληροφορικής υπερλεωφόρου και την ψηφιακή επανάσταση. Κάποια μέρα οι κοινοί άνθρωποι θα διέθεταν τους προσωπικούς τους υπολογιστές, οι οποίοι θα συνδέονταν μεταξύ τους μέσω τηλεφωνικών

γραμμών. Ο Ντίφι πίστευε ότι αν στο μέλλον οι άνθρωποι χρησιμοποιούσαν τους υπολογιστές τους για να ανταλλάσουν ηλεκτρονικά μηνύματα, τότε είχαν το δικαίωμα να κρυπτογραφούν τα μηνύματα τους ώστε να διασφαλίζεται το απόρρητο της ιδιωτικής 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 συναντιώνται μέσω του Διαδικτύου, και διερωτήθηκε πως θα μπορούσαν να ανταλλάσουν κρυπτογραφημένα μηνύματα. Επίσης προβληματίστηκε πάνω στο σενάριο όπου κάποιος θέλει να αγοράσει μέσω του Διαδικτύου ένα προϊόν. Πως 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 δύο περιπτώσεις οι δύο πλευρές έπρεπε προφανώς να διαθέτουν ένα κοινό κλειδί, όμως πως θα μπορούσαν να ανταλλάσουν κλειδιά με ασφάλεια; Ο αριθμός των προσωπικών επαφών και των ηλεκτρονικών μηνυμάτων ανάμεσα στο κοινό θα ήταν τεράστιος, και άρα η διανομή κλειδιών θα ήταν ανεφάρμοστη. Ο Ντίφι φοβόταν ότι η ανάγκη για διανομή κλειδιών θα απέκλειε το ευρύ κοινό από την πρόσβαση στην ψηφιακή ασφάλεια, και του έγινε έμμονη ιδέα να βρει μια λύση για το πρόβλημα.

Το 1974 ο Ντίφι, που ακόμη ήταν περιπλανώμενος κρυπτογράφος, επισκέφτηκε το Εργαστήριο Τόμας Τζ. Ουότσον της IBM, όπου είχε προσκληθεί να δώσει μια διάλεξη. Μίλησε για τις διάφορες στρατηγικές επίθεσης στο πρόβλημα της διανομής κλειδιών, όμως όλες του οι ιδέες ήταν πολύ πειραματικές, και το ακροατήριο εξέφρασε τον σκεπτικισμό του για τις προοπτικές εξεύρεσης λύσης. Η μόνη θετική απάντηση στην παρουσίαση του Ντίφι ήλθε από τον Άλαν Κονχάιμ, έναν από τους πιο έμπειρους κρυπτογράφους της IBM, που ανέφερε ότι κάποιος άλλος είχε πρόσφατα επισκεφτεί το Εργαστήριο και είχε δώσει μια διάλεξη με το ίδιο θέμα. Επρόκειτο για τον Μάρτιν Χέλμαν, καθηγητή στο πανεπιστήμιο Στάνφορντ της Καλιφόρνιας. Το ίδιο απόγευμα, ο Ντίφι πήρε το αυτοκίνητο του και ξεκίνησε το ταξίδι των 5.000 χιλιομέτρων προς τη Δυτική Ακτή, για να συναντήσει το μοναδικό άτομο που έμοιαζε να μοιράζεται την εμμονή του. Η συμμαχία των Ντίφι και Χέλμαν έμελλε να εξελιχτεί σε μια από τις δυναμικότερες συνεργασίες στον τομές της κρυπτογραφίας.

Ο Μάρτιν Χέλμαν γεννήθηκε το 1945 σε μια εβραϊκή γειτονιά του Μπρονξ, αλλά όταν ήταν τεσσάρων ετών η οικογένεια του μετακόμισε σε μια συνοικία όπου επικρατούσαν οι καθολικοί Ιρλανδοί. Όπως λέει ο ίδιος, η μετακίνηση αυτή άλλαξε για πάντα τη στάση του απέναντι στη ζωή και υιοθέτησε μια στάση αυτοάμυνας του τύπου «ποιος θέλει να είναι σαν τους άλλους;». ο Χέλμαν αποδίδει το ενδιαφέρον του για τα κρυπτογράμματα στην επίμονη επιθυμία του να είναι διαφορετικός. Οι συνάδελφοι του τον έλεγαν τρελό που ήθελε να κάνει έρευνα στην κρυπτογραφία, επειδή θα ανταγωνιζόταν την NSA και τον προϋπολογισμό της των δισεκατομμυρίων δολαρίων. Πως μπορούσε να ελπίζει ότι θα ανακάλυπτε κάτι που εκείνοι δεν το γνώριζαν ήδη; Αλλά και να έβρισκε κάτι τέτοιο, η NSA θα το χαρακτήριζε άκρως απόρρητο.

Ακριβώς την αποχή που αρχίζει την έρευνα του ο Χέλμαν, έπεσε στα χέρια του και το βιβλίο του ιστορικού Ντέιβιντ Καν με τίτλο «οι Κωδικοθραύστες». Το βιβλίο αυτό ήταν η πρώτη λεπτομερής παρουσίαση της εξέλιξης των κρυπτογραμμάτων, και σαν τέτοιο αποτελούσε την ιδανική εισαγωγή για έναν εκκολαπτόμενο κρυπτογράφο. Οι Κωδικοθραύστες ήταν ο μοναδικός σύντροφος του Χέλμαν στην έρευνα του, μέχρι το Σεπτέμβριο του 1974, όταν δέχτηκε ένα απροσδόκητο τηλεφώνημα από τον Ουίτφιλντ Ντίφι, ο οποίος είχε διασχίσει την Αμερική για να τον βρει. Ο Χέλμαν δεν είχε ακούσει ποτέ για τον Ντίφι, αλλά συμφώνησε απρόθυμα να τον συναντήσει για μισή ώρα το ίδιο απόγευμα. Στο τέλος της συνομιλίας τους, ο Χέλμαν είχε αντιληφθεί ότι ο Ντίφι ήταν το καλύτερα ενημερωμένο άτομο που είχε ποτέ συναντήσει. Το αίσθημα ήταν αμοιβαίο.

Καθώς ο Χέλμαν δεν διέθετε μεγάλη χρηματοδότηση, δεν μπορούσε να προσλάβει το νέο του συνεργάτη ως ερευνητή. Έτσι ο Ντίφι γράφτηκε στο πανεπιστήμιο σαν μεταπτυχιακός φοιτητής. Μαζί οι Χέλμαν και Ντίφι άρχισαν να μελετούν το πρόβλημα της διανομής κλειδιών, προσπαθώντας απελπισμένα να βρουν λύση στο κοπιώδες έργο της μεταφοράς τους σε φυσικά πρόσωπα διαμέσου τεραστίων αποστάσεων. Στην πορεία προσχώρησε στην ομάδα τους και ο Ραλφ Μέρκλε. Ο Μέρκλε ήταν ένας πρόσφυγας της διανόησης αφού είχε μεταναστεύσει από μια άλλη ερευνητική ομάδα, όπου ο καθηγητής δεν συμπαθούσε καθόλου τα απραγματοποίητο όνειρο της επίλυσης του προβλήματος που αφορούσε στη διανομή κλειδιών.

Το όλο πρόβλημα της διανομής των κλειδιών είναι μια κλασική περίπτωση φαύλου κύκλου. Αν δύο άτομα θέλουν να ανταλλάξουν ένα μυστικό μήνυμα από το τηλέφωνο, ο αποστολέας θα πρέπει να το κρυπτογραφήσει. Για να κρυπτογραφήσει το μυστικό μήνυμα, ο

αποστολέας θα πρέπει να χρησιμοποιήσει ένα κλειδί, που είναι μυστικό το ίδιο, οπότε υπάρχει το πρόβλημα της διαβίβασης του μυστικού κλειδιού στον αποδέκτη, ώστε να μεταδοθεί το μυστικό μήνυμα. Με δυο λόγια, προτού δύο άτομα ανταλλάξουν ένα μυστικό, θα πρέπει ήδη να μοιράζονται ένα μυστικό (κλειδί).

Για να συλλάβουμε καλύτερα το πρόβλημα της διανομής των κλειδιών, 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 Μπομπ 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 συναντιώνται η Αλίκη και ο Μπομπ μια φορά την εβδομάδα και να ανταλλάσουν όσα κλειδιά χρειάζονται για να καλύψουν όλα τα μηνύματα που θα στέλνουν ο ένας στον άλλο τις επόμενες επτά ημέρες. Το να ανταλλάσουν τα κλειδιά αυτοπροσώπως είναι οπωσδήποτε ασφαλές, αλλά άβολο, και αν ο ένας από τους δύο 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 δύο περιπτώσεις, η ανταλλαγή κλειδιών είναι αναπόφευκτη. Επί δύο χιλιάδες χρόνια, αυτό θεωρείτο ως αξίωμα της κρυπτογραφίας – μια αδιαμφισβήτητη αλήθεια. Υπάρχει, ωστόσο, ένα θεωρητικό πείραμα που μοιάζει να αντικρούει το αξίωμα αυτό.

Φανταστείτε ότι η Αλίκη και ο Μπομπ ζουν σε μια χώρα όπου το ταχυδρομικό σύστημα είναι εντελώς διεφθαρμένο, και οι ταχυδρομικοί υπάλληλοι διαβάζουν όλη τη μη προστατευμένη αλληλογραφία. Μια μέρα η Αλίκη θέλει να στείλει ένα άκρως προσωπικό μήνυμα στον Μπομπ. Το τοποθετεί σε ένα σιδερένιο κουτί, το οποίο κλείνει και ασφαλίζει με λουκέτο και κλειδί. Όταν όμως το κουτί φτάσει στον Μπομπ, εκείνος δεν μπορεί να το ανοίξει, επειδή δεν έχει το κλειδί. Η Αλίκη μπορεί να σκεφτεί να βάλει το κλειδί σε ένα άλλο κουτί, να το κλειδώσει και να το στείλει στον Μπομπ, όμως χωρίς το κλειδί του δεύτερου λουκέτου εκείνος δεν μπορεί να ανοίξει το δεύτερο κουτί, και άρα δεν μπορεί να πάρει το κλειδί που ανοίγει το πρώτο κουτί. Ο μόνος τρόπος αντιμετώπισης του προβλήματος είναι να βγάλει η Αλίκη ένα αντίγραφο του κλειδιού της και να το δώσει στον Μπομπ όταν

συναντηθούν για καφέ. Μέχρι εδώ απλώς εξέθεσα το πρόβλημα με ένα νέο σενάριο. Η αποφυγή της διανομής κλειδιών, μοιάζει λογικά αδύνατη – σίγουρα η Αλίκη, αν θέλει να κλειδώσει κάτι σε ένα κουτί ώστε μόνο ο Μπομπ να μπορεί να το ανοίξει, θα πρέπει να του δώσει αντίγραφο του κλειδιού. Ή, με κρυπτογραφικούς όρους, αν η Αλίκη θέλει να κρυπτογραφήσει ένα μήνυμα έτσι ώστε μόνο ο Μπομπ να μπορεί να το αποκρυπτογραφήσει, θα πρέπει να δώσει αντίγραφο του κλειδιού. Η ανταλλαγή των κλειδιών αποτελεί αναπόφευκτα μέρος της κρυπτογράφησης – ή μήπως όχι;

Τώρα ας φανταστούμε το εξής σενάριο. Όπως και πριν, η Αλίκη θέλει να στείλει ένα άκρως προσωπικό μήνυμα στον Μπομπ. Και πάλι τοποθετεί το μυστικό της μήνυμα σε ένα σιδερένιο κουτί, το κλειδώνει και το στέλνει στον Μπομπ. Όταν εκείνος 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 δύο λουκέτα. Αφαιρεί το δικό της λουκέτο, και αφήνει μόνο το λουκέτο του Μπομπ να ασφαλίζει το κουτί. Τέλος, ξαναστέλνει το κουτί πίσω στον Μπομπ. Και εδώ βρίσκεται η κρίσιμη διαφορά: τώρα ο Μπομπ μπορεί να ανοίξει το κουτί, επειδή είναι ασφαλισμένο με το δικό του λουκέτο, για το οποίο μόνο αυτός έχει κλειδί.

Οι συνέπειες αυτής της μικρής ιστορίας είναι τεράστιες. Αποδεικνύει ότι ένα μυστικό μήνυμα μπορεί να ανταλλαγεί με ασφάλεια μεταξύ δύο 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 ιστορία με κρυπτογραφικούς όρους. Η Αλίκη χρησιμοποιεί το κλειδί της για να κρυπτογραφήσει ένα μήνυμα προς τον Μπομπ, ο οποίος το κρυπτογραφεί ξανά με το 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 κλειδιών φαίνεται να έχει λυθεί, εφόσον το σύστημα της διπλής κρυπτογράφησης δεν απαιτεί ανταλλαγή κλειδιών. Υπάρχει ωστόσο ένα σοβαρό εμπόδιο στην εφαρμογή ενός συστήματος όπου η Αλίκη κρυπτογραφεί, ο Μπομπ κρυπτογραφεί, η Αλίκη αποκρυπτογραφεί και ο Μπομπ αποκρυπτογραφεί. 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 πρέπει να αποκρυπτογραφηθεί πρώτο, όμως ήταν η Αλίκη εκείνη που αφαίρεσε πρώτη την κρυπτογράφηση της, πριν ο Μπομπ αφαιρέσει τη δική του. Η σημασία της σειράς γίνεται ευκολότερα αντιληπτή αν εξετάσουμε κάτι που κάνουμε κάθε μέρα. Το πρωί φοράμε τις κάλτσες μας και στη συνέχεια τα παπούτσια μας, και το βράδυ βγάζουμε πρώτα τα παπούτσια και μετά τις κάλτσες – είναι αδύνατον το αντίθετο. Είμαστε υποχρεωμένοι να ακολουθούμε το πρόσταγμα «τελευταίο προστιθέμενο, πρώτο αφαιρούμενο».

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 υπακούει στον κανόνα «τελευταίο προστιθέμενο, πρώτο αφαιρούμενο». 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 της Αλίκης. Η σειρά είναι θεμελιώδης ακόμη 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 η σωστή. Η Αλίκη χρησιμοποιεί το κλειδί της για να κρυπτογραφήσει ένα μήνυμα προς τον Μπομπ, και στη συνέχεια ο Μπομπ κρυπτογραφεί εκ νέου το αποτέλεσμα χρησιμοποιώντας το δικό του κλειδί. Κατόπιν η Αλίκη χρησιμοποιεί το κλειδί της για να διενεργήσει μια μερική αποκρυπτογράφηση, και τέλος ο Μπομπ επιχειρεί να χρησιμοποιήσει το δικό του κλειδί για να ολοκληρώσει την αποκρυπτογράφηση.

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 m e a t n o o n*

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, μπορούμε να διαπιστώσουμε, αν η σειρά της αποκρυπτογράφησης αντιστραφεί, και ο Μπομπ αποκρυπτογραφήσει πριν από την Αλίκη, υπακούοντας στον κανόνα «τελευταίο προστιθέμενο, πρώτο αφαιρούμενο», το αποτέλεσμα θα είναι το αρχικό μήνυμα. Αν όμως η σειρά είναι τόσο σημαντική, για ποιο λόγο το σύστημα με τα λουκέτα μοιάζει να λειτουργεί στην ιστορία με τα κλειδωμένα κουτιά; Η απάντηση είναι ότι η σειρά δεν έχει σημασία στα λουκέτα. Μπορώ να βάλω είκοσι λουκέτα σε ένα κουτί και να τα ξεκλειδώσω με οποιαδήποτε σειρά, και στο τέλος το κουτί θα ανοίξει. Δυστυχώς, τα συστήματα κρυπτογράφησης είναι πολύ πιο ευαίσθητα από τα λουκέτα στο θέμα της σειράς.

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 του προβλήματος σχετικά με τη διανομή κλειδιών. Πέρασαν μήνες και μήνες προσπαθώντας να βρουν μια λύση. Όλες τους οι ιδέες κατέληγαν σε πλήρη αποτυχία, όμως εκείνοι φέρονταν σαν τέλειοι τρελοί και επέμεναν. Η έρευνα τους επικεντρώθηκε στην εξέταση διαφόρων μαθηματικών συναρτήσεων. Συνάρτηση είναι οποιαδήποτε μαθηματική πράξη μετατρέπει έναν αριθμό σε άλλο. Για παράδειγμα, ο πολλαπλασιασμός είναι μια μορφή συνάρτησης, επειδή μετατρέπει τον αριθμό 3 σε 6 ή το 9 σε 18. Επιπλέον, μπορούμε να θεωρήσουμε όλες τις μορφές κρυπτογράφησης μέσω υπολογιστή ως συναρτήσεις, εφόσον μετατρέπουμε έναν αριθμό (το κανονικό κείμενο) σε έναν άλλο αριθμό (κρυπτογραφικό κείμενο).

Οι περισσότερες μαθηματικές συναρτήσεις χαρακτηρίζονται ως αμφιμονοσήμαντες, επειδή εύκολα εκτελούνται και εύκολα αντιστρέφονται. Για παράδειγμα, ο διπλασιασμός είναι μια αμφιμονοσήμαντη συνάρτηση, επειδή είναι εύκολο να διπλασιάσουμε έναν αριθμό για να παράγουμε έναν καινούριο, και εξίσου εύκολο να αντιστρέψουμε τη συνάρτηση και από το διπλασιασμένο αριθμό να

πάρουμε πάλι τον αρχικό. Ο ευκολότερος τρόπος για να κατανοήσουμε την ιδέα της αμφιμονοσήμαντης συνάρτησης είναι να την παρομοιάσουμε με μια καθημερινή δραστηριότητα. Όταν ανάβουμε το φως με τον διακόπτη, η πράξη αυτή είναι μια συνάρτηση, επειδή μετατρέπει έναν κοινό ηλεκτρικό λαμπτήρα σε ένα αναμμένο ηλεκτρικό λαμπτήρα. Η συνάρτηση αυτή είναι αμφιμονοσήμαντη επειδή αν ανάψουμε έναν διακόπτη, είναι εύκολο να τον σβήσουμε και να επαναφέρουμε τον λαμπτήρα στην αρχική του κατάσταση.

Ωστόσο, ο Ντίφι και Χέλμαν δεν ενδιαφέρονταν για τις αμφιμονοσήμαντες συναρτήσεις. Επικέντρωσαν την προσοχή τους στις μονοσήμαντες. Όπως αποδεικνύει η ίδια η λέξη, μια μονοσήμαντη συνάρτηση εύκολα εκτελείται, αλλά πολύ δύσκολα ακυρώνεται. Με άλλα λόγια, οι αμφιμονοσήμαντες συναρτήσεις είναι αντιστρέψιμες, ενώ οι μονοσήμαντες όχι. Και εδώ ο καλύτερος τρόπος για να επεξηγήσουμε μια μονοσήμαντη συνάρτηση είναι να την περιγράψουμε με όρους μιας καθημερινής δραστηριότητας. Η πράξη της ανάμειξης κίτρινης και μπλε βαφής ώστε να προκύψει πράσινη είναι μια μονοσήμαντη συνάρτηση, επειδή είναι εύκολο να ανακατέψει κανείς την μπογιά, αλλά αδύνατον να διαχωρίσει το μείγμα. Μια άλλη μονοσήμαντη συνάρτηση είναι το σπάσιμο του αβγού, επειδή είναι εύκολο να σπάσει κανείς ένα αβγό, αλλά αδύνατον να το επαναφέρει κατόπιν στην αρχική του κατάσταση. Για το λόγο αυτό οι μονοσήμαντες συναρτήσεις μερικές φορές αποκαλούνται συναρτήσεις του Ζημιάρη.

Η **μοδιακή αριθμητική** (modular arithmetic), που στα σχολεία ενίοτε την αποκαλούν και ωρολογιακή αριθμητική, είναι ένας τομέας των μαθηματικών πλούσιος σε μονοσήμαντες συναρτήσεις. Στη μοδιακή αριθμητική, οι μαθηματικοί εξετάζουν μια πεπερασμένη ομάδα αριθμών με κυκλική διάταξη, όπως οι αριθμοί σε ένα ρολόι. Για παράδειγμα έχουμε ένα ρολόι που παριστά το μοδιακό 7 (modulo 7 ή πρότυπο 7), έχει δηλαδή 7 αριθμούς από το 0 ως το 6. Για να βρούμε το άθροισμα 2+3,αρχίζουμε από το δύο, προχωράμε 3 θέσεις και βρίσκουμε το 5, που είναι η ίδια απάντηση όπως και στην κανονική αριθμητική. Για να βρούμε το άθροισμα 2+6, αρχίζουμε πάλι από το 2 και προχωράμε 6 θέσεις, όμως αυτή τη φορά περνάμε από την αρχή του κύκλου και φτάνουμε στο 1, αποτέλεσμα διαφορετικό από αυτό που θα είχαμε στα κανονικά μαθηματικά. Τα αποτελέσματα αυτά γράφονται ως εξής:

2+3 = 5 (modulo 7) και 2+6 = 1 (modulo 7)

Η μοδιακή αριθμητική είναι σχετικά απλή, και στην πραγματικότητα την εφαρμόζουμε κάθε μέρα, όταν μιλάμε για την ώρα.

Αν τώρα είναι 9 το πρωί και έχουμε μια συνάντηση σε 8 ώρες, λέμε ότι η συνάντηση είναι στις 5 και όχι στις 17. Νοερά υπολογίσαμε 9+8 κατά μέτρο 12. Γράφουμε:

9+8 = 5 (modulo 12)

Συνήθως οι μαθηματικοί, αντί να φαντάζονται ρολόγια, εκτελούν μοδιακούς υπολογισμούς σύμφωνα με την ακόλουθη συνταγή. Πρώτον, εκτελούν τον υπολογισμό στην κανονική αριθμητική. Δεύτερον, για να βρούμε την απάντηση στη (modulo χ), διαιρούμε την κανονική απάντηση δια του χ και σημειώνουμε το υπόλοιπο. Το υπόλοιπο αυτό είναι η απάντηση στη (modulo χ). Παράδειγμα : για να βρούμε το αποτέλεσμα της πράξης 11*9 (modulo 13) κάνουμε τα εξής:

11*9=99

99/13=7, υπόλοιπο 8

11*9=8 (modulo 13)

Οι συναρτήσεις που εκτελούνται στο περιβάλλον της μοδιακής αριθμητικής τείνουν να συμπεριφέρονται ακανόνιστα, πράγμα που με τη σειρά του τις καθιστά μονοσήμαντες. Αυτό γίνεται φανερό όταν συγκρίνουμε μια απλή συνάρτηση στην κανονική αριθμητική με το αντίστοιχο στη μοδιακή. Στην πρώτη περίπτωση, η συνάρτηση είναι αμφιμονοσήμαντη και εύκολα αντιστρέψιμη, ενώ στην δεύτερη είναι μονοσήμαντη και αντιστρέφεται εύκολα. Ας πάρουμε σαν παράδειγμα τη συνάρτηση 3^x. Αυτό σημαίνει ότι παίρνουμε ένα αριθμό χ και πολλαπλασιάζουμε το 3 με τον εαυτό του χ φορές ώστε να προκύψει ο νέος αριθμός. Για παράδειγμα, αν χ=2, εκτελούμε την πράξη που ορίζει η συνάρτηση και έχουμε:

$3^x = 3^2 = 3*3 = 9$

Με άλλα λόγια, το 9 προκύπτει με τη βοήθεια του 2. Στην κανονική αριθμητική, όσο αυξάνει η τιμή του χ, τόσο αυξάνεται και το αποτέλεσμα της συνάρτησης. Συνεπώς, αν μας δοθεί το τελικό αποτέλεσμα, θα είναι σχετικά εύκολο να κάνουμε τους υπολογισμούς προς τα πίσω και να συμπεράνουμε τον αρχικό αριθμό. Για παράδειγμα, αν το αποτέλεσμα είναι 81, μπορούμε να συμπεράνουμε ότι χ=4, επειδή $3^4 = 81$. Αν κάναμε λάθος και εικάζαμε ότι χ=5 θα μπορούσαμε να υπολογίσουμε ότι $3^5 = 243$, και θα καταλαβαίναμε ότι η επιλογή μας για το χ είναι υπερβολικά μεγάλη. Θα μπορούσαμε τότε να μειώσουμε την επιλογή μας για το χ στο 4, και θα είχαμε την σωστή απάντηση. Με δυο

λόγια, ακόμη και αν μαντέψουμε λάθος, μπορούμε να επανέλθουμε στη σωστή τιμή του χ, και έτσι να αντιστρέψουμε τη συνάρτηση.

Ωστόσο, στη μοδιακή αριθμητική, η ίδια συνάρτηση δεν συμπεριφέρεται τόσο λογικά. Φαντασθείτε ότι μας λένε πως 3^x στη (modulo 7) μας δίνει 1, και μας ζητούν να βρούμε την τιμή του χ. Καμιά τιμή δεν μας έρχεται στο μυαλό, γιατί γενικά δεν είμαστε εξοικειωμένοι με τη μοδιακή αριθμητική. Μπορούμε να κάνουμε μια εικασία ότι χ=5, και να υπολογίσουμε το αποτέλεσμα του 3^5 (modulo 7). Η απάντηση που προκύπτει είναι το 5, το οποίο είναι υπερβολικά μεγάλο, εφόσον εμείς ψάχνουμε για μια απάντηση που να ισούται με 1. Θα μπορούσαμε να μπούμε στον πειρασμό να μειώσουμε την τιμή του χ και να ξαναπροσπαθήσουμε. Όμως στην περίπτωση αυτή θα ακολουθούσαμε λάθος κατεύθυνση, αφού η σωστή απάντηση είναι χ = 6.

Στην κανονική αριθμητική, μπορούμε να δοκιμάζουμε τους αριθμούς και να καταλαβαίνουμε πότε πλησιάζουμε στη σωστή λύση ή πότε απομακρυνόμαστε. Το περιβάλλον της μοδιακής αριθμητικής δεν μας δίνει βοηθητικά στοιχεία, και η αναστροφή των συναρτήσεων είναι πολύ δυσκολότερη. Συχνά ο μόνος τρόπος για να αναστρέψουμε μια συνάρτηση στη μοδιακή αριθμητική είναι να καταρτίσουμε έναν πίνακα επιλύοντας τη συνάρτηση για πολλές τιμές του χ, μέχρι να βρούμε τη σωστή απάντηση. Και ναι μεν η κατάρτιση ενός πίνακα μπορεί να μην είναι πολύ κουραστική, όταν έχουμε να κάνουμε με σχετικά μικρούς αριθμούς, όμως θα ήταν εξοντωτικά επώδυνο να καταρτίσουμε έναν πίνακα για μια συνάρτηση όπως η 453χ (modulo 21997).Πρόκειται για κλασικό παράδειγμα μονοσήμαντης συνάρτησης : Θα μπορούσα να επιλέξω μια τιμή για το χ και να υπολογίσω το αποτέλεσμα της συνάρτησης, αν όμως σας έδινα ένα αποτέλεσμα, ας πούμε το 5.787, θα σας ήταν τρομερά δύσκολο να αναστρέψετε τη συνάρτηση και να συμπεράνετε την επιλογή μου για το χ. Εγώ έκανα τους υπολογισμούς μου και βρήκα το 5.787 μέσα σε δευτερόλεπτα, όμως εσείς θα χρειαζόσασταν ώρες για να καταρτίσετε τον πίνακα και να βρείτε ποια τιμή έδωσα στο χ.

Ύστερα από δύο χρόνια εμμονής στη μοδιακή αριθμητική και στις 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. Ύστερα από μισή ώρα ξέφρενου μουντζουρώματος χαρτιών, 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 Υ και Ρ. Όλες σχεδόν οι τιμές είναι κατάλληλες, υπάρχουν όμως κάποιοι περιορισμοί, όπως ότι το Υ πρέπει να είναι μικρότερο του Ρ. Οι τιμές αυτές δεν είναι μυστικές και έτσι η Αλίκη μπορεί να τηλεφωνήσει στον Μπομπ και να του υποδείξει, ας πούμε, ότι Υ = 7 και Ρ = 11. Ακόμη και αν η τηλεφωνική γραμμή δεν είναι ασφαλής, και η αδίστακτη Εύα ακούσει αυτή τη συνομιλία, δεν έχει καμία σημασία, όπως θα δούμε αργότερα. Τώρα η Αλίκη και ο Μπομπ έχουν συμφωνήσει στη μονοσήμαντη συνάρτηση 7^x (modulo 11). Στο σημείο αυτό μπορούν να ξεκινήσουν τη διαδικασία της απόπειρας καθορισμού ενός μυστικού κλειδιού χωρίς να συναντηθούν. Επειδή εργάζονται παράλληλα, εξηγώ τις ενέργειές τους στις δύο στήλες του πίνακα.

