ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ **Ε**ΦΑΡΜΟΣΜΕΝΩΝ **Μ**ΑΘΗΜΑΤΙΚΩΝ **Κ**ΑΙ **Φ**ΥΣΙΚΩΝ **Ε**ΠΙΣΤΗΜΩΝ

ΚΑΤΕΥΘΥΝΣΗ ΜΑΘΗΜΑΤΙΚΟΥ

Κρυπτογραφία και Ελλειπτικές Καμπύλες

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΤΣΑΚΤΣΗΡΑ ΔΗΜΗΤΡΙΟΥ

Επιβλέπων : Παπαϊωάννου Αλέξανδρος

Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2011

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ

ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΚΑΤΕΥΘΥΝΣΗ ΜΑΘΗΜΑΤΙΚΟΥ

Κρυπτογραφία και Ελλειπτικές Καμπύλες

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΤΣΑΚΤΣΗΡΑ ΔΗΜΗΤΡΙΟΥ

Επιβλέπων : Παπαϊωάννου Αλέξανδρος

Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 14η Ιουλίου 2011.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Παπαϊωάννου Αλέξανδρος	Στεφανέας Πέτρος	Κουκουβίνος Χρήστος
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2011

ΤΣΑΚΤΣΗΡΑΣ ΔΗΜΗΤΡΙΟΣ

Διπλωματούχος Σχολής Μαθηματικών και Φυσικών Επιστημών Ε.Μ.Π.

Περίληψη

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.

Τα κρυπτογραφικά συστήματα που βασίζονται στις ελλειπτικές καμπύλες, αποτελούν ένα πολύ σημαντικό κομμάτι της κρυπτογραφίας δημόσιου κλειδιού και τα τελευταία χρόνια όλο και περισσότεροι επιστήμονες ασχολούνται με τη μελέτη τους. Το πλεονέκτημα των συστημάτων αυτών σε σχέση με τα συμβατικά κρυπτογραφικά συστήματα (π.χ. RSA) είναι ότι χρησιμοποιούν μικρότερες παραμέτρους και κλειδιά, προσφέροντας τα ίδια επίπεδα ασφάλειας.

Για το λόγο αυτό, τα κρυπτογραφικά συστήματα ελλειπτικών καμπυλών προτιμούνται σε συσκευές περιορισμένων πόρων, όπως οι έξυπνες κάρτες (smart cards) και τα κινητά τηλέφωνα. Ένα από τα πιο θεμελιώδη προβλήματα στα κρυπτογραφικά συστήματα ελλειπτικών καμπυλών, είναι η γένεση ελλειπτικών καμπυλών, κατάλληλων να προσφέρουν την ασφάλεια που απαιτείται από τις κρυπτογραφικές εφαρμογές.

Τέλος, γίνεται αναφορά στη γλώσσα προδιαγραφής Isabelle και τις προσπάθειες που έχουν γίνει για να προδιαγραφεί αλγεβρικά το κρυπτοσύστημα RSA.

Λέξεις Κλειδιά: <<κρυπτογραφία, ψηφιακές υπογραφές, RSA, Isabelle, γλώσσα προδιαγραφής, ελλειπτικές καμπύλες>>

Abstract

Diploma Thesis Title: “Cryptography and Elliptic Curves”

Abstract: The word cryptography comes from the geek words “kryptos” (=hidden) and “grapho” (=write) and it is a scientific sector that deals with the study, the development and the use of techniques of coding and decoding in order to hide the content of a message.

Cryptography is a part of the science of cryptology, which deals with the study of safe communication. Its main purpose is to provide tools and mechanisms to 2 or more members so as to communicate without interruptions from anyone else.

The cryptographic systems, which are based upon elliptic curves, are a very essential part of public key cryptography and during the last years more and more scientists study them. The advantage of these systems compared to conventional cryptographic systems (e.g. RSA) is that they use less parameters and keys, offering the same safety levels.

For this reason, the cryptographic elliptic curve systems are used in machines, such as smart cards and cell phones. One of the fundamental problems in such systems is the creation of elliptic curves which offer the safety that is required from the cryptographic applications.

Finally, there is a reference to the algebraic specification of RSA. It is an attempt that has been made with the use of the algebraic llanguage Isabelle.

Ευχαριστίες

Η διπλωματική αυτή εργασία δεν θα είχε ολοκληρωθεί ποτέ χωρίς τη συμβολή ορισμένων ανθρώπων. Κατ' αρχάς θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου Α. Παπαϊωάννου, για την καθοδήγηση που μου παρείχε σε κάθε φάση της δημιουργίας της, για την υποστήριξη και εμπιστοσύνη που έδειξε στο πρόσωπο μου. Επίσης θα ήθελα να ευχαριστήσω τον καθηγητή μου Π. Στεφανέα και το συνάδελφο Ν. Τριανταφύλλου για τη συνεισφορά στην κατανόηση της γλώσσας Isabella.

Εκτός από τους άμεσα συμβαλλόμενους, θα ήθελα να ευχαριστήσω τους γονείς μου Γιώργο και Δέσποινα για τη στήριξη που μου παρείχαν, οικονομική και συναισθηματική, για την επιτυχή διεκπεραίωση των σπουδών μου.

Τέλος, πάνω απ' όλα, θα ήθελα να ευχαριστήσω το σημαντικότερο άτομο στη ζωή μου, την Ηρώ, που με ενέπνευσε για την ενασχόληση με την κρυπτογραφία, για τη συνεχή βοήθεια και στήριξη για την ολοκλήρωση της διπλωματικής μου εργασίας, καθώς επίσης και καθ' όλη τη διάρκεια των σπουδών μου.

Πίνακας περιεχομένων

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

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

Η κρυπτογραφία είναι ένας κλάδος της επιστήμης της κρυπτολογίας, η οποία ασχολείται με τη μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς σε 2 ή περισσότερα μέλη, έτσι ώστε να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη. Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη "κρυπτός" και τη λέξη "λόγος" και χωρίζεται σε δύο κλάδους: την Κρυπτογραφία και την Κρυπτανάλυση.

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

Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες (αντικειμενικοί σκοποί):

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 δε μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.

Μη απάρνηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δε 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.

1.1 ΒΑΣΙΚΟΙ ΟΡΙΣΜΟΙ

Κρυπτογράφηση (*encryption*) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου, ούτως ώστε να μη μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.

Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση (*decryption*)**.

Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

Αρχικό κείμενο (*plaintext*) είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (*key*) είναι ένας αριθμός αρκετών bits που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (*ciphertext*) είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγορίθμου και ενός κλειδιού πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (*cryptanalysis*) είναι η επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής, ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

Στο σχήμα, που ακολουθεί, φαίνονται η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης:

Σχήμα: *Ένα τυπικό σύστημα κρυπτογράφησης – αποκρυπτογράφησης*

Η κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγορίθμου κρυπτογράφησης (cipher) και ενός κλειδιού κρυπτογράφησης (key). Συνήθως ο αλγόριθμος κρυπτογράφησης είναι γνωστός, οπότε η εμπιστευτικότητα του κρυπτογραφημένου μηνύματος, που μεταδίδεται, βασίζεται ως επί το πλείστον στη μυστικότητα του κλειδιού κρυπτογράφησης. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

1.2 ΒΑΣΙΚΗ ΑΡΧΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Ο αντικειμενικός στόχος της κρυπτογραφίας είναι να δώσει τη δυνατότητα σε 2 πρόσωπα, έστω το Βύρωνα και την Αλίκη , να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας

αντίπαλος), να μη μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων.

Ένα κρυπτοσύστημα (σύνολο διαδικασιών κρυπτογράφησης - αποκρυπτογράφησης) αποτελείται από μία πεντάδα (P,C,k,E,D):

Το P είναι ο χώρος όλων των δυνατών μηνυμάτων ή αλλιώς αρχικών κειμένων.

Το C είναι ο χώρος όλων των δυνατών κρυπτογραφημένων μηνυμάτων ή αλλιώς κρυπτοκειμένων.

Το k είναι ο χώρος όλων των δυνατών κλειδιών, ή αλλιώς κλειδοχώρος.

Η E είναι ο κρυπτογραφικός μετασχηματισμός ή κρυπτογραφική συνάρτηση.

Η D είναι η αντίστροφη συνάρτηση ή μετασχηματισμός αποκρυπτογράφησης.

Η συνάρτηση κρυπτογράφησης E δέχεται δύο παραμέτρους, μέσα από τον χώρο P και τον χώρο k και παράγει μία ακολουθία που ανήκει στο χώρο C. Η συνάρτηση αποκρυπτογράφησης D δέχεται 2 παραμέτρους, το χώρο C και το χώρο k και παράγει μια ακολουθία που ανήκει στο χώρο P.

Το Σχήμα Επικοινωνίας λειτουργεί με τον ακόλουθο τρόπο:

Ο αποστολέας επιλέγει ένα κλειδί μήκους *n* από το χώρο κλειδιών με τυχαίο τρόπο, όπου τα n στοιχεία του κλειδιού είναι στοιχεία από ένα πεπερασμένο αλφάβητο.

Αποστέλλει το κλειδί στον παραλήπτη μέσα από ένα ασφαλές κανάλι.

Ο αποστολέας δημιουργεί ένα μήνυμα από το χώρο μηνυμάτων.

Η συνάρτηση κρυπτογράφησης παίρνει τις δυο εισόδους (κλειδί και μήνυμα) και παράγει μια κρυπτοακολουθία συμβόλων (ένα γρίφο) και η ακολουθία αυτή αποστέλλεται διαμέσου ενός μη ασφαλούς καναλιού.

Η συνάρτηση αποκρυπτογράφησης παίρνει ως όρισμα τις 2 τιμές (κλειδί και γρίφο) και παράγει την ισοδύναμη ακολουθία μηνύματος.

Ο αντίπαλος παρακολουθεί την επικοινωνία, ενημερώνεται για την κρυπτοακολουθία αλλά δεν έχει γνώση για την κλείδα που χρησιμοποιήθηκε και δε μπορεί να αναδημιουργήσει το μήνυμα. Αν ο αντίπαλος επιλέξει να παρακολουθεί όλα τα μηνύματα θα προσανατολιστεί στην εξεύρεση του κλειδιού. Αν ο αντίπαλος ενδιαφέρεται μόνο για το υπάρχον μήνυμα θα παράγει μια εκτίμηση για την πληροφορία του μηνύματος.

Στο σημείο αυτό, όμως, αξίζει να κάνουμε μια ιστορική αναδρομή στην πορεία της τέχνης των κρυμμένων μυστικών.

Πρώτη Περίοδος Κρυπτογραφίας (1900 π.Χ. - 1900 μ.Χ.)

Κατά τη 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 στη 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 πηγή τον Kahn[1]). Επίσης, ως το αρχαιότερο βιβλίο κρυπτοκωδίκων 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 τη «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση τη 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 και όταν ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.

Στην αρχαιότητα χρησιμοποιήθηκαν κυρίως συστήματα, τα οποία βασίζονταν στη στεγανογραφία[2] 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

---

1 Kahn Louis Isadore: διεθνούς φήμης Αμερικανός αρχιτέκτονας. Αναφερθείσα πηγή: *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, 1200, 1996.

2 Στεγανογραφία: σε αντίθεση με την κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει την πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη "αθώα" πληροφορία με τέτοιον τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της.

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 δε διασώθηκε, αλλά αν και χαμένο, θεωρείται το πρώτο βιβλίο κρυπτολογίας. Το σύστημα αντικατάστασης του Καίσαρα, χρησιμοποιήθηκε ευρύτατα και τους επόμενους αιώνες.

Στη διάρκεια του Μεσαίωνα, η κρυπτολογία ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, κάτι που συνετέλεσε στην καθυστέρηση της ανάπτυξής 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 σημαντικότερη 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 του Γάλλου Champolion, 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 προσπάθειά 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». Παρόλ' αυτά, η προσπάθειά του άνοιξε το δρόμο προς τη 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. Μία με ιερογλυφικά, μία στα ελληνικά και μία σε ιερατική γραφή. Δύο μεγάλοι αποκρυπτογράφοι της εποχής, ο Γιάνγκ και κυρίως ο Σαμπολιόν, μοιράστηκαν τη 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 δε 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 τη Γραμμική γραφή Α, τόσο χρονικά όσο και τοπικά, όπως προκύπτει από τις ανασκαφές στο ανάκτορο των Μαλίων της Κρήτης. Εμφανίζεται στο Δίσκο της Φαιστού, που ανακαλύφθηκε το 1908 στη Νότια Κρήτη. Πρόκειται για μια κυκλική πινακίδα, που χρονολογείται γύρω στο 1700 π.Χ. και φέρει γραφή με τη μορφή δύο σπειρών. Τα σύμβολα δεν είναι χειροποίητα, αλλά έχουν χαραχθεί με τη βοήθεια μίας ποικιλίας σφραγίδων, καθιστώντας το Δίσκο ως το αρχαιότερο δείγμα στοιχειοθεσίας. Δεν υπάρχει άλλο ανάλογο εύρημα και έτσι η αποκρυπτογράφηση στηρίζεται σε πολύ περιορισμένες πληροφορίες. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Οι πρώτες επιγραφές με Γραμμική γραφή ανακαλύφθηκαν από τον Άρθουρ Έβανς (Sir Arthur Evans), το 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 στη 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 σύμβολά 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 τη 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 στη 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 τη 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 τα φυλλοειδή και «σελιδόσχημα», τα οποία 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, χρησιμοποιούσαν ετικέτες: ένα σφαιρίδιο πηλού, εντυπωμένο στην πρόσθια πλευρά, στο οποίο καταγράφονταν συνοπτικές πληροφορίες. Συστηματικά, με τη 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. Στη 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 (Αίνιγμα). Προσπάθησε να μεταφέρει την πείρα του στην κρυπτανάλυση της Γραμμικής Β, αλλά χωρίς επιτυχία μέχρι τότε. Ωστόσο, 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 τοποθετείται στις αρχές του 20ού 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 τη 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 κρυπτανάλυσή 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 τη διάρκεια αυτής της περιόδου, η κρυπτανάλυσή τους είναι συνήθως επιτυχημένη. Οι Γερμανοί έκαναν εκτενή χρήση (σε διάφορες παραλλαγές) ενός συστήματος γνωστού ως Enigma (Αίνιγμα).

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 βασίζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δε μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι, λίγο πριν τη Γερμανική εισβολή στην Πολωνία, 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, του Biuro Szyfrow (Γραφείο Κωδίκων), κατέληξαν σε συνεργασία με τους Βρετανούς και τους Γάλλους μετά από αυτή την εξέλιξη. Η συνεργασία αυτή συνεχίστηκε από τον Άλαν Τιούριγκ (Alan Turing)[3], τον Γκόρντον Ουέλτσμαν (Gordon Welchman) και από πολλούς άλλους στο Μπλέτσλεϊ Πάρκ (Bletchley Park), κέντρο της Βρετανικής Υπηρεσίας αποκρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma, με τη 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 το 1940) έσπασαν αρκετά κρυπτοσυστήματα του Ιαπωνικού ναυτικού. Το σπάσιμο ενός από αυτά, του JN-25, οδήγησε στην αμερικανική νίκη στη Ναυμαχία της Μιντγουέι καθώς και στην εξόντωση του Αρχηγού του Ιαπωνικού Στόλου Ιζορόκου Γιαμαμότο.

Το Ιαπωνικό Υπουργείο Εξωτερικών χρησιμοποίησε ένα τοπικά ανεπτυγμένο κρυπτογραφικό σύστημα 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

3 Turing Alan: Άγγλος μαθηματικός, κρυπταναλυτής και επιστήμονας των υπολογιστών. Με τη βοήθεια της μηχανής Turing έδωσε μία προτυποποίηση των εννοιών “αλγόριθμοι” και “υπολογιστικότητα”, που έπαιξαν σημαντικό ρόλο στη δημιουργία του σύγχρονου υπολογιστή. Κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου, ο Turing εργάστηκε για τη Βρετανική Κυβέρνηση σπάζοντας Γερμανικούς κωδικούς. Πέθανε την ημέρα των 42ων γενεθλίων του, αυτοκτονώντας με κυάνιο.

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 στο Β' Παγκόσμιο Πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA. 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 έναν 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 προανήγγειλε την απόβαση. Η Γερμανική ηγεσία δεν έλαβε υπόψη της αυτήν την προειδοποίηση.

Οι Πολωνοί, από την άλλη, 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 τη "σπάσει" και έτσι αναγκάστηκαν να την αλλάξουν βιαστικά. Τα μηνύματα που εστάλησαν με Lacida δεν ήταν, ωστόσο, συγκρίσιμα με αυτά του Enigma, αλλά η παρεμπόδιση θα μπορούσε να έχει σημάνει το τέλος της κρίσιμης κρυπταναλυτικής Πολωνικής προσπάθειας.