Αν παρακολουθήσετε τα στάδια του πίνακα, θα δείτε ότι η Αλίκη και ο Μπομπ, χωρίς να συναντηθούν, συμφώνησαν στο ίδιο κλειδί, το οποίο μπορούν να χρησιμοποιήσουν για να κρυπτογράφηση DES. (Στην πραγματικότητα το σύστημα DES χρησιμοποιεί πολύ μεγαλύτερους αριθμούς ως κλειδιά, και η διαδικασία της ανταλλαγής που περιγράφεται στον πίνακα 26 θα στηριζόταν σε πολύ μεγαλύτερους αριθμούς, ώστε να προκύψει το κατάλληλο κλειδί DES). Εφαρμόζοντας το σχήμα του Χέλμαν, η Αλίκη και ο Μπομπ κατόρθωσαν να συμφωνήσουν σε ένα κλειδί χωρίς να χρειαστεί να συναντηθούν και να το ψιθυρίσει ο ένας στον άλλο. Το εκπληκτικό επίτευγμα είναι ότι το μυστικό κλειδί συμφωνήθηκε μέσω μιας ανταλλαγής πληροφοριών σε μια κοινή τηλεφωνική γραμμή. Αν όμως η Εύα έχει παγιδεύσει τη γραμμή αυτή, τότε ξέρει και το κλειδί – ή μήπως όχι ;

Ας εξετάσουμε το σχήμα του Χέλμαν από την οπτική γωνία της Εύας. Αν έχει παγιδεύσει τη γραμμή, τότε γνωρίζει μόνο τα εξής δεδομένα : ότι η συνάρτηση είναι 7^x (modulo 11), ότι η Αλίκη στέλνει α = 2 και ο Μπομπ στέλνει β = 4. Για να βρει το κλειδί, θα πρέπει να κάνει ότι κάνει ο Μπομπ, δηλαδή να μετατρέψει το α στο κλειδί γνωρίζοντας το Β, ή να κάνει ότι κάνει η Αλίκη, δηλαδή να μετατρέψει το β στο κλειδί γνωρίζοντας το Α. Όμως η Εύα δεν γνωρίζει τις τιμές των Α και Β, επειδή η Αλίκη και ο Μπομπ δεν αντάλλαξαν τους αριθμούς και τους κράτησαν μυστικούς. Η Εύα βρίσκεται σε αδιέξοδο. Έχει μόνο μια ελπίδα: θεωρητικά, θα μπορούσε να υπολογίσει το Α από το α επειδή το α προέκυψε από την εισαγωγή του Α σε μια συνάρτηση, και η Εύα γνωρίζει την συνάρτηση. Ή θα μπορούσε να υπολογίσει το Β από το β, επειδή το β προέκυψε από την εισαγωγή του Β σε μια συνάρτηση την οποίαν η Εύα γνωρίζει. Δυστυχώς όμως για την Εύα, ενώ είναι εύκολο για την Αλίκη να μετατρέψει το Α σε α και για τον Μπομπ να μετατρέψει

το Β σε β, είναι πολύ δύσκολο για την Εύα να αντιστρέψει τ ην διαδικασία ιδίως αν οι αριθμοί είναι πολύ μεγάλοι.

Πίνακας: Η γενική μονοσήμαντη συνάρτηση είναι Y* (modulo P). Η Αλίκη και ο Μπομπ επέλεξαν τιμές για τα Y και P, και συνεπώς συμφώνησαν στη μονοσήμαντη συνάρτηση 7* (modulo 11).

	Αλίκη	**Μπομπ**
Στάδιο 1	Η Αλίκη επιλέγει έναν αριθμό π.χ. το 3, και τον κρατά μυστικό. Ονομάζουμε τον αριθμό της Α.	Ο Μπομπ επιλέγει έναν αριθμό π.χ. το 6, και τον κρατά μυστικό. Ονομάζουμε τον αριθμό του Β.
Στάδιο 2	Η Αλίκη εισάγει το 3 στη μονοσήμαντη συνάρτηση και βρίσκει το αποτέλεσμα της πράξης 7Α (modulo 11): 73 (mod 11) = = 343 (mod 11) = 2.	Ο Μπομπ εισάγει το 6 στη μονοσήμαντη συνάρτηση και βρίσκει το αποτέλεσμα της πράξης 7Β (modulo 11): 76 (mod 11) = =117.649 (mod 11) = 4.
Στάδιο 3	Η Αλίκη ονομάζει το αποτέλεσμα αυτού του υπολο-γισμού α, και στέλνει το αποτέλεσμά της το 2, στον Μπομπ.	Ο Μπομπ ονομάζει το αποτέλεσμα αυτού του υπολο-γισμού β, και στέλνει το αποτέλεσμά του το 4, στην Αλίκη.

ΑΝΤΑΛΛΑΓΗ Κανονικά αυτή είναι κρίσιμη στιγμή. Η Αλίκη και ο Μπομπ ανταλλάσουν πληροφορίες, και η Εύα έχει την ευκαιρία να κρυφακούσει τις λεπτομέρειες της ανταλλαγής. Ωστόσο, αποδεικνύεται ότι η Εύα μπορεί να κρυφακούσει χωρίς να επηρεάζει την τελική ασφάλεια του συστήματος. Η Αλίκη και ο Μπομπ χρησιμοποιούν την ίδια τηλεφωνική γραμμή στην οποία ανταλλάσσουν τις αξίες των Y και P, και η Εύα υποκλέπτει τους δύο ανταλλασσόμενους αριθμούς,2 και 4. Όμως οι αριθμοί αυτοί δεν είναι κλειδί και επομένως δεν έχουν καμιά αξία για την Εύα.

Στάδιο	Η Αλίκη παίρνει το αποτέλεσμα	Ο Μπομπ παίρνει το αποτέλεσμα

4 του Μπομπ και βρίσκει το αποτέλεσμα της πράξης $\beta^A \pmod{11}$:

$43 \pmod{11} = 64 \pmod{11} =$

$= 9.$

της Αλίκης και βρίσκει το αποτέλεσμα της πράξης $\alpha^B \pmod{11}$:

$26 \pmod{11} = 64 \pmod{11} =$

$= 9.$

Το κλειδί Ως εκ θαύματος, η Αλίκη και ο Μπομπ κατέληξαν στον ίδιο αριθμό, το 9. Αυτό είναι το κλειδί !

Ο Μπομπ και η Αλίκη αντάλλαξαν όσες ακριβώς πληροφορίες χρειάζονταν για να μπορέσουν να καταλήξουν στο κλειδί, αλλά οι πληροφορίες αυτές δεν ήταν αρκετές για την Εύα ώστε να βρει το κλειδί. Ως αναλογικό παράδειγμα για το σύστημα του Χέλμαν, φαντασθείτε ένα κρυπτόγραμμα που με κάποιον τρόπο χρησιμοποιεί ως κλειδί το χρώμα. Πρώτον ας υποθέσουμε όλοι, μαζί και η Αλίκη, ο Μπομπ και η Εύα, έχουν από ένα δοχείο των τριών λίτρων που περιέχει ένα λίτρο κίτρινη μπογιά. Αν η Αλίκη και ο Μπομπ θέλουν να συμφωνήσουν σε ένα μυστικό κλειδί, προσθέτει ο καθένας τους στο δικό του δοχείο από ένα λίτρο με το δικό του μυστικό χρώμα. Η Αλίκη θα μπορούσε να προσθέσει μια απόχρωση μοβ, ενώ ο Μπομπ κόκκινο. Στη συνέχεια στέλνει ο ένας στον άλλο το δικό του δοχείο με το ανάμεικτο χρώμα. Τέλος, η Αλίκη παίρνει το μείγμα του Μπομπ και προσθέτει ένα λίτρο από το δικό της μυστικό χρώμα, και ο Μπομπ παίρνει το μείγμα της Αλίκης και προσθέτει και αυτός ένα λίτρο από το δικό του μυστικό χρώμα. Τώρα και τα δύο δοχεία περιέχουν το ίδιο χρώμα μπογιά, εφόσον το καθένα τους περιέχει ένα λίτρο μοβ και ένα λίτρο κόκκινο. Ως κλειδί χρησιμοποιείται το ακριβές χρώμα των διπλά ανακατεμένων δοχείων. Η Αλίκη δεν έχει ιδέα ποιο χρώμα πρόσθεσε ο Μπομπ, και ο Μπομπ δεν έχει ιδέα ποιο χρώμα πρόσθεσε η Αλίκη, όμως και οι δυο τους κατέληξαν στο ίδιο αποτέλεσμα. Στο μεταξύ, η Εύα είναι έξαλλη. Ακόμη και αν υποκλέψει τα ενδιάμεσα δοχεία, δεν μπορεί να συμπεράνει το χρώμα των τελικών δοχείων, το οποίο είναι το συμφωνημένο κλειδί. Μπορεί να δει το χρώμα του μείγματος στο δοχείο όπου το κίτρινο έχει αναμειχθεί με το μυστικό χρώμα του Μπομπ, μπορεί να δει και το χρώμα του μείγματος στο άλλο δοχείο, όπου το κίτρινο έχει αναμειχθεί με το μυστικό χρώμα της Αλίκης, αλλά για να βρει το κλειδί, πρέπει οπωσδήποτε να γνωρίζει τα αρχικά μυστικά χρώματα του Μπομπ και της Αλίκης. Όμως η Εύα δεν μπορεί να συμπεράνει τα μυστικά χρώματα του Μπομπ και της Αλίκης κοιτάζοντας τα δοχεία με τα μείγματα. Ακόμη και αν πάρει δείγμα από ένα μείγμα

δεν μπορεί να διαχωρίσει την μπογιά ώστε να βρεί το μυστικό χρώμα, επειδή η ανάμειξη της μπογιάς είναι μονοσήμαντη συνάρτηση.

Ο Χέλμαν κατέληξε στο εύρημά του μια νύχτα που δούλευε ως αργά στο σπίτι του, και όταν πια ολοκλήρωσε τους υπολογισμούς του, η ώρα ήταν πολύ περασμένη για να τηλεφωνήσει στους Ντίφι και Μέρκλε. Έπρεπε να περιμένει ως το επόμενο πρωί για να αποκαλύψει την ανακάλυψή του στους δύο μοναδικούς ανθρώπους στον κόσμο που είχαν πιστέψει ότι είναι εφικτή μια λύση στο πρόβλημα της διανομής των κλειδιών. «Η μούσα ψιθύρισε σε μένα», λέει ο Χέλμαν, « όμως τα θεμέλια τα θέσαμε όλοι μαζί». Ο Ντίφι αναγνώρισε αμέσως την ισχύ του επιτεύγματος του Χέλμαν : « Ο Μάρτι εξήγησε το σύστημα του της ανταλλαγής κλειδιών σε όλη την αφοπλιστική απλότητα . Ακούγοντάς τον, συνειδητοποίησα ότι η ιδέα κλωθογύριζε εδώ και κάποιον καιρό στην άκρη του μυαλού μου, αλλά δεν βγήκε ποτέ στην επιφάνεια».

Το σύστημα ανταλλαγής κλειδιών Ντίφι - Χέλμαν - Μέρκλε, όπως είναι γνωστό, επιτρέπει στην Αλίκη και τον Μπομπ να καθορίσουν ένα μυστικό μέσω μιας δημόσιας συζήτησης. Πρόκειται για μια από τις πιο ρηξικέλευθες ανακαλύψεις στην ιστορία της επιστήμης, και υποχρέωσε το κρυπτογραφικό κατεστημένο να ξαναγράψει τους κανόνες της κρυπτογράφησης. Οι Ντίφι, Χέλμαν και Μέρκλε απέδειξαν δημόσια το εύρημά τους στην Εθνική Συνδιάσκεψη της Πληροφορικής τον Ιούνιο του 1976, αφήνοντας κατάπληκτο το ακροατήριο των ειδικών της κρυπτογραφίας. Την επόμενη χρονιά κατέθεσαν αίτηση ευρεσιτεχνίας. 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 ανταλλάσουν δύο αριθμούς, να καθορίζουν 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 την φύση του ήταν άβολο. Φαντασθείτε ότι η Αλίκη ζει στη Χαβάη και ότι θέλει να στείλει ένα μήνυμα μέσω ηλεκτρονικού ταχυδρομείου στον Μπομπ στην Κωνσταντινούπολη. Ο Μπομπ πιθανότατα κοιμάται, όμως η χαρά του ηλεκτρονικού ταχυδρομείου είναι ότι η Αλίκη μπορεί να στείλει ανά πάσα στιγμή ένα μήνυμα, το οποίο θα περιμένει μέσα στον υπολογιστή του Μπομπ μέχρι αυτός να ξυπνήσει. Αν όμως η Αλίκη θέλει να κρυπτογραφήσει το μήνυμά της, τότε θα πρέπει να συμφωνήσει με τον Μπομπ σε ένα κλειδί, και για να γίνει αυτό είναι προτιμότερο να είναι και οι δυο τους συνδεδεμένοι στο δίκτυο την ίδια στιγμή – ο καθορισμός ενός κλειδιού απαιτεί αμοιβαία

ανταλλαγή πληροφοριών. Στην πραγματικότητα, η Αλίκη θα πρέπει να περιμένει μέχρι να ξυπνήσει ο Μπομπ. Εναλλακτικά, θα μπορούσε να του διαβιβάσει το δικό της τμήμα της ανταλλαγής κλειδιού, και να περιμένει 12 ώρες για την απάντησή του, οπότε και καθορίζεται το κλειδί και η Αλίκη μπορεί, αν δεν έχει κοιμηθεί η ίδια, να κρυπτογραφήσει και να μεταδώσει το μήνυμα. Και στις δύο περιπτώσεις, το σύστημα του Χέλμαν για την ανταλλαγή κλειδιών καταργεί τον αυθόρμητο χαρακτήρα του ηλεκτρονικού ταχυδρομείου.

Ο Χέλμαν κατέρριψε ένα από τα θεμελιώδη αξιώματα της κρυπτογραφίας και απέδειξε ότι ο Μπομπ και η Αλίκη δεν χρειαζόταν να συναντηθούν για να συμφωνήσουν σε ένα μυστικό κλειδί. Στη συνέχεια κάποιος έπρεπε απλώς να επινοήσει ένα πιο αποτελεσματικό σχήμα για να ξεπεραστεί το πρόβλημα της διανομής κλειδιών.

➢ Η γέννηση της κρυπτογραφίας δημοσίου κλειδιού

Η Μαίρη Φίσερ δεν ξέχασε ποτέ την πρώτη φορά που ο Ουίτφιλντ Ντίφι της ζήτησε να βγουν ραντεβού.«Ήξερε ότι ήμουν λάτρης του διαστήματος, και έτσι μου ‘πρότεινε να πάμε να δούμε μια εκτόξευση. Ο Ουίτ μου εξήγησε ότι εξήγησε ότι έφευγε το ίδιο απόγευμα για να δει το Σκάιλαμπ να απογειώνεται, και έτσι οδηγήσαμε όλη τη νύχτα, και φτάσαμε εκεί περίπου στις 3 τα ξημερώματα. Το πουλί ήταν καθ’ οδόν, όπως έλεγαν εκείνες τις ημέρες. Ο Ουίτ διέθετε διαπιστευτήρια Τύπου, εγώ όμως όχι. Όταν λοιπόν ζήτησαν να πιστοποιήσω την ταυτότητά μου και με ρώτησαν ποια είμαι, ο Ουίτ είπε «Η γυναίκα μου». Ήταν 16 Νοεμβρίου του 1973 ». τελικά παντρεύτηκαν στ’ αλήθεια, και τα πρώτα χρόνια η Μαίρη στήριξε τον άντρα της στους κρυπτογραφικούς διαλογισμούς του. Ο Ντίφι εργαζόταν ακόμη ως μεταπτυχιακός φοιτητής, πράγμα που σήμαινε ότι έπαιρνε μόνο έναν πενιχρό μισθό. Για να τα φέρουν βόλτα, η Μαίρη, που είχε σπουδάσει αρχαιολόγος, έπιασε δουλειά στην British Petroleum.

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. Συχνά περνούσε μεγάλες περιόδους άγονου στοχασμού, και σε μια περίπτωση, το 1975, είχε απογοητευθεί τόσο πολύ που είπε στη Μαίρη ότι δεν ήταν παρά ένας αποτυχημένος

επιστήμονας που δεν θα κατάφερνε ποτέ τίποτε. Έφτασε μάλιστα να της πει ότι θα ήταν καλύτερα γι' αυτήν να βρει κάποιον άλλο. Η Μαίρη του απάντησε ότι πίστευε απόλυτα σ'αυτόν, και μόλις δύο εβδομάδες μετά, ο Ντίφι συνέλαβε την πραγματικά λαμπρή ιδέα του.

Ακόμη θυμάται πως άστραψε η ιδέα στο μυαλό του, και μετά σχεδόν χάθηκε : Κατέβηκα κάτω να πάρω μια κόκα κόλα, και σχεδόν ξέχασα την ιδέα μου. Θυμόμουν ότι σκεφτόμουν κάτι ενδιαφέρον, αλλά δεν μπορούσα να θυμηθώ τι ακριβώς. Ξαφνικά η ιδέα επανήλθε, ανεβάζοντας την αδρεναλίνη μου στα ύψη. Για πρώτη φορά από τότε που άρχισα να εργάζομαι πάνω στην κρυπτογραφία, είχα την επίγνωση ότι βρήκα κάτι πραγματικά σημαντικό. Όλα όσα είχα ανακαλύψει μέχρι τότε στον τομέα αυτό μου φαίνονταν απλώς τεχνικές λεπτομέρειες». Ήταν απόγευμα, και έπρεπε να περιμένει ακόμη δύο ώρες μέχρι να γυρίσει σπίτι η Μαίρη. «Ο Ουίτ με περίμενε στην πόρτα», θυμάται εκείνη. «Με μια παράξενη έκφραση στο πρόσωπό του, είπε ότι είχε να μου ανακοινώσει κάτι σημαντικό. Μπήκα μέσα, και τότε μου είπε : ¨Κάθισε σε παρακαλώ, θέλω να σου μιλήσω. Πιστεύω πως έκανα μια μεγάλη ανακάλυψη – ξέρω ότι είμαι ο πρώτος που βρήκε κάτι τέτοιο¨. Για μια στιγμή ένιωσα σαν να σταμάτησε ο κόσμος. Είχα την αίσθηση ότι ζούσα σε μια ταινία του Χόλυγουντ».

Ο Ντίφι είχε επινοήσει ένα νέο τύπο κρυπτογραφήματος, που περιλάμβανε το λεγόμενο **ασύμμετρο κλειδί**. Όλες οι κρυπτογραφικές τεχνικές 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 – η σχέση τους είναι συμμετρική. Αντίθετα σε ένα ασύμμετρο σύστημα κλειδιών, όπως δείχνει και η ίδια η λέξη, το κλειδί της κρυπτογράφησης δεν είναι ταυτόσημο 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 δύο

κλειδιά, της κρυπτογράφησης και της αποκρυπτογράφησης, είναι που προσδίδει στο ασύμμετρο κρυπτόγραμμα τον ιδιαίτερο χαρακτήρα του.

Στο σημείο αυτό αξίζει να τονίσουμε ότι ο Ντίφι είχε μεν συλλάβει τη γενική αρχή του ασύμμετρου κρυπτογράμματος , αλλά δεν διέθετε ένα συγκεκριμένο παράδειγμά του. Ωστόσο, η έννοια και μόνο του ασύμμετρου κρυπτογράμματος ήταν επαναστατική. Αν οι κρυπτογράφοι κατόρθωναν να βρουν ένα πραγματικά λειτουργικό ασύμμετρο κρυπτόγραμμα, ένα σύστημα το οποίο να εκπληρώνει τις απαιτήσεις του Ντίφι, τότε οι συνέπειες για την Αλίκη και τον Μπομπ θα ήταν τεράστιες. Η Αλίκη θα μπορούσε να δημιουργήσει το δικό της ζευγάρι κλειδιών: ένα κλειδί κρυπτογράφησης και ένα κλειδί αποκρυπτογράφησης. Αν υποθέσουμε ότι το ασύμμετρο κρυπτόγραμμα είναι μια μορφή κρυπτογράφησης μέσω υπολογιστή, τότε το κλειδί κρυπτογράφησης της Αλίκης είναι ένας αριθμός, και το κλειδί της για την αποκρυπτογράφηση είναι ένας διαφορετικός αριθμός. Η Αλίκη κρατάει το κλειδί της αποκρυπτογράφησης μυστικό, και γι' αυτό συνήθως αποκαλείται **ιδιωτικό κλειδί** της Αλίκης. Αντίθετα, το κλειδί της κρυπτογράφησης το ανακοινώνει δημόσια, ώστε όλοι να έχουν πρόσβαση σ' αυτό, και γι' αυτό συνήθως αποκαλείται **δημόσιο κλειδί** της Αλίκης. Αν ο Μπομπ θέλει να στείλει στην Αλίκη ένα μήνυμα, απλώς βρίσκει το δημόσιο κλειδί της, που αναγράφεται σε μια λίστα αντίστοιχη με τον τηλεφωνικό κατάλογο, και το χρησιμοποιεί για να κρυπτογραφήσει το μήνυμα. Στη συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στην Αλίκη, και όταν αυτή το παίρνει, μπορεί να το αποκρυπτογραφήσει χρησιμοποιώντας το ιδιωτικό της κλειδί αποκρυπτογράφησης. Με τον ίδιο τρόπο, αν ο Τσάρλι, ο Ντον ή ο Έντουαρντ θέλουν να στείλουν στην Αλίκη ένα κρυπτογραφημένο μήνυμα, μπορούν και αυτοί να βρουν το δημόσιο κλειδί της για την κρυπτογράφηση, και σε κάθε περίπτωση μόνο η Αλίκη έχει πρόσβαση στο ιδιωτικό κλειδί αποκρυπτογράφησης που απαιτείται για να αποκρυπτογραφεί τα μηνύματα.

Το μεγάλο πλεονέκτημα αυτού του συστήματος είναι ότι δεν υπάρχει κανένα πηγαινέλα, όπως συμβαίνει με την ανταλλαγή κλειδιών κατά το σύστημα Ντίφι – Χέλμαν – Μέρκλε. Ο Μπομπ δεν χρειάζεται να περιμένει να πάρει πληροφορίες από την Αλίκη πριν μπορέσει να κρυπτογραφήσει ένα μήνυμα και να της το στείλει. Το μόνο που έχει να κάνει, είναι να βρει το δημόσιο κλειδί της κρυπτογράφησης. Επιπλέον, το ασύμμετρο κρυπτόγραμμα λύνει και το πρόβλημα της διανομής των κλειδιών. Η Αλίκη δεν είναι υποχρεωμένη να μεταφέρει με ασφάλεια στον Μπομπ το δημόσιο κλειδί της κρυπτογράφησης. Το εντελώς αντίθετο : μπορεί τώρα να το δημοσιοποιήσει όσο ευρύτερα γίνεται.

Θέλει όλος ο κόσμος να ξέρει το δημόσιο κλειδί της για την κρυπτογράφηση, ώστε να μπορεί οποιοσδήποτε να της στέλνει κρυπτογραφημένα μηνύματα. Ταυτόχρονα, ακόμη και αν όλος ο κόσμος γνωρίζει το δημόσιο κλειδί της Αλίκης, κανείς, ούτε και η Εύα, δεν μπορεί να αποκρυπτογραφήσει κανένα μήνυμα που έχει κρυπτογραφηθεί με αυτό, επειδή η γνώση του δημόσιου κλειδιού δεν βοηθά σε τίποτε την αποκρυπτογράφηση. Πράγματι, από τη στιγμή που ο Μπομπ κρυπτογραφήσει ένα μήνυμα χρησιμοποιώντας το δημόσιο κλειδί της Αλίκης, ούτε καν ο ίδιος δεν μπορεί να το αποκρυπτογραφήσει. Μόνο η Αλίκη, που κατέχει το ιδιωτικό κλειδί, μπορεί να αποκρυπτογραφήσει το μήνυμα.

Το σύστημα αυτό βρίσκεται στους αντίποδες του παραδοσιακού συμμετρικού κρυπτογράμματος, όπου η Αλίκη πρέπει να κοπιάσει για να μεταφέρει με ασφάλεια στον Μπομπ το κλειδί της κρυπτογράφησης. Σε ένα συμμετρικό κρυπτόγραμμα, το κλειδί της κρυπτογράφησης είναι το ίδιο με αυτό της αποκρυπτογράφησης, και έτσι η Αλίκη και ο Μπομπ πρέπει να παίρνουν τεράστιες προφυλάξεις για να διασφαλίσουν ότι το κλειδί δεν θα πέσει στα χέρια της Εύας. Αυτή είναι η ρίζα του προβλήματος της διανομής των κλειδιών.

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 μόνο το πρόσωπο που έχει το κλειδί μπορεί να το ανοίξει. Το κλείδωμα (η κρυπτογράφηση) είναι εύκολο, είναι κάτι που ο καθένας μπορεί να κάνει, όμως το ξεκλείδωμα (η 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, φαντασθείτε ότι η Αλίκη σχεδιάζει ένα λουκέτο και ένα κλειδί. Κρατάει για λογαριασμό 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, πηγαίνει στο τοπικό ταχυδρομείο, ζητάει ένα ¨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 κλεισίματός του ισοδυναμεί με το δημόσιο κλειδί της κρυπτογράφησης, επειδή ολοι έχουν πρόσβαση στα λουκέτα και ο καθένας μπορεί να χρησιμοποιήσει ένα λουκέτο για να σφραγίσει ένα μήνυμα με σε ένα κουτί. Το κλειδί του λουκέτου ισοδυναμεί με το ιδιωτικό κλειδί της αποκρυπτογράφησης, επειδή μόνο η Αλίκη το έχει, μόνο αυτή μπορεί να

ανοίξει το λουκέτο και μόνο αυτή μπορεί να αποκτήσει πρόσβαση στο μήνυμα που βρίσκεται μέσα στο κουτί.

Το σύστημα φαίνεται απλό όταν περιγράφεται με όρους λουκέτων, αλλά δεν είναι καθόλου εύκολο να βρεθεί μια μαθηματική συνάρτηση που να κάνει την ίδια δουλειά, κάτι που να μπορεί να ενσωματωθεί σε ένα εφαρμόσιμο κρυπτογραφικό σύστημα. Για να μετατραπούν τα ασύμμετρα κρυπτογράμματα από λαμπρή ιδέα σε πρακτική εφεύρεση, έπρεπε κάποιος να ανακαλύψει την κατάλληλη μαθηματική συνάρτηση. Ο Ντίφι σκεπτόταν έναν ειδικό τύπο μονοσήμαντης συνάρτησης, που θα μπορούσε να αντιστρέφεται κάτω από εξαιρετικές συνθήκες. 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 εύκολα αντιστρέφεται.