Λίγο πριν τελειώσουμε με τη δεύτερη αυτή περίοδο της κρυπτογραφίας, αξίζει να κάνουμε μία αναφορά στον επιτυχή Αμερικανικό κώδικα που βασίστηκε στη γλώσσα των Ναβάχο (Navajo). Το 1942, οι πρώτοι 29 νεοσύλλεκτοι συγκεντρώθηκαν στο στρατόπεδο εκπαίδευσης ναυτικών. Έτσι, στο Στρατόπεδο Pendleton, στο Oceanside της California, η πρώτη ομάδα δημιούργησε τον κώδικα Ναβάχο. Ανέπτυξαν ένα λεξικό και όλες οι κώδικες λέξεις έπρεπε να απομνημονευθούν κατά τη διάρκεια της εκπαίδευσης. Οι στρατιώτες Ναβάχο μπορούσαν να κρυπτογραφήσουν, να μεταδώσουν και να αποκρυπτογραφήσουν ένα μήνυμα 3 γραμμών στα Αγγλικά σε 20 δευτερόλεπτα. Οι μηχανές της εποχής εκείνης απαιτούσαν 30 λεπτά για να κατορθώσουν το ίδιο. Σχεδόν 400 στρατιώτες Ναβάχο πήραν μέρος σε κάθε επίθεση της Αμερικής: Guadalcanal, Tarawa, Pelelin, Iwo Jima. Οι πεζοναύτες κυριάρχησαν στον Ειρηνικό Ωκεανό από το 1942 έως το 1945. Υπηρέτησαν και στις 6 μονάδες πεζοναυτών, στους καταδρομείς και στους αλεξιπτωτιστές, μεταδίδοντας μηνύματα μέσω τηλεφώνου και ραδιοφώνου στη μητρική τους γλώσσα – έναν κώδικα που οι Ιάπωνες ποτέ δεν κατάφεραν να σπάσουν.

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, που αναμφισβήτητα είναι ο πατέρας των μαθηματικών συστημάτων επικοινωνίας. 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. Με αυτές τις δημοσιεύσεις του, αλλά και με άλλες εργασίες του επάνω στην θεωρία δεδομένων και επικοινωνίας, καθιέρωσε μια στέρεη 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 (δηλαδή 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 ομοσπονδιακό 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 Βέλγους - Φλαμανδούς κρυπτογράφους, για να είναι το AES. Ο DES και οι ασφαλέστερες παραλλαγές του, όπως ο 3DES ή TDES, χρησιμοποιούνται ακόμα σήμερα, ενσωματωμένα σε πολλά εθνικά και οργανωτικά πρότυπα. Εν τούτοις, 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 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 τη χρήση του 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.

1.3 ΕΙΔΗ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΩΝ

Τα μοντέρνα κρυπτοσυστήματα χωρίζονται σε δύο κατηγορίες: τα συστήματα συμμετρικής κρυπτογραφίας και τα συστήματα ασύμμετρης κρυπτογραφίας. Παρόλο που στην παρούσα εργασία θα ασχοληθούμε μόνο με συστήματα ασύμμετρης κρυπτογραφίας, παρακάτω αναφέρουμε επιγραμματικά και τα δύο είδη των μοντέρνων κρυπτοσυστημάτων.

Α) Συμμετρικά Κρυπτοσυστήματα

Συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά τη διαδικασία της κρυπτογράφησης αποκρυπτογράφησης ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από τη φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων.

Τα στάδια της επικοινωνίας του συμμετρικού κρυπτοσυστήματος είναι τα ακόλουθα:

Ο Βύρωνας ή η Αλίκη αποφασίζει για ένα κλειδί, το οποίο το επιλέγει τυχαία μέσα από τον κλειδοχώρο.

Η Αλίκη αποστέλλει το κλειδί στο Βύρωνα μέσα από ένα ασφαλές κανάλι.

Ο Βύρωνας δημιουργεί ένα μήνυμα όπου τα σύμβολα m ανήκουν στο χώρο των μηνυμάτων.

Κρυπτογραφεί το μήνυμα με το κλειδί που έλαβε από την Αλίκη και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται.

Η Αλίκη λαμβάνει την κρυπτοσυμβολοσειρά και στη συνέχεια με το ίδιο κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

Παράδειγμα κρυπτογράφησης

Έχουμε το αρχικό μήνυμα, (ένα σύνολο δυαδικών ψηφίων (bits) {μi, όπου i = 1, 2, …, n}), και το κλειδί γνωστό σε αποστολέα και παραλήπτη, (ένα άλλο σύνολο δυαδικών ψηφίων {κi, όπου i = 1, 2, …, n}). Αν δημιουργήσουμε το γρίφο που θα αποσταλεί, (ένα σύνολο δυαδικών ψηφίων γi, που να ικανοποιούν τη σχέση {γi = μi XOR[4] κi, όπου i = 1, 2, …, n}), τότε θα ισχύει επίσης ότι {μi = γi XOR κi, όπου i = 1, 2, …, n} και ο παραλήπτης του γρίφου με χρήση του κλειδιού θα αναδημιουργήσει το μήνυμα.

Μηνύματα μεγάλου μήκους μπορούν να κρυπτογραφούνται σε ομάδες των n δυαδικών ψηφίων.

Β) Ασύμμετρα Κρυπτοσυστήματα

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Χαρακτηριστικό του είναι ότι έχει δύο είδη κλειδιών: ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους, ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι πως ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο.

Τα στάδια της επικοινωνίας του ασύμμετρου κρυπτοσυστήματος είναι τα ακόλουθα:

Η γεννήτρια κλειδιών του Βύρωνα παράγει 2 ζεύγη κλειδιών.

Η γεννήτρια κλειδιών της Αλίκης παράγει 2 ζεύγη κλειδιών.

Η Αλίκη και ο Βύρωνας ανταλλάσσουν τα δημόσια ζεύγη.

Ο Βύρωνας δημιουργεί ένα μήνυμα, όπου τα σύμβολα m ανήκουν στο χώρο των μηνυμάτων.

---

4 Η λογική έκφραση "XOR", πολύ γνωστή από τους προγραμματιστές, χρησιμοποιείται ως αποκλειστική αλλαγή. Όταν χρησιμοποιείται μεταξύ δύο συνθηκών, μέσα σ' ένα φίλτρο, το αποτέλεσμα θα εμφανιστεί στην οθόνη μόνο αν μια από τις δύο συνθήκες ισχύει, αλλά όχι όταν ισχύουν και οι δύο, όπως γίνεται με τη λογική έκφραση "OR".

Κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί της Αλίκης και η παραγόμενη κρυπτοσυμβολοσειρά αποστέλλεται.

Η Αλίκη λαμβάνει την κρυπτοσυμβολοσειρά και στη συνέχεια με το ιδιωτικό της κλειδί την αποκρυπτογραφεί και η έξοδος που παράγεται είναι το μήνυμα.

1.4 Η ΚΡΥΠΤΟΓΡΑΦΙΑ ... ΣΗΜΕΡΑ

Τα τελευταία χρόνια, η κρυπτογραφία είναι ένα από τα πιο δημοφιλή θέματα συζητήσεων μέσα στο Διαδίκτυο. Έχει γίνει συνείδηση στους χρήστες του δικτύου ότι η ασφάλεια των πληροφοριών, του πιο πολύτιμου ίσως αγαθού στις μέρες μας, πρέπει να μας απασχολεί όλους. Γι' αυτό, κάθε τόσο βλέπουμε να εμφανίζονται νέα προϊόντα προστασίας δεδομένων, νέοι αλγόριθμοι και φυσικά όλο και μεγαλύτερα κλειδιά (κωδικοί).

Η κοινή λογική μάς λέει πως όσο πιο μεγάλο είναι το κλειδί, που χρησιμοποιούμε για την κρυπτογράφηση των δεδομένων μας, τόσο περισσότερο χρόνο και υπολογιστική ισχύ θα χρειαστεί κάποιος για να το αποκρυπτογραφήσει. Για παράδειγμα, αν κρυπτογραφηθεί ένα μήνυμα χρησιμοποιώντας κλειδί με μέγεθος 56 bit (π.χ. DES), τότε οι πιθανοί συνδυασμοί που πρέπει να δοκιμάσει κάποιος για να το αποκρυπτογραφήσει είναι 2 εις την 56η (72.057.600.000.000.000 συνδυασμοί). Αυτή η μέθοδος, η δοκιμή όλων των δυνατών συνδυασμών μέχρι να βρεθεί ο σωστός, έχει γίνει γνωστή με το όνομα ωμή βία (brute force).

Βέβαια τα πράγματα δεν είναι ακριβώς έτσι, μιας και ο αριθμός αυτός (2 εις την 56η) αναφέρεται στο σύνολο των συνδυασμών. Μπορεί κανείς να φανεί τυχερός και να βρει το σωστό κωδικό με την πρώτη προσπάθεια ή άτυχος και να τον βρει με την τελευταία. Στατιστικά, αυτό θα γίνει κάπου στη μέση, δηλαδή στους 36.028.800.000.000.000 συνδυασμούς.

Οι ειδικοί λένε πως πρέπει να χρησιμοποιούμε όλο και μεγαλύτερα κλειδιά, διότι το κόστος των Η/Υ μειώνεται συνεχώς και γίνεται όλο και πιο εύκολο να δοκιμάσει κανείς έναν έναν όλους τους δυνατούς συνδυασμούς μέχρι να βρει το σωστό κλειδί. Σήμερα συνιστώνται κλειδιά μεγέθους 1024 bit ή μεγαλύτερα (1024 bit = 1.797.700.000 συνδυασμοί).

Με την υπάρχουσα τεχνολογία Η/Υ, για να σπάσει κάποιος έναν κώδικα με κλειδί 1024 bit θα χρειαζόταν πάρα πολλά χρόνια ή ένα απίστευτο ποσό χρημάτων για να αγοράσει ή νοικιάσει τους μισούς Η/Υ του κόσμου...

Μπορεί όμως και όχι!

Τα τελευταία χρόνια, έχει αναπτυχθεί ένα νέο είδος κρυπτοαναλυτικών (αποκρυπτογραφικών) επιθέσεων που βασίζεται στα ιδιαίτερα χαρακτηριστικά κάθε προγράμματος κρυπτογράφησης. Ο κρυπτοαναλυτής μελετάει το χρόνο που κάνει κάθε κρυπτογράφηση για να ολοκληρωθεί, την κατανάλωση ρεύματος, τις εκπομπές ακτινοβολίας της συσκευής, τις αντιδράσεις του προγράμματος σε κάθε λανθασμένη εισαγωγή δεδομένων κ.λπ. και χρησιμοποιεί αυτά τα στοιχεία για να "μαντέψει" το κλειδί που χρησιμοποιείται για την κρυπτογράφηση.

Τέτοιες τακτικές έχουν χρησιμοποιηθεί με μεγάλη επιτυχία για να "ξεκλειδώσουν" έξυπνες κάρτες (smart cards)[5], Internet electronic commerce servers και άλλους μηχανισμούς ασφαλείας. Υπάρχουν, βέβαια, κάποιοι ρομαντικοί που τις χαρακτηρίζουν ανέντιμες (unfair), γιατί δε βασίζονται στα μαθηματικά αλλά σε ανάλυση στο φυσικό επίπεδο (ελαττώματα του λογισμικού και του υλικού που χρησιμοποιείται για την κρυπτογράφηση). Αυτό όμως είναι δευτερεύον. Δεν υπάρχουν κανόνες καλής συμπεριφοράς, όταν προσπαθείς να βρεις τα μυστικά του αντιπάλου σου και σίγουρα κανείς δεν θα είναι τόσο ρομαντικός, ώστε να εγκαταλείψει το πανίσχυρο όπλο της επίθεσης στο φυσικό επίπεδο (Side-channel cryptanalysis)[6]. Για να γίνει μάλιστα αντιληπτό πόσο ισχυρές είναι αυτές οι τεχνικές, αρκεί να σας αναφέρουμε πως για να μπορέσει κάποιος να βρει το κλειδί του γνωστού κρυπτογραφικού αλγόριθμου DES με το μαθηματικό τρόπο (αναλύοντας όλες τις πιθανές λύσεις), θα πρέπει να κάνει περίπου 5,5 εκατομμύρια περισσότερες προσπάθειες απ' ότι με μια επίθεση στο φυσικό επίπεδο (ο υπολογισμός αυτός αναφέρεται σε σύστημα που δεν έχει καμία προστασία από επιθέσεις του τύπου αυτού).

Το συμπέρασμα που βγαίνει από τα παραπάνω δεν είναι καθόλου ενθαρρυντικό. Αν και οι κατασκευαστές κρυπτογραφικών προϊόντων προσπαθούν να τα προστατέψουν από τέτοιες επιθέσεις, θα χρειαστεί να περάσουν αρκετά χρόνια μέχρι να εμφανιστούν και να δοκιμαστούν ειδικά πρότυπα προστασίας από επιθέσεις στο φυσικό επίπεδο. Μέχρι, όμως, να έρθει εκείνη η ημέρα, δυστυχώς θα πρέπει να

---

5 Η έξυπνη κάρτα είναι μια κάρτα, η οποία μοιάζει πολύ, εξωτερικά, με την πιστωτική κάρτα. Η πιστωτική κάρτα είναι ένα κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία, στην οποία είναι εγγεγραμμένα κάποια στοιχεία του χρήστη. Η έξυπνη κάρτα, αντίθετα, ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή με χρυσό, προσαρμοσμένο στη μια πλευρά της. Η βασική διαφορά των δύο καρτών είναι ότι, ενώ τα δεδομένα στη μαγνητική ταινία είναι εύκολο να παραλλαχθούν ή και να διαγραφούν (ακόμη και τυχαία), αυτό δεν είναι δυνατό στην έξυπνη κάρτα, γιατί ο μικροεπεξεργαστής της δεν περιέχει δεδομένα για το χρήστη. Ο μικροεπεξεργαστής της κάρτας και ο υπολογιστής, με τον οποίο συνδέεται, επικοινωνούν πριν ο μικροεπεξεργαστής επιτρέψει την πρόσβαση στα δεδομένα που περιέχονται στη μνήμη της κάρτας. Με τον τρόπο αυτό αποτρέπεται η παραχάραξη των δεδομένων κι έτσι ο χρήστης διασφαλίζεται, αν η κάρτα του βρεθεί σε διαφορετικά από τα δικά του χέρια.

6 Οποιαδήποτε επίθεση που βασίζεται σε φυσικές υλοποιήσεις ενός κρυπτοσυστήματος, παρά σε θεωρητικές αδυναμίες των αλγορίθμων. Για παράδειγμα, πληροφορίες συγχρονισμού, κατανάλωση ενέργειας, ηλεκτρομαγνητικές διαρροές κλπ.

θεωρούμε όλα τα προγράμματα κρυπτογράφησης πολύ λιγότερο αποτελεσματικά απ' ότι πιστεύαμε μέχρι σήμερα.

ΚΕΦΑΛΑΙΟ 2

ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ – ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ

Η θεωρία αριθμών και οι αλγεβρικές δομές τα τελευταία χρόνια χρησιμοποιούνται όλο και περισσότερο στην κρυπτολογία. Αριθμοθεωρητικοί αλγόριθμοι χρησιμοποιούνται ευρέως εξαιτίας εν μέρει της ανακάλυψης των κρυπτογραφικών σχημάτων τα οποία στηρίζονται σε μεγάλους πρώτους αριθμούς. Από την άλλη πλευρά, αν ο ακέραιος n είναι πρώτος, τότε οι ακέραιοι modulo n αποκτούν τη δομή ενός πεπερασμένου σώματος. Επίσης, οι ελλειπτικές καμπύλες επί πεπερασμένων σωμάτων παρέχουν παραδείγματα ομάδων των οποίων η δομή είναι εξίσου απλή ή απλούστερη από τη δομή της πολλαπλασιαστικής ομάδας $(Z_p^*, \cdot)$.

Η θεωρία των αριθμών είναι ο κλάδος της επιστήμης των μαθηματικών που ασχολείται με τη μελέτη των ιδιοτήτων των ακεραίων. Λέγοντας ακέραιοι δεν εννοούμε μόνο τους αριθμούς της ακολουθίας των φυσικών 1, 2, 3, … (θετικοί ακέραιοι), αλλά και το μηδέν και τους αρνητικούς ακεραίους -1, -2, -3, … Το άθροισμα, η διαφορά και το γινόμενο δύο ακεραίων α και b είναι επίσης ακέραιος, αλλά το πηλίκο που προκύπτει από τη διαίρεση του α με το b (αν ο b δεν είναι μηδέν) μπορεί να είναι ακέραιος, μπορεί όμως και να μην είναι.

Στην περίπτωση κατά την οποία το πηλίκο που προκύπτει από τη διαίρεση του α με τον b είναι ένας ακέραιος, έστω q, θα έχουμε $\alpha = b \cdot q$, δηλαδή ο α είναι ίσος με το γινόμενο του b επί έναν ακέραιο. Τότε λέμε ότι ο α είναι διαιρετός από τον b ή ότι ο b διαιρεί τον α. Εδώ χαρακτηρίζεται ο α πολλαπλάσιο του b και ο b διαιρέτης του α. Το ότι ο b διαιρεί τον α συμβολίζεται με $b|\alpha$.

2.1 Ο ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ

Στα επόμενα θα θεωρούμε μόνο τους θετικούς διαιρέτες των αριθμών. Κάθε ακέραιος που διαιρεί τους ακεραίους α, b λέγεται κοινός διαιρέτης των αριθμών αυτών. Ο μεγαλύτερος από αυτούς τους κοινούς διαιρέτες λέγεται μέγιστος κοινός διαιρέτης και συμβολίζεται με gcd(α, b). Μια και οι κοινοί διαιρέτες είναι πεπερασμένοι το πλήθος, η ύπαρξη του μέγιστου κοινού διαιρέτη γίνεται φανερή. Αν gcd(α, b) = 1, τότε οι α, b χαρακτηρίζονται σαν πρώτοι μεταξύ τους. Αν δύο οποιοιδήποτε από τους αριθμούς α, b είναι πρώτοι μεταξύ τους, τότε οι α, b χαρακτηρίζονται σαν ανά ζεύγη πρώτοι. Είναι φανερό ότι ένα πλήθος αριθμών που είναι ανά ζεύγη πρώτοι, θα είναι και μεταξύ τους πρώτοι· στην περίπτωση δύο αριθμών, οι έννοιες «ανά ζεύγη πρώτοι» και «πρώτοι μεταξύ τους» συμπίπτουν.