Ο Ντίφι δημοσίευσε ένα περίγραμμα της ιδέας του το καλοκαίρι του 1975, και από τότε και άλλοι επιστήμονες πήραν μέρος στην έρευνα για μια κατάλληλη μονοσήμαντη συνάρτηση, η οποία θα πληρούσε τα κριτήρια που απαιτούνταν για ένα ασύμμετρο κρυπτόγραμμα. Αρχικά υπήρχε μεγάλη αισιοδοξία, αλλά στο τέλος του έτους κανείς δεν είχε κατορθώσει να βρει τίποτε. Όσο περνούσαν οι μήνες, φαινόταν όλο και πιο πιθανό ότι δεν υπάρχουν ειδικές μονοσήμαντες συναρτήσεις. Η ιδέα του Ντίφι έμοιαζε να λειτουργεί στη θεωρία , αλλά όχι και στην πράξη. Ωστόσο, στο τέλος του 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, και είχαν δημιουργήσει το σύστημα Ντίφι-Χέλμαν – Μέρκλε, το οποίο ήταν εφαρμόσιμο, αλλά ατελές. Επίσης, είχαν προτείνει την ιδέα του ασύμμετρου κρυπτογράμματος, ένα σύστημα τέλειο, αλλά ως τότε ανεφάρμοστο. Συνέχισαν την έρευνά τους στο Πανεπιστήμιο Στάνφορντ, επιχειρώντας να βρουν μια ειδική μονοσήμαντη συνάρτηση που θα έκανε πραγματικότητα τα ασύμμετρα κρυπτογράμματα. Ωστόσο, οι ίδιοι απέτυχαν να κάνουν αυτή την ανακάλυψη. Τον αγώνα δρόμου για την εύρεση ενός ασύμμετρου κρυπτογράμματος τον κέρδισε μια άλλη τριάδα ερευνητών, 5.000 χιλιόμετρα μακριά, στην ανατολική ακτή της Αμερικής.

➢ ΟΙ ΚΥΡΙΩΣ ΥΠΟΠΤΟΙ

«Μια μέρα που μπήκα στο γραφείο του Ρον Ρίβεστ », θυμάται ο Λέοναρντ Άντλεμαν, «τον βρήκα να κρατάει στα χέρια του εκείνο το άρθρο. Άρχισε να μου λέει, ¨Αυτοί οι τύποι από το Στάνφορντ έχουν βρει αυτό το μπλα, μπλα, μπλα¨. Και θυμάμαι ότι τότε σκέφτηκα, ¨Καλά όλα αυτά, Ρον, αλλά έχω να σου μιλήσω για κάτι άλλο¨. Δεν είχα την παραμικρή ιδέα για την ιστορία της κρυπτογραφίας και δεν με ενδιέφεραν καθόλου τα όσα μου έλεγε». Το άρθρο που είχε ενθουσιάσει τόσο τον Ρον Ρίβεστ ήταν γραμμένο από τους Ντίφι και Χέλμαν, και περιέγραφε την ιδέα των ασύμμετρων κρυπτογραμμάτων. Τελικά ο Ρίβεστ έπεισε τον Άντλεμαν ότι στο συγκεκριμένο πρόβλημα ίσως να υπεισέρχονταν κάποια ενδιαφέροντα μαθηματικά, και μαζί αποφάσισαν να επιχειρήσουν να βρουν μα μονοσήμαντη συνάρτηση που να ανταποκρίνεται στις απαιτήσεις ενός ασύμμετρου κρυπτογράμματος. Στο κυνήγι αυτό τους ακολούθησε και ο Άντι Σαμίρ. Και οι τρεις εργάζονταν ως ερευνητές στον όγδοο όροφο του Εργαστηρίου Επιστήμης των Υπολογιστών του MIT.

Οι Ρίβεστ, Σαμίρ και Άντλεμαν συγκροτούσαν μια τέλεια ομάδα. Ο Ρίβεστ είναι επιστήμονας των Υπολογιστών με μια τρομακτική ικανότητα να αφομοιώνει νέες ιδέες και να τις εφαρμόζει σε απίθανα σημεία. Πάντα ενημερωνόταν για τις τελευταίες επιστημονικές ανακοινώσεις, πράγμα που τον ενέπνευσε να επινοήσει μια ολόκληρη σειρά από παράξενες και θαυμαστές υποψήφιες για τη θέση της μονοσήμαντης συνάρτησης στην οποία θα βασιζόταν ένα ασύμμετρο κρυπτόγραμμα. Ωστόσο, όλες οι υποψήφιες είχαν και από κάποιο ελάττωμα. Ο Σαμίρ, επίσης επιστήμονας των υπολογιστών, διαθέτει ακτινοβόλο διάνοια και την ικανότητα να βλέπει μέσα από τα θραύσματα και να επικεντρώνεται στον πυρήνα ενός προβλήματος. Και αυτός είχε διάφορες εμπνεύσεις για τη διατύπωση ενός ασύμμετρου κρυπτογράμματος, όμως και οι δικές του ιδέες ήταν αναπόφευκτα ατελείς. Ο Άντλεμαν, μαθηματικός με απίστευτη αντοχή, υπομονή και πειθαρχία, είχε κυρίως την ευθύνη να εντοπίζει τα ελαττώματα στις ιδέες των Ρίβεστ και Σαμίρ, έτσι ώστε να μην σπαταλούν χρόνο ακολουθώντας απατηλές οδούς. Οι Ρίβεστ και Σαμίρ πέρασαν ένα χρόνο διατυπώνοντας νέες ιδέες, τις οποίες ο Άντλεμαν απέρριπτε. Η τριάδα άρχισε να απελπίζεται, αλλά δεν είχαν επίγνωση ότι αυτή η διαδικασία των συνεχόμενων αποτυχιών αποτελούσε απαραίτητο μέρος της έρευνας τους, καθώς τους απομάκρυνε από τις άγονες περιοχές των μαθηματικών και τους οδηγούσε σε πιο γόνιμα εδάφη. Τελικά, οι προσπάθειες τους ανταμείφθηκαν.

Τον Απρίλιο του 1977, οι Ρίβεστ, Σαμίρ και Άντλεμαν πέρασαν το εβραϊκό Πάσχα στο σπίτι ενός φοιτητή, και αφού κατανάλωσαν σημαντικές ποσότητες κρασιού, επέστρεψε ο καθένας στο σπίτι του γύρω στα μεσάνυχτα. Ο Ρίβεστ, μην μπορώντας να κοιμηθεί, ξάπλωσε στο κρεβάτι του διαβάζοντας ένα εγχειρίδιο μαθηματικών. Στο νου του στριφογύριζε το ερώτημα που τον προβλημάτιζε επί βδομάδες – είναι δυνατή η κατασκευή ενός ασύμμετρου κρυπτογράμματος; Είναι δυνατό να βρεθεί μια μονοσήμαντη συνάρτηση που να μπορεί να αντιστραφεί μόνον εάν ο αποδέκτης έχει στην κατοχή του κάποια ειδική πληροφορία; Ξαφνικά η ομίχλη άρχισε να διαλύεται, και το μυαλό του φωτίστηκε. Πέρασε την υπόλοιπη νύχτα σχηματοποιώντας την ιδέα του, και πριν ξημερώσει είχε ουσιαστικά γράψει ένα πλήρες επιστημονικό άρθρο. Ο Ρίβεστ είχε κάνει μια σπουδαία ανακάλυψη, η οποία όμως είχε ωριμάσει μέσα από μια συνεργασία ενός χρόνου με τους Σαμίρ και Άντλεμαν, και δεν θα ήταν δυνατή χωρίς αυτούς. Ο Ρίβεστ τελείωσε το άρθρο αναγράφοντας τους συγγραφείς αλφαβητικά: Άντλεμαν, Ρίβεστ, Σαμίρ.

Το άλλο πρωί, ο Ρίβεστ παρέδωσε τη μελέτη του στον Άντλεμαν, που άρχισε τη συνηθισμένη διαδικασία του διαμελισμού της, όμως αυτή τη φορά δεν βρήκε κανένα λάθος. Η μόνη του κριτική αφορούσε τον κατάλογο των συγγραφέων. «Είπα στον Ρον να αφαιρέσει το όνομά μου από το άρθρο », θυμάται ο Άντλεμαν. «Του είπα ότι ήταν δική του επινόηση, όχι δική μου. Όμως ο Ρον αρνήθηκε, και αρχίσαμε μια συζήτηση για το θέμα αυτό. Τελικά συμφωνήσαμε να πάω σπίτι μου, να το σκεφτώ για μια νύχτα και να αποφασίσω τι ήθελα να κάνω. Την άλλη μέρα επέστρεψα και πρότεινα στον Ρον να είμαι ο τρίτος συγγραφέας. Θυμάμαι ότι πίστευα πως το άρθρο αυτό θα ήταν το λιγότερο ενδιαφέρον από όλα όσα είχαν το όνομά μου». Ο Άντλεμαν δεν θα μπορούσε να πέσει περισσότερο έξω. Το σύστημα που ονομάστηκε RSA (Rivest, Shamir, Adleman), και όχι ARS, αναδείχτηκε στο πιο σημαντικό κρυπτόγραμμα στη σύγχρονη κρυπτογραφία.

Πριν εξερευνήσουμε την ιδέα του Ρίβεστ, ας θυμηθούμε με συντομία τι ήταν αυτό που έψαχναν οι επιστήμονες για να κατασκευάσουν ένα ασύμμετρο κρυπτόγραμμα:

1. Η Αλίκη πρέπει να δημιουργήσει ένα δημόσιο κλειδί, το οποίο στη συνέχεια θα πρέπει να δημοσιεύσει, ώστε ο Μπομπ (και οποιοσδήποτε άλλος) να μπορεί να το χρησιμοποιεί για να κρυπτογραφεί τα μηνύματά του προς αυτήν. Επειδή το δημόσιο κλειδί είναι μονοσήμαντη συνάρτηση, θα πρέπει να είναι

ουσιαστικά αδύνατον για οποιονδήποτε να το αναστρέψει και να αποκρυπτογραφήσει τα μηνύματα της Αλίκης.

2. Ωστόσο η Αλίκη χρειάζεται να αποκρυπτογραφεί τα μηνύματα που της στέλνουν. Θα πρέπει επομένως να κρατάει ένα ιδιωτικό κλειδί μια ειδική πληροφορία που να της, επιτρέπει να αναστρέφει το αποτέλεσμα του δημόσιου κλειδιού. Συνεπώς η Αλίκη (και μόνο η Αλίκη) έχει τη δύναμη να αποκρυπτογραφεί όποιο μήνυμα της στέλνουν.

Στην καρδιά του ασύμμετρου κρυπτογράμματος του Ρίβεστ βρίσκεται μια μονοσήμαντη συνάρτηση βασισμένη στο είδος των μοδιακών συναρτήσεων που περιγράψαμε προηγουμένως στο παρόν κεφάλαιο. Η μονοσήμαντη συνάρτηση του Ρίβεστ μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση ενός μηνύματος – το μήνυμα, που στην πραγματικότητα είναι ένας αριθμός, εισάγεται στη συνάρτηση, και το αποτέλεσμα είναι το κρυπτογραφικό κείμενο, επίσης ένας αριθμός. Δεν θα περιγράψω εδώ λεπτομερώς τη μονοσήμαντη συνάρτηση του Ρίβεστ, αλλά θα εξηγήσω μια ιδιαίτερη πτυχή της, που είναι γνωστή απλά ως Ν, επειδή το Ν είναι αυτό που την καθιστά αντιστρέψιμη κάτω από ορισμένες συνθήκες και επομένως ιδανική για να χρησιμοποιηθεί ως ασύμμετρο κρυπτόγραμμα.

Το Ν είναι σημαντικό επειδή είναι μια μεταβλητή συνιστώσα της μονοσήμαντης συνάρτησης, που σημαίνει ότι κάθε άτομο μπορεί να επιλέγει μια διαφορετική τιμή του Ν, και να προσωποποιεί τη μονοσήμαντη συνάρτηση. Προκειμένου να επιλέξει την προσωπική της τιμή του Ν, η Αλίκη παίρνει δύο πρώτους αριθμούς, τους p και q, και τους πολλαπλασιάζει μεταξύ τους. Πρώτος αριθμός είναι εκείνος που δεν έχει άλλο διαιρέτη εκτός από τον εαυτό του και το 1. Για παράδειγμα, το 7 είναι πρώτος αριθμός, επειδή κανείς αριθμός εκτός από το 1 και το 7 δεν μπορεί να το διαιρέσει χωρίς να αφήσει υπόλοιπο. Ομοίως, το 13 είναι πρώτος αριθμός, επειδή μόνο οι αριθμοί 1 και 13 το διαιρούν χωρίς να αφήνουν υπόλοιπο. Αντίθετα, το 8 δεν είναι πρώτος αριθμός, επειδή μπορεί να διαιρεθεί από το 2 και το 4.

Έτσι, η Αλίκη θα μπορούσε να επιλέξει ως πρώτους αριθμούς τους p=17.159 και q = 10.247. Ο πολλαπλασιασμός των δύο αυτών αριθμών δίνει Ν = 17.159 Χ 10.247 = 175.828.273. Η επιλογή της Αλίκης για το Ν γίνεται ουσιαστικά το δημόσιο κλειδί της για την κρυπτογράφηση, και θα μπορούσε να το τυπώσει στην επισκεπτήρια κάρτα της, να το βάλει στο Διαδίκτυο ή να το δημοσιεύσει σε έναν κατάλογο δημοσίων κλειδιών, μαζί με τις τιμές όλων των άλλων για το

Ν. Αν ο Μπομπ θέλει να κρυπτογραφήσει ένα μήνυμα προς την Αλίκη, βρίσκει στον κατάλογο την τιμή της Αλίκης για το Ν (175.828.273) και την εισάγει στο γενικό τύπο της μονοσήμαντης συνάρτησης, που είναι επίσης δημόσια γνωστός. Τώρα ο Μπομπ έχει μια μονοσήμαντη συνάρτηση διαμορφωμένη με βάση το δημόσιο κλειδί της Αλίκης, η οποία επομένως μπορεί να αποκληθεί μονοσήμαντη συνάρτηση της Αλίκης. Για να κρυπτογραφήσει ένα μήνυμα προς την Αλίκη παίρνει τη μονοσήμαντη συνάρτηση της Αλίκης εισάγει το μήνυμα, καταγράφει το αποτέλεσμα και το στέλνει στην Αλίκη.

Μέχρι αυτό το σημείο, το κρυπτογραφημένο μήνυμα είναι ασφαλές, επειδή κανείς δεν μπορεί να το αποκρυπτογραφήσει. Το μήνυμα έχει κρυπτογραφηθεί με μια μονοσήμαντη συνάρτηση, και εξ ορισμού είναι πολύ δύσκολο η συνάρτηση αυτή να αναστραφεί ώστε να αποκρυπτογραφηθεί το μήνυμα. Παραμένει ωστόσο το ερώτημα: Πώς μπορεί η Αλίκη να αποκρυπτογραφήσει το μήνυμα; Για να διαβάζει τα μηνύματα που της στέλνουν , η Αλίκη θα πρέπει να έχει έναν τρόπο να αναστρέφει την μονοσήμαντη συνάρτηση. Χρειάζεται να έχει πρόσβαση σε κάποια ειδική πληροφορία που να της επιτρέπει να αποκρυπτογραφήσει το μήνυμα. Ευτυχώς για την Αλίκη, ο Ρίβεστ σχεδίασε την μονοσήμαντη συνάρτηση κατά τέτοιο τρόπο, ώστε να είναι αναστρέψιμη από κάποιον που γνωρίζει τις τιμές των p και q, δηλαδή των δύο πρώτων αριθμών που το γινόμενο τους δίνει το Ν είναι 175.828.273, δεν έχει αποκαλύψει τις τιμές της για τα p και q, και έτσι μόνο αυτή κατέχει την ειδική πληροφορία που χρειάζεται για να αποκρυπτογραφεί τα μηνύματα που λαμβάνει.

Μπορούμε να θεωρήσουμε το Ν ως το δημόσιο κλειδί, την πληροφορία που είναι διαθέσιμη σε όλους, την πληροφορία που απαιτείται για την κρυπτογράφηση μηνυμάτων προς την Αλίκη· αντίθετα, τα p και q, αποτελούν το ιδιωτικό κλειδί, προσιτό μόνο στην Αλίκη, την πληροφορία που χρειάζεται για την αποκρυπτογράφηση των μηνυμάτων.

Υπάρχει ωστόσο ένα ερώτημα που θα πρέπει να απαντηθεί αμέσως. Αν όλοι γνωρίζουν το Ν το δημόσιο κλειδί, τότε δεν μπορούν να συμπεράνουν τα p και q, το ιδιωτικό κλειδί, και να διαβάσουν τα μηνύματα που απευθύνονται στην Αλίκη; Στο κάτω κάτω, το Ν δημιουργήθηκε από τα p και q. Στην πραγματικότητα αποδεικνύεται ότι αν ο Ν είναι αρκετά μεγάλο, είναι ουσιαστικά αδύνατον να συναχθούν από αυτό οι τιμές των p και q, και αυτή είναι ίσως η πιο ωραία και κομψή πτυχή του ασύμμετρου κρυπτογράμματος RSA.

Η Αλίκη δημιούργησε το Ν επιλέγοντας τα p και q, και στη συνέχεια πολλαπλασιάζοντας τα. Το θεμελιώδες σημείο είναι ότι αυτή η πράξη είναι από μόνη της μια μονοσήμαντη συνάρτηση. Για να αποδείξουμε τη μονοσήμαντη φύση του πολλαπλασιασμού πρώτων αριθμών, μπορούμε να πάρουμε δύο πρώτους αριθμούς, λ.χ., τους 9.419 και 1.933, και να τους πολλαπλασιάσουμε. Με μια αριθμομηχανή, μέσα σε λίγα δευτερόλεπτα έχουμε την απάντηση : 18.206.927. Αν αντίθετα, μας δώσουν το 18.206.927 και μας ζητήσουν να βρούμε τους πρώτους παράγοντες (τους δύο αριθμούς που πολλαπλασιαζόμενοι μας δίνουν γινόμενο 18.206.927), θα μας χρειαστεί πολύ περισσότερος χρόνος. Αν αμφιβάλλετε για τη δυσκολία της εύρεσης των πρώτων παραγόντων, αναλογισθείτε το εξής. Χρειάστηκαν μόνο δέκα δευτερόλεπτα για να παραγάγω τον αριθμό 1.709.023, όμως θα σας πάρει σχεδόν ένα απόγευμα για να βρείτε, με μια αριθμομηχανή, τους πρώτους παράγοντες του.

Το σύστημα της ασύμμετρης κρυπτογραφίας, γνωστό ως RSA, λέγεται ότι είναι μια μορφή **κρυπτογραφίας δημόσιου κλειδιού**. Για να διαπιστώσουμε πόσο ασφαλές είναι το RSA μπορούμε να το εξετάσουμε από την οπτική γωνία της Εύας, και να προσπαθήσουμε να σπάσουμε ένα μήνυμα της Αλίκης προς τον Μπομπ. Για να κρυπτογραφήσει ένα μήνυμα προς τον Μπομπ, η Αλίκη πρέπει να βρει στον κατάλογο το δημόσιο κλειδί του Μπομπ. Για να δημιουργήσει το δημόσιο κλειδί του, ο Μπομπ επέλεξε τους δικούς του πρώτους αριθμούς, τους p_β και q_β, και τους πολλαπλασίασε για να προκύψει το Νβ: Τους pβ και qβ τους κράτησε μυστικούς γιατί αυτοί αποτελούν το ιδιωτικό του κλειδί της αποκρυπτογράφησης, ενώ δημοσιοποίησε το Νβ, που ισούται με 408.508.091. Έτσι η Αλίκη εισάγει το δημόσιο κλειδί του Μπομπ, το N_β, στη γενική μονοσήμαντη συνάρτηση, και στη συνέχεια κρυπτογραφεί το μήνυμά της προς αυτόν, Όταν λάβει το κρυπτογραφημένο μήνυμα, ο Μπομπ μπορεί να αναστρέψει τη συνάρτηση και να το αποκρυπτογραφήσει, χρησιμοποιώντας τις τιμές του για τα p_β και q_β, που αποτελούν το ιδιωτικό του κλειδί. Στο μεταξύ η Εύα έχει υποκλέψει το μήνυμα καθ' οδόν. Η μόνη της ελπίδα να το αποκρυπτογραφήσει, είναι να αναστρέψει τη μονοσήμαντη συνάρτηση, και αυτό είναι εφικτό μόνο αν γνωρίζει τα p_β και q_β. Ο Μπομπ έχει κρατήσει μυστικές τις αριθμητικές αξίες των p_β και q_β, αλλά η Εύα γνωρίζει, όπως όλος ο κόσμος, ότι το N_β είναι 408.508.091. Επιχειρεί λοιπόν να συναγάγει τις τιμές των p_β και q_β υπολογίζοντας ποιοι αριθμοί πρέπει να πολλαπλασιαστούν μεταξύ τους για να δώσουν γινόμενο 408.508.091, μια διαδικασία γνωστή ως **παραγοντοποίηση.**

Η παραγοντοποίηση είναι πολύ χρονοβόρα, όμως πόσο ακριβώς χρόνο θα χρειαζόταν η Εύα για να βρει τους παράγοντες του 408.508.091; Υπάρχουν διάφορες συνταγές για να επιχειρήσει κανείς να παραγοντοποιήσει το Νβ. Παρότι ορισμένες από αυτές είναι ταχύτερες από κάποιες άλλες, όλες τους στηρίζονται στο να δοκιμάζεις διαδοχικά όλους τους πρώτους αριθμούς για να δεις αν διαιρούν το N_β χωρίς να αφήνουν υπόλοιπο. Για παράδειγμα το 3 είναι πρώτος αριθμός, αλλά δεν είναι παράγοντας του N_β, επειδή δεν το διαιρεί τέλεια. Έτσι η Εύα προχωρεί στον επόμενο πρώτο αριθμό, το 5. Ούτε το 5 είναι παράγοντας, οπότε η Εύα προχωρεί στον επόμενο πρώτο αριθμό κ.ο.κ. Τελικά η Εύα φτάνει στο δισχιλιοστό πρώτο αριθμό το 18.313, που όντως είναι παράγοντας του 408.508.091. Έχοντας βρει τον ένα παράγοντα, είναι εύκολο να βρει και τον άλλο, που είναι το 22.307. Αν η Εύα είχε μια αριθμομηχανή και ήταν σε θέση να ελέγχει τέσσερις πρώτους αριθμούς ανά λεπτό, θα χρειαζόταν 500 λεπτά, δηλαδή πάνω από 8 ώρες, για να βρει τα p_β και q_β. Με άλλα λόγια, η Εύα θα μπορούσε να ανακαλύψει το ιδιωτικό κλειδί του Μπομπ σε λιγότερο από μία μέρα, και επομένως θα ήταν σε θέση να αποκρυπτογραφήσει το υποκλαπέν μήνυμα σε λιγότερο από μια μέρα.

Αυτό το επίπεδο ασφαλείας δεν είναι ιδιαίτερα υψηλό, αλλά ο Μπομπ θα μπορούσε να είχε επιλέξει πολύ μεγαλύτερους πρώτους αριθμούς, και έτσι θα είχε αυξήσει την ασφάλεια του ιδιωτικού του κλειδιού. Για παράδειγμα, θα μπορούσε να επιλέξει πρώτους αριθμούς της τάξης του 10^{65} (αυτό σημαίνει 1 ακολουθούμενο από 65 μηδενικά, ή εκατό χιλιάδες εκατομμύρια, εκατομμύρια, εκατομμύρια, εκατομμύρια, εκατομμύρια, εκατομμύρια, εκατομμύρια, εκατομμύρια, εκατομμύρια, εκατομμύρια). Αυτό θα έδινε στο Ν μια τιμή της τάξης περίπου του 10^{130} (10^{65} Χ 10^{65}). Ένας υπολογιστής θα μπορούσε να πολλαπλασιάσει τους δύο πρώτους αριθμούς και να παραγάγει το Ν μέσα σε ένα δευτερόλεπτο, όμως αν η Εύα ήθελε να αναστρέψει τη διαδικασία και να βρει τις τιμές των p_β και q_β, θα χρειαζόταν απείρως περισσότερο χρόνο. Το πόσο χρόνο ακριβώς εξαρτάται από την ταχύτητα του υπολογιστή της Εύας. Ο ειδικός σε θέματα ασφάλειας υπολογιστών Σίμσον Γκάρφινκελ εκτίμησε ότι ένας υπολογιστής Intel Pentium στα 100MHz , με 8MB RAM, θα χρειαζόταν περίπου 50 χρόνια για να παραγοντοποιήσει έναν αριθμό της τάξης του 10^{130} . Οι κρυπτογράφοι έχουν συνήθως μια δόση παράνοιας και εξετάζουν τα πιο καταστροφικά σενάρια, όπως μια παγκόσμια συνωμοσία με στόχο το σπάσιμο των κρυπτογραμμάτων τους. Έτσι ο Γκάρφινκελ εξέτασε τι θα συνέβαινε αν εκατό εκατομμύρια προσωπικοί υπολογιστές (όσοι δηλαδή πουλήθηκαν συνολικά το 1995) συνεργάζονταν γι' αυτό το σκοπό. Το

αποτέλεσμα είναι ότι ένας αριθμός της τάξης του 10^{130} μπορεί να παραγοντοποιηθεί σε 15 περίπου δευτερόλεπτα. Κατά συνέπεια, σήμερα είναι γενικά παραδεκτό ότι για πραγματική ασφάλεια, είναι αναγκαία η χρήση ακόμη μεγαλυτέρων πρώτων αριθμών. Για τις σημαντικές τραπεζικές συναλλαγές, το N τείνει να είναι τουλάχιστον της τάξης του 10^{308} . Για να σπάσει ένα τέτοιο κρυπτόγραμμα, θα χρειάζονταν οι συντονισμένες προσπάθειες εκατό εκατομμυρίων προσωπικών υπολογιστών επί χίλια και πλέον χρόνια. Όταν οι τιμές των p και q είναι αρκετά μεγάλες, το RSA είναι απόρθητο .

Η μόνη επιφύλαξη για την ασφάλεια της κρυπτογραφίας δημόσιου κλειδιού τύπου RSA είναι ότι κάποια στιγμή στο μέλλον κάποιος μπορεί να βρει έναν γρήγορο τρόπο παραγοντοποίησης του N. Μπορούμε να φαντασθούμε ότι σε μια δεκαετία από τώρα, ή ακόμη και αύριο, κάποιος θα ανακαλύψει μια μέθοδο ταχείας παραγοντοποίησης, οπότε το RSA θα αχρηστευθεί. Ωστόσο επί δύο χιλιάδες και πλέον χρόνια οι μαθηματικοί προσπαθούν να βρουν ένα σύντομο δρόμο, και ως τώρα δεν το έχουν καταφέρει : η παραγοντοποίηση παραμένει ένας τρομερά χρονοβόρος υπολογισμός. Οι περισσότεροι μαθηματικοί πιστεύουν ότι η παραγοντοποίηση είναι ένα έργο εγγενώς δυσχερές, και ότι υπάρχει κάποιος μαθηματικός νόμος που απαγορεύει οποιαδήποτε συντόμευση. Αν έχουν δίκιο, τότε το RSA φαίνεται ασφαλές για το προβλέψιμο μέλλον.

Το μεγάλο πλεονέκτημα της κρυπτογραφίας δημοσίου κλειδιού τύπου RSA είναι ότι καταργεί όλα τα προβλήματα που συνδέονταν με τα παραδοσιακά κρυπτογράμματα και τις μεθόδους ανταλλαγής των κλειδιών. Η Αλίκη δεν χρειάζεται πλέον να ανησυχεί για την ασφαλή μεταφορά του κλειδιού στον Μπομπ, ή για το ενδεχόμενο να υποκλέψει το κλειδί η Εύα. Πράγματι, η Αλίκη δεν ενδιαφέρεται για το ποιος θα δει το δημόσιο κλειδί – όσοι περισσότεροι, τόσο καλύτερα, εφόσον το δημόσιο κλειδί βοηθά μόνο την κρυπτογράφησης, όχι την αποκρυπτογράφηση. Το μόνο πράγμα που πρέπει να παραμείνει μυστικό είναι το ιδιωτικό κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση, και η Αλίκη μπορεί να το κρατά πάντα για λογαριασμό της.

Το RSA ανακοινώθηκε για πρώτη φορά τον Αύγουστο του 1977, όταν ο Μάρτιν Γκάρντνερ έγραψε ένα άρθρο με τίτλο Ένα νέο είδος κρυπτογράμματος που θα χρειάζονταν εκατομμύρια χρόνια για να σπάσει, για τη στήλη του Μαθηματικά παιχνίδια στο περιοδικό Scientific American.Αφού εξηγούσε την κρυπτογραφία δημόσιου κλειδιού, ο Γκάρντνερ απηύθυνε μια πρόκληση στους αναγνώστες του. Παρέθεσε

ένα κρυπτογραφικό κείμενο, δίνοντας και το δημόσιο κλειδί που είχε χρησιμοποιηθεί για την κρυπτογράφησή του :

N = 114.381.625.757.888.867.669.235.779.976.146.612.010.218.

296.721.242.362.562.561.842.935.706.935.845.733.897.830.597.

123.563.958.705.058.989.075.147.599.290.026.879..543.541.

Η πρόκληση ήταν να παραγοντοποιηθεί το N σε p και q, και στη συνέχεια οι αριθμοί αυτοί να χρησιμοποιηθούν για την αποκρυπτογράφηση του μηνύματος. Το βραβείο ήταν 100 δολάρια. Ο Γκάρντνερ δεν διέθετε στη στήλη του αρκετό χώρο για να εξηγήσει τις τεχνικές λεπτομέρειες του RSA, και αντ' αυτού ζήτησε από τους αναγνώστες του να γράψουν στο Εργαστήριο Επιστήμης των Υπολογιστών του MIT, το οποίο με τη σειρά του θα τους έστελνε ένα τεχνικό υπόμνημα που είχε μόλις καταρτίσει. Οι Ρίβεστ, Σαμίρ και Άντλεμαν εξεπλάγησαν με τις τρεις χιλιάδες αιτήσεις που δέχτηκαν. Ωστόσο, δεν απάντησαν αμέσως, επειδή ανησυχούσαν μήπως η δημόσια διανομή της ιδέας τους θέσει σε κίνδυνο τις πιθανότητες τους να πάρουν αριθμό ευρεσιτεχνίας, οι τρεις τους οργάνωσαν ένα πάρτι για να το γιορτάσουν. Εκεί καθηγητές και φοιτητές κατανάλωναν πίτσες και μπίρα, ενώ ταυτόχρονα γέμιζαν με τεχνικά υπομνήματα για τους αναγνώστες του Scientific American.

Όσο για την πρόκληση του Γκάρντνερ, χρειάστηκαν 17 χρόνια για να σπάσει το κρυπτόγραμμα. Στις 26 Απριλίου 1994, μια ομάδα εξακοσίων εθελοντών ανήγγειλε τους παράγοντες του N :

q= 3.490.529.510.847.650.949.147.849.619.903.898.133.417.764.

638.493.387.843.990.820.577

p = 32.769.132.993.266.709.549.961.988.190.834.461.413.

177.624.967.992.942.539.798.288.533.

Χρησιμοποιώντας αυτές τις τιμές ως ιδιωτικό κλειδί, κατόρθωσαν να αποκρυπτογραφήσουν το μήνυμα. Το μήνυμα ήταν μια σειρά από

αριθμούς, που όμως όταν μετατρέπονταν σε γράμματα, έδιναν τη φράση ¨the magic words are squeamish ossifrage ¨ (οι μαγικές λέξεις είναι μυγιάγγιχτο γεράκι). Το πρόβλημα της παραγοντοποίησης το είχαν κατανείμει μεταξύ τους οι εθελοντές, που προέρχονταν από τα τέσσερα σημεία του πλανήτη : Αυστραλία, Βρετανία, Αμερική, Βενεζουέλα. Οι εθελοντές περνούσαν τον ελεύθερο χρόνο τους μπροστά στις κεντρικές μονάδες και τους πανίσχυρους υπολογιστές τους, ο καθένας τους ασχολούμενος με ένα μέρος του προβλήματος. Στην πραγματικότητα, ένα δίκτυο υπολογιστών από όλο τον κόσμο εργάζονταν ταυτόχρονα για να απαντήσουν στην πρόκληση του Γκάρντνερ. Ακόμη και αν ληφθεί υπόψη η κολοσσιαία παράλληλη προσπάθεια, κάποιοι αναγνώστες και πάλι θα απορήσουν που το RSA έσπασε σε τόσο σύντομο διάστημα, θα πρέπει όμως να σημειώσουμε ότι η πρόκληση του Γκάρντνερ βασιζόταν σε μια σχετικά μικρή τιμή του N, της τάξης του 10129 . Σήμερα οι χρήστες του RSA επιλέγουν πολύ μεγαλύτερες τιμές για να διασφαλίζουν σημαντικές πληροφορίες. Είναι πλέον συνηθισμένη υπόθεση να κρυπτογραφούνται μηνύματα με τόση μεγάλη τιμή του N, ώστε όλοι οι υπολογιστές του πλανήτη να χρειάζονται περισσότερο χρόνο από την ηλικία του σύμπαντος για να σπάσουν το κρυπτόγραμμα.

➢ Η εναλλακτική ιστορία της κρυπτογράφησης δημόσιου κλειδιού

Τα είκοσι προηγούμενα χρόνια, οι Ντίφι, Χέλμαν και Μέρκλε έγιναν διάσημοι παγκοσμίως ως οι κρυπτογράφοι που επινόησαν την έννοια της κρυπτογραφίας δημόσιου κλειδιού, ενώ οι Ρίβεστ, Σαμίρ, και Άντλεμαν αναγνωρίστηκαν για την ωραιότερη εφαρμογή αυτής της ιδέας, την ανάπτυξη του RSA. Ωστόσο, μια πρόσφατη ανακοίνωση υποδεικνύει ότι τα βιβλία της Ιστορίας πρέπει να ξαναγραφτούν. Κατά τη βρετανική κυβέρνηση, η κρυπτογραφία δημόσιου κλειδιού επινοήθηκε για πρώτη φορά στο Τσέλτενχαμ, στο Κυβερνητικό Αρχηγείο Επικοινωνιών (GCHQ), τον άκρως απόρρητο οργανισμό που συγκροτήθηκε από τα απομεινάρια του Μπλίτσλεϊ Παρκ μετά το Δεύτερο Παγκόσμιο Πόλεμο. Είναι μια ιστορία αξιοθαύμαστης επινοητικότητας, ανωνύμων ηρώων και μιας κυβερνητικής συγκάλυψης που κράτησε δεκαετίες.

Η ιστορία αρχίζει στα τέλη της δεκαετίας του 1960, όταν οι βρετανοί στρατιωτικοί άρχισαν να ανησυχούν για το πρόβλημα της διανομής κλειδιών. Με το βλέμμα στραμμένο στην επερχόμενη δεκαετία του 1970, οι ανώτεροι επιτελικοί αξιωματικοί φαντάζονταν ένα σενάριο όπου η σμίκρυνση των ασυρμάτων και η μείωση του κόστους θα είχαν ως αποτέλεσμα κάθε στρατιώτης να βρίσκεται σε διαρκή επαφή, μέσω ασυρμάτου, με το διοικητή του. Τα πλεονεκτήματα της ευρείας διάδοσης των επικοινωνιών θα ήταν τεράστια, όμως οι επικοινωνίες θα έπρεπε οπωσδήποτε να κρυπτογραφούνται και το πρόβλημα της διανομής των κλειδιών θα ήταν ανυπέρβλητο. 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. Το επαχθές φορτίο της διανομής των κλειδιών θα στραγγάλιζε τελικά οποιαδήποτε επέκταση των επικοινωνιών. Στις αρχές του 1969, οι στρατιωτικοί ζήτησαν από τον Τζέιμς Έλις, έναν από τους πλέον επιφανείς κυβερνητικούς κρυπτογράφους της Βρετανίας, να αναζητήσει τρόπους αντιμετώπισης του προβλήματος της διανομής των κλειδιών.

Ο Έλις ήταν χαρακτήρας περίεργος και ελαφρώς εκκεντρικός. Καυχιόταν ότι είχε γυρίσει ταξιδεύοντας το μισό κόσμο πριν καν γεννηθεί – η σύλληψή του έγινε στη Βρετανία, αλλά γεννήθηκε στην Αυστραλία. Στη συνέχεια, μωρό ακόμη, επέστρεψε στο Λονδίνο και μεγάλωσε στο Ιστ Εντ της δεκαετίας του 1920. Στο σχολείο το κύριο ενδιαφέρον του ήταν οι θετικές επιστήμες. Σπούδασε Φυσική στο Αυτοκρατορικό Κολέγιο, και στη συνέχεια προσελήφθη στο Ερευνητικό Κέντρο της Ταχυδρομικής Υπηρεσίας στο Ντόλις Χιλ, εκεί που ο Τόμι Φλάουερς είχε κατασκευάσει τον Κολοσσό, τον πρώτο κωδικοθραύστη υπολογιστή. Το κρυπτογραφικό τμήμα του Ντόλις Χιλ τελικά απορροφήθηκε από το GCHQ και έτσι την 1η Απριλίου του 1965 ο Έλις μετακόμισε στο Τσέλτενχαμ και αποτέλεσε μέλος της νεοσύστατης Ομάδας Ασφαλείας των Επικοινωνιών και της Ηλεκτρονικής (CESG : Communications – Electronics Security Group), ενός ειδικού τμήματος του GCHQ που είχε ως αντικείμενο την ασφάλεια των βρετανικών επικοινωνιών. Επειδή εμπλεκόταν σε ζητήματα εθνικής ασφαλείας, ο Έλις είχε δώσει όρκο εχεμύθειας σε όλη τη διάρκεια της σταδιοδρομίας του. Παρότι η σύζυγος και η οικογένειά του γνώριζαν ότι εργαζόταν στο GCHQ, αγνοούσαν τις ανακαλύψεις του, και δεν είχαν ιδέα ότι ήταν ένας από τους πιο διακεκριμένους κωδικοπλάστες του έθνους.

Παρά τις κωδικοπλαστικές του ικανότητες, ο Έλις δεν τέθηκε ποτέ επικεφαλής σε καμία σημαντική ερευνητική ομάδα του GCHQ. Ήταν λαμπρό πνεύμα, αλλά ήταν και απρόβλεπτος, εσωστρεφής και

φύσει ασυμβίβαστος με την ομαδική εργασία. Ο συνάδελφός του Ρίτσαρντ Ουόλτον θυμάται:

Ο τρόπος εργασίας του ήταν μάλλον ιδιόρρυθμος και ουσιαστικά δεν είχε προσαρμοστεί στις καθημερινές δραστηριότητες του GCHQ. Όμως στον τομέα της επινόησης νέων ιδεών, ήταν εξαιρετικός. Ενίοτε τα γραφόμενά του ήταν κάπως ακαταλαβίστικα, όμως ήταν άκρως καινοτόμος και πάντα πρόθυμος να αμφισβητήσει τις καθιερωμένες αντιλήψεις. Αν στο GCHQ ήταν όλοι σαν τον Έλις, θα είχαμε στ' αλήθεια μπελάδες, όμως μπορούμε να ανεχθούμε μεγαλύτερο ποσοστό τέτοιων ανθρώπων από ότι οι περισσότερες οργανώσεις. Κατορθώνουμε και συμβιώνουμε με αρκετούς ανθρώπους σαν κι αυτόν.

Ένα από τα μεγαλύτερα προσόντα του Έλις ήταν το εύρος των γνώσεών του. Διάβαζε όποιο επιστημονικό περιοδικό έπεφτε στα χέριά του και ποτέ δεν πετούσε τίποτε. Για λίγους ασφαλείας, οι υπάλληλοι του GCHQ πρέπει να καθαρίζουν τα γραφεία τους κάθε απόγευμα και να κλειδώνουν τα πάντα σε κουτιά ασφαλείας, με αποτέλεσμα τα κουτιά ασφαλείας του Έλις να είναι μονίμως γεμάτα με τα πιο απίθανα δημοσιεύματα. Απέκτησε τη φήμη του γκουρού της κρυπτογραφίας, και κάθε φορά που οι άλλοι ερευνητές αντιμετώπιζαν κάποιο άλυτο πρόβλημα, χτυπούσαν την πόρτα του με την ελπίδα ότι οι τεράστιες γνώσεις και η πρωτοτυπία του θα τους έδιναν τη λύση. Πιθανότατα εξαιτίας αυτής της φήμης, του ζητήθηκε να εξετάσει το πρόβλημα της διανομής των κλειδιών.

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 προϋπολογισμό στρατιωτικής ασφαλείας. Όμως ο Έλις αντί για μια ήπια προσέγγιση του προβλήματος, άρχισε αμέσως να ψάχνει για μια πλήρη και ριζική λύση. «Πάντα προσέγγιζε οποιοδήποτε πρόβλημα θέτοντας το ερώτημα, ¨Είναι όντως αυτό που θέλουμε να κάνουμε;», λέει ο Ουόλτον. «Όντας ο Τζέιμς αυτός που ήταν, ένα από τα πρώτα πράγματα που έκανε ήταν να αμφισβητήσει το αξίωμα ότι ήταν απαραίτητο αποστολέας και αποδέκτης να μοιράζονται μυστικά δεδομένα, και εννοώ το κλειδί. Δεν υπήρχε κανένα θεώρημα που να λέει ότι πρέπει να μοιράζεσαι ένα μυστικό. Αυτό ήταν κάτι το αμφισβητήσιμο».

Ο Έλις άρχισε την επίθεσή του στο πρόβλημα ψαχουλεύοντας στους σωρευμένους θησαυρούς του των επιστημονικών άρθρων. Πολλά χρόνια αργότερα, θυμόταν τη στιγμή που ανακάλυψε ότι η διανομή των κλειδιών δεν αποτελεί αναπόφευκτα μέρος της κρυπτογραφίας:

Το γεγονός που άλλαξε αυτή την αντίληψη ήταν η ανακάλυψη μιας αναφοράς της Bell Telephone από την περίοδο του πολέμου. Ο άγνωστος συντάκτης της αναφοράς περιέγραφε 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 το θόρυβο, αφού ο ίδιος τον είχε προσθέσει και συνεπώς ήξερε τι ήταν. Τα προφανή πρακτικά μειονεκτήματα αυτού του συστήματος εμπόδισαν τη χρήση του στην πράξη, αλλά έχει ορισμένα ενδιαφέροντα χαρακτηριστικά. Η διαφορά του από τη συμβατική κρυπτογράφηση είναι ότι στην περίπτωση αυτή ο δέκτης παίρνει μέρος στη διαδικασία της κρυπτογράφησης ...Έτσι γεννήθηκε η ιδέα.

Θόρυβος είναι ο τεχνικός όρος για οποιοδήποτε σήμα που προσβάλλει μια 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 σύστημα 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 επικοινωνίας που τη συνδέει με τον Μπομπ. Ο Μπομπ τότε θα μπορούσε να στείλει ένα μήνυμα στην Αλίκη, και αν η Εύα είχε παγιδεύσει τη γραμμή, δεν θα ήταν σε θέση να διαβάσει 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 διαβάσει 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 αυτό 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.

Ο Έλις ανέλυσε λεπτομερώς το σκεπτικό του σε ένα υπόμνημα : «Η επόμενη ερώτηση είναι η προφανής. Μπορεί να γίνει αυτό χωρίς τη συνήθη κρυπτογράφηση; Μπορούμε να παραγάγουμε ένα ασφαλές κρυπτογραφημένο μήνυμα, αναγνώσιμο από τον επίσημο αποδέκτη, χωρίς προηγουμένη μυστική ανταλλαγή κλειδιού ; Το ερώτημα αυτό μου ήλθε στο μυαλό μια νύχτα που ήμουν ξαπλωμένος και η απόδειξη της θεωρητικής δυνατότητας μου πήρε μόλις λίγα λεπτά. Είχαμε ένα θεώρημα ύπαρξης. Το αδιανόητο ήταν τώρα εφικτό».(Ένα θεώρημα ύπαρξης αποδεικνύει ότι μια συγκεκριμένη έννοια είναι εφικτή, αλλά δεν ασχολείται με τις λεπτομέρειές της). Με άλλα λόγια, ως εκείνη τη στιγμή, η αναζήτηση μιας λύσης στο πρόβλημα της διανομής κλειδιών

ήταν σαν να ψάχναμε μια βελόνα σε έναν αχυρώνα, με την πιθανότητα η βελόνα να μην ήταν καν εκεί. Όμως χάρη στο θεώρημα ύπαρξης, ο Έλις τώρα ήξερε ότι η βελόνα βρισκόταν κάπου εκεί μέσα.

Οι ιδέες του Έλις έμοιαζαν πολύ με τις αντίστοιχες των Ντίφι, Χέλμαν και Μέρκλε, με τη διαφορά ότι ο Έλις προηγείτο αρκετά χρόνια από αυτούς. Ωστόσο, κανείς δεν έμαθε ποτέ για τη δουλειά του, επειδή ήταν υπάλληλος της Βρετανικής Κυβέρνησης και συνεπώς είχε δώσει όρκο εχεμύθειας. Στο τέλος του 1969, ο Έλις φαίνεται ότι είχε φτάσει στο ίδιο αδιέξοδο που θα έφτανε η τριάδα του Στάνφορντ το 1975. Είχε αποδείξει στον εαυτό του ότι η κρυπτογραφία δημοσίου κλειδιού (ή η μη μυστική κρυπτογραφία, όπως την αποκαλούσε) ήταν εφικτή, και είχε αναπτύξει την έννοια του διαχωρισμού δημόσιου και ιδιωτικού κλειδιού. Γνώριζε επίσης ότι έπρεπε να βρει μια ειδική μονοσήμαντη συνάρτηση, η οποία θα μπορούσε να αναστραφεί εάν 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.

Στο σημείο αυτό ο Έλις αποκάλυψε το επίτευγμά του στους προϊσταμένους του. Οι αντιδράσεις τους παραμένουν ακόμη απόρρητο υλικό, αλλά ο Ρίτσαρντ Ουόλτον, σε μια συνέντευξη, μου παρέφρασε τα διάφορα υπομνήματα που ανταλλάχτηκαν. Καθισμένος με το χαρτοφύλακά του στα γόνατα και με το κάλυμμα να με εμποδίζει να δω τα χαρτιά, άρχισε να φυλλομετράει τα έγγραφα :

Δεν μπορώ να σας δείξω τα χαρτιά που έχω εδώ μέσα, επειδή έχουν ακόμη τυπωμένες παντού πάνω τους κακές λέξεις όπως ΑΚΡΩΣ ΑΠΟΡΡΗΤΟΝ. Η ουσία είναι ότι η ιδέα του Τζέιμς πηγαίνει στο αφεντικό, ο οποίος τη βάζει στα εξερχόμενα, όπως κάνουν πάντα τα αφεντικά, έτσι ώστε να την εξετάσουν οι ειδικοί. Οι ειδικοί αποφαίνονται ότι όσα λέει ο Τζέιμς είναι απολύτως αληθή. Με άλλα λόγια, δεν μπορούν να τον βγάλουν παλαβό. Ταυτόχρονα, δεν μπορούν να σκεφτούν έναν τρόπο πρακτικής εφαρμογής της ιδέας του. Έτσι, μένουν εντυπωσιασμένοι από την επινοητικότητα του Τζέιμς, αλλά δεν ξέρουν πώς να την εκμεταλλευτούν.

Τα τρία επόμενα χρόνια , τα πιο λαμπρά πνεύματα του GCHQ αγωνίζονταν να βρουν μια μονοσήμαντη συνάρτηση που να εκπληρώνει τις απαιτήσεις του Έλις, αλλά δεν προέκυψε τίποτε. Ώσπου, το Σεπτέμβριο του 1973, προστέθηκε στην ομάδα ένας νέος μαθηματικός. Ο Κλίφορντ Κοκς είχε πρόσφατα αποφοιτήσει από το Πανεπιστήμιο του Κέμπριτζ, όπου είχε ειδικευτεί στη θεωρία των αριθμών, μια από τις καθαρότερες μορφές μαθηματικών. Όταν προσελήφθη στο GCHQ, γνώριζε ελάχιστα για την κρυπτογράφηση και τον σκιερό κόσμο των στρατιωτικών και διπλωματικών επικοινωνιών. Έτσι του όρισαν έναν

μέντορα, τον Νικ Πάτερσον, που τον καθοδήγησε τις πρώτες του εβδομάδες στο GCHQ.

Ύστερα από έξι περίπου εβδομάδες, ο Πάτερσον μίλησε στον Κοκς για « μια πραγματική φοβερή ιδέα ». Συνόψισε τη θεωρία του Έλις περί κρυπτογραφίας δημόσιου κλειδιού και του εξήγησε ότι κανείς δεν είχε μπορέσει ακόμη να βρει μια μαθηματική συνάρτηση που να ταιριάζει στη θεωρία. Ο Πάτερσον τα είπε αυτά στον Κοκς επειδή επρόκειτο για την πιο ερεθιστική κρυπτογραφική ιδέα που κυκλοφορούσε και όχι επειδή πίστευε ότι ο νεαρός μαθηματικός θα επιχειρούσε να λύσει το πρόβλημα. Ωστόσο όπως εξηγεί ο Κοκς, την ίδια κιόλας μέρα στρώθηκε στη δουλειά. «Δεν συνέβαινε τίποτε το ιδιαίτερο κι έτσι είπα να σκεφτώ πάνω σε αυτή την ιδέα. Επειδή είχα δουλέψει πάνω στη θεωρία των αριθμών, ήταν φυσικό να σκεφτώ για τις μονοσήμαντες συναρτήσεις, κάτι που μπορείς να κάνεις, αλλά δεν μπορείς να το αναστρέψεις. Οι πρώτοι αριθμοί και η παραγοντοποίηση ήταν η πιο φυσική επιλογή και αυτό έγινε το σημείο εκκινήσεώς μου.» Ο Κοκς είχε αρχίσει να διατυπώνει αυτό που αργότερα θα γινόταν γνωστό ως ασύμμετρο κρυπτόγραμμα RSA. Οι Ρίβεστ, Σαμίρ και Άντλεμαν ανακάλυψαν τη δική τους φόρμουλα για την κρυπτογραφία δημόσιου κλειδιού το 1977, όμως τέσσερα χρόνια νωρίτερα ο νεαρός απόφοιτος του Κέμπριτζ διήνυε την ίδια ακριβώς διανοητική διαδρομή. «Από την αρχή ως το τέλος», θυμάται ο Κοκς, η « όλη διαδικασία δεν μου πήρε πάνω από μισή ώρα. Ήμουν ιδιαίτερα ευχαριστημένος με τον εαυτό μου ˝ Υπέροχα ˝, σκέφτηκα. ˝ Μου δόθηκε ένα πρόβλημα και το έλυσα ˝».

Ο Κοκς δεν είχε πλήρη εκτίμηση της σημασίας της ανακάλυψης του. Αγνοούσε ότι τα λαμπρότερα μυαλά του GCHQ πάλευαν με το πρόβλημα επί τρία χρόνια και δεν ήξερε ότι είχε πραγματοποιήσει ένα από τα μεγαλύτερα κρυπτογραφικά επιτεύγματα του αιώνα. Η αφέλεια του Κοκς ίσως να εξηγεί εν μέρει την επιτυχία του, αφού του επέτρεψε να προσεγγίσει το πρόβλημα με αυτοπεποίθηση και όχι με διστακτικότητα. Ο Κοκς μίλησε στον μέντορά του για την ανακάλυψή του και στη συνέχεια ο Πάτερσον το ανέφερε στη διοίκηση. Ο Κοκς ήταν πολύ συγκρατημένος και από πολλές απόψεις παρέμεινε νεοσύλλεκτος, ενώ αντίθετα ο Πάτερσον είχε πλήρη εκτίμηση των συμφραζομένων του προβλήματος και ήταν πιο ικανός να αντιμετωπίσει τα τεχνικά ζητήματα που αναπόφευκτα θα προέκυπταν. Σύντομα άρχισαν να πλησιάζουν τον Κοκς, το παιδί θαύμα, άτομα εντελώς άγνωστά του και να του δίνουν συγχαρητήρια. Ένας από αυτούς ήταν και ο Τζέιμς Έλις, ο οποίος ανυπομονούσε να γνωρίσει τον άνθρωπο που είχε κάνει το όνειρό του πραγματικότητα. Επειδή ο Κοκς δεν αντιλαμβανόταν ακόμη το μέγεθος του επιτεύγματος του, οι

λεπτομέρειες αυτής της συνάντησης δεν τον εντυπωσίασαν ιδιαίτερα και έτσι σήμερα, μετά από είκοσι και πλέον χρόνια, δεν θυμάται καθόλου την αντίδραση του Έλις.

Όταν τελικά ο Κοκς συνειδητοποίησε τι είχε κάνει, σκέφτηκε με δέος ότι η ανακάλυψή του ίσως να απογοήτευε τον Τζ. Χ. Χάρντι, έναν από τους μεγαλύτερους άγγλους μαθηματικούς του πρώτου μισού του 20ού αιώνα. Στο έργο του Η απολογία του μαθηματικού, γραμμένο το 1940, ο Χάρντι δήλωνε υπερήφανα: «Τα αληθινά μαθηματικά δεν έχουν καμία επίδραση στον πόλεμο. Κανείς ως τώρα δεν έχει ανακαλύψει κάποιον πολεμικό στόχο που να εξυπηρετείται από τη θεωρία των αριθμών ». Ως αληθινά μαθηματικά νοούνται τα καθαρά μαθηματικά, όπως η θεωρία των αριθμών που αποτελούσε την καρδιά της εργασίας του Κοκς. Ο Κοκς απέδειξε ότι ο Χάρντι έσφαλλε. Τώρα οι δαίδαλοι της θεωρίας των αριθμών μπορούσαν να βοηθούν τους στρατηγούς να σχεδιάζουν τις μάχες τους με πλήρη μυστικότητα. Επειδή η εργασία του Κοκς είχε συνέπειες στις στρατιωτικές επικοινωνίες, του απαγόρευσαν, όπως και στον Έλις, να πει σε οποιονδήποτε εκτός GCHQ για το επίτευγμά του. Η συνεργασία του με μια μυστική κυβερνητική υπηρεσία σήμαινε ότι δεν μπορούσε να το αποκαλύψει ούτε στους γονείς του ούτε στους πρώην συμφοιτητές του από το Πανεπιστήμιο του Κέμπριτζ. Το μόνο πρόσωπο στο οποίο μπορούσε να μιλήσει ήταν η γυναίκα του, η Τζιλ, επειδή και αυτή εργαζόταν στο GCHQ.

Παρότι η ιδέα του Κοκ ήταν ένα από τα πιο ισχυρά μυστικά του GCHQ, έπασχε κατά το ότι προπορευόταν της εποχής της. Ο Κοκς είχε ανακαλύψει μια μαθηματική συνάρτηση που επέτρεπε την κρυπτογραφία δημόσιου κλειδιού, αλλά παρέμεινε η δυσκολία της εφαρμογής του συστήματος. Η κρυπτογράφηση με αυτή τη μέθοδο 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. Οι Κοκς και Έλις είχαν αποδείξει ότι το φαινομενικά ανέφικτο ήταν εφικτό, αλλά κανείς δεν μπορούσε να βρει έναν τρόπο για να το εφαρμόσει στην πράξη.

Στις αρχές του επόμενου έτους, το 1974, ο Κοκς εξήγησε την εργασία του πάνω στην κρυπτογραφία δημοσίου κλειδιού στον Μάλκολμ Ουίλιαμσον, που είχε πρόσφατα προσληφθεί στο GCHQ ως κρυπτογράφος. Οι δυο άντρες τύχαινε να είναι παλιοί φίλοι. Είχαν και

οι δύο τελειώσει το δημοτικό σχολείο του Μάντσεστερ, που είχε ως έμβλημα του το Sapere ayde (τόλμησε να γίνεις σοφός). Τα δύο αγόρια, ως μαθητές, είχαν εκπροσωπήσει τη Βρετανία στη Μαθηματική Ολυμπιάδα του 1968 στη Σοβιετική Ένωση. Αφού φοίτησαν μαζί στο πανεπιστήμιο του Κέμπριτζ, τράβηξε ο καθένας τον δρόμο του για δύο χρόνια, τώρα όμως ξαναβρίσκονταν στο GCHQ. Αντάλλασσαν μαθηματικές ιδέες από τα έντεκα χρόνια τους, όμως η αποκάλυψη της κρυπτογραφίας δημοσίου κλειδιού από τον Κοκς ήταν για τον Ουίλιαμσον η πιο συγκλονιστική ιδέα που είχε ακούσει ποτέ.