Προκειμένου να βρούμε το μέγιστο κοινό διαιρέτη, αλλά και να συνάγουμε τις πιο σπουδαίες ιδιότητές του, εφαρμόζουμε τον Ευκλείδειο αλγόριθμο. Αυτός συνίσταται στην εξής διαδικασία:

Έστω ότι οι α και b είναι θετικοί ακέραιοι. Θα ισχύει η εξής ακολουθία ισοτήτων:

$\alpha = bq_2 + r_2 \qquad , 0 < r_2 < b$

$b = r_1q_3 + r_3 \qquad , 0 < r_3 < r_2$

$r_2 = r_3q_4 + r_4 \qquad , 0 < r_4 < r_3$

……..

$r_{\kappa-2} = r_{n-1}q_n + r_n \quad , 0 < r_n < r_{n-1}$

$r_{n-1} = r_nq_{n+1}$

η οποία σταματά όταν βρούμε κάποιο υπόλοιπο $r_{n-1} = 0$. Αυτό το τελευταίο πρέπει κάποτε να συμβεί, αφού η ακολουθία b, r_2, r_3, … σα φθίνουσα ακολουθία ακεραίων δε μπορεί να περιέχει περισσότερους από b το πλήθος θετικούς ακεραίους.

2.2 ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

Ο αριθμός 1 έχει μόνον ένα θετικό διαιρέτη, συγκεκριμένα τον 1. Εξαιτίας αυτού του γεγονότος, ο αριθμός 1 κατέχει μοναδική θέση στην ακολουθία των φυσικών αριθμών.

Κάθε ακέραιος, μεγαλύτερος από τον 1, έχει τουλάχιστον δύο διαιρέτες: τον 1 αι τον εαυτό του. Αν αυτοί οι διαιρέτες είναι και οι μοναδικοί θετικοί διαιρέτες του ακεραίου αυτού, τότε αυτός λέγεται πρώτος. Ένας ακέραιος μεγαλύτερος του 1 που έχει και άλλους θετικούς διαιρέτες εκτός από το 1 και τον εαυτό του λέμε ότι είναι σύνθετος.

Ο ελάχιστος, διάφορος του 1, διαιρέτης ενός ακεραίου μεγαλύτερου του ένα, είναι πρώτος αριθμός. Πραγματικά, έστω ότι q είναι ο μικρότερος διαιρέτης, διάφορος του 1, ενός ακεραίου $\alpha > 1$. Αν ο q ήταν σύνθετος, τότε θα είχε κάποιο διαιρέτη q_1, τέτοιον ώστε $1 < q_1 < q$. Αλλά μιας και ο α είναι διαιρετός από τον q, θα είναι επίσης διαιρετός από τον q_1 και αυτό έρχεται σε αντίθεση με την υπόθεσή μας σχετικά με τον q.

2.3 ΤΕΤΡΑΓΩΝΙΚΑ ΥΠΟΛΟΙΠΑ

ΟΡΙΣΜΟΣ: Έστω η ισοτιμία $x^2 \equiv \alpha \pmod n$

όπου n φυσικός αριθμός και α ακέραιος αριθμός πρώτος προς τον n. Τότε ο α θα καλείται τετραγωνικό υπόλοιπο modulo n. Για κάθε περιττό πρώτο αριθμό υπάρχουν ακριβώς $(p - 1)/2$ τετραγωνικά υπόλοιπα modulo p. αν ο αριθμός α είναι τετραγωνικό υπόλοιπο modulo p, τότε ισχύει

$$\alpha^{(p-1)/2} \equiv 1 \pmod p,$$

ενώ αν ο α δεν είναι τετραγωνικό υπόλοιπο modulo p, τότε ισχύει

$\alpha^{(p-1)/2} \equiv -1 \pmod{p}$.

Οι ισοτιμίες αυτές μπορούν να χρησιμοποιηθούν για να ελεγχθεί εάν ένας αριθμός είναι τετραγωνικό υπόλοιπο ή όχι.

Το σύμβολο του Legendre (α/p), όπου p είναι ένας περιττός πρώτος αριθμός και α ένας ακέραιος αριθμός πρώτος προς τον p, ορίζεται ως εξής:

$$(\alpha/p) \equiv \alpha^{(p-1)/2} \pmod{p}$$

και

(α/p) = -1, αν ο α δεν είναι τετραγωνικό υπόλοιπο modulo p ή

(α/p) = 1, αν ο α είναι τετραγωνικό υπόλοιπο modulo p.

2.4 ΤΕΤΡΑΓΩΝΙΚΕΣ ΜΟΡΦΕΣ

ΟΡΙΣΜΟΣ: Ένα πολυώνυμο της μορφής

$$F(x_1, \ldots, x_m) = {}^{m}\sum_{i\,j\,=\,1} c_{ij}\, x_i\, x_j,$$

όπου οι συντελεστές c_{ij} είναι ακέραιοι, καλείται ακέραια τετραγωνική μορφή.

Αν m = 2, τότε η τετραγωνική μορφή F καλείται δυαδική. Ένας ακέραιος n λέμε ότι μπορεί να αναπαρασταθεί από την ακέραια τετραγωνική μορφή F αν υπάρχουν ακέραιοι $z_1, \ldots, z_m$ έτσι ώστε $n = F(z_1, \ldots, z_m)$.

Εξισώσεις της μορφής $f(x_1, \ldots, x_m) = 0$, όπου $f(x_1, \ldots, x_m)$ είναι ένα πολυώνυμο n μεταβλητών με ακέραιους συντελεστές καλούνται Διοφαντικές εξισώσεις. Οι εξισώσεις πήραν το όνομά τους από τον Έλληνα μαθηματικό Διόφαντο, ο οποίος έζησε τον 3ο αιώνα π.Χ. Και ήταν ο πρώτος που μελέτησε συστηματικά εξισώσεις τέτοιας μορφής.

2.5 ΟΜΑΔΕΣ

Έστω Ε ένα μη κενό σύνολο. Καλούμε πράξη επί του Ε μια απεικόνιση $E \times E \rightarrow E$. Για παράδειγμα, η πρόσθεση και ο πολλαπλασιασμός είναι πράξεις επί του Z.

Ένας ζεύγος (G, *), όπου G είναι ένα μη κενό σύνολο και * μία πράξη από το $G_r * G_r \rightarrow G$ με $(x, y) \rightarrow x * y$

καλείται ομάδα (group), αν η πράξη * έχει τις εξής ιδιότητες:

$x * (y * z) = (x * y) * z$ για κάθε x, y, z Є G (προσεταιριστικός νόμος)

υπάρχει α Є G τέτοιο ώστε για κάθε x Є G να ισχύει

$$x * g = x = g * x$$

για κάθε x Є G, υπάρχει x' Є G τέτοιο ώστε

$$x * x' = g = x' * x.$$

4. Η πράξη είναι κλειστή.

Το g είναι το μοναδικό στοιχείο που έχει την ιδιότητα και καλείται ουδέτερο στοιχείο της ομάδας G. Για κάθε x Є G το στοιχείο x' είναι μοναδικό και καλείται

συμμετρικό του x. Αν επιπλέον η πράξη * είναι αντιμεταθετική, δηλαδή έχει την ιδιότητα x * y = y * x, για κάθε x, y Є G, τότε η ομάδα G καλείται αντιμεταθετική ή αβελιανή. Συχνά, συμβολίζουμε την πράξη * μιας ομάδας (G, *) σαν πολλαπλασιασμό. Τότε η ομάδα καλείται πολλαπλασιαστική και γράφουμε xy αντί για x * y. Όταν η ομάδα G είναι αβελιανή, συχνά συμβολίζουμε την πράξη * και σαν πρόσθεση. Τότε η ομάδα καλείται προσθετική, οπότε γράφουμε x + y αντί για x * y.

2.6 ΔΑΚΤΥΛΙΟΙ – ΣΩΜΑΤΑ

Δακτύλιος λέγεται μια αλγεβρική δομή <R, +, *>, η οποία αποτελείται από ένα σύνολο R, με τουλάχιστον δύο στοιχεία {0, 1}, εφοδιασμένο με δύο διμελείς πράξεις + και * που ορίζονται σε αυτό και οι οποίες αποκαλούνται αντίστοιχα πρόσθεση και πολλαπλασιασμός, έτσι ώστε να ικανοποιούνται τα ακόλουθα αξιώματα:

Το <R, +> (δηλαδή το R μαζί με την πρόσθεση +) είναι μια αβελιανή ομάδα με ουδέτερο στοιχείο το 0:

(a + b) + c = a + (b + c)

a + b = b + a

0 + a = a + 0 = a

Για κάθε a, υπάρχει (-a) τέτοιο ώστε a + - a = -a + a = 0

Ο πολλαπλασιασμός (*) ικανοποιεί την προσεταιριστική ιδιότητα (δηλαδή α*(β*γ) = (α*β)*γ).

Ο πολλαπλασιασμός (*) είναι επιμεριστικός ως προς την πρόσθεση. Δηλαδή, για κάθε a, b, c ϵ R ισχύουν ο αριστερός επιμεριστικός νόμος, a*(b + c) = a*b + a*c και ο δεξιός επιμεριστικός νόμος (a + b)*c = a*c + b*c.

Και οι δύο πράξεις είναι κλειστές στο R.

Εάν επιπλέον ορίζεται στο δακτύλιο μοναδιαίο στοιχείο, δηλαδή ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό (*), ο δακτύλιος λέγεται δακτύλιος με μοναδιαίο, δακτύλιος με μονάδα ή 1 – δακτύλιος.

Αν ο πολλαπλασιασμός είναι μεταθετικός, δηλαδή ισχύει a*b = b*a, για κάθε a, b, τότε ο δακτύλιος λέγεται αντιμεταθετικός ή μεταθετικός.

Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο, που θα το συμβολίζουμε με 1. Ένα στοιχείο u ϵ R λέγεται αντιστρέψιμο αν έχει πολλαπλασιαστικό αντίστροφο στον R, δηλαδή: Το u είναι αντιστρέψιμο, αν και μόνο αν υπάρχει b ϵ R τέτοιο ώστε a * b = 1 = b * a.

Αν κάθε μη μηδενικό στοιχείο του R είναι αντιστρέψιμο, τότε ο R λέγεται δακτύλιος διαίρεσης.

Ας σημειωθεί στο σημείο αυτό ότι οι δύο πράξεις + και * που περιγράφονται μπορούν να είναι οποιεσδήποτε δύο πράξεις που ικανοποιούν τις συνθήκες που αναφέρονται πιο πάνω, όχι αναγκαστικά η πρόσθεση και ο πολλαπλασιασμός. Έχει επικρατήσει να ονομάζονται «πρόσθεση» και «πολλαπλασιασμός» οι δύο αυτές πράξεις των δακτυλίων για λόγους απλότητας.

Ένας αντιμεταθετικός δακτύλιος διαίρεσης είναι σώμα. Ειδικότερα, κάθε σώμα είναι δακτύλιος.

Σώμα , δηλαδή, είναι ένα σύνολο F αντικειμένων οποιουδήποτε είδους, μαζί με δύο δυαδικές πράξεις + και * ορισμένες στο F, οι οποίες απεικονίζουν σε 2 στοιχεία a και b που ανήκουν στο F, άλλα στοιχεία, a + b και a * b, πάλι στο F (ορισμός κλειστότητας). Και ισχύουν οι εξής ιδιότητες:

(a + b) + c = a + (b + c)

Υπάρχει στοιχείο 0 που ανήκει στο F τέτοιο ώστε

a + 0 = a για κάθε a που ανήκει στο F και

Για κάθε a που ανήκει στο F υπάρχει b που ανήκει στο F τέτοιο ώστε a + b = 0.

a + b = b + a. Δηλαδή να ισχύει η αντιμεταθετική ιδιότητα στο F.

(a * b) * c = a * (b * c)

Υπάρχει αριθμός 1 που ανήκει στο F τέτοιος ώστε

a * 1 = a.

Υπάρχει, για κάθε a διάφορο του 0, ένα b, τέτοιο ώστε a * b = 1.

a * b = b * a

a * (b + c) = a * b + a * c

Γνωστά παραδείγματα σωμάτων είναι το Q, το R και το σώμα των μιγαδικών αριθμών C.

2.7 ΣΩΜΑΤΑ ΕΠΕΚΤΑΣΗΣ

Ένα σώμα K θα λέγεται σώμα επέκτασης ή απλά επέκταση ενός άλλου σώματος F, αν το F είναι υποσύνολο του K. Στην περίπτωση αυτή το F λέγεται υπόσωμα του K. Με K/F ή [K:F] θα δηλώνεται ότι το σώμα K είναι σώμα επέκτασης του F.

Για παράδειγμα, οι μιγαδικοί αριθμοί αποτελούν σώμα επέκτασης των πραγματικών αριθμών και οι πραγματικοί αριθμοί αποτελούν σώμα επέκτασης των ρητών αριθμών.

Επεκτάσεις K του σώματος Q των ρητών αριθμών μπορούν να κατασκευαστούν εύκολα αν προσθέσουμε σε αυτό έναν αλγεβρικό αριθμό θ. Αλγεβρικός καλείται ένας αριθμός αν είναι ρίζα ενός πολυωνύμου με ρητούς συντελεστές. Η επέκταση θα συμβολίζεται ως K = Q(θ). Τα στοιχεία α της επέκτασης K έχουν τότε τη μορφή:

$$\alpha = \alpha_0 + \alpha_1\theta + ... + \alpha_{n-1}\theta^{n-1}$$

όπου $\alpha_i \in Q$ για i = 0, ..., n-1 και n είναι ο βαθμός του ανάγωγου πολυωνύμου του θ. Το n καλείται επίσης βαθμός της επέκτασης K. Τα $[1, \theta, ..., \theta^{n-1}]$ αποτελούν μια βάση της επέκτασης K, γιατί κάθε αριθμός που ανήκει στην επέκταση μπορεί να κατασκευαστεί από τους n αυτούς αριθμούς.

2.8 ΠΕΠΕΡΑΣΜΕΝΑ ΣΩΜΑΤΑ ΤΑΞΗΣ p

Για δοθέντα πρώτο p, το πεπερασμένο σώμα τάξεως p, GF(p) ορίζεται ως η αλγεβρική δομή $(Z_p, +_p, *_p)$, το σύνολο δηλαδή $Z_p = \{0, 1, 2, \ldots, p-1\}$ εφοδιασμένο με τις αριθμητικές πράξεις, modulo p – πρόσθεση mod p και πολλαπλασιασμός mod

p. Το σύνολο $Z_n = \{0, 1, 2, , \ldots, n-1\}$, των ακεραίων, εφοδιασμένο με τις αριθμητικές πράξεις, modulo n, είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο και ότι κάθε ακέραιος στο Z_n έχει αντίστροφο αν και μόνον αν ο ακέραιος αυτός είναι σχετικά πρώτος με τον n. Αν ο n είναι πρώτος, τότε όλοι οι μη μηδενικοί ακέραιοι στο Z_n είναι σχετικά πρώτοι με τον n και επομένως υπάρχει ένα (πολλαπλασιαστικό) αντίστροφο στοιχείο για κάθε ακέραιο στο $Z_n^* = Z_n - \{0\}$:

Για κάθε $\alpha \in Z_n^*$, υπάρχει $z \in Z_n^*$, $\alpha \cdot z \equiv 1 \pmod p$.

2.9 ΤΟ ΣΩΜΑ F_pm (ΣΩΜΑ GALOIS)

Το σώμα F_pm αποτελεί επέκταση του σώματος Z_p και ο βαθμός της επέκτασης είναι m. Τα σώματα της μορφής F_pm, με $p > 1$ και $m > 0$, ονομάζονται και σώματα Galois (Galois fields). Κάθε στοιχείο s του F_pm αναπαρίσταται ως εξής:

$$s = {}^{m-1}\sum_{i=0} \alpha_i x^i = \alpha_0 + \alpha_1 x + \ldots + \alpha_{m-1} x^{m-1},$$

όπου $\alpha_i \in F_p$. Η πρόσθεση (αφαίρεση) δύο στοιχείων s και q του F_pm πραγματοποιείται με την πρόσθεση (αφαίρεση) των συντελεστών των αντίστοιχων πολυωνύμων στο F_p (δηλαδή modulo p). Πιο απλά

$$s \pm q = {}^{m-1}\sum_{i=0} \alpha_i x^i \pm {}^{m-1}\sum_{i=0} b_i x^i = {}^{m-1}\sum_{i=0} (\alpha_i + b_i) \pmod p \; x_i$$

όπου α_i και b_i είναι οι συντελεστές των πολυωνύμων s και q αντίστοιχα.

Για τον υπολογισμό του πολλαπλασιασμού δύο στοιχείων του F_pm χρειάζεται να οριστεί ένα ανάγωγο πολυώνυμο βαθμού m. Το πολυώνυμο αυτό πρέπει να είναι ανάγωγο στο F_p. Έστω λοιπόν $s, q \in F_pm$. Το γινόμενό τους $u = sq$ υπολογίζεται σε δύο βήματα:

Πολυωνυμικός πολλαπλασιασμός

$u' = sq = ({}^{m-1}\sum_{i=0} \alpha_i x^i) ({}^{m-1}\sum_{i=0} b_i x^i) = {}^{2m-2}\sum_{i=0} c_i' x^i.$

Αναγωγή στο $F_p m$

Το πολυώνυμο u' που προκύπτει στο πρώτο βήμα έχει βαθμό 2m – 2. Το τελικό αποτέλεσμα όμως του πολλαπλασιασμού των στοιχείων s και q πρέπει να ανήκει στο $F_p m$, δηλαδή να είναι ένα πολυώνυμο βαθμού m – 1. Για αυτό το σκοπό χρειάζεται αναγωγή στο $F_p m$ με χρήση του πολυωνύμου αναγωγής.