Ο Ουίλιαμσον έφυγε και άρχισε να προσπαθεί να αποδείξει ότι ο Κοκς είχε κάνει κάποιο λάθος και ότι η κρυπτογραφία δημοσίου κλειδιού δεν υπήρχε στην πραγματικότητα. Διερεύνησε τα μαθηματικά ψάχνοντας για κάποιο ψεγάδι. Η κρυπτογραφία δημοσίου κλειδιού έμοιαζε πολύ ωραία για να είναι αληθινή, και ο Ουίλιαμσον ήταν σε τέτοιο βαθμό αποφασισμένος να βρει ένα λάθος, που πήρε το πρόβλημα στο σπίτι του. Οι υπάλληλοι του GCHQ δεν επιτρέπεται να παίρνουν δουλειά στο σπίτι, επειδή όσα κάνουν είναι άκρως απόρρητα, και το οικιακό περιβάλλον είναι δυνάμει ευάλωτο στην κατασκοπία. Όμως το πρόβλημα είχε τόσο πολύ σφηνωθεί στο μυαλό του Ουίλιαμσον, που δεν μπορούσε να σταματήσει να το σκέφτεται. Έτσι, κατά παράβαση των κανονισμών, μετέφερε την εργασία του σπίτι του, όπου πέρασε πέντε ώρες προσπαθώντας να βρει μια ατέλεια. «Ουσιαστικά απέτυχα», λέει ο Ουίλιαμσον. «Αντ' αυτού, βρήκα μια άλλη λύση στο πρόβλημα της διανομής των κλειδιών». Ο Ουίλιαμσον ανακάλυπτε τη μέθοδο Ντίφι – Χέλμαν – Μέρκλε για την ανταλλαγή κλειδιών περίπου ταυτόχρονα με τον Μάρτιν Χέλμαν. Η αρχική του αντίδραση αντικατοπτρίζει την κυνική του διάθεση.

Το 1975, οι Τζέιμς Έλις, Κλίφορντ Κοκς και Μάλκολμ Ουίλιαμσον είχαν ήδη ανακαλύψει όλες τις θεμελιώδεις πτυχές της κρυπτογραφίας δημοσίου κλειδιού, όμως έπρεπε να κρατήσουν το στόμα τους κλειστό. Οι τρείς Βρετανοί ήταν υποχρεωμένοι να καθίσουν και να βλέπουν, ενώ οι θεωρίες τους ανακαλύπτονταν ξανά τα τρία επόμενα χρόνια από τους Ντίφι, Χέλμαν, Μέρκλε, Ρίβεστ, Σαμίρ και Άντλεμαν. Παραδόξως, το GCHQ ανακάλυψε το σύστημα RSA πριν από την ανταλλαγή κλειδιών κατά τη μέθοδο Ντίφι – Χέλμαν – Μέρκλε, ενώ στον έξω κόσμο συνέβη το αντίστροφο. Ο επιστημονικός τύπος ανέφερε τα επιτεύγματα που πραγματοποιήθηκαν στο Στάνφορντ και το MIT, και οι ερευνητές, των οποίων οι εργασίες δημοσιεύτηκαν στα επιστημονικά περιοδικά, έγιναν διάσημοι στην κοινότητα των κρυπτογράφων.

Το μόνο παράπονο του Ουίλιαμσον είναι ότι το GCHQ δεν κατόρθωσε να αποκτήσει την ευρεσιτεχνία της κρυπτογραφίας δημοσίου κλειδιού. Όταν οι Κοκς και Ουίλιαμσον πραγματοποίησαν τα πρώτα επιτεύγματα, η διοίκηση του GCHQ θεωρούσε ομόφωνα ότι κάτι τέτοιο ήταν αδύνατον για δύο λόγους. Πρώτον , για να πάρουν την ευρεσιτεχνία, θα έπρεπε να αποκαλύψουν τις λεπτομέρειες της εργασίας τους, πράγμα ασυμβίβαστο με τις αρχές του GCHQ. Δεύτερον, στις αρχές της δεκαετίας του 1970 δεν ήταν διόλου σαφές αν η ευρεσιτεχνία κάλυπτε και τους αλγόριθμους. Στο σημείο αυτό ο Ουίλιαμσον ήθελε να βγει στη δημοσιότητα για να μπλοκάρει την αίτηση ευρεσιτεχνίας των Ντίφι και Χέλμαν, όμως υπερίσχυσε η αντίθετη γνώμη των προϊσταμένων του, που δεν ήταν αρκετά οξυδερκείς ώστε να προβλέψουν την ψηφιακή επανάσταση και τις δυνατότητες της κρυπτογραφίας δημοσίου κλειδιού. Στις αρχές της δεκαετίας του 1980. Είχαν ήδη αρχίσει να μετανιώνουν για την απόφαση τους, καθώς οι εξελίξεις στον χώρο των υπολογιστών και οι πρώτες εμβρυακές μορφές του Διαδικτύου καθιστούν σαφές ότι τόσο το RSA, όσο και το σύστημα ανταλλαγής κλειδιών Ντίφι – Χέλμαν – Μέρκλε θα είχαν τεράστια εμπορική επιτυχία. Το 1996, η εταιρία που ήταν υπεύθυνη για τα προϊόντα RSA, η RSA Data Security Inc., πουλήθηκε αντί 200 εκατομμυρίων δολαρίων.

Παρότι το έργο που γινόταν στο GCHQ παρέμενε άκρως απόρρητο, υπήρχε μια άλλη οργάνωση που γνώριζε τα βρετανικά επιτεύγματα. Η Υπηρεσία Εθνικής Ασφάλειας των ΗΠΑ, η NSA, ήξερε για την δουλειά των Έλις, Κοκς και Ουίλιαμσον, και πιθανότητα μέσω της NSA άκουσε ο Ουίτφιλντ Ντίφι κάποιες φήμες για τις αποκαλύψεις των Βρετανών. Το Σεπτέμβριο του 1982, ο Ντίφι αποφάσισε να ελέγξει αν υπήρχε στις φήμες αυτές κάποιες δόσεις αλήθειας, και ταξίδεψε με τη γυναίκα του ως το Τσέλτενχαμ για να μιλήσει αυτοπροσώπως με τον Τζέιμς Έλις. Συναντήθηκαν σε μια παμπ της περιοχής, και σχεδόν αμέσως η Μαίρη εντυπωσιάστηκε με το σπάνιο χαρακτήρα του Έλις.

Ο Ντίφι και ο Έλις συζήτησαν διάφορα ζητήματα, από αρχαιολογία μέχρι το πώς τα ποντίκια σε ένα βαρέλι βελτιώνουν τη γεύση του μηλίτη, κάθε φορά όμως που η συζήτηση στρεφόταν προς την κρυπτογραφία, ο Έλις άλλαζε ευγενικά το θέμα. Στο τέλος της επίσκεψης του, και ενώ ετοιμαζόταν να φύγει, ο Ντίφι δεν μπόρεσε πια να κρατηθεί και έθεσε απερίφραστα στον Έλις την ερώτηση που είχε στ΄ αλήθεια στο μυαλό του: «Πες μου, πώς επινόησες την κρυπτογραφία δημοσίου κλειδιού;» Ύστερα από μια μεγάλη παύση, ο Έλις τελικά ψιθύρισε: « λοιπόν, δεν ξέρω πόσα επιτρέπεται να πω. Ας πούμε ότι εσείς καταφέρατε πολύ περισσότερα στο θέμα αυτό από μας».

Το γεγονός ότι το GCHQ επινόησε πρώτο την κρυπτογραφία δημοσίου κλειδιού δεν μειώνει την αξία των επιτευγμάτων των πανεπιστημιακών ερευνητών που την ανακάλυψαν ξανά. Πρώτοι αυτοί συνειδητοποίησαν τις δυνατότητες της κρυπτογραφίας δημοσίου κλειδιού και καθοδήγησαν την εφαρμογή της. Επιπλέον, είναι πολύ πιθανόν το GCHQ να μην αποκάλυπτε ποτέ το έργο του, παρεμποδίζοντας έτσι την εφαρμογή μιας μορφής κρυπτογράφησης που θα επέτρεπε στην ψηφιακή επανάσταση να αναπτύξει πλήρως τις δυνατότητες της. Τέλος, η ανακάλυψη των πανεπιστημιακών ήταν εντελώς ανεξάρτητη από την αντίστοιχη του GCHQ και διανοητικά ισάξια της. Ο πανεπιστημιακός χώρος είναι εντελώς απομονωμένος από τον τομέα της άκρως απόρρητης έρευνας, και οι εκπρόσωποι του δεν έχουν πρόσβαση στα εργαλεία και την απόρρητη γνώση που μπορεί να κρύβει ο κόσμος των μυστικών υπηρεσιών. Αντίθετα, οι κυβερνητικοί ερευνητές έχουν πάντα πρόσβαση στην πανεπιστημιακή βιβλιογραφία. Μπορούμε να θεωρήσουμε αυτόν τον τύπο ροής πληροφοριών σαν μια μονοσήμαντη συνάρτηση – οι πληροφορίες ρέουν ελεύθερα προς τη μια κατεύθυνση, αλλά απαγορεύεται η διοχέτευση τους προς την αντίθετη.

Όταν ο Ντίφι μίλησε στον Χέλμαν για τους Έλις, Κοκς και Ουίλιαμσον, εκείνος παρατήρησε ότι οι ανακαλύψεις των πανεπιστημιακών θα έπρεπε να αποτελούν υποσημείωση στην ιστορία της άκρως απόρρητης έρευνας, και οι αντίστοιχες του GCHQ υποσημείωση στην ιστορία της πανεπιστημιακής έρευνας. Ωστόσο, σε εκείνη τη φάση κανείς εκτός από το GCHQ, την NSA, τον Ντίφι και τον Χέλμαν δεν ήξερε τίποτε για την άκρως απόρρητη έρευνα, και έτσι η τελευταία δεν μπορούσε καν να θεωρηθεί υποσημείωση.

Στα μέσα της δεκαετίας του 1980, το κλίμα στο GCHQ άρχισε να αλλάζει, και η διοίκηση σκεφτόταν να ανακοινώσει δημόσια την εργασία των Έλις, Κοκς και Ουίλιαμσον. Τα μαθηματικά της κρυπτογραφίας δημοσίου κλειδιού είχαν ήδη καθιερωθεί στο δημόσιο τομέα, και φαινόταν ότι δεν υπήρχε κανένας λόγος να το κρατούν πλέον μυστικό. Αντίθετα, οι Βρετανοί θα είχαν σαφή οφέλη αν αποκάλυπταν το πρωτοποριακό έργο τους πάνω στην κρυπτογραφία δημοσίου κλειδιού.

Ο Πίτερ Ράιτ ήταν απόστρατος αξιωματικός των βρετανικών μυστικών υπηρεσιών, και η έκδοση των απομνημονευμάτων του με τίτλο «κυνηγός κατασκόπων» προκάλεσε μεγάλη αμηχανία στη βρετανική κυβέρνηση. Έτσι πέρασαν άλλα 13 χρόνια μέχρι το GCHQ να ανακοινώσει τελικά δημόσια τα επιτεύγματα του – 28 χρόνια μετά την αρχική ανακάλυψη του Έλις. Το 1997 ο Κλίφορντ Κοκς ολοκλήρωσε μια σημαντική, μη απόρρητη εργασία πάνω στο σύστημα RSA, η οποία θα

ενδιέφερε την ερευνητική κοινότητα και δεν θα αποτελούσε κίνδυνο για την ασφάλεια αν δημοσιευόταν. Ως αποτέλεσμα, του ζήτησαν να παρουσιάσει μια ανακοίνωση στο συνέδριο του Ινστιτούτου Μαθηματικών που θα γινόταν στο Σιρεντσέστερ. Η αίθουσα θα ήταν γεμάτη ειδικούς της κρυπτογραφίας. Μια χούφτα από αυτούς θα ήξεραν ότι ο Κοκς, που θα μιλούσε για μία μόνο πτυχή του RSA, ήταν στην πραγματικότητα ο αφανής εφευρέτης του. Υπήρχε ο κίνδυνος κάποιος να θέσει μια ενοχλητική ερώτηση του τύπου «Εσείς επινοήσατε το RSA;» Τι θα έπρεπε να κάνει τότε ο Κοκς; Σύμφωνα με την πολιτική του GCHQ, όφειλε να αρνηθεί το ρόλο του στην ανάπτυξη του RSA, και να αναγκαστεί έτσι να πει ψέματα για ένα θέμα που ήταν εντελώς αβλαβές. Η κατάσταση ήταν εντελώς γελοία, και το GCHQ αποφάσισε ότι ήταν πια καιρός να αλλάξει η πολιτική του. Έδωσε λοιπόν στον Κοκς την άδεια να αρχίσει την ομιλία του παρουσιάζοντας μια σύντομη ιστορία της συνεισφοράς του GCHQ στην κρυπτογραφία δημοσίου κλειδιού.

Στις 18 Δεκεμβρίου του 1997 ο Κοκς παρουσίασε την ανακοίνωση του. Ύστερα από τρεις σχεδόν δεκαετίες μυστικότητας, οι Έλις, Κοκς και Ουίλιαμσον κέρδισαν την αναγνώριση που τους άξιζε. Δυστυχώς, ο Τζέιμς Έλις είχε πεθάνει ένα μήνα πριν, στις 25 Νοεμβρίου 1997, σε ηλικία 73 ετών. Ο Έλις προστέθηκε στον κατάλογο των ειδικών της κρυπτογραφίας, των οποίων η συνεισφορά δεν αναγνωρίστηκε όσο ζούσαν. Το σπάσιμο του κρυπτογράμματος Βιζενέρ από τον Τσαρλς Μπάμπατζ δεν αποκαλύφθηκε ποτέ στη διάρκεια της ζωής του, επειδή η εργασία του ήταν ανεκτίμητης αξίας για τις βρετανικές δυνάμεις στην Κριμαία. Έτσι, όλη η αναγνώριση πήγε στον Φρίντριχ Καζίσκι. Με τον ίδιο τρόπο, η συμβολή του Άλαν Τιούρινγκ στην πολεμική προσπάθεια ήταν απαράμιλλη, και όμως η κυβερνητική μυστικότητα απαιτούσε να μην αποκαλυφθεί η εργασία του πάνω στο Αίνιγμα.

Το 1987, ο Έλις συνέταξε ένα απόρρητο έγγραφο που κατέγραφε τη συμβολή του στην κρυπτογραφία δημοσίου κλειδιού και το οποίο περιλάμβανε τις σκέψεις του για την μυστικότητα που τόσο συχνά περιβάλλει τι κρυπτογραφικό έργο: «Η κρυπτογραφία είναι μια άκρως ασυνήθιστη επιστήμη. Οι περισσότεροι επιστήμονες έχουν σαν στόχο τους να είναι οι πρώτοι που θα δημοσιεύσουν την εργασία τους, γιατί το έργο τους αποκτά αξία μέσω της διάδοσης. Αντίθετα, η κρυπτογραφία αποκτά τη μεγαλύτερη αξία της 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 τους έξω. Η αποκάλυψη αυτών των μυστικών συνήθως επιτρέπεται, στο όνομα της ιστορικής ακρίβειας, μόνον όταν έχει αποδειχθεί ότι η συνέχιση της μυστικότητας δεν μπορεί πια να αποφέρει κανένα όφελος.»

Κβαντικές Πύλες

➢ ΓΕΝΙΚΑ

Οι κλασικοί υπολογιστές αποτελούνται από αγωγούς και λογικές πύλες, οι οποίες συγκροτούν κυκλώματα. Οι αγωγοί μεταφέρουν την πληροφορία με τη μορφή τάσης ή ρεύματος από πύλη σε πύλη. Οι λογικές πύλες επεξεργάζονται και μετατρέπουν την πληροφορία που έρχεται στην είσοδό με τη μορφή τάσης ή ρεύματος από πύλη σε πύλη. Οι λογικές πύλες επεξεργάζονται και μετατρέπουν την πληροφορία που έρχεται στην είσοδό τους σύμφωνα με τον πίνακα αληθείας τους.

Οι λογικές πύλες στους κλασικούς υπολογιστές είναι φυσικά συστήματα κατασκευασμένα από πυρίτιο και αποτελούνται από τρανζίστορς.

Στους κβαντικούς υπολογιστές οι κβαντικές πύλες αντιπροσωπεύουν δράσεις που ασκούνται σε qubits ή σε κβαντικούς καταχωρητές. Οι δράσεις στα κβαντικά συστήματα αντιπροσωπεύονται από τελεστές οι οποίοι περιγράφονται από πίνακες. Μία άλλη σημαντική διαφορά είναι ότι η πληροφορία δε διέρχεται μέσα από τις κβαντικές πύλες. Η πληροφορία βρίσκεται αποθηκευμένη σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί. Στους κβαντικούς υπολογιστές το κάθε qubit χαρακτηρίζεται από υπέρθεση της κατάστασης |0> και |1>. Η κβαντική πύλη θα είναι ένα είδος κυκλώματος, το οποίο πραγματοποιεί πράξεις σε qubits για κάποιο χρονικό διάστημα, ενώ σε αντίθεση με τις κλασικές, είναι πάντα αντιστρεπτές άρα θα έχουν τον ίδιο αριθμό εισόδων και εξόδων.

➢ ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ

- Κβαντική πύλη αδράνειας.
- Κβαντική πύλη μετατόπισης φάσης
- Κβαντική πύλη Hadamard
- Κβαντική πύλη ελεγχόμενης άρνησης(CNOT)
- Κβαντική πύλη ελεγχόμενης μετατόπισης φάσης
- Κβαντική πύλη διπλά ελεγχόμενης άρνησης(CCNOT)
- Κβαντική πύλη Fredkin

ΤΑ qubits

➢ ΓΕΝΙΚΑ

Η επιστήμη της κβαντικής πληροφορίας αρχίζει με τη γενίκευση του μπιτ, που είναι η θεμελιώδης πηγή της κλασσικής πληροφορίας, στο κβαντικό bit ή απλά qubit. Όπως τα bits είναι ιδεατά αντικείμενα, που έχουν αποκοπεί από τις αρχές της κλασσικής φυσικής, έτσι και τα qubits είναι ιδεατά κβαντικά αντικείμενα αποκομμένα από τις αρχές της κβαντικής μηχανικής.

Τα bits μπορούν να παρασταθούν με περιοχές μαγνήτισης δίσκων, ηλεκτρικές τάσεις σε κυκλώματα, ή ακόμη και με σημάδια από μολύβι πάνω στο χαρτί. Η λειτουργία αυτών των κλασσικών φυσικών καταστάσεων ως μπιτς, δεν εξαρτάται από τις λεπτομέρειες πως τα παραστήσαμε. Παρόμοια οι ιδιότητες ενός qubit, είναι ανεξάρτητες από τη συγκεκριμένη φυσική του αναπαράσταση π.χ. ως κάποιου σπιν ενός ατομικού πυρήνα ή ως πόλωση ενός φωτονίου.

Ένα bit περιγράφεται από την κατάστασή του 0 ή 1. Παρόμοια, ένα qubit περιγράφεται από την κβαντική του κατάσταση. Δύο διαφορετικές δυνατές καταστάσεις για ένα qubit, αντιστοιχούν στο 0 και στο 1 ενός κλασσικού μπιτ. Στην κβαντομηχανική όμως κάθε αντικείμενο που έχει δύο διαφορετικές καταστάσεις έχει αναγκαστικά και μια περιοχή ολόκληρη άλλων καταστάσεων, που λέγονται υπερθέσεις και οι οποίες περιέχουν τις αρχικές δύο καταστάσεις κατά ένα μεταβλητό ποσοστό την κάθε μια.

Οι επιτρεπόμενες καταστάσεις ενός qubit είναι κατ' αρχήν όλες εκείνες οι καταστάσεις που είναι διαθέσιμες για ένα μπιτ, το οποίο εμφυτεύεται σε έναν κβαντικό κόσμο. Οι καταστάσεις του qubit αντιστοιχούν σε σημεία επί της επιφανείας μιας σφαίρας, όπου το 0 και το 1 είναι ο Νότιος και Βόρειος πόλος της.

Η συνέχεια της περιοχής της σφαίρας μεταξύ των καταστάσεων 0 και 1, δημιουργεί πολλές από τις παράδοξες ιδιότητες της κβαντικής πληροφορίας.

Πόση κλασσική πληροφορία μπορεί ν' αποθηκευτεί σε ένα qubit; Κάποια επιχειρήματα δείχνουν ότι η ποσότητα της πληροφορίας είναι άπειρη: Για να καθορίσουμε μια κβαντική κατάσταση χρειάζεται να καθορίσουμε το "πλάτος" και "μήκος" του αντίστοιχου σημείου επί της σφαίρας και τουλάχιστον κατ' αρχήν αυτό μπορεί να γίνει με όσο μεγάλη ακρίβεια θέλουμε.

Οι αριθμοί αυτοί μπορούν να κωδικοποιήσουν μια μεγάλου μήκους ακολουθία ψηφίων. Για παράδειγμα η σειρά 011101101... μπορεί να κωδικοποιηθεί ως μια κατάσταση με πλάτος 01 μοίρες, 11 πρώτα λεπτά, και 01,101 δεύτερα λεπτά της μοίρας.

Το επιχείρημα αυτό αν και ακούγεται εύλογο είναι λανθασμένο. Μπορεί πράγματι κάποιος να κωδικοποιήσει άπειρη ποσότητα πληροφορίας σε ένα qubit, αλλά δεν μπορεί ποτέ να ανακτήσει όλη αυτή την πληροφορία από το qubit.

Η πιο απλή προσπάθεια να διαβάσει την κατάσταση του qubit με μια μέτρησή του, θα δώσει ως αποτέλεσμα είτε 0 είτε 1, (Νότιο ή Βόρειο πόλο), με την πιθανότητα για οποιοδήποτε εξαγόμενο να καθορίζεται από το πλάτος της αρχικής κατάστασης.

Θα μπορούσατε ίσως να επιλέξετε μια διαφορετική μέτρηση, χρησιμοποιώντας πιθανόν τον άξονα "Μελβούρνη-Αζόρες" αντί για "Βόρειο-Νότιο", αλλά και πάλι μόνο ένα μπιτ πληροφορίας θα ήταν το εξαγόμενο. Το εξαγόμενο αυτό θα εξαρτιόταν και πάλι από τις πιθανότητες που θα καθόριζαν και πάλι το πλάτος και μήκος της κατάστασης στο νέο σύστημα συντεταγμένων. Όποια μέτρηση και αν επιλέξουμε, σβήνεται όλη η πληροφορία του qubit, εκτός από το απλό μπιτ που αποκαλύπτει η μέτρηση.

Οι αρχές της κβαντικής μηχανικής μας εμποδίζουν να εξάγουμε περισσότερο από ένα μόνο μπιτ πληροφορίας, άσχετα από το πόσο έξυπνα έχουμε κωδικοποιήσει το qubit ή πόσο έξυπνα κάνουμε τη μέτρησή μας.

Το εκπληκτικό αυτό αποτέλεσμα αποδείχτηκε το 1973 από τον Alexander S. Holevo του Μαθηματικού Ινστιτούτου του Steklov στη Μόσχα, μετά από μια εικασία που είχε διατυπώσει το 1964 ο J. P. Gordon των εργαστηρίων AT&T Bell.

Είναι σαν το qubit να περιέχει κρυμμένη πληροφορία, την οποία μπορούμε μεν να χειριστούμε αλλά δεν μπορούμε να έχουμε κατευθείαν πρόσβαση σ' αυτή. Μια καλύτερη αντιμετώπιση είναι όμως να θεωρήσουμε αυτή την κρυμμένη πληροφορία σα να είναι μια μονάδα κβαντικής πληροφορίας μάλλον, παρά μια άπειρη ακολουθία από κλασσικά bits στα οποία δεν έχουμε πρόσβαση.

ΑΛΓΟΡΙΘΜΟΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ ΤΟΥ SHOR

➢ ΓΕΝΙΚΑ

Το 1994 ο Peter Shor απέδειξε ότι με τη χρήση κβαντικών υπολογιστών μπορεί εύκολα και γρήγορα να αναλυθούν σε γινόμενο δύο πρώτων αριθμών μεγάλοι ακέραιοι αριθμοί. Με έναν κβαντικό υπολογιστή απαιτείται πολυωνυμική αύξηση του χρόνου υπολογισμού για γραμμική αύξηση του μεγέθους n, δηλαδή του αριθμού των ψηφίων του αριθμού που έχει δύο πρώτους παράγοντες. Οι γρηγορότεροι κλασικοί αλγόριθμοι για το ίδιο πρόβλημα είναι υπερ-πολυωνυμικοί σε συνάρτηση με τον αριθμό ψηφίων n. Η μέθοδος που πρότεινε ο Shor είναι γνωστή ως «κβαντικός αλγόριθμος του Shor». Είναι ένας κβαντικός αλγόριθμος παραγοντοποίησης ενός ακεραίου αριθμού N, που πραγματοποιείται σε χρόνο O (log N)^3 & διάστημα O (log N).

Η μέθοδος κρυπτογράφησης δημοσίου κλειδιού – RSA – χρησιμοποιεί ένα δημόσιο κλειδί, έστω N, το οποίο είναι το γινόμενο δύο πρώτων αριθμών (για πρακτικούς λόγους διαλέγω πολύ μεγάλους αριθμούς!). Ένας γνωστός τρόπος για να σπάσει ο κώδικας αυτός είναι η παραγοντοποίηση του N. Δεδομένου ότι το N είναι ένας πολύ μεγάλος αριθμός με πολλά πολλά ψηφία (ως γινόμενο των πολύ μεγάλων αριθμών που παραπάνω διαλέξαμε) , με τους κλασικούς αλγόριθμους, η διαδικασία της παραγοντοποίησης, απαιτεί πολύ χρόνο, πολύ μεγαλύτερο από το χρόνο (log N). Από την άλλη πλευρά, οι πιθανοτικοί αλγόριθμοι (περιλαμβάνει πολλούς αλγόριθμους κβαντικής κρυπτογραφίας όπως τον αλγόριθμο του Σορ), δίνουν τη σωστή απάντηση σε χρόνο περίπου (log N) και με τη σταθερή οριακή πιθανότητα. Με την εκτέλεση του αλγορίθμου πολλές φορές, η σωστή απάντηση μπορεί να βρεθεί με εκθετικά μικρό λάθος.

Το πρόβλημα που προσπαθούμε να λύσουμε είναι δεδομένου του N, ψάχνουμε να βρούμε τον ακέραιο αριθμό n, μεταξύ 1 και N, που να διαιρεί το N.

Ο αλγόριθμος του Σορ αποτελείται από δύο μέρη:

1. Μείωση του προβλήματος παραγοντοποίησης στο πρόβλημα της εύρεσης της περιόδου.
2. Εύρεση της περιόδου.

Το πρώτο μέρος μπορεί να εκτελεστεί και από έναν απλό κλασικό υπολογιστή , ενώ το δεύτερο μόνο από κβαντικό υπολογιστή με τη βοήθεια του κβαντικού μετασχηματισμού Fourier.

➢ ΚΛΑΣΙΚΟ ΚΟΜΜΑΤΙ

Το κλασικό μέρος μπορεί να χωριστεί σε 7 βήματα:

1. Επιλέγουμε έναν τυχαίο αριθμό , έστω α, για τον οποίο ισχύει α<N.
2. Υπολογίζουμε τον Μέγιστο Κοινό Διαιρέτη των δύο αριθμών.
3. Αν ο ΜΚΔ (α, N) ≠ 1, τότε έχουμε βρει έναν παράγοντα του N.
4. Αν ο ΜΚΔ (α, N) = 1, τότε βρίσκουμε την περίοδο r της συνάρτησης
   $$f(x)=a^x \bmod N$$
   Δηλαδή το μικρότερο ακέραιο αριθμό r για τον οποίο ισχύει f(x+r)=f(x).
5. Αν το r είναι περιττός, τότε επιστρέφουμε στο βήμα 1.
6. Αν $\alpha^{r/2} \equiv (-1 \bmod N)$, τότε επιστρέφουμε στο βήμα 1.
7. Ο ΜΚΔ $(\alpha^{r/2} \pm 1, N)$ είναι ο αριθμός που παραγοντοποιεί το N.