Έστω ότι το πολυώνυμο αυτό είναι το $p(x) = {}^{m}\sum_{i=0} p_i x^i$. Επομένως:

$$u = u' \pmod{p(x)} = {}^{2m-2}\sum_{i=0} c_i' x^i \pmod{{}^{m}\sum_{i=0} p_i x^i} = {}^{m-1}\sum_{i=0} c_i x^i.$$

Συνήθως ως πολυώνυμο αναγωγής χρησιμοποιείται κάποιο της μορφής $p(x) = x^m - \omega$ (όπου ω ένα τυχαίο στοιχείο του σώματος F_p), γιατί έτσι η αναγωγή γίνεται πιο αποδοτικά. Η πράξη της αντιστροφής ενός στοιχείου στο $F_p m$ είναι πολύ πιο χρονοβόρα και πολύπλοκη από αυτή του πολλαπλασιασμού και θα πρέπει να αποφεύγεται όσο γίνεται όταν χρησιμοποιείται το σώμα επέκτασης $F_p m$.

2.10 ΚΙΝΕΖΙΚΟ ΘΕΩΡΗΜΑ ΥΠΟΛΟΙΠΩΝ

Το Κινέζικο θεώρημα υπολοίπων μας παρέχει μια μέθοδο επίλυσης συστημάτων γραμμικών ισοτιμιών. Οι λύσεις μπορούν να βρεθούν χρησιμοποιώντας έναν εύκολο και αποδοτικό αλγόριθμο.

Έστω $m_1, \ldots, m_r \in N$ ανά δύο σχετικώς πρώτοι αριθμοί, δηλαδή

$$\gcd(m_i, m_j) = 1, \text{ για } i \neq j.$$

Έστω $\alpha_1, \alpha_2, \ldots, \alpha_r$ ακέραιοι. Τότε υπάρχει ακέραιος x τέτοιος ώστε

$$x \equiv \alpha_1 \pmod{m_1}$$

…

$$x \equiv \alpha_r \pmod{m_r}$$

Επιπλέον, το υπόλοιπο x mod M είναι μοναδικό, όπου $M = m_1 \cdot \ldots \cdot m_r$.

Η πρόταση αυτή σημαίνει ότι υπάρχει μια ένα – προς – ένα αντιστοιχία μεταξύ των κλάσεων καταλοίπων modulo M και των πλειάδων κλάσεων υπολοίπων modulo $m_1, \ldots, m_r$. Αυτή η ένα – προς – ένα αντιστοιχία διατηρεί την προσθετική και πολλαπλασιαστική δομή.

<u>*Κινέζικο Θεώρημα Υπολοίπων:*</u> Έστω $m_1, \ldots, m_r \in N$ ανά δύο σχετικώς πρώτοι αριθμοί, δηλαδή $\gcd(m_i, m_j) = 1$, για $i \neq j$. Έστω $M = m_1 \cdot \ldots \cdot m_r$. Τότε η απεικόνιση

$$f : Z_M \rightarrow Z_{m1} \times \ldots \times Z_{mr}$$

$$[x] \rightarrow ([x \bmod m_1], \ldots, [x \bmod m_r])$$

είναι ένας ισομορφισμός δακτυλίων.

Αν $(G, \circ)$ και $(H, *)$ είναι ομάδες και $f : G \rightarrow H$ είναι μια συνάρτηση τέτοια,

ώστε για κάθε $a, b \in G$,

$$f(a \circ b) = f(a) * f(b),$$

τότε η f λέγεται *ομοιομορφισμός* ομάδων. Αν επιπλέον η f είναι ένα-προς-ένα και επί, τότε η f λέγεται *ισομορφισμός* ομάδων και οι ομάδες *ισομορφικές*, συμβολικά $(G, \circ) \approx (H, *)$ ή απλά $G \approx H$.

ΚΕΦΑΛΑΙΟ 3

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ – ΚΡΥΠΤΟΣΥΣΤΗΜΑ RSA – ΚΡΥΠΤΟΣΥΣΤΗΜΑ ELGAMAL

3.1 ΚΡΥΠΤΟΓΡΑΦΙΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δε μοιράζονται ένα κοινό μυστικό κλειδί, όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Συγκεκριμένα, κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί θα πρέπει να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

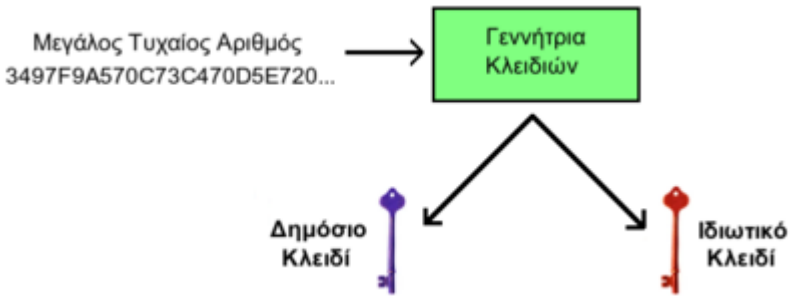
Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος, όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά τη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος.

Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πώς γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με τη σειρά του να αποκρυπτογραφήσει το μήνυμα; Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης (ηλεκτρονικά μηνύματα, διαδικτυακές αγορές κοκ).

3.1.1ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ

Α) ΔΗΜΙΟΥΡΓΙΑ ΚΛΕΙΔΙΩΝ

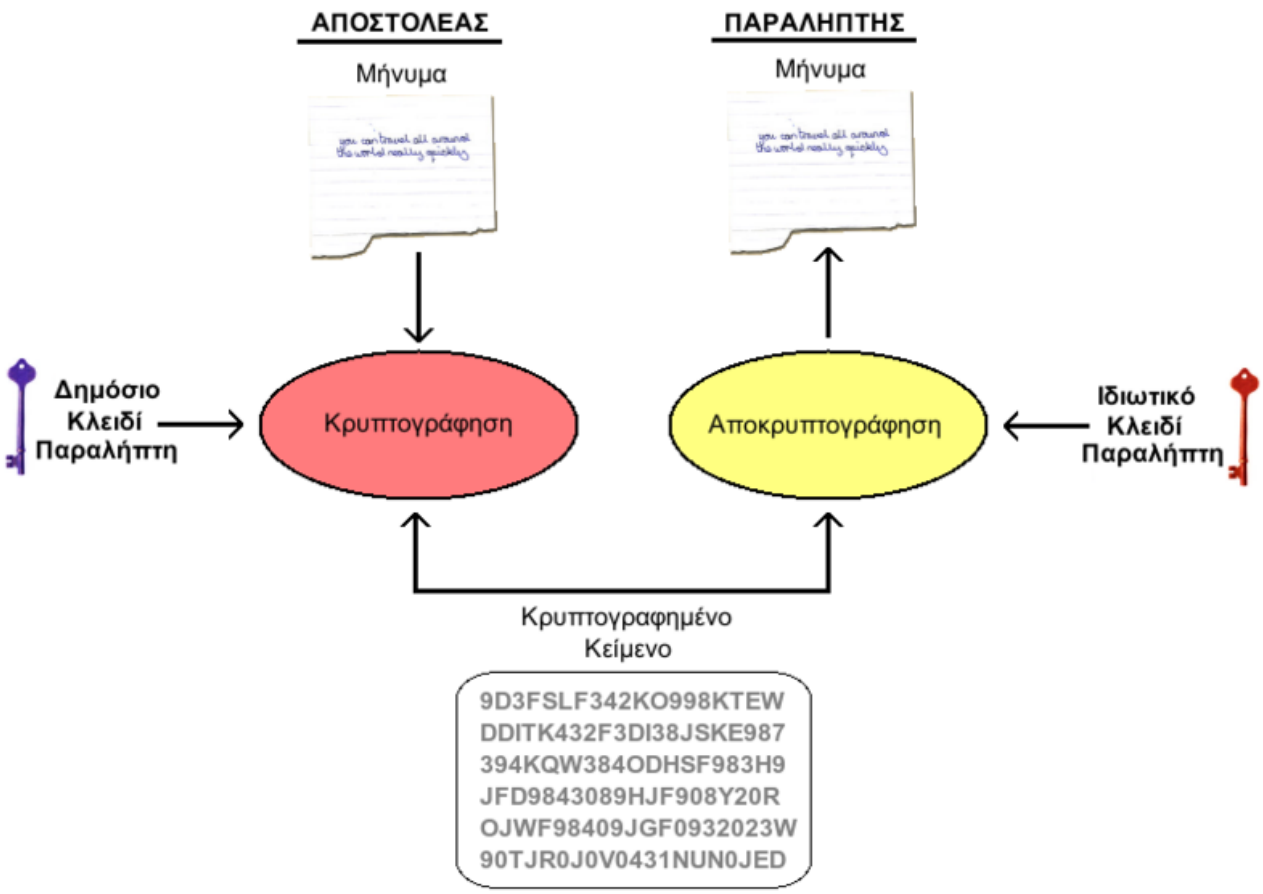
Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις, οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στην γεννήτρια κλειδιών, τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης, ο τυχαίος αριθμός παράγεται ως εξής: Κατά τη διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5 λεπτά και καλεί το χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στη συνέχεια, για να παράξει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από τη συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.



Σχήμα: *Τρόπος λειτουργίας της γεννήτριας κλειδιών*

Β) ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημένο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στην συνέχεια, στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Δεδομένου ότι το ιδιωτικό κλειδί του παραλήπτη είναι γνωστό μονάχα στον ίδιο και σε κανέναν άλλον, ο παραλήπτης είναι ο μόνος που μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Άρα, λοιπόν, με αυτόν τον τρόπο ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος.



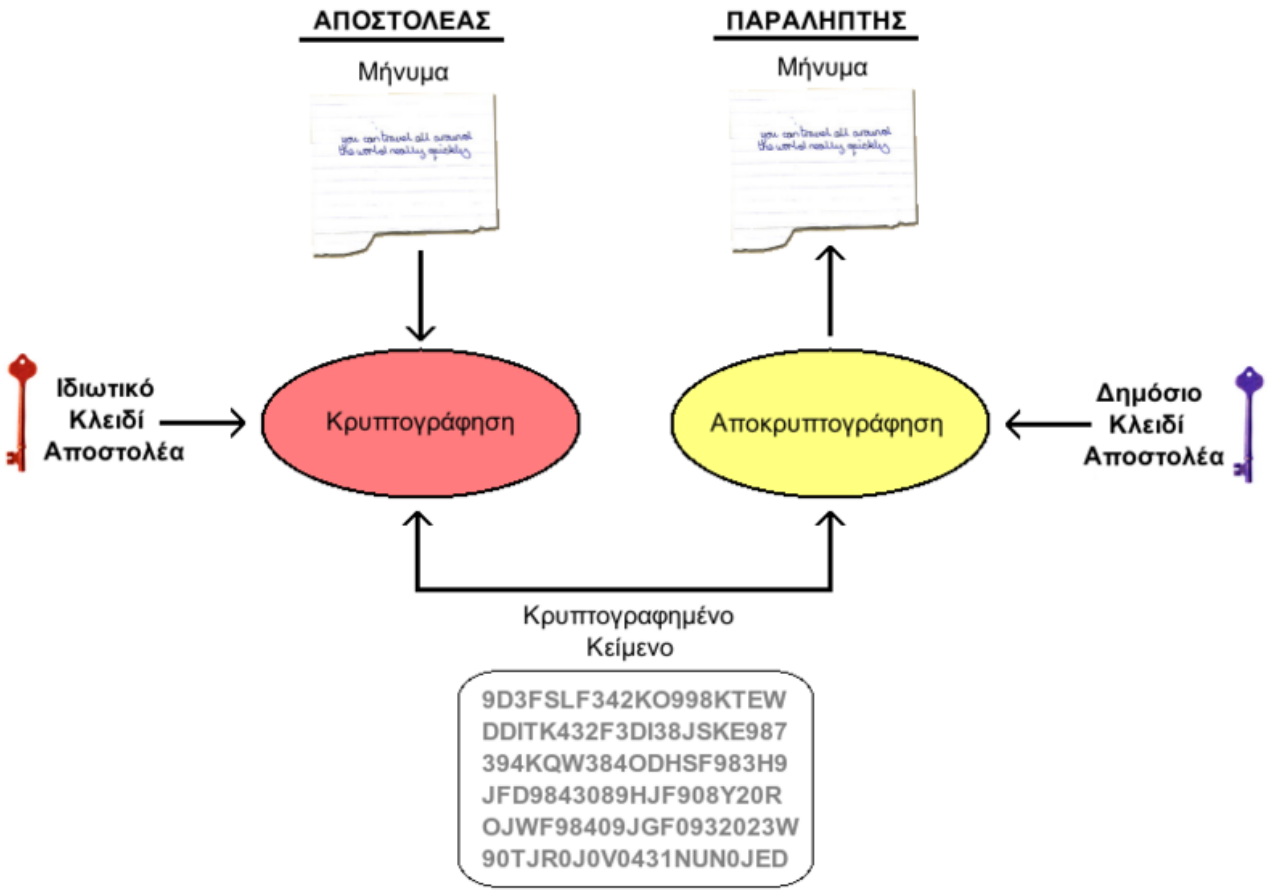
Σχήμα: *Επίτευξη εμπιστευτικότητας αλλά όχι πιστοποίησης χρησιμοποιώντας κρυπτογραφικούς αλγόριθμους δημοσίου κλειδιού.*

Η παραπάνω μέθοδος μπορεί να εξασφαλίσει την εμπιστευτικότητα, αλλά όχι την πιστοποίηση του αποστολέα. Αυτό, με λίγα λόγια, σημαίνει πως η παραπάνω μέθοδος δε μπορεί να εγγυηθεί την ταυτότητα του αποστολέα. Πράγματι, ο αποστολέας μπορεί να δηλώσει ψευδή ταυτότητα και ο παραλήπτης να νομίσει ότι το συγκεκριμένο μήνυμα προήλθε από άλλο πρόσωπο.

Γ) ΠΙΣΤΟΠΟΙΗΣΗ

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να

γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στη συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του. Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα.



Σχήμα: *Επίτευξη αυθεντικοποίησης αλλά όχι εμπιστευτικότητας χρησιμοποιώντας κρυπτογραφικούς αλγόριθμους δημοσίου κλειδιού.*

Δ) ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗ

Συνδυάζοντας τις δύο τεχνικές που παρουσιάστηκαν παραπάνω είναι εφικτό να επιτύχουμε εμπιστευτικότητα του μηνύματος και πιστοποίηση του αποστολέα. Δηλαδή αφενός το μήνυμα παραμένει γνωστό μόνο στον αποστολέα και τον παραλήπτη και αφετέρου ο παραλήπτης γνωρίζει με ασφάλεια ποιος του έστειλε το μήνυμα. Για να επιτευχθεί αυτό, ο αποστολέας μπορεί να κρυπτογραφήσει το μήνυμα πρώτα με το δικό του ιδιωτικό κλειδί και στη συνέχεια με το δημόσιο κλειδί του παραλήπτη. Όταν ο παραλήπτης λάβει το μήνυμα, θα πρέπει να χρησιμοποιήσει το ιδιωτικό του κλειδί για να το αποκρυπτογραφήσει (εμπιστευτικότητα) και στη συνέχεια να αποκρυπτογραφήσει το αποτέλεσμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα (πιστοποίηση).

Ε) ΠΑΡΑΔΕΙΓΜΑ ΑΠΟ ΤΗΝ ΚΑΘΗΜΕΡΙΝΗ ΖΩΗ

Θα παρουσιάσουμε ένα αναλογικό παράδειγμα από την καθημερινή ζωή το οποίο περιγράφει την κρυπτογράφηση δημόσιου κλειδιού ή ασύμμετρη κρυπτογράφηση. Έστω η Alice και ο Bob θέλουν να επικοινωνήσουν με ασφάλεια χρησιμοποιώντας το δημόσιο ταχυδρομείο. Η Alice θέλει να στείλει ένα καμουφλαρισμένο-κρυφό μήνυμα στον Bob και περιμένει μια καμουφλαρισμένη-κρυφή απάντηση από αυτόν.

Σύμφωνα με την κρυπτογράφηση συμμετρικού κλειδιού η Alice θα βάλει το μήνυμά της μέσα σε ένα κουτί με λουκέτο για το οποίο έχει το κλειδί. Στέλνει το κλειδαμπαρωμένο κουτί με το δημόσιο ταχυδρομείο στον Bob. Ο Bob έχει ένα ίδιο κλειδί (το οποίο έχει πάρει από την Alice στο παρελθόν, σε διαπροσωπική συνάντηση που είχαν) και μόλις λαμβάνει το κουτί, ανοίγει το λουκέτο και διαβάζει το μήνυμα. Ο Bob βάζει το μήνυμά του στο κουτί, το κλειδώνει και το στέλνει με δημόσιο ταχυδρομείο στην Alice.

Το πρόβλημα εδώ είναι ότι το κλειδί για το λουκέτο είναι κοινό και για την Alice και για τον Bob και για να δώσει αντίγραφο του κλειδιού ο ένας με τον άλλον θα πρέπει να συναντηθούν, γιατί δεν είναι ασφαλές να το στείλουν με το δημόσιο ταχυδρομείο (ίσως τότε κάποια διεφθαρμένη υπάλληλος του ταχυδρομείου, π.χ. η Mallory θα μπορούσε να υποκλέψει το κλειδί και να δημιουργήσει ένα αντίγραφο ώστε στο μέλλον να υποκλέπτει ή να παραποιεί τα μηνύματα που ανταλλάσσονται στο κουτί).

Στην πράξη της ασύμμετρης κρυπτογραφίας, ο Bob και η Alice έχουν ξεχωριστές κλειδαριές. Πρώτα η Alice βάζει το μυστικό μήνυμα στο κουτί και το

κλειδώνει με το λουκέτο του οποίου έχει μόνο αυτή κλειδί. Στέλνει το κουτί στον Bob με απλό δημόσιο ταχυδρομείο. Όταν ο Bob λαμβάνει το κουτί, προσθέτει το δικό του λουκέτο στο κουτί και στο στέλνει πίσω στην Alice. Η Alice λαμβάνει το κουτί με δύο λουκέτα, αφαιρεί το δικό της λουκέτο και το στέλνει πίσω στον Bob. Όταν ο Bob λαμβάνει το κουτί έχει πάνω μόνο το δικό του λουκέτο, το οποίο μπορεί να ξεκλειδώσει και να δει το μήνυμα της Alice. Σε αυτό το παράδειγμα, η διαδικασία της αποκρυπτογράφησης είναι ίδια με την διαδικασία της κρυπτογραφίας.

Η κρίσιμη διαφορά στο κλειδί ασύμμετρης κρυπτογράφησης είναι ότι η Alice και ο Bob ποτέ δε χρειάζεται να στείλουν αντίγραφο του κλειδιού ο ένας στον άλλον. Σε αυτήν την περίπτωση αποφεύγουμε την περίπτωση της διεφθαρμένης υπαλλήλου στο ταχυδρομείο, τη Mallory, η οποία ενδέχεται να υποκλέψει το κλειδί κατά τη μεταφορά. Σε αυτήν την περίπτωση, η Alice και ο Bob δε χρειάζεται να εμπιστευτούν το δημόσιο ταχυδρομείο. Επιπρόσθετα, ο Bob επιτρέπει σε όποιον επιθυμεί να αντιγράψει το κλειδί του και τα μηνύματα της Alice προς τον Bob θα είναι εκτεθειμένα σε κίνδυνο υποκλοπής. Όμως, όλα τα μηνύματα της Alice προς άλλους θα είναι μυστικά, αφού οι υπόλοιποι θα παρέχουν διαφορετικά λουκέτα για να κλειδώσει η Alice το μήνυμα στο κουτί πριν το στείλει σε αυτούς.

3.2 ΜΟΝΟΔΡΟΜΕΣ ΣΥΝΑΡΤΗΣΕΙΣ ΜΕ ΜΥΣΤΙΚΗ ΠΟΡΤΑ

Μια συνάρτηση f είναι μονόδρομη, όταν δοθέντος x μπορεί να υπολογιστεί η f(x) με ευκολία, ενώ δοθέντος y, είναι υπολογιστικά αδύνατο να βρεθεί το $x = f^{-1}(y)$. Η έννοια του εύκολου υπολογισμού, αναφέρεται στις σχέσεις οι οποίες μπορούν να υπολογιστούν σε χρόνο που καθορίζεται από πολυωνυμική συνάρτηση χρόνου σε σχέση με την είσοδο.

Από τις μονόδρομες συναρτήσεις, αυτές που έχουν χρησιμότητα στην ασύμμετρη κρυπτογραφία είναι οι μονόδρομες συναρτήσεις με μυστική πόρτα.

ΟΡΙΣΜΟΣ: Μια μονόδρομη συνάρτηση με μυστική πόρτα είναι η οικογένεια αντιστρέψιμων συναρτήσεων f_k με τα παρακάτω χαρακτηριστικά:

δοθέντων k, x, ο υπολογισμός της $y = f_k(x)$ είναι εύκολος,

δοθέντων k, y, ο υπολογισμός της $x = f_k^{-1}(y)$ είναι εύκολος,

δοθέντος y, ο υπολογισμός της $y = f_k^{-1}(x)$ είναι αδύνατος.

Η ποσότητα k ονομάζεται μυστική πόρτα και είναι η ποσότητα εκείνη που απαιτείται για να είναι δυνατή η αντιστροφή της f_k.

Με βάση την παραπάνω θεωρία, οι Diffie και Hellman εισήγαγαν την έννοια του ασύμμετρου κρυπτοσυστήματος. Σύμφωνα με τους Diffie και Hellman (1976), ένα ασύμμετρο κρυπτοσύστημα θα πρέπει να πληροί τις ακόλουθες απαιτήσεις:

Είναι υπολογιστικά εύκολο για το Βύρωνα να δημιουργήσει ένα ζεύγος κλειδιών, ke_b (δημόσιο κλειδί) και kd_b (ιδιωτικό κλειδί).

Είναι υπολογιστικά εύκολο για την Αλίκη, η οποία γνωρίζει το δημόσιο κλειδί του Βύρωνα, να κρυπτογραφήσει ένα μήνυμα p με την κρυπτογραφική πράξη:

$c = e_{keb}(p)$

Είναι υπολογιστικά εύκολο για το Βύρωνα, ο οποίος γνωρίζει το ιδιωτικό του κλειδί, να αποκρυπτογραφήσει το c με την κρυπτογραφική πράξη:

$p = d_{kdb}(c)$

Είναι υπολογιστικά αδύνατο για τον αντίπαλο ο οποίος γνωρίζει το δημόσιο κλειδί του Βύρωνα ke_b, να καθορίσει το ιδιωτικό κλειδί του Βύρωνα kd_b.

Είναι υπολογιστικά αδύνατο για τον αντίπαλο, ο οποίος γνωρίζει το δημόσιο κλειδί του Βύρωνα ke_b και το κρυπτοκείμενο c, να ανακαλύψει το απλό κείμενο p.

3.3 ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RSA

Το κρυπτοσύστημα των Rivest, Shamir, Adleman είναι ένα από τα πιο παλιά και διαδεδομένα κρυπτοσυστήματα δημοσίου κλειδιού.

Η ασφάλεια του κρυπτοσυστήματος βασίζεται στο δύσκολο πρόβλημα της παραγοντοποίησης ενός σύνθετου ακεραίου σε γινόμενο πρώτων παραγόντων.

ΟΡΙΣΜΟΣ: Έστω p και q δύο πρώτοι αριθμοί και n = pq. Το κρυπτοσύστημα όπου $F = G = Z_n$,

$$K = \{(p, q, n, k_e, k_d): k_e k_d \equiv 1 \pmod{\varphi(n)}\}$$

ορίζει το κρυπτοσύστημα RSA, με πράξη κρυπτογράφησης:

$$e_k(m) = m^{ke} \bmod n$$

και πράξη αποκρυπτογράφησης:

$$d_k(c) = ck_d \bmod n.$$

Το δημόσιο κλειδί αποτελείται από τους ακεραίους k_e και n, ενώ το ιδιωτικό κλειδί αποτελείται από τα p, q, k_d.

Μπορούμε να επαληθεύσουμε ότι η πράξη της αποκρυπτογράφησης δίνει το αρχικό απλό κείμενο ως εξής:

$$c^{kd} \equiv (m^{ke})^{kd} \pmod{n}, \qquad (1)$$

αλλά επειδή

$$k_e k_d \equiv 1 \pmod{\varphi(n)}$$

έπεται ότι

$$k_e k_d = w\varphi(n) + 1$$

για κάποια σταθερά $w > 1$.

Έτσι η (1) γίνεται:

$$c^{kd} \equiv m^{w\varphi(n)} \cdot m \pmod{n}$$

και λόγω του Θεωρήματος του Euler σύμφωνα με το οποίο:

$$m^{\varphi(n)} \equiv 1 \pmod{n},$$

θα είναι και

$$\begin{aligned} c^{kd} &\equiv 1^{w} \cdot m \pmod{n} \\ &\equiv m \pmod{n}. \end{aligned}$$

Παρόμοιο αποτέλεσμα έχουμε και στην περίπτωση όπου ένα κείμενο κρυπτογραφείται με k_d και αποκρυπτογραφείται με k_e. Η αντιμεταθετική ιδιότητα που ισχύει στο εκθετικό γινόμενο έχει ως αποτέλεσμα και οι πράξεις της κρυπτογράφησης και αποκρυπτογράφησης να είναι αμοιβαία αντίστροφες, δηλαδή:

$$p = c^{kd} \equiv (m^{ke})^{kd} \equiv (m^{kd})^{ke} \pmod{n}.$$

3.3.1 ΑΝΑΛΥΣΗ ΤΟΥ RSA

Η πρακτική αξία του RSA οφείλεται στο γεγονός ότι αφενός μεν δεν υπάρχει αλγόριθμος ο οποίος να εντοπίζει τους πρώτους παράγοντες ενός σύνθετου ακεραίου, αφετέρου δε ο υπολογισμός μεγάλης δύναμης ενός αριθμού σε modular αριθμητική μπορεί να γίνει σε επιτρεπτό (γραμμικό) χρόνο.

Η πρώτη παρατήρηση αφορά την ασφάλεια του κρυπταλγορίθμου. Οι πρώτοι αριθμοί p και q θα πρέπει να είναι αρκετά μεγάλοι, ώστε ο καλύτερο γνωστός αλγόριθμος παραγοντοποίησης να απαιτεί χρόνο μεγαλύτερο από αυτόν με τον οποίο πρέπει να προστατευθούν τα δεδομένα. Στον ακόλουθο πίνακα παρουσιάζονται ενδεικτικά μεγέθη και αντίστοιχες περιπτώσεις στις οποίες θα πρέπει να εφαρμοσθούν τα μεγέθη αυτά:

p,q	$n = p \cdot q$	χρόνος προστασίας	τύπος δεδομένων
256 bits	512 bits	μερικές εβδομάδες	πληροφορίες που επηρεάζουν βραχυπρόθεσμα το χρηματιστήριο (π.χ. απόφαση συγχώνευση δύο εταιρειών)
512 bits	1024 bits	50 – 100 χρόνια	προσωπικά μυστικά
1024 bits	2048 bits	> 100 χρόνια	εμπορικά μυστικά, προσωπικά δεδομένα
2048 bits	4096 bits	≈ ηλικία του Σύμπαντος	στρατιωτικά μυστικά

Όσον αφορά τον υπολογισμό της ύψωσης ακεραίου σε δύναμη, ο αλγόριθμος «επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού» είναι αποτελεσματικός, αφού η πολυπλοκότητά του είναι (γραμμικώς) ανάλογη με το μέγεθος των ακεραίων που λαμβάνουν μέρος στην εκθετική πράξη.

Η συνάρτηση ύψωσης ακεραίου σε δύναμη

Θεωρούμε την οικογένεια συναρτήσεων $f_\alpha(x) = x^\alpha \bmod n$, για δεδομένο ακέραιο n. Η συνάρτηση αυτή ορίζει τη βασική κρυπτογραφική πράξη του κρυπτοσυστήματος RSA (όπου n το γινόμενο δύο πρώτων). Η συνάρτηση είναι περιοδική ως προς τον εκθέτη α.

Ας εξετάσουμε αρχικά την περίπτωση n = p, όπου p είναι πρώτος. Στον Πίνακα πιο κάτω παρουσιάζονται τα αποτελέσματα της συνάρτησης για $0 < x < p$, p = 17. Ο εκθέτης α είναι διατεταγμένος κατά γραμμές.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1
3	1	8	10	13	6	12	3	2	15	14	5	11	4	7	9	16
4	1	16	13	1	13	4	4	16	16	4	4	13	1	13	16	1
5	1	15	5	4	14	7	11	9	8	6	10	3	13	12	2	16
6	1	13	15	16	2	8	9	4	4	9	8	2	16	15	13	1
7	1	9	11	13	10	14	12	15	2	5	3	7	4	6	8	16
8	1	1	16	1	16	16	16	1	1	16	16	16	1	16	1	1
9	1	2	14	4	12	11	10	8	9	7	6	5	13	3	15	16
10	1	4	8	16	9	15	2	13	13	2	15	9	16	8	4	1
11	1	8	7	13	11	5	14	2	15	3	12	6	4	10	9	16
12	1	16	4	1	4	13	13	16	16	13	13	4	1	4	16	1
13	1	15	12	4	3	10	6	9	8	11	7	14	13	5	2	16
14	1	13	2	16	15	9	8	4	4	8	9	15	16	2	13	1
15	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Σχήμα: *Τιμές της $f_\alpha(x)$ mod 17*

Από τον παραπάνω πίνακα παρατηρούμε ότι $5^{11} = 11 \bmod 17$ και $11^3 = 5 \bmod 17$. Επίσης παρατηρούμε ότι $7^{11} = 14 \bmod 17$ και $14^3 = 7 \bmod 17$. Γενικά μπορούμε να διαπιστώσουμε ότι αν $x^{11} = y \bmod 17$, τότε $y^3 = x \bmod 17$ ή ισοδύναμα ότι η $f_{11}(x)$ είναι η αντίστροφη της $f_3(x)$.

Οι αντίστροφες σχέσεις, modulo 17, του 3 και 11, μπορούν να επαληθευτούν με το θεώρημα του Fermat. Για δεδομένο x είναι:

$$x^{11\cdot 3} \equiv x^{33} \equiv x \pmod{17},$$

λόγω του ότι

$$x^{17-1} \equiv 1 \pmod{17}$$

οπότε και

$$x^{33} \equiv x^{32} \cdot x \equiv (x^{17-1})^2 \cdot x \equiv 1^2 \cdot x \equiv x \pmod{17}.$$

Από τις συναρτήσεις $f_\alpha(x)$ μας ενδιαφέρουν αυτές οι οποίες είναι αντιστρέψιμες. Για παράδειγμα, στον παραπάνω πίνακα η $f_2(x)$ δεν είναι αντιστρέψιμη, διότι $f_2(8) = f_2(9) = 13$. Οι δυνάμεις εκείνες οι οποίες ορίζουν αντιστρέψιμες συναρτήσεις είναι εκείνες που δεν έχουν κοινούς παράγοντες με τον $p - 1$, στην περίπτωσή μας με τον 16. Το $p - 1$ προκύπτει από το Θεώρημα του Fermat, όπου μπορούμε να παρατηρήσουμε ότι οι πράξεις στους εκθέτες γίνονται ουσιαστικά modulo $(p - 1)$. Έτσι δύο συναρτήσεις $f_\alpha(x)$ και $f_b(x)$ είναι αντίστροφες, αν

$$\alpha \cdot b \equiv 1 \bmod (p - 1).$$

Είναι φανερό ότι δοθέντων α και p, είναι εύκολο να βρεθεί ο $\alpha^{-1} = b$, με τον εκτεταμένο αλγόριθμο του Ευκλείδη.

Λόγω του ότι για να υπολογισθεί η δύναμη ενός ακεραίου modulo n θα πρέπει να είναι γνωστό το modulus, οι συναρτήσεις $f_\alpha(x) \bmod n$ δεν έχουν κρυπτογραφικό ενδιαφέρον όταν το n είναι πρώτος αριθμός, διότι λόγω του Θεωρήματος του Fermat ο υπολογισμός του αντιστρόφου του εκθέτη είναι εύκολος. Έτσι, εξετάζουμε την περίπτωση όπου το n είναι σύνθετος ακέραιος και για την ακρίβεια είναι γινόμενο δύο πρώτων.

Στον πίνακα πιο κάτω έχουν υπολογισθεί οι τιμές της $f_\alpha(x) \bmod 15$. Γνωρίζουμε ότι $15 = 3 \cdot 5$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	1	4	9	1	10	6	4	4	6	10	1	9	4	1
3	1	8	12	4	5	6	13	2	9	10	11	3	7	14
4	1	1	6	1	10	6	1	1	6	10	1	6	1	1
5	1	2	3	4	5	6	7	8	9	10	11	12	13	14
6	1	4	9	1	10	6	4	4	6	10	1	9	4	1
7	1	8	12	4	5	6	13	2	9	10	11	3	7	14
8	1	1	6	1	10	6	1	1	6	10	1	6	1	1
9	1	2	3	4	5	6	7	8	9	10	11	12	13	14
10	1	4	9	1	10	6	4	4	6	10	1	9	4	1
11	1	8	12	4	5	6	13	2	9	10	11	3	7	14
12	1	1	6	1	10	6	1	1	6	10	1	6	1	1

Σχήμα: *Τιμές της $f_\alpha(x) \bmod 15$*

Παρατηρούμε ότι η συνάρτηση είναι περιοδική ως προς τον εκθέτη, με μέγιστη περίοδο $T = 4$, να συμβαίνει για $f_\alpha(2)$, $f_\alpha(3)$, $f_\alpha(7)$, $f_\alpha(12)$, $f_\alpha(13)$. Για οποιαδήποτε x ($x \neq 0$) και α θα είναι:

$$f_\alpha(x) \equiv f_{a+T}(x) \pmod n$$

ή ισοδύναμα:

$$x^{T+1} \equiv x \pmod n.$$

Από την παραπάνω σχέση προκύπτει ότι για δύο εκθέτες α και b οι οποίοι ορίζουν αντίστροφες συναρτήσεις θα πρέπει να ισχύει:

$$\alpha \cdot b \equiv 1 \bmod(T).$$

Για n γινόμενο δύο πρώτων p και q, η περίοδος υπολογίζεται εύκολα από τη σχέση:

$$T = \text{lcm}\,(p - 1, q - 1),$$

όπου lcm( ) το ελάχιστο κοινό πολλαπλάσιο. Συνεπώς, η περίοδος δε μπορεί να υπολογισθεί αν δεν είναι γνωστοί οι παράγοντες p και q του n και κατ' επέκταση δοθέντος εκθέτη α, δε μπορεί να υπολογισθεί αποτελεσματικά ο αντίστροφος b, για μεγάλους p και q. Σε αυτήν την παρατήρηση στηρίζεται η ασφάλεια του RSA.

Επίσης, προκειμένου να ορίζεται η αντίστροφη της $f_\alpha(x) \bmod n$, θα πρέπει ο εκθέτης να ορίζει ενριπτική[7] συνάρτηση. Παρόμοια με την $f_\alpha(x) \bmod p$, όπου ο εκθέτης θα πρέπει να μην έχει κοινούς παράγοντες με τον p, στην περίπτωση της $f_\alpha(x) \bmod n$, ο εκθέτης θα πρέπει να μην έχει κοινούς παράγοντες με τον (p – 1) και τον (q – 1).