➢ ΚΒΑΝΤΙΚΟ ΚΟΜΜΑΤΙ

Τα κομμάτι αυτό είναι η υπορουτίνα εύρεσης περιόδου.

Τα κβαντικά κυκλώματα που χρησιμοποιούνται είναι σχεδιασμένα για κάθε τυχαία επιλογή N που βασίζεται στη συνάρτηση $f(x)=a^x \bmod N$. Γνωρίζοντας το N, υπολογίζουμε το Q, όπου $Q= 2^q$, τέτοιο ώστε $N^2 \leq Q \leq 2N^2$. Αυτό συνεπάγεται ότι Q/r > N. Οι κατάλογοι εισαγωγής και εξαγωγής qubits, θα κρατήσουν τις υπερθέσεις των τιμών από το 0 έως το Q-1, έτσι ώστε το καθένα να έχει q qubits. Υπάρχει το ενδεχόμενο κάποια πράγματα να εμφανιστούν δύο φορές, για να αποφευχθεί η κβαντική αποσυνοχή και γιατί υπάρχουν N διαφορετικά x, που παράγουν την ίδια f(x), ακόμη και όταν $r \rightarrow N/2$.

Το κβαντικό μέρος μπορεί να χωριστεί σε 8 βήματα:

1. Γράφουμε τους καταλόγους με τη μορφή
   $$Q^{-1/2} \Sigma \mid x> \mid 0>$$

όπου το x παίρνει τιμές από 0 ,έως Q-1. Αυτή η κατάσταση είναι μια υπέρθεση Q καταστάσεων.

2. Κατασκευάζουμε την f(x), την εφαρμόζουμε στην παραπάνω κατάσταση και έχουμε
$$Q^{-1/2}\sum | x> | f(x)>$$

3. Εφαρμόζουμε τον κβαντικό μετασχηματισμό Fourier στον κατάλογο εισαγωγής. Ο μετασχηματισμός αυτός λειτουργεί με την υπέρθεση $Q=2^q$ καταστάσεων και χρησιμοποιεί την $Q^{οστή}$ ρίζα της μονάδας που είναι $\omega = e^{2\pi i/Q}$ για να κάνει τη διανομή οποιασδήποτε κατάστασης $| x>$ ίση απέναντι σε όλα τα Q των $| y>$ καταστάσεων, και το κάνει με διαφορετικό τρόπο για κάθε x: $U_{QFT} | x> = Q^{-1/2} \sum \omega^{xy} | y>$. Αυτό οδηγεί στην τελική κατάσταση $Q^{-1} \sum\sum \omega^{xy} | y> | f(x)>$, που είναι μια υπέρθεση μεταξύ $Q - Q^2$ καταστάσεων. Η κατάσταση $| y > | f(x_o) >$ μπορεί να παραγοντοποιηθεί ακόμα και όπου τα x και x_o έχουν την ίδια τιμή. Δεδομένου ότι το $\omega = e^{2\pi i/Q}$ είναι η $Q^{οστή}$ ρίζα της μονάδας, το r είναι η περίοδος της συνάρτησης f, το x_o είναι το μικρότερο από τα x που παράγονται από την f(x) ($x_o < r$), το b κινείται από το 0 έως το $[(Q- x_o-1)/ r]$, έτσι ώστε $x_o+ r b < q$. Το ω^{ry} είναι ένα μοναδιαίο διάνυσμα στο μιγαδικό επίπεδο, αφού το ω είναι ρίζα της μονάδας και τα r , y είναι ακέραιοι αριθμοί, και ο συντελεστής $Q^{-1} | y> | f(x_o)>$ στην τελική κατάσταση είναι : $\sum \omega^{xy} = \sum \omega^{(xo+rb)y} = \omega^{xoy} \sum\omega^{rby}$ όπου $x= f(x)-f(x_o)$. Κάθε όρος του αθροίσματος αποτελεί μια μερική λύση του αποτελέσματος. Όταν τα μοναδιαία διανύσματα ω^{rby} κινούνται στο μιγαδικό επίπεδο με την κατεύθυνση του θετικού πραγματικού άξονα, τότε γίνεται αντιληπτή ή κβαντική παρέμβαση.

4. Κάνουμε μια μέτρηση. Έτσι έχουμε ένα αποτέλεσμα y για τον κατάλογο εισαγωγής και ένα αποτέλεσμα $f(x_o)$ για τον κατάλογο εξαγωγής. Δεδομένου ότι η f(x) είναι περιοδική, η πιθανότητα μέτρησης του ζευγαριού $y - f(x_o)$ δίνεται από τη σχέση $| Q^{-1}\sum\omega^{xy} |^2 = Q^{-2} | \sum \omega^{(xo+rb)y} |^2$.

5. Από την παραπάνω ανάλυση προκύπτει ‘ότι το yr/Q είναι κοντά σε έναν ακέραιο αριθμό. Το μετατρέπουμε σε άρρητο. Στη συνέχεια ονομάζουμε τον παρανομαστή r′ και θεωρούμε ότι είναι ένα πιθανό r.

6. Αν ισχύει $f(x) = f(x+r')$, η διαδικασία έχει ολοκληρωθεί με επιτυχία.

7. Αν δεν ισχύει τότε δοκιμάζουμε για άλλες πιθανές τιμές του r. Οι τιμές αυτές είναι τιμές κοντά στο y και στα πολλαπλάσια του r′ . Αν επαληθευτεί η σχέση, τότε η διαδικασία έχει ολοκληρωθεί με επιτυχία.

8. Αν δεν φανούμε τυχεροί με τα πιθανά r, τότε επιστρέφουμε στο βήμα 1.

➢ ΕΠΕΞΕΡΓΑΣΙΑ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ

❖ ΚΛΑΣΙΚΟ ΚΟΜΜΑΤΙ

Οι ακέραιοι που είναι μικρότεροι του N και ταυτόχρονα πρώτοι αριθμοί, σχηματίζουν ένα πεπερασμένο σύνολο με πρωτεύουσα πράξη τον πολλαπλασιασμό modulo N.

Μετά το βήμα 3 εμφανίζεται ο ακέραιος α στην υποομάδα. Αν αυτή η ομάδα είναι πεπερασμένη, τότε το α έχει πεπερασμένο όριο το r. Ο μικρότερος δυνατός ακέραιος για τον οποίο ισχύει αυτό είναι ο $\alpha^r \equiv 1 \mod N$.

Έστω ότι μπορούμε να βρούμε το r, το οποίο είναι άρτιο. Τότε $\alpha^r-1 = (\alpha^{r/2}-1)(\alpha^{r/2}+1) \equiv 0 \mod N$.

Το r είναι ο μικρότερος θετικός ακέραιος για τον οποίο $\alpha^r \equiv 1$.

Το N δεν μπορεί να διαιρέσει το $(\alpha^{r/2}-1)$.

Αν το N δεν μπορεί να διαιρέσει ούτε το $(\alpha^{r/2}+1)$, τότε το N έχει έναν τετριμμένο κοινό παράγοντα με καθένα από αυτά.

❖ ΚΒΑΝΤΙΚΟ ΚΟΜΜΑΤΙ

Ο αλγόριθμος του Σορ, για να υπολογίσει την περίοδο, στηρίζεται στην υπέρθεση δύο ή περισσότερων καταστάσεων. Για τον υπολογισμό της περιόδου μιας συνάρτησης f(x), γίνεται ταυτόχρονος υπολογισμός σε όλα τα σημεία της ταυτόχρονα.

Η κβαντική μηχανική δεν επιτρέπει τον ταυτόχρονο υπολογισμό. Μια μέτρηση οδηγεί σε μια και μόνο πιθανή τιμή, οι υπόλοιπες καταστρέφονται. Για την αποφυγή αυτού του προβλήματος, θα μετρήσουμε πρώτα την f(x) χωρίς να μετρήσουμε το x. Στη συνέχεια θα κάνουμε κάποια αντίγραφα της κατάστασης, τα οποία στην πραγματικότητα αποτελούν την υπέρθεση των καταστάσεων που έχουν την ίδια f(x). Μετρώντας το x, βρίσκουμε διαφορετικές τιμές για κάθε x που αντικαθιστούμε στην f(x), γεγονός που οφείλεται στην περιοδικότητα της συνάρτησης. Επειδή όμως, δεν είναι δυνατή η ακριβής αντιγραφή μιας κβαντικής κατάστασης, η μέθοδος αυτή δεν έχει αποτέλεσμα.

Η λύση στο παραπάνω πρόβλημα είναι ο μετασχηματισμός της υπέρθεσης σε μια άλλη κατάσταση, η οποία θα μας δώσει με

μεγαλύτερη ακρίβεια τη σωστή απάντηση. Εργαλείο μας είναι ο κβαντικός μετασχηματισμός Fourier.

➢ ΠΡΟΒΛΗΜΑΤΑ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ

Ο Σορ έπρεπε να αντιμετωπίσει 3 προβλήματα εφαρμογής. Όλα τους έπρεπε να εφαρμοστούν γρήγορα, δηλ μπορούν να εφαρμοστούν σε διάφορες κβαντικές πύλες.

1. Δημιουργία υπέρθεσης καταστάσεων. Μπορεί να γίνει με την εφαρμογή των πυλών Hadamard σε όλα τα qubits στον κατάλογο εισαγωγής. Μια εναλλακτική προσέγγιση, είναι η χρήση του κβαντικού μετασχηματισμού Fourier..

2. Εφαρμογή της συνάρτησης f(x) σαν κβαντική μετατροπή. Για να το επιτύχει χρησιμοποίησε επαναλαμβανόμενη τετραγωνοποίηση για τον εκθετικό μετασχηματισμό.

3. Εκτέλεση του κβαντικού μετασχηματισμού Fourier. Χρησιμοποιώντας τις ελεγχόμενες πύλες περιστροφής και τις πύλες Hadamard, ο Σορ σχεδίασε ένα κύκλωμα για τον κβαντικό μετασχηματισμό Fourier ($Q = 2^q$) που χρησιμοποιεί $q(q-1)/2 = O((\log Q)^2)$ πύλες.

Όλοι αυτοί οι μετασχηματισμοί βοηθούν στην προσέγγιση της περιόδου r. Για να διευκολύνουμε την διαδικασία, υποθέτουμε ότι υπάρχει ένα y τέτοιο ώστε yr/Q να είναι ακέραιος. Παρατηρούμε ότι $e^{-2\pi i byr/Q} = 1$, για όλους τους ακέραιους b. Επομένως το άθροισμα του οποίου το τετράγωνο μας δίνει την πιθανότητα στο μέτρο y θα είναι Q/r, δεδομένου ότι το b παίρνει τιμές κατά προσέγγιση Q/r και έτσι η πιθανότητα είναι $1/r^2$. Υπάρχει ry τέτοιο ώστε το yr/Q να είναι ακέραιος και υπάρχουν r πιθανότητες για το $f(x_o)$, ώστε το άθροισμα όλων αυτών να είναι 1.

ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΒΕΛΤΙΩΝΟΥΝ ΤΗΝ ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

➢ ΓΕΝΙΚΑ

Μια ομάδα επιστημόνων των εργαστηρίων στο Los Alamos, σε συνεργασία με ερευνητές από το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας και το Κολέγιο Albion, πέτυχε την διανομή κβαντικού κλειδιού (QKD) σε μήκος κύματος 1.550 nm μέσω μιας οπτικής ίνας μήκους 50 χιλιομέτρων. Η εργασία αυτή θα μπορούσε να επιταχύνει την ανάπτυξη QKD για ασφαλείς επικοινωνίες στις οπτικές ίνες σε αποστάσεις πέρα από τα σημερινά τεχνολογικά όρια.

Στην έρευνα που δημοσιεύθηκε στο Applied Physics Letters, η ομάδα περιγράφει τη χρήση των νέων υπεραγωγικών αισθητήρων (TES) για να διανείμει το κρυπτογραφικό κλειδί σε μήκη κύματος 1.550 nm μέσω μιας οπτικής ίνας 50 χιλιομέτρων. Οι TES θα μπορούσαν να αυξήσουν το εύρος και την απόδοση πέρα από τα σημερινά επίπεδα ανίχνευσης των φωτονίων στην QKD. Αντίθετα από τις ευαίσθητες φωτοδιόδους ενός φωτονίου (APD) που χρησιμοποιούνται σήμερα στα συστήματα οπτικών ινών στα συστήματα QKD, οι αισθητήρες TES ανιχνεύουν τα φωτόνια μετρώντας μικρές αυξήσεις της θερμοκρασίας σε ένα υπεραγωγικό υλικό που προκαλείται από την απορρόφηση των μεμονωμένων φωτονίων.

Η κβαντικός φυσικός Danna Rosenberg του Los Alamos λέει ότι οι TES δίνουν σημαντικά υψηλότερες αποδοτικότητες ανίχνευσης ενός μόνου φωτονίου και χαμηλότερους ρυθμούς σκοτεινής αρίθμησης από τις προηγούμενες φωτοδιόδους APD. Η υψηλή αποδοτικότητα και η χαμηλή πιθανότητα σκοτεινών αριθμήσεων, που συνδέονται με το σχετικά σύντομο χρόνο αποκατάστασης των νέων αισθητήρων TES, θα επιτρέψουν υψηλότερους ρυθμούς μετάδοσης μυστικών κλειδιών σε ακόμα μεγαλύτερες αποστάσεις από τα σημερινά συστήματα τα βασισμένα στις παλαιές φωτοδιόδους APD."

Εκτός από την υιοθέτηση των TES, η ομάδα πειραματίστηκε με φωτεινό οπτικό παλμό και ηλεκτρικούς μηχανισμούς συγχρονισμού σημάτων. Μια μέθοδος του συγχρονισμού περιλάμβανε την αποστολή ενός φωτεινού παλμού 1.310 nm αμέσως πριν σταλεί ένας παλμός 1.550 nm. Χρησιμοποιήθηκε ένας φωτεινός παλμός για να μειώσει τα λάθη της μετάδοσης που μπορεί να εμφανιστούν λόγω της αλλαγής στο μήκος ή τις οπτικές ιδιότητες της ίνας σύνδεσης. Χρησιμοποιήθηκε δε ένας μηχανισμός συγχρονισμού με ένα ατομικό ρολόι ρουβιδίου για να συγχρονίσει τους αποστολείς και τους δέκτες πληροφοριών.

Όταν χρησιμοποιούνται με ηλεκτρικούς μηχανισμούς συγχρονισμού, οι νέοι αισθητήρες TES έχουν τη δυνατότητα να αυξήσουν τις αποστάσεις για τις οποίες θα μπορούσαν να χρησιμοποιηθούν οι οπτικές ίνες στην διανομή κβαντικού κλειδιού. Αν χρησιμοποιήσουμε το τρέχον σύστημα, οι μέγιστες αποστάσεις μετάδοσης για στοιχεία με φωτεινό παλμό και ηλεκτρικό συγχρονισμό είναι 83 χιλιόμετρα και 138 χιλιόμετρα, αντίστοιχα. Πιο περίπλοκες μέθοδοι με φιλτράρισμα φωτονίων από ό,τι χρησιμοποίησαν οι πειραματιστές, κάποια μέρα μπορεί να επιτρέψουν στους χρήστες να στείλουν κβαντικά κλειδιά ασφαλώς σε αποστάσεις παραπάνω από 270 χιλιόμετρα, έναντι του σημερινού των 122 χιλιομέτρων.

Επί του παρόντος, η κβαντική κρυπτογραφία χρησιμοποιείται σε γεωγραφικώς περιορισμένα δίκτυα. Το βασικό πλεονέκτημα της τεχνικής — ότι όποιος υποκλέπτει τη μετάδοση ενός κλειδιού το μεταβάλλει ταυτόχρονα κατά μη αναστρέψιμο τρόπο — σημαίνει επίσης ότι το σήμα που μεταφέρει κβαντικά κλειδιά δεν μπορεί να ενισχυθεί από τον εξοπλισμό του δικτύου που αντισταθμίζει την εξασθένηση του σήματος και του επιτρέπει να φτάσει μέχρι τον επόμενο επαναλήπτη. Ένας οπτικός ενισχυτής θα αλλοίωνε τα q-μπιτ.

Προκειμένου να μεγαλώσουν την εμβέλεια αυτών των ζεύξεων, οι ερευνητές αναζητούν μέσα διάδοσης για τη διανομή των κβαντικών κλειδιών ικανοποιητικότερα από τις οπτικές ίνες. Οι επιστήμονες ανέβηκαν σε βουνοκορφές — όπου το υψόμετρο ελαχιστοποιεί τις ατμοσφαιρικές αναταράξεις — για να αποδείξουν ότι η αποστολή φωτονίων διαμέσου του αέρα αποτελεί εφαρμόσιμη λύση. Ένα τέτοιο πείραμα που έγινε το 2002 στο Εθνικό Εργαστήριο του Λος Άλαμος δημιούργησε μια ζεύξη μήκους 10 χιλιομέτρων. Και ένα άλλο, το οποίο πραγματοποιήθηκε τον ίδιο χρόνο από την Βρετανική QinetiQ και το Πανεπιστήμιο Ludwig Maximilian του Μονάχου έζευξε με επιτυχία δύο βουνοκορφές στις νότιες Άλπεις που απείχαν 23 χιλιόμετρα.

Με τη βελτίωση της τεχνολογίας αυτής — με τη χρησιμοποίηση μεγαλύτερων τηλεσκοπίων για ανίχνευση, καλύτερων φίλτρων και αντανακλαστικών επικαλύψεων — πιθανώς να καταστεί δυνατόν να κατασκευαστεί ένα σύστημα ικανό να εκπέμπει και να λαμβάνει σήματα σε αποστάσεις μεγαλύτερες των 1.000 χιλιομέτρων. Τέτοια εμβέλεια επαρκεί για να επιτευχθεί η επικοινωνία με δορυφόρους που περιφέρονται γύρω από τη Γη σε χαμηλή τροχιά. Ένα δίκτυο από τέτοιους δορυφόρους θα επέτρεπε την επικοινωνία σε παγκόσμιο επίπεδο.

Η Ευρωπαϊκή Υπηρεσία Διαστήματος βρίσκεται στα αρχικά στάδια της εκπόνησης ενός σχεδίου για την επίτευξη πειραματικής επικοινωνίας μεταξύ εδάφους και δορυφόρου. Επίσης, η Ευρωπαϊκή Ένωση ξεκίνησε τον Απρίλιο του 2004 μια προσπάθεια για να αναπτύξει την κβαντική κρυπτογράφηση σε δίκτυα επικοινωνιών, προσπάθεια στην

οποία εν μέρει παρακίνησε η επιθυμία να αντιμετωπιστεί η κατασκοπευτική δραστηριότητα του Echelon, ενός συστήματος που υποκλέπτει ηλεκτρονικά μηνύματα για λογαριασμό των υπηρεσιών πληροφοριών των ΗΠΑ, της Βρετανίας και άλλων κρατών.

Πριν λίγα χρόνια η id Quantique και μια συνεργαζόμενη εταιρεία, ο παροχέας υπηρεσιών πληροφοριών Deckpoint που εδρεύει στη Γενεύη, παρουσίασαν ένα δίκτυο το οποίο επέτρεπε σε μια συστοιχία διακομιστών στη Γενεύη να αποθηκεύει τα αντίγραφα ασφαλείας της σε απόσταση 10 χιλιομέτρων, με τα νέα κλειδιά να διανέμονται μέσω μιας ζεύξης προστατευμένης με αλγορίθμους κβαντικής κρυπτογραφίας.

Η κβαντική κρυπτογραφία δεν αποκλείεται να αποδειχτεί ευάλωτη σε ορισμένες ανορθόδοξες μορφές προσβολής. Ο υποκλοπέας θα μπορούσε, για παράδειγμα, να σαμποτάρει τους ανιχνευτές του αποδέκτη έτσι ώστε τα ληφθέντα q-μπιτ να διαρρεύσουν στην οπτική ίνα δια της οποίας μεταδόθηκαν και να υποκλαπούν. Και φυσικά, η υποκλοπή με βοήθεια εκ των έσω θα αποδεικνύεται πάντα αναπότρεπτη.

«Η προδοσία είναι η κύρια μέθοδος» παρατηρεί ο Seth Lloyd, ειδικός στον τομέα της κβαντικής πληροφορικής του Τεχνολογικού Ινστιτούτου της Μασαχουσέτης. «Η κβαντική μηχανική δεν μπορεί να κάνει απολύτως τίποτα σε αυτή την περίπτωση». Παρά ταύτα, στην ανατέλλουσα εποχή της κβαντικής πληροφορίας, τούτοι οι νέοι τρόποι για την τήρηση των μυστικών φαίνεται πως θα αποδειχτούν καλύτεροι από οτιδήποτε άλλο μπορεί να βρει κανείς στα βιβλία κρυπτογραφίας.

ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΚΒΑΝΤΟΜΗΧΑΝΙΚΗ

➢ ΓΕΝΙΚΑ

Πόσο ασφαλείς είναι οι επικοινωνίες μας; Για πόσο καιρό θα είμαστε μάρτυρες υποκλοπών τόσο σε εθνικό όσο και σε προσωπικό επίπεδο; Υπάρχει λύση στο πρόβλημα της ασφάλειας; Η κβαντική κρυπτογραφία είναι η πιο υποσχόμενη μέθοδος για αυτό το θέμα και η ανάπτυξη της είναι η πρόκληση των καιρών.

Η κβαντομηχανική έχει αλλάξει τη μορφή του κόσμου μας. Το τρανζίστορ, το λέιζερ, η υπεραγωγιμότητα, η ατομική βόμβα, είναι πρώιμες εφαρμογές της θεωρίας και είναι μερικές μόνο από αυτές που άλλαξαν τη μορφή του κόσμου μας. Το τρανζίστορ έκανε δυνατή μια δραματική αύξηση στην υπολογιστική μας ισχύ. Παρόλα αυτά, αν υπάρχει αρκετός διαθέσιμος χρόνος και η πρώτη υπολογιστική μηχανή με γρανάζια του Charles Babbage θα μπορούσε να κάνει τους ίδιους υπολογισμούς. Κατά βάθος, οι σύγχρονες υπολογιστικές μηχανές μας είναι κλασσικές συσκευές. Θα μπορούσαν λοιπόν κάποια γνήσια κβαντικά φαινόμενα να τιθασευτούν για υπολογιστικούς σκοπούς;

Για πολλά χρόνια, οι μαθηματικοί έψαχναν για ένα σύστημα που θα επέτρεπε σε δύο ανθρώπους να ανταλλάσσουν πληροφορίες με απόλυτη ασφάλεια. Στη δεκαετία του ‘40 ο Claude Shannon απέδειξε ότι αυτός ο στόχος είναι ανέφικτος, εκτός κι αν τα δύο μέρη που επικοινωνούν μοιράζονται ένα τυχαίο μυστικό κλειδί, το οποίο έχει τόσο μήκος όσο και το μήνυμα που θέλουν να ανταλλάξουν. Επιπλέον, αυτό το μυστικό κλειδί μπορεί να χρησιμοποιηθεί μόνο μια φορά.

Στην κβαντική κρυπτογραφία όμως, αυτό το απαισιόδοξο θεώρημα μπορεί να ξεπεραστεί αν εκμεταλλευτούμε τόσο την αδυναμία να μετρηθεί με ακρίβεια η κβαντική πληροφορία όσο και την διαταραχή που προκαλείται αναπόφευκτα από τέτοιες μετρήσεις. Όταν η πληροφορία κωδικοποιείται κατάλληλα σε κβαντικές καταστάσεις, κάθε προσπάθεια από κάποιον να αποκτήσει πρόσβαση σ' αυτήν, περιέχει αναγκαστικά την πιθανότητα να καταστραφεί ανεπανόρθωτα η πληροφορία. Η διαταραχή αυτή μπορεί ν' ανιχνευτεί από τους νόμιμους χρήστες της, επιτρέποντας έτσι την εγκατάσταση μιας ασφαλούς σύνδεσης χωρίς την προϋπόθεση να μοιράζονται ένα κοινό μυστικό κλειδί.

Είναι ενδιαφέρον να σημειώσουμε ότι οι κβαντικοί υπολογιστές απειλούν τα περισσότερα από τα κλασσικά κρυπτογραφικά σχήματα που είναι εν χρήσει σήμερα, αλλά η κβαντική κρυπτογραφία προσφέρει μια ασφαλή εναλλακτική λύση χωρίς προϋποθέσεις.

Ο πιο προφανής σκοπός της κρυπτογραφίας ήταν πάντα η ασφαλής μεταβίβαση εμπιστευτικών πληροφοριών. Κατά τις τρεις όμως προηγούμενες δεκαετίες, γνωρίσαμε την ανάπτυξη νέων εφαρμογών για τις τεχνικές της κρυπτογραφίας, όπως είναι η ψηφιακή υπογραφή και η ασφαλής επεξεργασία μιας πληροφορίας από πολλούς ανθρώπους συγχρόνως. Παρόλα αυτά, όλες αυτές οι κλασσικές έννοιες μπορούν να νικηθούν αν κάποιοι διαθέτουν απεριόριστη υπολογιστική ισχύ. Συν τοις άλλοις, οι περισσότερες από τις προτεινόμενες βελτιώσεις δεν μπορούν να αντισταθούν σε επιθέσεις κβαντικών υπολογιστών. Μετά την επιτυχία της κβαντικής κρυπτογραφίας στην ασφαλή επικοινωνία, ήταν φυσικό να ελπίζουμε ότι οι κβαντικές τεχνικές θα μας βοηθούσαν και στην ανάπτυξη ασφαλών πρωτοκόλλων χωρίς τρωτά σημεία γι αυτές τις πιο εξεζητημένες εργασίες.

Μια από τις πιο απλές εργασίες είναι γνωστή ως "δέσμευση των bit" - μια μάλλον αφηρημένη αλλά μεγάλης σημασίας ιδέα για την επίτευξη των κρυπτογραφικών σκοπών. Σ' ένα σχήμα "δέσμευσης των bits", ένα πρόσωπο (ας το πούμε Αλίκη), καταγράφει και φυλάσσει ένα bit, στέλνοντας κάτι σ' ένα άλλο πρόσωπο (ας τον πούμε Μπομπ). Αργότερα η Αλίκη μπορεί να αποκαλύψει το τι είχε δεσμεύσει, αφήνοντας έτσι τον Μπομπ να μάθει τι ήθελε να μεταδώσει. Το σχήμα αυτό αποκρύπτει κάτι, εφόσον είναι αδύνατο για τον Μπομπ να μάθει οτιδήποτε για το δεσμευμένο bit με ανάλυση των όσων του είχε στείλει η Αλίκη.

Για πολλά χρόνια, ο σχεδιασμός ενός πρωτοκόλλου που θα απέκρυπτε και θα δέσμευε τα bits, με χρήση κβαντικών μέσων, εθεωρείτο ως κλειδί για να ξεκλειδώσουμε κάθε τι που θέλουμε να κάνουμε με την κρυπτογραφία.

Κάποτε, μεταξύ του 2015 και του 2020, οι επιστήμονες λένε ότι ελπίζουν τα δυαδικά bits θα κωδικοποιηθούν σε σωματίδια - όπως είναι τα φωτόνια ή τα ηλεκτρόνια. Αυτά τα κβαντικά bits θα επέτρεπαν στους υπολογιστές να εκτελέσουν ταυτόχρονα πολλαπλάσιους σύνθετους υπολογισμούς.

Ο κβαντικός υπολογισμός θα αυξήσει την ισχύ επεξεργασίας των υπολογιστών τόσο, που ουσιαστικά θα είναι σαν τη μετάβαση από τον άβακα στον υπολογιστή", λέει ο Charles Ross, ένας σύμβουλος στην εταιρεία Cientifica, που συμμετείχε στις δοκιμές του κβαντικού

υπολογισμού. Αυτή η έρευνα χρηματοδοτήθηκε από την Ευρωπαϊκή Επιτροπή το 1998.