Από τους εκθέτες α και $b = \alpha^{-1} \bmod T$, λόγω της αντιμεταθετικότητας, μπορεί οποιοσδήποτε να επιλεχθεί ως δημόσιο κλειδί, οπότε ο άλλος θα θεωρηθεί ιδιωτικό κλειδί. Ωστόσο, για την αποφυγή εξαντλητικής αναζήτησης προτιμάται ο μικρότερος από τους δύο να είναι το δημόσιο κλειδί και ο μεγαλύτερος το ιδιωτικό κλειδί.

Σχέση μεταξύ lcm (p – 1, q – 1) και φ(n)

Στην παραπάνω ανάλυση της συνάρτησης ύψωσης σε εκθέτη υπολογίσαμε το ελάχιστο κοινό πολλαπλάσιο μεταξύ των (p – 1) και (q – 1), ενώ στον ορισμό του κρυπτοσυστήματος RSA η αντίστοιχη πράξη είναι η φ(n).

Η ποσότητα lcm (p – 1, q – 1) ονομάζεται συνάρτηση Carmichael και συμβολίζεται με ψ(n). Η ψ(n) είναι διαιρέτης της φ(n), δηλαδή:

---

7 Ενριπτική ή ερριπτική ή ένα-προς-ένα συνάρτηση, ή απλώς ένριψη, λέγεται μια συνάρτηση f: $X \to Y$, όταν για κάθε x, y ϵ X, $f(x) = f(y) \to x = y$.

$\varphi(n) = c \cdot \psi(n)$,

για κάποιον ακέραιο c. Έτσι, κατ' επέκταση, για δεδομένο α, με gcd (α, n) = 1, ισχύει:

$$\alpha^{\psi(n)} \equiv 1 \pmod{n}.$$

Αυτό είναι γνωστό ως Θεώρημα του Charmichael και είναι γενίκευση του θεωρήματος του Euler.

3.3.2 ΑΣΦΑΛΕΙΑ ΤΟΥ RSA

Αν και ο RSA θεωρείται ασφαλής κρυπταλγόριθμος για μεγάλες παραμέτρους, υπάρχουν ορισμένες απειλές που οφείλονται κυρίως στη μη προσεκτική υλοποίηση και εκτέλεση του κρυπτοσυστήματος. Ωστόσο, θα πρέπει να αναφέρουμε ότι ο ισχυρισμός που ετέθη πιο πάνω σχετικά με την ασφάλεια του RSA και τη δυσκολία παραγοντοποίησης ενός σύνθετου ακεραίου, δεν είναι απόλυτα σωστός, με την έννοια ότι δεν έχει αποδειχθεί ότι η ασφάλεια του RSA εξαρτάται αποκλειστικά από την παραγοντοποίηση των ακεραίων. Βέβαια, στην περίπτωση που ανακαλυφθεί αλγόριθμος ο οποίος μπορεί να παραγοντοποιεί σε πολυωνυμικό χρόνο έναν ακέραιο, το RSA δεν είναι ασφαλές.

Το αντίστροφο, όμως, δεν είναι αληθές. Υπάρχουν επιθέσεις οι οποίες μπορούν να προσβάλλουν ένα κρυπτοσύστημα RSA, όπου δεν απαιτείται γνώση των παραγόντων του n.

3.3.3 ΕΠΙΘΕΣΗ ΣΕ ΚΟΙΝΟ modulus

Η επίθεση σε κοινό modulus μπορεί να εκφρασθεί σε περιπτώσεις όπου υπάρχει μια ομάδα επικοινωνούντων που έχουν κλειδιά των οποίων το n είναι το ίδιο.

Έστω ένα απλό κείμενο m και δύο ζευγάρια κλειδιών (e_1, d_1) και (e_2, d_2) τα οποία έχουν κοινό modulus, n. Η κρυπτογράφηση του απλού κειμένου με τα δύο δημόσια κλειδιά θα δώσει αντίστοιχα:

$c_1 = m^{e1} \bmod n$ και

$c_2 = m^{e2} \bmod n$.

Αν gcd (e_1, e_2) = 1, τότε υπάρχουν ακέραιοι w και v, τέτοιοι ώστε:

$we_1 + ve_2 = 1$.

Επειδή, όμως, είναι e_1, $e_2 > 0$, έπεται ότι κάποιο από τα w και v είναι αρνητικό και το άλλο θετικό. Έστω ότι $w < 0$. Τότε ο αντίπαλος έχοντας γνώση των κρυπτοκειμένων και των δημόσιων κλειδιών, μπορεί να ανακτήσει το μήνυμα υπολογίζοντας:

$(c_1^{-1})^{-w} \cdot c_2^{v} \equiv m^{we1+ve2} \equiv m \pmod n$.

Η επίθεση είναι δυνατή σε περιπτώσεις ομάδας χρηστών όπου η δημιουργία των κλειδιών γίνεται από ένα κέντρο δημιουργίας κλειδιών το οποίο χρησιμοποιεί την ίδια διαδικασία για τη δημιουργία των κλειδιών των μελών της ομάδας. Η κρυπτογράφηση ενός μηνύματος με περισσότερα από ένα δημόσια κλειδιά εμφανίζεται σε περιπτώσεις εκπομπής, όπου μια οντότητα στέλνει το μήνυμα σε πολλούς αποδέκτες.

3.4 ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ ELGAMAL

Το 1984 ο Taher ElGamal παρουσίασε ένα κρυπτοσύστημα βασισμένο στο Πρόβλημα του Διακριτού Λογαρίθμου. Το κρυπτοσύστημα αυτό βασίζεται στην

υπόθεση ότι ο διακριτός λογάριθμος δε μπορεί να βρεθεί σε εφικτό χρόνο, ενώ η αντίστροφη εφαρμογή της δύναμης μπορεί να υπολογιστεί αποτελεσματικά.

Το αυθεντικό σύστημα δημοσίου κλειδιού που προτάθηκε από τους Diffie και Hellman απαιτεί αλληλεπίδραση και από τις δύο πλευρές για να υπολογιστεί ένα κοινό ιδιωτικό κλειδί. Αυτό δημιουργεί προβλήματα αν το κρυπτοσύστημα πρέπει να εφαρμοστεί σε συστήματα επικοινωνίας όπου και οι δύο πλευρές δε δύνανται να αλληλεπιδρούν σε λογικό χρόνο εξαιτίας καθυστερήσεων στη μετάδοση ή τη μη διαθεσιμότητα του παραλήπτη.

Έτσι, ο ElGamal απλοποίησε τον αλγόριθμο ανταλλαγής κλειδιών των Diffie – Hellman εισάγοντας έναν τυχαίο εκθέτη k. Αυτός ο εκθέτης είναι μία αντικατάσταση του ιδιωτικού εκθέτη του παραλήπτη. Εξαιτίας αυτής της απλοποίησης ο αλγόριθμος μπορεί να χρησιμοποιηθεί για να κρυπτογραφήσει προς μία κατεύθυνση, χωρίς την απαίτηση η δεύτερη πλευρά να παίρνει ενεργά μέρος. Η εξέλιξη του κλειδιού εδώ είναι ότι ο αλγόριθμος μπορεί να χρησιμοποιηθεί για κωδικοποίηση ηλεκτρονικών μηνυμάτων, τα οποία μεταδίδονται μέσω δημοσίων υπηρεσιών store – and – forward.

Δημιουργία Κλειδιού

Η βασική απαίτηση για ένα κρυπτογραφικό σύστημα είναι τουλάχιστον ένα κλειδί για συμμετρικούς αλγορίθμους και δύο κλειδιά για ασύμμετρους αλγορίθμους.

Με τον αλγόριθμο elGamal, μόνο ο παραλήπτης χρειάζεται να δημιουργήσει ένα κλειδί εκ των προτέρων και να το δημοσιοποιήσει.

Ο Μπομπ, για να δημιουργήσει το κλειδί του, θα ακολουθήσει τα εξής βήματα:

Αρχικά ο Μπομπ χρειάζεται να δημιουργήσει ένα μεγάλο σε μήκος πρώτο αριθμό p και το γεννήτορα g μιας πολλαπλασιαστικής ομάδας Z_p^* των ακεραίων modulo p.

Τώρα ο Μπομπ επιλέγει έναν ακέραιο b από την ομάδα Z τυχαία και με τον περιορισμό $1 \leq b \leq p - 2$. Αυτός θα είναι ο ιδιωτικός εκθέτης.

Στο σημείο αυτό, μπορούμε να υπολογίσουμε το τμήμα του δημοσίου κλειδιού $g^b \bmod p$. Το δημόσιο κλειδί του Μπομπ στο κρυπτοσύστημα elGamal είναι η τριπλέτα (p, g, g^b) και το ιδιωτικό του κλειδί είναι b.

Το δημόσιο κλειδί τώρα χρειάζεται να δημοσιοποιηθεί χρησιμοποιώντας κάποια μέσα, έτσι ώστε η Αλίκη να είναι σε θέση να το πάρει.

Διαδικασία Κωδικοποίησης

Για να κωδικοποιήσει ένα μήνυμα M στο Μπομπ, η Αλίκη χρειάζεται πρώτα να αποκτήσει την τριπλέτα των δημοσίων κλειδιών του (p, g, g^b) από έναν εξυπηρέτη κλειδιών ή λαμβάνοντάς το από εκείνον μέσω μη κωδικοποιημένου ηλεκτρονικού μηνύματος. Δεν τίθεται θέμα ασφάλειας σ' αυτήν την μετάδοση, καθώς το μόνο μυστικό μέρος, το b, αποστέλλεται στο g^b. Αφού η βασική υπόθεση του κρυπτοσυστήματος elGamal λέει ότι είναι ανέφικτο να υπολογίσει το διακριτό λογάριθμο, αυτό είναι ασφαλές.

Για την κρυπτογράφηση του μηνύματος M, η Αλίκη πρέπει να ακολουθήσει τα παρακάτω βήματα:

Η Αλίκη πρέπει να αποκτήσει το τμήμα του δημόσιου κλειδιού του Μπομπ (p, g, g^b) από έναν επίσημο και έμπιστο εξυπηρέτη κλειδιών.

Γράφει το M σαν ένα σύνολο ακεραίων (m_1, m_2,…) στο διάστημα {1, …, p-1} Αυτοί οι ακέραιοι θα κωδικοποιηθούν ένας προς έναν.

Σ' αυτό το βήμα, η Αλίκη επιλέγει έναν τυχαίο εκθέτη k που παίρνει τη θέση του ιδιωτικού εκθέτη του παραλήπτη στην ανταλλαγή κλειδιών των Diffie – Hellman. Η τυχαιότητα εδώ είναι ένας κρίσιμος παράγοντας, καθώς η πιθανότητα του να μαντέψουμε το k δίνει μία αισθητή ποσότητα της απαραίτητης πληροφορίας για να αποκρυπτογραφήσουμε το μήνυμα στον εισβολέα.

Για να μεταδώσει τον τυχαίο εκθέτη k στο Μπομπ, η Αλίκη υπολογίζει το g^k mod p και το συνδυάζει με το κρυπτογράφημα που πρέπει να σταλεί στο Μπομπ.

Εδώ, η Αλίκη κρυπτογραφεί το μήνυμα M με το κρυπτογράφημα C. Επαναλαμβάνει αυτή τη διαδικασία πάνω στο σύνολο που δημιουργήθηκε στο βήμα 2 και υπολογίζει για κάθε ένα από τα m_i:

$$c_i = m_i * (g^b)^k$$

Το κρυπτογράφημα είναι το σύνολο όλων των c_i, με $0 < i < |M|$.

Το τελικό κρυπτογραφημένο μήνυμα C αποστέλλεται στο Μπομπ μαζί με το δημόσιο κλειδί $g^k \bmod p$ που προκύπτει από τον τυχαίο ιδιωτικό εκθέτη.

Ακόμα κι αν ο εισβολέας ακούσει τη μετάδοση και σε ένα δεύτερο βήμα αποκτούσε το τμήμα του δημόσιου κλειδιού g^b του Μπομπ από έναν εξυπηρέτη κλειδιών, και πάλι δε θα μπορούσε να παράξει το g^{b*k}, όπως προκύπτει από το πρόβλημα του διακριτού Λογαρίθμου.

Ο ElGamal συμβουλεύει να χρησιμοποιούμε έναν τυχαίο k για κάθε ένα από τα μπλοκ των m_i. Αυτό βελτιώνει πολύ την ασφάλεια, καθώς η επίγνωση ενός μπλοκ m_j δεν οδηγεί τον εισβολέα στη γνώση των άλλων m_i. Αυτό οφείλεται στο ότι αν $c_1 = m_1 * (g^b)^k \bmod p$ και $c_2 = m_2 * (g^b)^k \bmod p$, γνωρίζοντας μόνο το m_1 το επόμενο τμήμα του μηνύματος m_2 μπορεί να υπολογιστεί από τον παρακάτω τύπο:

$$m_1 / m_2 = c_1 / c_2.$$

Διαδικασία αποκωδικοποίησης

Αφού λάβει το κρυπτογραφημένο μήνυμα C και το τυχαίο δημόσιο κλειδί g^k, Ο Μπομπ πρέπει να χρησιμοποιήσει τον αλγόριθμο κρυπτογράφησης για να μπορέσει να διαβάσει το μήνυμα M. Αυτός ο αλγόριθμος μπορεί να διαιρεθεί σε κάποια απλά βήματα:

Το κρυπτοσύστημα elGamal βοήθησε την Αλίκη να καθορίσει ένα διαμοιραζόμενο μυστικό κλειδί χωρίς την παρέμβαση του Μπομπ. Αυτό το διαμοιραζόμενο μυστικό είναι ο συνδυασμός του ιδιωτικού εκθέτη του Μπομπ και του τυχαίου εκθέτη k που επιλέχθηκε από την Αλίκη. Το διαμοιραζόμενο κλειδί καθορίζεται από την ακόλουθη ισότητα:

$$(g^k)^{p-1-b} = (g^k)^{-b} = b^{-bk}$$

Για κάθε ένα από τα κομμάτια c_i ο Μπομπ τώρα υπολογίζει το κείμενο χρησιμοποιώντας τα

$m_i = (g^k)^{-b} * c_i \bmod p$

Αφού συνδυάσει όλα τα m_i μπλοκ πίσω στο M, ο Μπομπ μπορεί να διαβάσει το μήνυμα που έστειλε η Αλίκη.

3.4.1 ΑΣΦΑΛΕΙΑ ΤΟΥ ELGAMAL

Το κρυπτοσύστημα elGamal είναι τόσο ασφαλές, όσο είναι δύσκολο να λυθεί το πρόβλημα του Διακριτού λογαρίθμου, δεδομένου ότι δεν επιλέγονται αδύναμοι τυχαίοι εκθέτες ή πρώτοι αριθμοί.

Η ύπαρξη ενός τυχαίου αριθμού k έχει ως αποτέλεσμα τη δυνατότητα αντιστοίχισης του απλού κειμένου σε p – 1 κρυπτοκείμενα. Η διαδικασία όπου το απλό κείμενο αναμειγνύεται με μια τυχαία μεταβλητή ονομάζεται διαδικασία δημιουργίας συνθηκών τυχαιότητας. Το βήμα αυτό, το οποίο δεν υπάρχει στο RSA, καθιστά το κρυπτοσύστημα elGamal ανθεκτικότερο σε επιθέσεις παρόμοιες με αυτές που παρουσιάστηκαν για το RSA. Βέβαια, η χρήση του τυχαίου αριθμού εισάγει έναν επιπλέον κίνδυνο που οδηγεί σε μια πρόσθετη απαίτηση. Για κάθε μήνυμα που κρυπτογραφείται, θα πρέπει να επιλέγεται διαφορετικός τυχαίος k. Στην περίπτωση που δύο μηνύματα m και m’ κρυπτογραφηθούν με τον ίδιο k, τότε για τα αντίστοιχα κρυπτοκείμενα που θα προκύψουν (y_1, y_2) και (y_1’, y_2’), η γνώση του ενός μηνύματος επιτρέπει του άλλου από το λόγο:

$$\frac{y_2}{y_{2'}} = \frac{mb^r}{m'b^r} = \frac{m}{m'} .$$

Ακόμα ένα πρόβλημα που μπορεί να αναφερθεί είναι ότι η Αλίκη βασίζεται στην αυθεντικότητα του δημοσίου κλειδιού που ανακτά από το Μπομπ. Αυτό είναι ένα λιγότερο πρόβλημα αν το δημόσιο κλειδί παραδίδεται μέσω άμεσης επαφής, αλλά χρησιμοποιώντας το σύστημα σε ένα μεγάλο δίκτυο όπως το Διαδίκτυο άλλα μέσα πρέπει να βρεθούν. Η πιο κοινή εγκατάσταση είναι ένας κεντρικός εξυπηρέτης

κλειδιών. Οι χρήστες στέλνουν τα δημόσια κλειδιά τους εκεί μετά τη δημιουργία τους, έτσι ώστε άλλοι να μπορούν να τα φορτώσουν και να τα χρησιμοποιήσουν για κρυπτογράφηση ή επικύρωση υπογραφής. Αν ένας μοχθηρός εισβολέας καταφέρει να προμηθεύσει την Αλίκη με το κλειδί του και την κάνει να πιστέψει ότι είναι το κλειδί του Μπομπ, τότε εκείνη θα κρυπτογραφούσε το μήνυμα στον εισβολέα και όχι στον σωστό παραλήπτη, το Μπομπ. Αν το μήνυμα δεν είναι υπογεγραμμένο, ο εισβολέας μπορεί τότε να κρυπτογραφήσει το μήνυμα ξανά, αυτή τη φορά με το κλειδί του Μπομπ και το στέλνει στο Μπομπ. Αυτό ονομάζεται επίθεση Man – In – The – Middle (Άνθρωπος – Στη – Μέση). Τουλάχιστον ο άνδρας στη μέση θα μπορούσε να ανιχνευθεί αν η Αλίκη υπέγραφε και κρυπτογραφούσε το μήνυμα, αφού ο Μπομπ θα παρατηρούσε το αλλαγμένο περιεχόμενο όταν θα επιβεβαίωνε την υπογραφή.

Τέλος, όσον αφορά το μέγεθος του p, το κατώτατο όριο που προτείνεται είναι 1024 bits. Γενικά, κατά την κρυπτογράφηση με το κρυπτοσύστημα elGamal, το μέγεθος των παραμέτρων αποτελεί σημαντικό κριτήριο υλοποίησης, λόγω του αυξημένου χρόνου που απαιτείται για την κρυπτογράφηση (δύο πράξεις ύψωσης σε δύναμη έναντι της μιας στην περίπτωση του RSA) και λόγω της διαστολής του κρυπτοκειμένου. Τα μειονεκτήματα αυτά έχουν σαν αποτέλεσμα να προτιμάται μικρότερο μέγεθος του modulus.

3.5 ΣΥΓΚΡΙΣΗ ΤΩΝ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΩΝ RSA ΚΑΙ ELGAMAL

Από τα μέσα του 1970, οπότε και συνελήφθη η ιδέα της κρυπτογράφησης του δημοσίου κλειδιού, έχει ανθίσει μία ερευνητική δραστηριότητα και έχουν γίνει αξιοσημείωτες θεωρητικές πρόοδοι. Καθώς περνούν τα χρόνια, πολλά συστήματα δημοσίου κλειδιού έχουν κερδίσει έδαφος στον εμπορικό κόσμο. Χωρίς αμφιβολία το γνωστότερο κρυπτοσύστημα δημοσίου κλειδιού είναι το σύστημα RSA των Rivest, Shamir και Adleman. Παρόλο που δεν είναι εξίσου γνωστό, άλλο ένα κρυπτοσύστημα δημοσίου κλειδιού με πρακτικό ενδιαφέρον είναι αυτό το elGamal. Το σύστημα αυτό και οι παραλλαγές του χρησιμοποιούν μία βασική επέκταση της ανταλλαγής κλειδιών των Diffie – Hellman για την κρυπτογράφηση, μαζί με ένα συνοδευτικό σχήμα υπογραφών. Τα συστήματα ελλειπτικών καμπυλών των Miller και Koblitz έχουν επίσης πρόσφατα τραβήξει αρκετή προσοχή σαν εναλλακτικές κρυπτογραφικές επιλογές.

Η ασφάλεια των κρυπτοσυστημάτων RSA και elGamal είναι γενικά ταυτισμένη με τη δυσκολία παραγοντοποίησης των ακεραίων και με τη δυσκολία υπολογισμού διακριτών λογαρίθμων σε πεπερασμένα σώματα.

Είναι γνωστό πως ο υπολογισμός διακριτών λογαρίθμων στο $GF(2^n)$ είναι ευκολότερος από την παραγοντοποίηση N ακεραίων των n bits, με τη χρήση των ήδη

γνωστών αλγορίθμων για κάθε πρόβλημα. Η διαφορά στην ασφάλεια ανάμεσα στα κρυπτοσυστήματα RSA και elGamal στο $GF(2^n)$ μπορεί να εξισωθεί με τη χρήση μεγαλύτερων σε μήκος bit n στο σύστημα elGamal.

ΚΕΦΑΛΑΙΟ 4

ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΕΛΛΕΙΠΤΙΚΩΝ ΚΑΜΠΥΛΩΝ

Τα κρυπτοσυστήματα ελλειπτικών καμπυλών δεν είναι νέα κρυπτοσυστήματα. Οι ελλειπτικές καμπύλες αποτελούν ένα μαθηματικό εργαλείο με το οποίο μπορούν να υλοποιηθούν γνωστά κρυπτοσυστήματα δημοσίου κλειδιού. Η εφαρμογή των ελλειπτικών καμπυλών στην κρυπτογραφία προτάθηκε από του Miller[8] (1986) και Koblitz[9] (1987), ανεξάρτητα.

Οι ελλειπτικές καμπύλες μπορούν να ορισθούν σε διάφορα σώματα, όπως στο σώμα των πραγματικών, των μιγαδικών κλπ. Ειδικότερα στην κρυπτογραφία, οι ελλειπτικές καμπύλες ορίζονται σε πεπερασμένα σώματα.

8 Miller Victor: Αμερικανός μαθηματικός στο Κέντρο Έρευνας Τηλεπικοινωνιών στο Princeton στο New Jersey. Οι κύριοι τομείς ενδιαφέροντός του είναι: Υπολογιστική Θεωρία Αριθμών, Συνδυαστική, Συμπίεση Δεδομένων και Κρυπτογραφία.

9 Koblitz Neal: Καθηγητής Μαθηματικών στο Πανεπιστήμιο της Washington στο τμήμα των Μαθηματικών. Επίσης είναι επίτιμος καθηγητής του Κέντρου Εφαρμοσμένης Κρυπτογραφικής Έρευνας στο Πανεπιστήμιο του Waterloo. Πέρα από τη δημιουργία των ελλειπτικών καμπυλών με τον Miller, είναι υπεύθυνος για τη δημιουργία της κρυπτογραφίας υπερελλειπτικών καμπυλών.

4.1 ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ ΣΤΟ ΣΩΜΑ ΤΩΝ ΠΡΑΓΜΑΤΙΚΩΝ ΑΡΙΘΜΩΝ

Αντίθετα από την αίσθηση που μπορεί να δημιουργεί ο "όρος" καμπύλη, μια ελλειπτική καμπύλη μπορεί να αποτελείται στην πραγματικότητα από δύο καμπύλες και ένα σημείο που βρίσκεται εκτός των καμπυλών.

Ξεκινώντας από την εξίσωση του κύκλου, θα προσθέσουμε διαδοχικά όρους έως ότου καταλήξουμε στην εξίσωση της ελλειπτικής καμπύλης. Ένας κύκλος με κέντρο O(0, 0), σύμφωνα με την Αναλυτική Γεωμετρία, ορίζεται από την εξίσωση:

$x^2 + y^2 = r^2$, στο επίπεδο,

όπου r η ακτίνα του κύκλου. Αν απεικονίσουμε όλα τα σημεία (x, y) ενός επιπέδου τα οποία ικανοποιούν την εξίσωση του κύκλου, θα πάρουμε την κυκλική καμπύλη του σχήματος:

Ο κύκλος είναι ειδική περίπτωση της έλλειψης, όπου α = b:

$$\alpha x^2 + by^2 = c.$$

Οι τιμές οι οποίες ικανοποιούν την εξίσωση της έλλειψης για δοσμένα α και b σχηματίζουν στο επίπεδο την καμπύλη του παρακάτω σχήματος:

Τόσο στην εξίσωση του κύκλου, όσο και στην εξίσωση της έλλειψης, οι μεταβλητές συνδέονται με δευτεροβάθμιες εξισώσεις. Αυτό έχει σαν αποτέλεσμα σε μια δοσμένη τιμή του x να αντιστοιχούν δύο τιμές για το y και αντίστροφα. Για δοσμένα διαφορετικά σημεία (x_1, y_1) και (x_2, y_2) της έλλειψης μπορεί να ορισθεί ευθεία η οποία περνά από τα σημεία αυτά. Η ευθεία θα τέμνει την έλλειψη μόνον σε αυτά τα δύο σημεία.

Στην περίπτωση της ελλειπτικής καμπύλης, η εξίσωση της καμπύλης είναι δευτεροβάθμια ως προς y αλλά τριτοβάθμια ως προς x. Η εξίσωση της ελλειπτικής καμπύλης δίνεται από τη σχέση:

$$y^2 = x^3 + \alpha x + b,$$

για σταθερές α και b. Θεωρούμε δύο διαφορετικά σημεία (x_1, y_1) και (x_2, y_2) της ελλειπτικής καμπύλης κι έστω η ευθεία

$$y = \lambda x + c$$

η οποία τέμνει την ελλειπτική καμπύλη στα σημεία αυτά. Αντικαθιστώντας την εξίσωση της ευθείας στην ελλειπτική καμπύλη θα είναι:

$$(\lambda x + c)^2 = x^3 + \alpha x + b,$$

η οποία είναι τριτοβάθμια εξίσωση με δύο από τις ρίζες τα x_1 και x_2. Υπάρχει όμως και η τρίτη ρίζα x_3, που αντιστοιχεί στο σημείο της ευθείας (x_3, $\lambda x_3 + c$). Συνεπώς, η ευθεία τέμνει την καμπύλη σε τρία σημεία.

Στο πιο κάτω σχήμα απεικονίζεται μια ελλειπτική καμπύλη και η ευθεία που τέμνει την καμπύλη σε τρία σημεία. Η ελλειπτική καμπύλη αποτελείται από τις καμπύλες του σχήματος και επιπλέον από ένα σημείο Ο που το ονομάζουμε "σημείο στο άπειρο" (point at infinity).

Για κάποιο συνδυασμό των α και b, η εξίσωση της ελλειπτικής καμπύλης δεν έχει τρεις διαφορετικές ρίζες (για y = 0). Αυτό συμβαίνει όταν

$$4\alpha^3 + 27b^2 = 0$$

και η ελλειπτική καμπύλη είναι της μορφής του παρακάτω σχήματος. Μία τέτοια ελλειπτική καμπύλη ονομάζεται ιδιάζουσα (singular).

Πρόσθεση σημείων ελλειπτικής καμπύλης

Αρχικά θα παρουσιάσουμε πώς ορίζεται γραφικά η πρόσθεση σημείων ελλειπτικής καμπύλης. Η πρόσθεση βασίζεται στο γεγονός ότι μια ευθεία μπορεί να τέμνει μια ελλειπτική καμπύλη σε τρία το πολύ σημεία.

Αν εξετάσουμε μια ελλειπτική καμπύλη θα διαπιστώσουμε ότι αυτή είναι συμμετρική ως προς τον άξονα x. Έτσι, μπορούμε να ορίσουμε το αντίθετο σημείο (-P) ενός σημείου (P) της καμπύλης όπως φαίνεται στο σχήμα:

Παρατηρούμε ότι αν P = (x, y), τότε -P = (x, -y). Γεωμετρικά αυτό περιγράφεται ως εξής: Υπολογίζουμε την ευθεία που διέρχεται από το σημείο P και το σημείο O (κατακόρυφη). Το τρίτο σημείο της καμπύλης είναι το -P. Το σημείο στο άπειρο είναι το σημείο εκείνο στο οποίο τέμνονται όλες οι παράλληλες με τον άξονα των y.

Επομένως το ουδέτερο στοιχείο στην πρόσθεση σημείων ελλειπτικής καμπύλης είναι το σημείο O:

$P + O = O + P = P$ και

$P + (-P) = O$.

Έστω τα σημεία P και Q της ελλειπτικής καμπύλης. Η ευθεία η οποία διέρχεται από τα P και Q, τέμνει την καμπύλη στο τρίτο σημείο το οποίο είναι το -(P + Q). Το σημείο (P + Q) θα είναι συμμετρικό του -(P + Q) ως προς τον άξονα x.

Στην περίπτωση που P = Q, θεωρούμε ότι τα δύο από τα τρία σημεία που τέμνουν την καμπύλη συμπίπτουν. Η ευθεία που ορίζεται είναι η εφαπτομένη στο σημείο P.

Στη συνέχεια θα περιγράψουμε την πράξη της πρόσθεσης σημείων ελλειπτικής καμπύλης αλγεβρικά. Κατά τον γραφικό υπολογισμό, τα δύο σημεία καθώς και το αντίθετο του αθροίσματος αυτών βρίσκονται στην ίδια ευθεία. Έστω τα δύο σημεία $P = (x_1, y_1)$ και $Q = (x_2, y_2)$. Τότε η ευθεία:

$$y = \lambda x + c$$

η οποία διέρχεται από τα σημεία αυτά θα έχει κλίση ίση με:

$$\lambda = (y_2 - y_1) / (x_2 - x_1).$$

Αν στην εξίσωση της ελλειπτικής καμπύλης θέσουμε όπου y την εξίσωση ευθείας, οι συντεταγμένες του σημείου $P + Q = (x_3, y_3)$ είναι:

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1.$$

Οι παραπάνω σχέσεις προέκυψαν για διαφορετικά σημεία P και Q. Στην περίπτωση όπου $Q = -P = (x_1, -y_1)$, η κλίση γίνεται άπειρη, γεγονός που μας οδηγεί στο σημείο O.

Τέλος, στην περίπτωση όπου P = Q, η πρόσθεση αντιστοιχεί με το διπλασιασμό του σημείου P. Η κλίση υπολογίζεται από την παραγώγιση της εξίσωσης της ελλειπτικής καμπύλης βάσει του θεωρήματος των πλεγμένων συναρτήσεων και είναι ίση με:

$$\lambda = (3x_1^2 + \alpha) / 2y_1,$$

ενώ οι συντεταγμένες ορίζονται από τις σχέσεις που υπολογίσθηκαν για διαφορετικά P και Q.

4.2 ΟΙ ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ ΟΡΙΣΜΕΝΕΣ modulo p

Η εισαγωγική παρουσίαση των ελλειπτικών καμπυλών στο σώμα των πραγματικών αριθμών είχε σκοπό τη γραφική απεικόνιση των καμπυλών και την παρουσίαση των εξισώσεων της πρόσθεσης σημείων της καμπύλης. Οι ελλειπτικές καμπύλες οι οποίες έχουν κρυπτογραφικό ενδιαφέρον είναι ορισμένες στο σώμα Z_p, όπου p είναι πρώτος και p > 3. Η πράξη της πρόσθεσης είναι επίσης εσωτερική στο Z_p και ορίζεται με τον ίδιο τρόπο. Επίσης, μας ενδιαφέρει η ελλειπτική καμπύλη να έχει τρεις διακριτές ρίζες (για y = 0), οπότε καταλήγουμε στον ακόλουθο ορισμό:

ΟΡΙΣΜΟΣ: Η ελλειπτική καμπύλη ορισμένη στο Z_p, για κάποιον πρώτο ακέραιο p > 3, είναι το σύνολο των στοιχείων $(x, y) \in Z_p \times Z_p$ τα οποία ικανοποιούν την εξίσωση:

$$y^2 \equiv x^3 + \alpha x + b \pmod p$$

όπου

$\alpha, b \in Z_p$

και

$4\alpha^3 + 27b^2 \neq 0 \pmod p$ – το σημείο να είναι ορατό, δηλαδή να υπάρχει παράγωγος της ελλειπτικής καμπύλης.

Η πρόσθεση δύο σημείων της ελλειπτικής καμπύλης στο Z_p ορίζεται με τον ίδιο τρόπο όπως και στους πραγματικούς αριθμούς. Έστω δύο σημεία $P = (x_1, y_1)$ και $Q = (x_2, y_2)$, της ελλειπτικής καμπύλης

$$y^2 \equiv x^3 + \alpha x + b \pmod p.$$

Το σημείο $P + Q = (x_3, y_3)$ το οποίο είναι επίσης σημείο της καμπύλης, θα έχει συντεταγμένες:

$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod p$ και

$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod p$

όπου:

$\lambda \equiv (y_2 - y_1) / (x_2 - x_1) \pmod p$, εάν $P \neq Q$

ή

$$\lambda \equiv (3x_1^2 + \alpha) / 2y_1 \pmod{p}, \qquad \text{εάν } P = Q.$$

Μία άλλη σημαντική ιδιότητα στις ελλειπτικές καμπύλες στο Z_p είναι ότι τα σημεία της ελλειπτικής καμπύλης μαζί με το σημείο Ο ορίζουν κυκλική υποομάδα. Αυτό σημαίνει ότι οποιοδήποτε σημείο ανήκει στην ελλειπτική καμπύλη εκτός του Ο είναι γεννήτορας αυτής. Δηλαδή, δοθέντος κάποιου σημείου Ρ της καμπύλης, η διαδοχική πρόσθεση του Ρ στον εαυτό του, θα διατρέξει όλα τα σημεία της καμπύλης. Αν η καμπύλη αποτελείται από n σημεία, τότε θα είναι:

$$2P = P + P = Q$$

$$3P = P + 2P = R$$

…

$$nP = O$$

$$(n + 1)P = P.$$

4.3 ΟΙ ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ ΟΡΙΣΜΕΝΕΣ ΣΤΟ GF(2^n)

Οι ελλειπτικές καμπύλες μπορούν να ορισθούν στο σώμα GF(2^n). Μαζί με τις ελλειπτικές καμπύλες ορισμένες στο Z_p, το Εθνικό Ινστιτούτο Τυποποίησης και τεχνολογίας (NIST), καθόρισε και τις καμπύλες ορισμένες στο GF(2^n). Ο βασικός

λόγος επιλογής του σώματος αυτού είναι η αποτελεσματική υλοποίηση των ελλειπτικών καμπυλών στο $GF(2^n)$ στις ψηφιακές τεχνολογίες.

Η εξίσωση της ελλειπτικής καμπύλης ορισμένης στο $GF(2^n)$ είναι η ακόλουθη:

$$y^2 + xy = x^3 + \alpha x^2 + b,$$

όπου $\alpha, b \in GF(2^n)$.

Η πρόσθεση δύο σημείων $P = (x_1, y_1)$ και $Q = (x_2, y_2)$ ορίζεται από τις σχέσεις:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + \alpha$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

όπου

$$\lambda = (y_2 + y_1) / (x_2 + x_1).$$

Στην περίπτωση όπου $P = Q$, η πρόσθεση αντιστοιχεί στο $2P$ με:

$$x_3 = \lambda^2 + \lambda + \alpha$$

$$y_3 = (\lambda + 1)x_1^2 + x_3$$

όπου

$\lambda = x_1 + y_1 / x_1$.