➢ ΠΡΑΚΤΙΚΗ ΕΦΑΡΜΟΓΗ

Ένας τρόπος αποστολής ενός κβαντοκρυπτογραφικού κλειδιού από τον αποστολέα στον παραλήπτη, ή αντιστρόφως, προϋποθέτει ένα λέιζερ ικανό να εκπέμπει μονήρη φωτόνια πολωμένα κατά δύο διαφορετικούς «τρόπους». Στον πρώτο τρόπο, τα φωτόνια έχουν πόλωση κατακόρυφη ή οριζόντια (ορθός τρόπος) στον δεύτερο, η πόλωση τους σχηματίζει με την κατακόρυφο γωνία ±45 μοιρών (πλάγιος τρόπος). Σε αμφότερους τους τρόπους, οι δύο αμοιβαίως ορθογώνιες πολώσεις αναπαριστούν το ψηφίο 0, η μία, και το ψηφίο 1, η άλλη. Η αποστολέας, που οι κρυπτογράφοι στα κείμενα τους κατά σύμβαση την ονομάζουν Αλίκη, μεταδίδει μία σειρά από μπιτ, διαλέγοντας τυχαία εάν τα φωτόνια θα σταλούν κατά τον ορθό ή τον πλάγιο τρόπο. Ο αποδέκτης, γνωστός ως Μπομπ στη σχετική βιβλιογραφία, επιλέγει επίσης τυχαία ποιον τρόπο θα χρησιμοποιήσει προκείμενου να μετρήσει τα εισερχόμενα μπιτ. Η αρχή της αβεβαιότητας του Heisenberg δεν του επιτρέπει να μετρήσει τα εισερχόμενα φωτόνια και με τους δύο τρόπους οφείλει να διαλέξει ή τον έναν ή τον άλλο. Από όλα τα φωτόνια, μόνο εκείνα όσα μέτρησε ο Μπομπ με τον ίδιο τρόπο με το οποίο εστάλησαν από την Αλίκη είναι βέβαιο ότι θα έχουν και για τους δύο την ίδια πόλωση επομένως, δε, ότι και τα μπιτ θα συμπίπτουν

Μετά τη μετάδοση, ο Μπομπ επικοινωνεί με την Αλίκη, επικοινωνία που δεν χρειάζεται να παραμείνει κρυφή, και την πληροφορεί ποιον από τους δύο τρόπους (τον ορθό ή τον πλάγιο) χρησιμοποίησε για να λάβει το κάθε φωτόνιο. Δεν αναφέρει όμως καθόλου ποια τιμή (Ο ή 1) αναπαριστούσε το κάθε φωτόνιο που μέτρησε. Η Αλίκη εν συνεχεία αποκαλύπτει στον Μπομπ ποια φωτόνια μετρήθηκαν σωστά. Και οι δύο τους αγνοούν τα φωτόνια που μετρήθηκαν με λάθος τρόπο. Τα μπιτ που μετρήθηκαν σωστά αποτελούν το κλειδί που θα χρησιμεύσει ως είσοδος για τον αλγόριθμο με τον οποίο θα κρυπτογραφηθεί ή θα αποκρυτογραφηθεί το μήνυμα.

Αν κάποιος τρίτος, η διαβόητη Εύα ας πούμε, προσπαθήσει να υποκλέψει το κλειδί, τότε, και πάλι χάρη στην αρχή του Heisenberg, δεν θα μπορέσει να πραγματοποιήσει μετρήσεις και με τους δύο τρόπους. Αν, λοιπόν, κάνει τη μέτρηση χρησιμοποιώντας λάθος τρόπο, ακόμη και αν αποστείλει στον Μπομπ τα μπιτ όπως ακριβώς τα μέτρησε, αναπόφευκτα θα εισαγάγει κάποια σφάλματα. Ο Μπομπ και η Αλίκη μπορούν να ανακαλύψουν τυχόν απόπειρες υπόκλοπής διαλέγοντας ορισμένα μπιτ και συγκρίνοντας τα για να εντοπίσουν σφάλματα.

Μερικές κυβερνητικές υπηρεσίες και χρηματοοικονομικοί οργανισμοί φοβούνται ότι ένα κρυπτογραφημένο μήνυμα θα μπορούσε να υποκλαπεί σήμερα και να κρατηθεί αποθηκευμένο επί μία δεκαετία ή και περισσότερο —οπότε και θα καθίστατο δυνατή η αποκρυπτογράφηση του με τη βοήθεια ενός κβαντικού υπολογιστή.

Σήμερα, η κβαντική κρυπτογραφία έχει προχωρήσει σημαντικά σε σχέση με την πειραματική διάταξη που στήθηκε πρόχειρα πάνω σε ένα τραπέζι στο γραφείο του Bennett. Ήδη υπάρχουν εταιρείες που δημιουργούν κβαντοκρυπτογραφικό συστήματα, ενώ η CIA και Τράπεζες των ΗΠΑ τα χρησιμοποιούν. Η αρχή έγινε το 2003 από δύο εταιρείες — την id Quantique στη Γενεύη και την MagiQ Technologies στη Νέα Υόρκη — που παρουσίασαν προϊόντα ικανά να μεταδώσουν ένα κβαντοκρυπτογραφικό κλειδί σε αποστάσεις πολύ μεγαλύτερες των 30 εκατοστών που διήνυαν τα φωτόνια στο πείραμα του Bennett. Ταυτόχρονα, η NEC, αφού έκανε μια εντυπωσιακή επίδειξη μετάδοσης σε απόσταση-ρεκόρ 150 χιλιομέτρων, εισήλθε και αυτή στην αγορά. Άλλες εταιρείες που δείχνουν ενδιαφέρον γι' αυτού του είδους την τεχνολογία, όπως η IBM, η Fujitsu και η Toshiba, διεξάγουν σύντονες προσπάθειες στο ερευνητικό επίπεδο

Τα προϊόντα που διατίθενται στην αγορά μπορούν να μεταδώσουν κλειδιά μέσω μεμονωμένων ζεύξεων οπτικών ινών σε αποστάσεις πολλών δεκάδων χιλιομέτρων. Ένα σύστημα της MagiQ κοστίζει από 70.000 έως 100.000 δολάρια. Ιδρυτής της εταιρείας αυτής κατά το 1999 είναι ο Robert Gelfond πρώην χρηματιστής της Γουόλ Στριτ.

Ανάμεσα στους πιθανούς μελλοντικούς αγοραστές κβαντοκρυπτογραφικών συστημάτων περιλαμβάνονται και παροχείς τηλεπικοινωνιακών υπηρεσιών (σαν τη Vodafon) οι οποίοι σχεδιάζουν να προσφέρουν μελλοντικά στους πελάτες τους μία υπερασφαλή υπηρεσία επικοινωνίας.

➢ ΠΡΟΒΛΗΜΑΤΑ

Τα κβαντικά κρυπτογραφημένα μηνύματα - που στέλνονται μέσω των οπτικών ινών - δεν μπορούν να ταξιδέψουν πολύ μακριά, και μπορούν να εργαστούν από σημείο σε σημείο - με άλλα λόγια, με υπολογιστές κατευθείαν συνδεδεμένους ο ένας με τον άλλο, κι όχι με υπολογιστές συνδεδεμένους σε δίκτυο.

Η Toshiba Ευρώπης, που δουλεύει με το Πανεπιστήμιο του Καίμπριτζ πάνω στην κβαντική κρυπτογραφία, τον περασμένο Ιούνιο έδειξε ότι μπορεί να μεταφέρει κβαντικά κρυπτογραφημένα μηνύματα μέχρι 120 χιλιόμετρα, αρκετά μακριά για πολλές εφαρμογές σε μητροπολιτικές περιοχές, λέει ο Andrew Shields, επικεφαλής της ομάδας κβαντικής πληροφορίας στο βρετανικό ερευνητικό εργαστήριο της Toshiba.

Προκειμένου να εργαστούν σε ένα περιβάλλον δικτύου και σε μεγαλύτερες αποστάσεις, απαιτείται να προστεθούν κβαντικοί επαναλήπτες - ένα είδος στοιχειώδους κβαντικού υπολογιστή - για να αναπαραγάγουν τα κβαντικά bits.

Συγχρόνως εργάζεται στον τομέα αυτό η Nec και η Hewlett-Packard από εταιρείες. Επίσης, επιστήμονες από την Ευρώπη, τις Ηνωμένες Πολιτείες (στο Los Alamos), τη Μεγάλη Βρετανία και την Αυστρία πειραματίζονται με τη διαβίβαση των κβαντικών κλειδιών μέσω του αέρα παρά με τις οπτικές ίνες. Η ιδέα είναι να σταλούν τα κβαντικά κλειδιά μέχρι τους δορυφόρους και έπειτα προς τα κάτω σε έναν άλλο προορισμό.

Συνολικά, περίπου 50 εκατομμύρια δολάρια από δημόσια και ιδιωτικά κεφάλαια θα επενδυθούν στο κβαντικό σύστημα κρυπτογραφίας, κατά τη διάρκεια των επόμενων τριών ετών.

➢ ΠΟΙΕΣ ΕΤΑΙΡΙΕΣ ΠΟΥΛΟΥΝ ΗΔΗ ΚΒΑΝΤΙΚΑ ΚΛΕΙΔΙΑ

- id quantique Γενεύη, Ελβετία: Σύστημα βασισμένο στις οπτικές ίνες ικανό να μεταδίδει κβαντοκρυπτογραφικά κλειδιά σε αποστάσεις δεκάδων χιλιομέτρων.
- NEC Τόκιο: Μετά την επίδειξη που έκανε το 2004 κατά την οποία μεταδόθηκαν κλειδιά στην απόσταση-ρεκόρ <των 150 χιλιομέτρων, σχεδιάζει να λανσάρει ένα προϊόν οπτικών ινών αρχές του 2006.
- Qinetiq στη Βρετανία: Παρέχει συστήματα κατόπιν συμβολαίου για τη μετάδοση κλειδιών δια του αέρος σε αποστάσεις ως και 10 χιλιομέτρων - έχει προμηθεύσει ένα τέτοιο σύστημα στην BBN Technotogies στο Κέιμπριτζ της Μασαχουσέτης.

Έτσι η νέα μέθοδος κρυπτογράφησης αποτελεί την πρώτη εμπορική εφαρμογή της επιστήμης της κβαντικής πληροφορίας, ενός γνωστικού πεδίου το οποίο συγκεντρώνει την κβαντική μηχανική και τη θεωρία της πληροφορίας. Εάν ευοδωθεί ο απώτερος τεχνολογικός στόχος που τίθεται στο εν λόγω πεδίο, τότε θα κατασκευαστεί ένας κβαντικός υπολογιστής τόσο ισχυρός ώστε να μη μας αφήνει άλλο τρόπο να προστατευτούμε από την κολοσσιαία αποκρυπτογραφική του ικανότητα εκτός από το να προσφύγουμε σε κβαντοκρυπτογραφικές τεχνικές.

«Απαραβίαστη» κβαντική κρυπτογράφηση δοκιμάστηκε σε δίκτυο υπολογιστών

➢ ΕΙΣΑΓΩΓΗ

Ο ατέλειωτος πόλεμος ανάμεσα στους χάκερ και τα συστήματα κρυπτογράφησης ευαίσθητων τηλεπικοινωνιών ίσως φτάνει στο τέλος του.
Το όραμα της τέλειας μυστικότητας ήρθε κοντύτερα με την παρουσίαση του πρώτου δικτύου που βασίζεται σε σύστημα κβαντικής κρυπτογράφησης, για το οποίο οι δημιουργοί του υποστηρίζουν ότι είναι ουσιαστικά απαραβίαστο.

Το καινοτόμο σύστημα παρουσιάσθηκε στη Βιέννη από επιστήμονες του ευρωπαϊκού προγράμματος SECOQC (Ασφαλείς Επικοινωνίες βασισμένες στην Κβαντική Κρυπτογραφία).

Η νέα μέθοδος, που αξιοποιεί τις μυστηριώδεις κβαντικές ιδιότητες των φωτονίων, μπορεί να χρησιμοποιηθεί μελλοντικά από κυβερνητικές και στρατιωτικές υπηρεσίες, χρηματοοικονομικούς οργανισμούς και άλλες εταιρίες με δίκτυο θυγατρικών, προκειμένου να πετύχουν τον ανώτερο δυνατό βαθμό ασφάλειας στα εμπιστευτικά μηνύματά τους.

Σύμφωνα με τον Αυστριακό συντονιστή του προγράμματος Κρίστιαν Μόνικ, η εμπορική αξιοποίηση της νέας μεθόδου αναμένεται μέσα στην επόμενη τριετία.

Η μετάδοση των δεδομένων, ανάμεσα σε έξι διαφορετικά κτίρια στη Βιέννη, πραγματοποιήθηκε μέσω κοινών καλωδίων οπτικών ινών τα οποία προσέφερε η Siemens.

Η κβαντική κρυπτογράφηση για δίκτυα είναι αποτέλεσμα δουλειάς 4,5 ετών από 41 συνεργαζόμενα πανεπιστήμια και ερευνητικά κέντρα 12 ευρωπαϊκών χωρών, υπό την καθοδήγηση του Αυστριακού Ερευνητικού Κέντρου, με τις «ευλογίες» ενός εκ των «πατέρων» της κβαντικής φυσικής, του αυστριακού επιστήμονα Αντον Τσάιλινγκερ του

πανεπιστημίου της Βιέννης.

Η μοντέρνα μη κβαντική κρυπτογραφία βασίζεται στη χρήση ψηφιακών «κλειδιών» που κωδικοποιούν τα δεδομένα πριν τα στείλουν μέσω ενός δικτύου και τα αποκρυπτογραφούν όταν φθάσουν στον προορισμό τους. Ο λήπτης πρέπει να έχει μια εκδοχή του «κλειδιού» του αποστολέα για να αποκτήσει πρόσβαση στα μεταβιβαζόμενα δεδομένα.

Η κβαντική κρυπτογραφία διαφέρει ριζικά από τα συστήματα ασφάλειας που χρησιμοποιούν τα σημερινά δίκτυα και τα οποία, παρά τις πολύπλοκες διαδικασίες στις οποίες βασίζονται, μπορούν τελικά να παραβιαστούν από όποιον έχει στα χέρια του χρόνο, χρήμα και μεγάλη υπολογιστική δύναμη.

➢ Η μυστική δύναμη των φωτονίων

Η κβαντική κρυπτογραφία χρησιμοποιεί τους νόμους της κβαντικής φυσικής, οι οποίοι θεωρούνται εγγενώς απαραβίαστοι. Η αρχική ιδέα της κβαντικής κρυπτογραφίας ξεκίνησε πριν 25 χρόνια από τον Τσαρλς Μπένετ της IBM και τον Ζιλ Μπρασάρ του πανεπιστημίου του Μόντρεαλ.

Βασίζεται στη γνωστή κβαντική «αρχή της απροσδιοριστίας» του Χάιζενμπεργκ, δηλαδή στο γεγονός ότι ένας παρατηρητής δεν μπορεί να μετρήσει την κβαντική πληροφορία χωρίς να την αλλοιώσει. Η νέα τεχνολογία λειτουργεί στέλνοντας δέσμες σωματιδίων φωτονίων, οι οποίες διαταράσσονται αν κάποιος επιχειρήσει να υποκλέψει το μήνυμα.

Το σύστημα χρησιμοποιεί «κλειδιά» που δημιουργούνται και διανέμονται μέσω τεχνολογιών κβαντικής κρυπτογράφησης. Κάθε μεταδιδόμενο φωτόνιο μεταφέρει ένα απόλυτα μυστικό «κλειδί» που κωδικοποιεί τα μεταφερόμενα δεδομένα, όπως συμβαίνει στα συνηθισμένα δίκτυα ηλεκτρονικών υπολογιστών. Το πλεονέκτημα είναι ότι κανείς (πέρα από τους δύο χρήστες στο συγκεκριμένο επικοινωνιακό κανάλι) δεν μπορεί να «κρυφακούσει» για να μάθει το κλειδί, χωρίς να αποκαλύψει τον εαυτό του.

Όπως αποδείχτηκε και στην επίδειξη που έγινε στη Βιέννη, όταν ένας εισβολέας προσπαθεί να υποκλέψει την κβαντική επικοινωνία, τα φωτόνια αλλοιώνονται και οι ανιχνευτές του δικτύου καταγράφουν την επίθεση, ενώ το σύστημα αυτόματα κλείνει για αυτοπροστασία χωρίς να έχει παραβιαστεί. Η επικοινωνία επαναλαμβάνεται αργότερα με ένα νέο «κλειδί».

Αν εξάλλου, για κάποιο λόγο, ένας κβαντικός σύνδεσμος σταματήσει να λειτουργεί, τα φωτόνια στέλνονται από εναλλακτικούς δρόμους αυτόματα μέσω του τηλεπικοινωνιακού δικτύου, έτσι ώστε οι δύο χρήστες παραμένουν σε συνεχή ασφαλή επικοινωνία.

Μέχρι σήμερα είχαν γίνει και άλλες απόπειρες για κβαντική κρυπτογράφηση, αλλά βασικά αφορούσαν μόνο την επικοινωνία ανάμεσα σε δύο άτομα (αποστολέα - λήπτη) και στο πλαίσιο αυτό ήδη υπάρχουν εμπορικές εφαρμογές από αρκετές εταιρίες. Οι λύσεις αυτές έχουν περιορισμένη εφαρμογή και αυξημένους κινδύνους (αν π.χ. κοπεί το καλώδιο οπτικής ίνας, η επικοινωνία διακόπτεται).

Αντίθετα, η εφαρμογή που παρουσιάστηκε στη Βιέννη, είναι η πρώτη που αξιοποιεί την κβαντική κρυπτογραφία σε περιβάλλον δικτύου, με ό,τι θετικό αυτό συνεπάγεται (μεγαλύτερη γεωγραφική κάλυψη, εναλλακτικές οδοί επαφής αποστολέα-λήπτη για συνεχή επικοινωνία κλπ).

Η πρώτη δημόσια εφαρμογή της κβαντικής κρυπτογραφίας έγινε το 2007 στις εκλογές στο καντόνι της Γενεύης στην Ελβετία, όπου το νέο σύστημα εγγυήθηκε ότι η ηλεκτρονική ψηφοφορία ήταν ασφαλής και ότι δεν χάθηκε καμία ψήφος στη μετάδοση από τα εκλογικά κέντρα.

➢ Είναι όμως όντως απαραβίαστη;

Η κβαντική κρυπτογραφία είναι, υποτίθεται, απαραβίαστη και μερικές τράπεζες ήδη την χρησιμοποιούν για να μεταφέρουν δεδομένα. Όμως προ ημερών ανακοινώθηκε από το Νορβηγικό Πανεπιστήμιο Επιστήμης και Τεχνολογίας στο Τροντχάιμ, σύμφωνα με δημοσίευμα της ηλεκτρονικής υπηρεσίας New Scientist, ότι ένας «ωτακουστής» μπορεί να την παραβιάσει χωρίς να αφήσει κανένα ίχνος, εκμεταλλευόμενος ένα πρόβλημα στον χρησιμοποιούμενο τεχνολογικό

εξοπλισμό.

Ο καθηγητής Βαντίμ Μακάροφ του νορβηγικού πανεπιστημίου και συνεργάτες του από τη Σουηδία και τη Ρωσία υποστηρίζουν ότι τυχόν κακόβουλοι τρίτοι μπορούν να ελέγξουν από μακριά τον εξοπλισμό του λήπτη και να αποκωδικοποιούν τα σήματα που, μέσω των φωτονίων, στέλνει ο αποστολέας. Όπως δήλωσαν, έχουν ανακαλύψει ότι δύο από τις τρεις συχνότερα χρησιμοποιούμενες συσκευές κβαντικής κρυπτογραφίας είναι ευάλωτες από άποψη ασφάλειας και μελετούν πώς θα ξεπεράσουν το πρόβλημα.

Αλλοι ερευνητές πάντως, όπως ο Νόρμπερτ Λιτκενχάους από το Ινστιτούτο Κβαντικής Πληροφορικής του Καναδά, δήλωσε ότι δεν θεωρεί πως το παραπάνω κενό ασφαλείας είναι σοβαρό. Το μέλλον θα δείξει αν οι αποκρυπτογράφοι θα μείνουν χωρίς δουλειά!

ΕΝΟΤΗΤΑ 3

ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ

ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ

➢ ΕΙΣΑΓΩΓΗ ΣΤΟΥΣ ΚΒΑΝΤΙΚΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ

Η ιδέα για τη δημιουργία ενός υπολογιστή που θα βασίζεται στις αρχές της κβαντομηχανικής διατυπώθηκε στις αρχές της δεκαετίας του ’80, όταν οι φυσικοί Richard Feynman, David Deutsch και Paul Benioff διαπίστωσαν ότι οι κλασικοί υπολογιστές είχαν βασικούς περιορισμούς στο χρόνο και στη μνήμη για την εκπόνηση βασικών λειτουργιών. Κατανόησαν ότι η συνεχής συρρίκνωση των στοιχείων που συσκευάζονται επάνω στα τσιπ πυριτίου θα έφθανε σε ένα σημείο όπου τα μεμονωμένα στοιχεία δεν θα ήταν μεγαλύτερα από μερικά άτομα. Η συνεχής μείωση, με λιθογραφικές τεχνικές, των διαστάσεων θα μπορούσε να φτάσει στις διαστάσεις των ατόμων και οι υπολογιστές θα μπορούσαν να κατασκευαστούν από το ίδιο το άτομο με παρουσία κβαντικών κανόνων.

Ο Feynman ήταν ο πρώτος που προσπάθησε να δώσει λύση στο παραπάνω θέμα με την παραγωγή ενός προτύπου που έδειχνε πώς ένα κβαντικό σύστημα θα μπορούσε να χρησιμοποιηθεί για να κάνει υπολογισμούς. Σύμφωνα με το πρότυπό του, ένας φυσικός θα μπορούσε να πραγματοποιήσει πειράματα στην κβαντική φυσική μέσα από έναν κβαντικό υπολογιστή.

Ο κβαντικός υπολογισμός (Quantum computing), στηρίζεται στην κβαντική τηλεμεταφορά για δημιουργία των κβαντικών πυλών λογικής που επεξεργάζονται τις πληροφορίες μέσα έναν κβαντικό υπολογιστή. Ο κβαντικός υπολογισμός εισάγει επίσης την έννοια των qubits, το κβαντικό ανάλογο του κλασσικού bit. Η διαφορά βρίσκεται στο γεγονός ότι ένα qubit μπορεί να είναι είτε 0 είτε 1 ταυτόχρονα!. Αυτό επιτρέπει ογκώδεις παράλληλους υπολογισμούς να εκτελεσθούν σε μερικά δευτερόλεπτα, διαδικασία που παίρνει εκατομμύρια ή και δισεκατομμύρια μέρες στα σημερινά computers.

Το βασικό χαρακτηριστικό ενός κβαντικού υπολογιστή είναι ότι μπορεί να επεξεργάζεται διαφορετικές λύσεις ενός προβλήματος ταυτόχρονα καταλήγοντας ταυτόχρονα σε πολλές εναλλακτικές, στοιχείο ιδιαίτερα χρήσιμο για την επίλυση προβλημάτων με πολλές μεταβλητές.

«Ένας κβαντικός υπολογιστής θα μπορεί να λύσει σύνθετα προβλήματα σε δευτερόλεπτα, τη στιγμή που ένας συμβατικός θα

χρειαζόταν απεριόριστο χρόνο», αναφέρει ο καθηγητής Ντέιβιντ Άουσαλομ του πανεπιστημίου της Καλιφόρνια.

➢ ΠΩΣ ΥΛΟΠΟΙΕΙΤΑΙ ΕΝΑΣ ΚΒΑΝΤΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ;

Στους κλασικούς υπολογιστές η πληροφορία κωδικοποιείται σε μία σειρά από bits τα οποία μέσω των λογικών πυλών μετασχηματίζονται για να παράγουν ένα τελικό αποτέλεσμα. Ομοίως ένας κβαντικός υπολογιστής χειρίζεται τα qubits μέσω των κβαντικών πυλών που υλοποιούν μετασχηματισμούς σε ένα ή σε ζευγάρι qubits. Τοποθετώντας τις κβαντικές πύλες σε μία συγκεκριμένη σειρά ένας κβαντικός υπολογιστής μπορεί να υλοποιήσει περίπλοκους μετασχηματισμούς σε μία σειρά από qubits από μία αρχική κατάσταση στην τελική. Έπειτα τα qubits μπορούν να μετρηθούν στην τελική τους κατάσταση και από τις μετρήσεις αυτές να εξαχθεί ένα τελικό υπολογιστικό αποτέλεσμα.

Τα περισσότερα μοντέρνα chips έχουν transistors στο μέγεθος των 180 nanometers, περισσότερο από 400 φορές στενότερα από ότι η ανθρώπινη τρίχα. Αλλά οι κατασκευαστές των chip δεν θα μπορούν να φτιάξουν chips μικρότερα των 124 nanometers, σύμφωνα με μια βασική αρχή της οπτικής που είναι γνωστή σαν κριτήριο του Rayleigh. Έτσι τα όρια των σημερινών τεχνικών βρίσκονται σε αυτή την περιοχή μεγέθους.

Θεωρητικά, αν χρησιμοποιηθούν τα πεπλεγμένα φωτόνια αντί για τα συμβατικά φωτόνια των laser, θα μπορούν να ξεπεράσουν οι τεχνικοί τα όρια των 124 nm, και να φτιαχτούν έτσι transistors μικρότερα από 64 nanometers. Τα πεπλεγμένα αυτά φωτόνια θα μπορούν να ταξιδεύουν μαζί και να συμπεριφέρονται σαν ένα μοναδικό φωτόνιο, αντί για δύο ξεχωριστά.
Αυτό οφείλεται στο ότι τα πεπλεγμένα φωτόνια έχουν ως σύστημα το μισό μήκος κύματος από ό,τι έχουν ως ατομικά σωματίδια - μία από τις παράδοξες συνέπειες των κβαντικών νόμων.

Τελικά η ομοιότητα στον υπολογισμό μεταξύ κλασικού και κβαντικού υπολογιστή θεωρητικά μπορεί να μας οδηγήσει στο συμπέρασμα ότι ένας κλασικός υπολογιστής μπορεί να προσομοιώσει ακριβώς έναν κβαντικό υπολογιστή. Όμως η προσομοίωση ενός

κβαντικού υπολογιστή από έναν κλασικό είναι ένα υπολογιστικά δύσκολο πρόβλημα (δηλαδή ένα πρόβλημα πολυπλοκότητας NP) επειδή οι συσχετισμοί μεταξύ των κβαντικών κομματιών είναι ποιοτικά διαφορετικοί από τους συσχετισμούς μεταξύ των κλασικών κομματιών .

Οι επιστήμονες ελπίζουν ότι οι κβαντικοί υπολογιστές, που θα κινούν τις πληροφορίες κατ' αυτό τον τηλεμεταφερόμενο τρόπο, και όχι από τα καλώδια και τα τσιπ του πυριτίου, θα είναι απείρως γρηγορότεροι και ισχυρότεροι από τους παρόντες υπολογιστές. Πιστεύουμε πως σε 5 ή 10 χρόνια οι προηγμένες κοινωνίες θα χρησιμοποιούν κβαντική πληροφορία.

➢ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΤΩΝ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Τα πλεονεκτήματα των κβαντικών υπολογιστών σε σχέση με τους κλασικούς είναι τα εξής:

1. Μεγαλύτερη ταχύτητα

2. Τεράστια μνήμη

3. Δυνατότητα επίλυσης ορισμένων «υπολογιστικά δύσκολων» κλασικών προβλημάτων (προβλήματα NP) σε πολυωνυμικό χρόνο.

➢ ΠΡΟΒΛΗΜΑΤΑ ΣΤΗΝ ΥΛΟΠΟΙΗΣΗ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ο πρώτος που επινόησε έναν κβαντικό υπολογιστικό αλγόριθμο ήταν ο Peter Shor που μπόρεσε εκμεταλλευόμενος την κβαντική δύναμη να παραγοντοποιήσει πολύ μεγάλους αριθμούς σε κλάσματα δευτερολέπτου. Αν και έχει σημειωθεί σημαντική πρόοδος από τη σύλληψη της ιδέας του κβαντικού υπολογιστή μέχρι σήμερα, ωστόσο υπάρχουν πολλά εμπόδια στην υλοποίησή του. Το κυριότερο πρόβλημα στη δημιουργία κβαντικών υπολογιστών είναι η ύπαρξη σφαλμάτων και η αντιμετώπισή τους. Το πρόβλημα που προκύπτει στη διόρθωση σφάλματος είναι ποια λάθη χρειάζονται διόρθωση (στην επόμενη παράγραφο περιγράφονται κώδικες διόρθωσης σφαλμάτων) . Η απάντηση είναι πρώτιστα εκείνα τα λάθη που προκύπτουν ως άμεσο

αποτέλεσμα αποσυσχετισμού (decoherence) ή από την τάση ενός κβαντικού υπολογιστή να αποσυντεθεί από μία δεδομένη κβαντική κατάσταση σε μία ασυνάρτητη κατάσταση καθώς αλληλεπιδρά με το περιβάλλον. Αυτές οι αλληλεπιδράσεις μεταξύ του περιβάλλοντος και των qubits είναι αναπόφευκτες και προκαλούν τη διακοπή των πληροφοριών που αποθηκεύονται στον κβαντικό υπολογιστή, και έτσι τα λάθη στον υπολογισμό.

➢ ΚΒΑΝΤΙΚΗ ΔΙΟΡΘΩΣΗ ΣΦΑΛΜΑΤΩΝ

Η διόρθωση σφαλμάτων είναι απαραίτητη στην υλοποίηση των κβαντικών υπολογιστών γιατί τα κβαντικά συστήματα αλληλεπιδρούν με το περιβάλλον. Αυτή η αλληλεπίδραση, όπως ειπώθηκε, μπορεί να οδηγήσει σε κατάρρευση του συστήματος και η ύπαρξη μηχανισμών για τη διόρθωση των λαθών είναι απαραίτητη.

Υπάρχουν δύο είδη λαθών που μπορεί να εισάγει το περιβάλλον στο

σύστημα. Αυτά είναι:

• Δυαδική αντιστροφή

• Αποσυσχετισμός

1. Δυαδική αντιστροφή (Bit flip)

Αρχικά υποθέτουμε ότι το σύστημά μας αποτελείται από ένα qubit. Ένα σφάλμα που μπορεί να προκύψει είναι όμοιο με αυτό σε έναν κλασικό υπολογιστή, είναι το σφάλμα της δυαδικής αντιστροφής. Αυτό το λάθος μετατρέπει την αρχική κατάσταση από π.χ. α 0 +b 1 σε α 1 +b 0 . Μπορεί να διορθωθεί αυτό το λάθος χρησιμοποιώντας κλασικούς κώδικες διόρθωσης. Μπορούμε να εφαρμόσουμε έναν κλασικό κώδικα επανάληψης και να το αποφύγουμε. Είναι σημαντικό να τονίσουμε ότι η δυαδική αντιστροφή είναι μία αντιστρεπτή πράξη πάνω στα qubits και για αυτό το λόγο μπορεί εύκολα να διορθωθεί.

2. Αποσυσχετισμός

Ένα άλλο σφάλμα που ενδεχομένως να προκύψει σε έναν κβαντικό υπολογιστή είναι λόγω του φαινόμενου του αποσυσχετισμού (decoherence) των κβαντικών καταστάσεων. Σε αυτή την περίπτωση ανεπιθύμητες όσο και τυχαίες αλληλεπιδράσεις των κβαντικών

καταχωρητών με το περιβάλλον οδηγούν στην κατάρρευση της κατάστασης του συστήματος. Αυτό ισοδυναμεί με «μέτρηση» του καταχωρητή η οποία είναι μία μη αντιστρεπτή διεργασία. Αν το σύστημα βρίσκεται σε μια αρχική κατάσταση και ένα δεύτερο qubit μετρηθεί η κατάσταση του συστήματος καταρρέει και κατά συνέπεια χάνεται με μη αναστρέψιμο τρόπο η αποθηκευμένη πληροφορία. Η επίλυση αυτού του προβλήματος είναι εξαιρετικά δύσκολη και η επαναφορά του συστήματος μετά από τέτοια λάθη είναι σχεδόν αδύνατη..

3. Διόρθωση σφαλμάτων

Στους κλασικούς υπολογιστές για τον περιορισμό των σφαλμάτων, κωδικοποιείται κάθε bit ως μια τριπλέτα από όμοια bits. Αν κάποιος θόρυβος αντιστρέψει ένα bit, το σφάλμα μπορεί να αποκατασταθεί επιδιορθώνοντας το μεμονωμένο bit της τριπλέτας.

Όσον αφορά τους κβαντικούς υπολογιστές, αρχικά φάνηκε ότι είναι αδύνατον να αναπτύξουμε κώδικες για την διόρθωση κβαντικών σφαλμάτων, διότι η κβαντομηχανική μας απαγορεύει να μάθουμε με βεβαιότητα την άγνωστη κατάσταση ενός κβαντικού αντικειμένου .

Ο κώδικας της απλής κλασικής τριπλέτας συνεπώς αποτυγχάνει διότι δεν μπορούμε να εξετάσουμε κάθε αντίγραφο ενός qubit χωρίς να καταστρέψουμε όλα τα αντίγραφα κατά την διαδικασία αυτή. Ακόμη χειρότερα, το να φτιάξουμε αντίγραφα στην αρχική κατάσταση δεν είναι απλό. Η κβαντομηχανική μας απαγορεύει να πάρουμε ένα άγνωστο qubit και να φτιάξουμε με αξιοπιστία ένα αντίγραφό του. Το αποτέλεσμα αυτό είναι γνωστό ως θεώρημα της αδυναμίας κλωνοποίησης.

Όμως στις αρχές 1990 ερευνητές της IBM υποστήριξαν ότι η κβαντική διόρθωση σφαλμάτων θα ήταν αναγκαία για τους κβαντικούς υπολογιστές, αλλά οι κλασικοί κώδικες δεν μπορούσαν να χρησιμοποιηθούν στον κβαντικό κόσμο. Απέδειξαν πως μπορούμε να κάνουμε κβαντική διόρθωση σφαλμάτων, χωρίς να μάθουμε ποτέ τις καταστάσεις των qubits.

Όπως και με τον κώδικα της τριπλέτας, κάθε τιμή παριστάνεται με ένα σύνολο από qubits. Τα qubits αυτά περνάνε μέσα από ένα κύκλωμα (το κβαντικό ανάλογο των λογικών πυλών) το οποίο βρίσκει με επιτυχία ένα σφάλμα στα qubits χωρίς να "διαβάσει" πραγματικά ποιες είναι οι ξεχωριστές καταστάσεις.

Η προστασία των κβαντικών καταστάσεων από τον θόρυβο επιτεύχθηκε με τη χρήση ενός συνδυασμού ιδεών από την επιστήμη της πληροφορίας και από τη βασική κβαντομηχανική. Η κβαντική διόρθωση

σφαλμάτων έχει δημιουργήσει επίσης πολλές ενδιαφέρουσες νέες ιδέες. Για παράδειγμα μερικά φυσικά συστήματα μπορεί να έχουν ένα τύπο φυσικής ανοχής στο θόρυβο. Αυτά τα συστήματα θα χρησιμοποιούν κβαντική διόρθωση σφαλμάτων, χωρίς την ανθρώπινη επέμβαση και θα μπορούν να επιδείξουν εξαιρετική αντίσταση στην καταστροφή της υπέρθεσης των καταστάσεων.

➢ ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΤΑΣΚΕΥΗΣ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Στην προσπάθειά τους να αναζητήσουν τον τρόπο κατασκευής ενός υπολογιστή που θα εκμεταλλευόταν τις αρχές της κβαντομηχανικής, πολλοί ερευνητές ακολουθούν διάφορες ετερόκλητες τεχνολογίες, συμπεριλαμβανομένων των κβαντικών υπολογιστών στερεάς κατάστασης, όπως δηλαδή και οι κλασικοί, των παγίδων ιόντων (ion-traps), υπολογιστών κοιλότητας κβαντικής ηλεκτροδυναμικής (cavity QED) καθώς και του πυρηνικού μαγνητικού συντονισμού (NMR).

1. Μοριακοί υπολογιστές

Τελευταία έχει αναπτυχθεί ένα νέο είδος υπολογιστικής διαδικασίας, η οποία στηρίζεται στην κίνηση των μορίων. Ερευνητές στην IBM έχουν καταφέρει να επιδείξουν λογικές πύλες χρησιμοποιώντας μία στοιβάδα μορίων μονοξειδίου του άνθρακα για να μεταφέρει δεδομένα. Οι συσκευές που γίνονται κατ' αυτό τον τρόπο έχουν διαστάσεις στην κλίμακα των νανομέτρων (10^{-9}), μεγέθους αρκετές τάξεις μικρότερες από την τεχνολογία πυριτίου των σημερινών συμβατικών υπολογιστών.

Η πυκνότητα των συστατικών στα μικροτσίπ πυριτίου έχει αυξηθεί εκθετικά τα τελευταία σαράντα χρόνια. Οι ερευνητές της IBM έχουν υπερνικήσει αυτό το πρόβλημα, σε γενικές γραμμές, με τη χρησιμοποίηση ενός ζεύγους, χαμηλής θερμοκρασίας, ηλεκτρονικών μικροσκοπίων σάρωσης, για να διευθετήσουν ζεύγη μορίων μονοξειδίου του άνθρακα σε μια επιφάνεια του χαλκού. Μετακίνησαν ένα απλό μόριο μονοξειδίου του άνθρακα παράλληλα με ένα από αυτά τα ζεύγη, έτσι ώστε τα τρία μόρια σχημάτισαν ένα σχήμα σαν την κεφαλή ενός βέλους. Εντούτοις, ο σχηματισμός αυτός ήταν ασταθής επειδή αύξησε την ενέργεια του συστήματος.

Οι ερευνητές της IBM χρησιμοποίησαν την αρχή αυτή για να κάνουν την πύλη AND. Τοποθέτησαν τρεις σειρές ζευγών μορίων σε μια μορφή Y, με ένα απλό μόριο στο κεντρικό σημείο, όπου συναντώνται οι σειρές. Δύο σειρές ενέργησαν ως είσοδοι και η τρίτη ενεργεί ως έξοδος. Εάν υπάρχει ένας καταρράκτης και στις δύο σειρές - δηλ. εάν υπάρχει ένα "1" και στις δύο εισόδους -μόρια θα πεταχτούν κατά μήκος των σειρών για να διαμορφώσουν την κεφαλή του βέλους με το απλό μόριο, που είναι ήδη στο σημείο όπου συναντώνται οι τρεις σειρές. Αυτή η κεφαλή έπειτα θα αποσυντεθεί, παράγοντας έναν καταρράκτη (δηλ. ένα σήμα) στην έξοδο. Οι ερευνητές χρησιμοποίησαν μια παρόμοια ρύθμιση που κάνει την πύλη OR. Δυστυχώς οι μοριακές συσκευές καταρρακτών που έγιναν από τους ερευνητές της IBM ήταν πολύ αργές και θα μπορούσαν μόνο να χρησιμοποιηθούν για να εκτελέσουν μια απλή λειτουργία. Για να επαναχρησιμοποιήσουν τις συσκευές αυτές οι ερευνητές έπρεπε να τοποθετήσουν τα μόρια πίσω στην αρχική θέση τους χρησιμοποιώντας ένα από τα ηλεκτρονικά μικροσκόπια σάρωσης. Για να είναι χρήσιμοι, οι μοριακοί υπολογιστές καταρρακτών θα χρειάζονταν έναν αυτόματο μηχανισμό που θα επαναρρύθμιζε μερικά από τα μόρια και θα άφηνε τα άλλα άθικτα για να ενεργήσουν ως καταχωρητές δεδομένων.

2. Παγίδες ιόντων

Μία νέα τεχνική για τη δημιουργία κβαντικών υπολογιστών είναι αυτή με τις παγίδες ιόντων. Ένας κβαντικός υπολογιστής, όπως έχουμε αναφέρει, λειτουργεί με κβαντικά bit (qubits), αντί των συνηθισμένων bit. Ένα qubit μπορεί να είναι όχι μόνο 0 ή 1 αλλά και μία υπέρθεση των δύο τιμών, στην οποία οι δύο προηγούμενες τιμές συνδυάζονται σε μια ενιαία κατάσταση. Μια σημαντική κατηγορία υπερθέσεων πολλών qubit είναι οι διαπλεγμένες καταστάσεις. Σε αυτό τις διαμορφώσεις, η κατάσταση του κάθε qubit διασυνδέεται με έναν λεπτό τρόπο με την κατάσταση του γειτονικού του. Πειράματα με τα ατομικά ιόντα περιλαμβάνουν τεράστιες ηλεκτρομαγνητικές παγίδες για να συγκρατηθούν τα ιόντα στη σειρά μέσα σε κενό. Αν και είναι καλό για τα πειράματα να γίνονται με έναν μικρό αριθμό ιόντων, είναι εντελώς

αδύνατον για τα μεγάλης κλίμακας συστήματα όπως ένας κβαντικός υπολογιστής, αν θέλουμε να έχει σημαντική χρήση.

Τελευταία όμως ερευνητές έχουν δείξει μια ιοντική παγίδα μεγέθους 100 μικρών μέσα σε ένα τσιπ ημιαγωγών. Χρησιμοποίησαν το τσιπ για να παγιδέψουν ένα μόνο ιόν καδμίου και το μετακίνησαν προς διαφορετικές θέσεις στην παγίδα εφαρμόζοντας ηλεκτρικά σήματα στα ηλεκτρόδια. Η παγίδα φτιάχτηκε με τη βοήθεια της καθιερωμένης μεθόδου της λιθογραφίας. Μια ηλεκτρομαγνητική παγίδα είναι αυτή που κρατά τα ιόντα σε σειρά μέσα σε κενό, ενώ λέιζερ χειρίζονται τις καταστάσεις τους.

Σε γενικές γραμμές οι τεχνικές μπορούν να ενσωματώσουν μεγαλύτερους αριθμούς ιόντων. Ένα εμπόδιο όμως ήταν ότι η ποιότητα της πεπλεγμένης κατάστασης μειώθηκε καθώς αυξανόταν ο αριθμός των ιόντων. Για να μειώσουν αυτό το λάθος, οι ερευνητές θα μπορούσαν να ρυθμίσουν τις λεπτομέρειες των παλμών του λέιζερ, χρησιμοποιώντας διαφορετικές καταστάσεις ιόντων για την αναπαράσταση του 0 και του 1, ή να δουλέψουν με ένα διαφορετικό είδος ιόντων συνολικά.

Για να είναι χρήσιμος ένας κβαντικός υπολογιστής πρέπει όχι μόνο να μπορούμε να δημιουργούμε ειδικές καταστάσεις qubit αλλά και να τις χειριζόμαστε με τρόπο που να διατηρούνται τα κβαντικά χαρακτηριστικά τους. Δηλαδή κάποιος να μπορεί να εκτελέσει κβαντικούς αλγορίθμους στον υπολογιστή. Ένας γνωστός αλγόριθμος είναι ο κβαντικός αλγόριθμος του Grover σε ένα σύστημα από δύο παγιδευμένα ιόντα καδμίου. Ο αλγόριθμος κάνει αναζήτηση μέσα σε μια βάση δεδομένων, όπου οι καταχωρήσεις έγιναν με έναν τυχαίο τρόπο. Η έρευνα ενός τυχαίου στοιχείου απαιτεί συνήθως την εξέταση κάθε καταχώρησης και άρα ο αντίστοιχος αλγόριθμος είναι τάξεως n, όπου n το μέγεθος της λίστας καταχωρήσεων. Ο κβαντικός αλγόριθμος αναζήτησης καταφέρνει το ίδιο σε αριθμό βημάτων που είναι τάξεως n

3. Cavity QED

Μία τρίτη ερευνητική κατεύθυνση για την υλοποίηση κβαντικών υπολογιστών είναι αυτή με τη χρήση κοιλότητας κβαντικής ηλεκτροδυναμικής (cavity QED).

Πιο συγκεκριμένα, η κβαντική ηλεκτροδυναμική (QED) είναι μια κβαντική θεωρία του ηλεκτρομαγνητισμού που περιγράφει τις αλληλεπιδράσεις της ακτινοβολίας με την φορτισμένη ύλη. Η QED είναι μια σχετικιστική θεωρία από τις εξισώσεις της οποίας προκύπτουν οι

εξισώσεις της ειδικής θεωρίας της σχετικότητας. Η κβαντική ηλεκτροδυναμική (που είναι βασικός κορμός των κβαντικών θεωριών πεδίου) θεωρεί ότι η ανάπτυξη των ηλεκτρομαγνητικών δυνάμεων αποδίδεται στην εκπομπή και την απορρόφηση φωτονίων ως σωματιδίων ανταλλαγής, τα οποία αντιπροσωπεύουν διαταραχές των ηλεκτρομαγνητικών πεδίων. Κατά τρόπο ανάλογο και τα ηλεκτρόνια μπορούν να θεωρηθούν ως διαταραχές αντίστοιχων κβαντισμένων πεδίων.

Αυτά όμως τα φωτόνια είναι εικονικά (virtual) δηλαδή δεν μπορούν να φανερωθούν ή να ανιχνευθούν με κανένα τρόπο επειδή η ύπαρξή τους παραβιάζει την διατήρηση της ενέργειας και της ορμής. Η ανταλλαγή σωματιδίων είναι όμοια με τη "δύναμη" της αλληλεπίδρασης, επειδή τα αλληλεπιδρώντας σωματίδια αλλάζουν την ταχύτητα και την κατεύθυνση της κίνησης τους καθώς αυτά ελευθερώνουν ή απορροφούν την ενέργεια ενός φωτονίου.

Τα φωτόνια μπορούν επίσης να εκπεμφθούν σε μια ελεύθερη κατάσταση, οπότε μόνο σ' αυτή την περίπτωση μπορούν να παρατηρηθούν.

Η αλληλεπίδραση των δύο φορτισμένων σωματιδίων συμβαίνει σε μια σειρά διαδικασιών αυξανόμενης πολυπλοκότητας. Στον απλούστερο τρόπο, μόνο ένα εικονικό φωτόνιο μπορεί να περιληφθεί. Σε μια διαδικασία δεύτερης τάξης, υπάρχουν δύο φωτόνια και ούτω καθ' εξής.

Οι διαδικασίες αντιστοιχούν σε όλους τους πιθανούς τρόπους στους οποίους μπορούν να αλληλεπιδράσουν τα σωματίδια κάνοντας ανταλλαγή εικονικών φωτονίων. Η κατασκευή των κβαντικών υπολογιστών με αυτή τη μέθοδο, συνίσταται στην παγίδευση ουδέτερων ατόμων και στην πόλωση φωτονίων. Η κβαντική πληροφορία αποθηκεύεται σε εσωτερικές καταστάσεις των ατόμων και είναι εύκολο να δημιουργηθούν αλληλεπιδράσεις με τα qubits.

4. Τεχνολογία NMR

Ο Πυρηνικός μαγνητικός Συντονισμός (NMR) είναι ένα φαινόμενο που έχει χρησιμοποιηθεί για τη δημιουργία κβαντικών υπολογιστών Η τεχνολογία NMR έχει χρησιμοποιηθεί παλιότερα σε ιατρικές εφαρμογές

και μία νέα προοπτική είναι και η χρήση της στους κβαντικούς υπολογιστές.

Η τεχνολογία αυτή έχει το πλεονέκτημα ότι μπορεί να χρησιμοποιηθεί σε θερμοκρασία δωματίου και έχει αποδειχθεί ότι είναι εύκολο να κατασκευαστεί με αυτή ένας κβαντικός υπολογιστής των 2 ή 3 qubits. Η βασική ιδέα είναι ότι ένας κβαντικός καταχωρητής είναι ένα μόριο που αποτελείται από δέκα άτομα. Κάθε qubit αναπαρίσταται με τον προσανατολισμό του σπιν του κάθε ατομικού πυρήνα στα άτομα του μορίου. Ο αριθμός των ατόμων ενός NMR κβαντικού υπολογιστή είναι ίσος με τον αριθμό των ατόμων σε κάθε μόριο.

Εκμεταλλευόμενοι τις ιδιότητες του φαινομένου ερευνητές κατάφεραν μέσω NMR πειραμάτων να αναπτύξουν θεμελιώδη εργαλεία που μπορούν να χρησιμοποιηθούν σε πολλούς μελλοντικούς τύπους κβαντικών υπολογιστών. Αυτή η τεχνολογία έχει αποδειχθεί ότι εύκολα μπορεί να σχεδιάσει 2 ή 3 qubits NMR κβαντικά συστήματα. Όμως τελευταία προσομοιώθηκε ένας υπολογιστής των 7-qubit με τη χρήση ενός νέου μορίου που αποτελείται από 7 πυρηνικά σπιν, όπου το κάθε ένα μπορεί να αλληλεπιδρά με το άλλο, ενώ οι αλληλεπιδράσεις αυτές μπορούν να ανιχνευτούν με όργανα NMR.

Βέβαια το φαινόμενο έχει κάποιες δυσκολίες όπως το γεγονός ότι είναι δύσκολο να διαχωριστούν τα qubits σε ένα μόριο από τις χημικές τους ιδιότητες στην περίπτωση μεγάλων μορίων. Επίσης είναι δύσκολο να αποσαφηνιστεί με ακρίβεια η αρχική κατάσταση. Είναι λοιπόν δύσκολο έως αδύνατο η τεχνολογία αυτή να χρησιμοποιηθεί σε υπολογιστές με περισσότερα από 12 qubits.

➢ Η ΠΡΟΟΠΤΙΚΗ ΚΑΙ ΤΟ ΜΕΛΛΟΝ ΤΩΝ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Οι κβαντικοί υπολογιστές δεν είναι κατάλληλοι για όλες τις υπολογιστικές διεργασίες. Παραδείγματος χάριν δεν μπορούν να επιταχύνουν την επεξεργασία κειμένου ή την πλοήγηση στο διαδίκτυο. Το πιθανότερο είναι να χρησιμοποιηθούν υβρίδια κλασικών και κβαντικών υπολογιστών στο μέλλον.

Η βασική μελλοντική τους εφαρμογή θα είναι η χρήση τους για την προστασία απόρρητων και προσωπικών δεδομένων γιατί θα είναι αδύνατο να μπορούν να εισέρχονται σε e-mails και τραπεζικούς

λογαριασμούς χρηστών του διαδικτύου, λόγω της ασφάλειας που θα παρέχουν. Επίσης, η αναζήτηση πληροφορίας στο διαδίκτυο θα διεξάγεται πολύ πιο γρήγορα, εφόσον υπάρχει κβαντικός αλγόριθμος αναζήτησης δεδομένων σε λίστα ο οποίος είναι μικρότερης τάξεως από τον αντίστοιχο κλασικό.

Τέλος μία άλλη εφαρμογή που έχει χρήση και στην καθημερινή ζωή είναι η βελτίωση στη χρήση GPS δηλαδή συστημάτων που χρησιμοποιούνται σε αυτοκίνητα για να ανιχνεύεται μία θέση προς αναζήτηση. Αυτά τα συστήματα βασίζονται σε ρολόγια που λειτουργούν με βάση τις αρχές της κβαντομηχανικής. Οι κβαντικοί υπολογιστές θα μπορούν να βελτιώσουν αυτές τις ρυθμίσεις και η αναζήτηση με τα μηχανήματα να δίνει καλύτερα και πιο έγκυρα αποτελέσματα.

Όπως αναφέρθηκε υπάρχουν διάφορες τεχνολογίες για την υλοποίηση κβαντικών υπολογιστών. Μέχρι στιγμής ο πρώτος κβαντικός υπολογιστής 2 qubits παρουσιάστηκε το 1998 από την IBM, η οποία το 1999 παρουσίασε κβαντικό υπολογιστή τριών qubits με δυνατότητα κβαντικής διόρθωσης σφαλμάτων ενώ από την ίδια εταιρεία το 2000 παρουσιάστηκε κβαντικός υπολογιστής των πέντε qubits. Ο τελευταίος υπολογιστής που έχει κατασκευαστεί είναι 7 qubits από τους Vandersypen, Steffen, Breyta, Yannoni, Sherwood, και Chuang το 2001 .

➢ Η ΠΡΩΤΗ ΠΩΛΗΣΗ ΚΒΑΝΤΙΚΟΥ ΥΠΟΛΟΓΙΣΤΗ

Τον αγόρασε αμερικανικός γίγαντας αεροδιαστημικής τεχνολογίας και συστημάτων ασφαλείας

Η πρώτη πώληση ενός κβαντικού υπολογιστή είναι γεγονός. Η Lockheed Martin που δραστηριοποιείται σε ένα ευρύ φάσμα δραστηριοτήτων υψηλής τεχνολογίας (αεροδιαστημική, ασφάλεια κ.α) και είναι η μεγαλύτερη προμηθεύτρια του αμερικανικού Πενταγώνου, αγόρασε έναν κβαντικό υπολογιστή από την εταιρία D-Wave που εδρεύει στον Καναδά.

Οι κβαντικοί υπολογιστές αναμένεται να φέρουν επανάσταση στον σύγχρονο κόσμο δίνοντας απίστευτη ώθηση σε κάθε τομέα έρευνας - από την πληροφορική και την φυσική μέχρι την ιατρική. Θα πρέπει να επισημανθεί βέβαια ότι οι ειδικοί υποστηρίζουν με την υπάρχουσα τεχνολογία θα χρειαστούν μερικές ακόμη δεκαετίες μέχρι να κάνει την εμφάνιση του ένας πλήρως λειτουργικός κβαντικός υπολογιστής.

Αυτό, σε συνδυασμό με τις ελάχιστες πληροφορίες που δίνονται στη δημοσιότητα για τον κβαντικό υπολογιστή που αγόρασε η Lockheed Martin, έχει οδηγήσει την επιστημονική κοινότητα στο να είναι ιδιαίτερα επιφυλακτική και να περιμένει την δημοσιοποίηση λεπτομερειών για τον μηχανισμό του υπολογιστή προκειμένου να τοποθετηθεί.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- http://el.wikipedia.org/wiki/%CE%A6%CF%89%CF%84%CE%BF%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%B9%CE%BA%CF%8C_%CF%86%CE%B1%CE%B9%CE%BD%CF%8C%CE%BC%CE%B5%CE%BD%CE%BF
- http://www.physics4u.gr/articles/2002/franckhertz.html
- http://users.sch.gr/apouliassis/Quantum%20Mechanics/photoelectric.htm
- http://www.physics4u.gr/articles/2002/comptonscatter.html
- el.wikipedia.org/wiki/Φαινόμενο_Κόμπτον
- http://hep.physics.uoc.gr/physics4/node19.html
- el.wikipedia.org/wiki/Κυματοσωματιδιακος_δυϊσμός
- Scientific American, Κβαντικά παράδοξα (Jim Al-Lhalili)
- Los Alamos National Laboratory , 3/2/2006

- ΣΤΕΦΑΝΟΣ ΤΡΑΧΑΝΑΣ - « ΚΒΑΝΤΟΜΗΧΑΝΙΚΗ Ι» - ΕΚΔΟΣΕΙΣ ΚΡΗΤΗΣ
- ΣΠΥΡΟΣ ΕΥΑΓΓΕΛΟΥ – «ΚΒΑΝΤΙΚΗ ΦΥΣΙΚΗ» - ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ 2001
- Γ. ΑΝΔΡΙΤΣΟΠΟΥΛΟΣ – «ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΒΑΝΤΟΜΗΧΑΝΙΚΗ» - ΕΚΔΟΣΕΙΣ ΠΑΠΑΣΩΤΗΡΙΟΥ
- RAYMOND A. SERWAY, CLEMENT J. MOSES, CURT A. MOYER – « ΣΥΓΧΟΝΗ ΦΥΣΙΚΗ» - ΕΚΔΟΣΕΙΣ ΚΡΗΤΗΣ
- SIMON SINGH – «ΚΩΔΙΚΕΣ ΚΑΙ ΜΥΣΤΙΚΑ» - ΕΚΔΟΣΕΙΣ ΤΡΑΥΛΟΣ
- WADE TRAPPE – LAWRENCE WASHINGTON –«INTRODUCTION TO CRYPTOGRAPHY» - ΔΕΥΤΕΡΗ ΕΚΔΟΣΗ