Το αντίθετο ενός σημείου P έχει συντεταγμένες $-P = (x_1, x_1 + y_1)$.

4.4 ΤΟ ΠΡΟΒΛΗΜΑ ΤΟΥ ΔΙΑΚΡΙΤΟΥ ΛΟΓΑΡΙΘΜΟΥ ΣΤΙΣ ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ

Δεδομένου ενός σημείου P, μπορούμε να υπολογίσουμε το P + P = 2P, είτε γραφικά με την εφαπτομένη στο P, είτε αλγεβρικά με τις εξισώσεις της πρόσθεσης για P = Q. Προτού παρουσιάσουμε το πρόβλημα του διακριτού λογάριθμου στις ελλειπτικές καμπύλες, θα δείξουμε πώς γίνεται ο (βαθμωτός) πολλαπλασιασμός ενός σημείου, δηλαδή τον τρόπο υπολογισμού του nP, για δοσμένο ακέραιο n.

Ο τρόπος υπολογισμού του nP είναι παρόμοιος με τον αλγόριθμο "επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού", για τον υπολογισμό ύψωσης ενός αριθμού σε δύναμη.

Ο αλγόριθμος επαναλαμβανόμενου τετραγωνισμού – και – πολλαπλασιασμού είναι μια αποτελεσματική μέθοδος να υψώσουμε έναν αριθμό α σε μια δύναμη n. Στις ελλειπτικές καμπύλες μπορούμε να ονομάσουμε τον αντίστοιχο αλγόριθμο "διπλασιασμού – και – πρόσθεσης", ο οποίος έχει ως εξής:

Έστω ένα σημείο P της ελλειπτικής καμπύλης και έστω ο ακέραιος n. Ζητείται το σημείο που αντιστοιχεί στο nP.

Είσοδος: n, P.

Έστω $Q \leftarrow O$, $i \leftarrow l-1$

Υπολογίζουμε τη δυαδική αναπαράσταση του n. Έστω $(c_0 c_1 ... c_{l-1})$ η δυαδική λέξη μήκους l bits, όπου

$n = {}^{l-1}\sum_{i=0} c_i \bullet 2^i$.

4. Επανάλαβε το βήμα έως ότου $i < 0$:

$Q \leftarrow 2Q$

Αν $c_i = 1$, τότε $Q \leftarrow Q + P$.

$i \leftarrow i - 1$

5. Έξοδος: Q.

ΟΡΙΣΜΟΣ: Έστω μια ελλειπτική καμπύλη ορισμένη στο Z_p. Έστω ένα σημείο P της καμπύλης κι ένα σημείο Q το οποίο αποτελεί βαθμωτό γινόμενο του P. Το πρόβλημα του διακριτού λογάριθμου στην ελλειπτική καμπύλη είναι ο καθορισμός της τιμής n, για την οποία είναι:

$$nP = Q.$$

4.5 ΑΣΦΑΛΕΙΑ ΤΩΝ ΕΛΛΕΙΠΤΙΚΩΝ ΚΑΜΠΥΛΩΝ

Έχει αποδειχθεί ότι η πολυπλοκότητα των μεθόδων που επιχειρούν να λύσουν το πρόβλημα του διακριτού λογάριθμου στις ελλειπτικές καμπύλες είναι της μορφής n^{α}, $\alpha > 0$. Είναι δηλαδή εκθετικά πιο αργοί από τη (λογαριθμική) πολυπλοκότητα του υπολογισμού βαθμωτών γινομένων του P.

Ωστόσο, υπάρχει μια κατηγορία ελλειπτικών καμπυλών, οι υπεριδιάζουσες (supersingular) ελλειπτικές καμπύλες οι οποίες δε θεωρούνται ασφαλείς, διότι υποπίπτουν σε επίθεση η οποία εκμεταλλεύεται έναν συγκεκριμένο ισομορφισμό μεταξύ των ελλειπτικών καμπυλών και των πεπερασμένων σωμάτων. Αν και οι συγκεκριμένες ελλειπτικές καμπύλες προτιμούνται λόγω της αποτελεσματικής σε ταχύτητα υλοποίησης των πράξεων, δε συνιστώνται.

Ένα άλλο κριτήριο ασφάλειας των ελλειπτικών καμπυλών είναι το πλήθος των σημείων μιας ελλειπτικής καμπύλης. Όσο μεγαλύτερος είναι ο αριθμός των σημείων μιας καμπύλης, τόσο μεγαλύτερη θα είναι και η εξαντλητική αναζήτηση. Γενικά, ο υπολογισμός σημείων μιας ελλειπτικής καμπύλης είναι δύσκολος. Ο Hasse[10] διατύπωσε ένα θεώρημα το οποίο θέτει τα φράγματα για το πλήθος των στοιχείων της ελλειπτικής καμπύλης. Σύμφωνα λοιπόν με τον Hasse, μια καμπύλη ορισμένη στο Z_p, αναμένεται να έχει σημεία μεταξύ των φραγμάτων:

10 Hasse Helmut: Γερμανός μαθηματικός που εργάστηκε πάνω στην αλγεβρική θεωρία αριθμών, γνωστός για τη συνεισφορά του στην εφαρμογή των p – αδικών αριθμών, της Διοφαντικής γεωμετρίας, αλλά και των τοπικών ζήτα συναρτήσεων.

$$p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p},$$

όπου |E| το πλήθος των σημείων της ελλειπτικής καμπύλης.

Οι Lenstra[11] και Verheul[12] εκτίμησαν ότι προκειμένου μια ελλειπτική καμπύλη να είναι ασφαλής έως το έτος 2020, η τάξη μεγέθους του p είναι 2^{160}, στην περίπτωση του Z_p και $n \approx 160$, στην περίπτωση του $GF(2^n)$. Συγκριτικά, για να έχουμε τον ίδιο βαθμό ασφάλειας στο πεπερασμένο σώμα Z_p με γεννήτορα $\alpha \in Z_p$ και αντίστοιχη πράξη το γινόμενο, η τάξη μεγέθους του p θα πρέπει να είναι 2^{1880}.

4.6 ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΕ ΕΛΛΕΙΠΤΙΚΕΣ ΚΑΜΠΥΛΕΣ: ΤΟ ΑΝΑΛΟΓΟ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ElGamal

Όπως αναφέρθηκε και νωρίτερα, οι ελλειπτικές καμπύλες δεν αποτελούν ένα νέο κρυπτοσύστημα, αλλά διατίθενται ως εργαλεία για την υλοποίηση υπαρχόντων κρυπτοσυστημάτων. Ένα από τα πιο απλά κρυπτοσυστήματα ελλειπτικών καμπυλών είναι το κρυπτοσύστημα ElGamal το οποίο θα παρουσιάσουμε στη συνέχεια και θα χρησιμοποιήσουμε το κρυπτοσύστημα αυτό ως βάση αντιστοίχισης των εννοιών ενός κρυπτοσυστήματος στο σώμα των ελλειπτικών καμπυλών.

Το σύνολο των απλών κειμένων, καθώς και το σύνολο των κρυπτοκειμένων αποτελείται από τα σημεία μιας ελλειπτικής καμπύλης. Υπάρχουν αποτελεσματικοί αλγόριθμοι οι οποίοι αντιστοιχίζουν απλό κείμενο σε σημεία ελλειπτικής καμπύλης. Έτσι, ένα απλό κείμενο εκφράζεται με τις συντεταγμένες ενός σημείου:

$$P_m = (x_m, y_m).$$

11 Lenstra Arjen: Ολλανδός μαθηματικός. Σπούδασε μαθηματικά στο Πανεπιστήμιο του Άμστερνταμ και αυτή τη στιγμή είναι καθηγητής στη Λωζάνη στο Εργαστήριο Κρυπτολογικών Αλγορίθμων.

12 Verheul Eric: Καθηγητής στο Πανεπιστήμιο Radboud του Nijmegen. Η έρευνά του επικεντρώνεται σε μαθηματικές εφαρμογές της ασφάλειας της πληροφορίας και κυρίως την κρυπτογραφία.

Για μια ακόμη φορά στο μοντέλο επικοινωνίας θεωρούμε την Αλίκη η οποία επιθυμεί να στείλει εμπιστευτικά ένα μήνυμα στο Βύρωνα. Όπως όλα τα συστήματα ασύμμετρης κρυπτογραφίας, απαιτείται μια αναφορική ποσότητα από την οποία θα προκύψουν το δημόσιο και ιδιωτικό κλειδί. Στις ελλειπτικές καμπύλες, η ποσότητα αυτή θα είναι ένα σημείο της ελλειπτικής καμπύλης. Έστω $G = (x_g, y_g)$ το σημείο αυτό. Ο Βύρων επιλέγει έναν ακέραιο n_b, ο οποίος αποτελεί το ιδιωτικό του κλειδί. Το δημόσιο κλειδί είναι το $\{P_b, G, \alpha, b\}$, όπου:

$$P_b = n_b G.$$

Η Αλίκη γνωρίζοντας το δημόσιο κλειδί του Βύρωνα, επιλέγει έναν ακέραιο k και κρυπτογραφεί το μήνυμα P_m σύμφωνα με την κρυπτογραφική πράξη:

$$C_m = (kG, P_m + kP_b).$$

Παρατηρούμε από την παραπάνω πράξη ότι το κρυπτοκείμενο αποτελείται από δύο σημεία. Η αποκρυπτογράφηση εκτελείται από το Βύρωνα ως εξής: Για το ζεύγος σημείων που ορίζουν το κρυπτοκείμενο, πολλαπλασιάζει το πρώτο σημείο με το ιδιωτικό του κλειδί και το αποτέλεσμα που προκύπτει αφαιρείται από το δεύτερο σημείο:

$$d_k(C_m) = (P_m + kP_b) - (n_b(kG)) = P_m + kn_bG - kn_bG = P_m.$$

Είναι φανερό ότι η ασφάλεια του κρυπτοσυστήματος ElGamal βασίζεται στο πρόβλημα του διακριτού λογάριθμου, όπως αυτό ορίζεται στις ελλειπτικές καμπύλες. Ο αντίπαλος έχει γνώση των $\{P_b, G, \alpha, b\}$ και από αυτά καλείται να ανακαλύψει το n_b που συνδέει τα P_b και G.

ΠΑΡΑΤΗΡΗΣΗ: Στο σημείο αυτό αξίζει να σημειωθεί ότι είναι δυνατό να υλοποιηθεί και ο RSA ως αλγόριθμος ελλειπτικής καμπύλης. Όμως, η βάση της ασφάλειας αυτού του αλγορίθμου είναι η δυσκολία παραγοντοποίησης μεγάλων ακεραίων και όχι το πρόβλημα του διακριτού λογαρίθμου, με αποτέλεσμα το μέγεθος των κλειδιών να μην είναι σημαντικά μικρότερο από αυτό του συνηθισμένου RSA. Έτσι, η πρόσθετη πολυπλοκότητα δεν έχει κάποιο σημαντικό όφελος, με αποτέλεσμα η χρήση του Elliptic Curve RSA να είναι ιδιαίτερα περιορισμένη.

ΚΕΦΑΛΑΙΟ 5

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

5.1 ΕΙΣΑΓΩΓΗ

Όπως έχει γίνει κατανοητό, η ανταλλαγή κλειδιών πολλές φορές συνοδεύεται από αυθεντικοποίηση. Η αυθεντικοποίηση μπορεί να περιλαμβάνει ψηφιακές υπογραφές όπου ένα μέλος αποδεικνύει την ταυτότητά του έμμεσα δείχνοντας ότι γνωρίζει κάποια μυστική ποσότητα πληροφορίας, η οποία είναι συνδεδεμένη με την ταυτότητα του μέλους.

Η αυθεντικοποίηση είναι δυνατή και σε κάποιο μήνυμα. Η αυθεντικοποίηση αναφέρεται σε δύο επίπεδα, στην αυθεντικοποίηση του καναλιού επικοινωνίας και στην αυθεντικοποίηση της πηγής. Η αυθεντικοποίηση του καναλιού επικοινωνίας μεταξύ δύο μελών σημαίνει ότι τα μέλη αυτά έχουν τη δυνατότητα να ελέγχουν ποια μηνύματα έχουν δημιουργηθεί και σταλεί από οποιονδήποτε από τους δύο, χωρίς να φαίνεται σε ποιον ανήκει το μήνυμα. Η αυθεντικοποίηση της πηγής αναφέρεται στη δυνατότητα διάκρισης του αποστολέα του μηνύματος.

Η αυθεντικοποίηση τόσο στην ταυτότητα ενός μέλους, όσο και σε ένα μήνυμα, μπορεί να πραγματοποιηθεί με μηχανισμούς ψηφιακών υπογραφών.

5.2 ΠΡΟΫΠΟΘΕΣΕΙΣ

Η κρυπτογραφία παρέχει τα εργαλεία ώστε να προστατευθούν δύο ή περισσότερα επικοινωνούντα μέλη από αντιπάλους. Οι τρόποι και ευκαιρίες επίθεσης του αντιπάλου καθορίζουν τις απαιτήσεις των μελών για προστασία. Η προστασία με τη σειρά της προσφέρεται στα μέλη με τη μορφή των κρυπτογραφικών υπηρεσιών.

Οι ψηφιακές υπογραφές απευθύνονται σε δύο κρυπτογραφικές υπηρεσίες: στην αυθεντικοποίηση και στη μη απάρνηση. Η αυθεντικοποίηση παρέχει προστασία από ενεργητικές επιθέσεις, όπου ο αντίπαλος έχει τη δυνατότητα να τροποποιεί ή να επαναμεταδίδει μηνύματα, κατά τέτοιον τρόπο ώστε τα μηνύματα να φαίνονται ότι προέρχονται από κάποια άλλη οντότητα. Η αυθεντικοποίηση παρέχει τη δυνατότητα ανίχνευσης των αυθαίρετων τροποποιήσεων ή επαναμεταδόσεων.

Κατά την ίδρυση μιας συνόδου επικοινωνίας όπου απαιτείται η αυθεντικοποίηση των ταυτοτήτων των επικοινωνούντων μελών, το κάθε μέλος αποδεικνύει την ταυτότητά του, προτού αρχίσει η ανταλλαγή πληροφοριών. Η ίδρυση της συνόδου επικοινωνίας συνοδεύεται και από την εδραίωση ενός κλειδιού συνόδου. Σε αυτό το στάδιο, ο αντίπαλος επιχειρεί να προσποιηθεί την ταυτότητα ενός ή και των δύο μελών, ώστε να ελέγξει την επιλογή του κλειδιού συνόδου. Η αυθεντικοποίηση των ταυτοτήτων των μελών αποκλείει τον αντίπαλο από μια τέτοια επίθεση.

Μια τρίτη απαίτηση είναι η μη απάρνηση. Αυτή η απαίτηση θεωρεί ότι ο αντίπαλος είναι κάποιο από τα (νόμιμα) επικοινωνούντα μέλη. Έστω ότι η Αλίκη και ο Μπομπ κλείνουν μια συμφωνία αγοραπωλησίας μετοχών. Η Αλίκη δεσμεύεται να πουλήσει στο Μπομπ έναν αριθμό μετοχών σε μια ορισμένη τιμή. Αν πέσει η τιμή της μετοχής προτού πραγματοποιηθεί η συναλλαγή, ο Μπομπ μπορεί να ισχυριστεί ότι δε συμφώνησε στην αγορά της μετοχής αυτής. Αν ανέβει η τιμή της μετοχής, η Αλίκη μπορεί να ισχυριστεί ότι ο Μπομπ δε ζήτησε μετοχές ή μπορεί να μεταβάλλει την ποσότητα και να ισχυρισθεί ότι ο Μπομπ ζήτησε λιγότερες μετοχές. Η υπηρεσία της μη απάρνησης προσφέρει αποδείξεις αφενός μεν ότι η Αλίκη δέχεται να πουλήσει έναν ορισμένο αριθμό μετοχών σε μια ορισμένη τιμή στο Μπομπ, αφετέρου δε ότι ο Μπομπ δέχεται να αγοράσει τον αριθμό των μετοχών στη συμφωνηθείσα τιμή. Η ψηφιακή υπογραφή παρέχει τους μηχανισμούς επίλυσης της αμφισβήτησης της συναλλαγής και μπορεί να γίνει στο βαθμό που η ψηφιακή υπογραφή θα έχει νομική ισχύ.

Συνοψίζοντας, οι απαιτήσεις ασφαλείας της ψηφιακής υπογραφής είναι οι εξής:

Αυθεντικοποίηση της πηγής του μηνύματος. Μεταξύ δύο επικοινωνούντων μελών, ο παραλήπτης ενός μηνύματος θα πρέπει να έχει τη δυνατότητα να επιβεβαιώσει την ταυτότητα του αποστολέα του μηνύματος.

Μη απάρνηση πηγής. Σε περίπτωση που ο αποστολέας αρνηθεί ότι έστειλε το μήνυμα, θα πρέπει ο παραλήπτης του μηνύματος να είναι σε θέση να αποδείξει ότι το μήνυμα στάλθηκε από τον αποστολέα.

Μη απάρνηση προορισμού. Σε περίπτωση που ο παραλήπτης αρνηθεί ότι παρέλαβε το μήνυμα, θα πρέπει να υπάρχει δυνατότητα απόδειξης ότι το μήνυμα παραλήφθηκε από τον παραλήπτη.

Η αυθεντικοποίηση της πηγής του μηνύματος προστατεύει τον αποστολέα ακόμα και σε περίπτωση που ο παραλήπτης τροποποιήσει το αρχικό μήνυμα του αποστολέα. Η ψηφιακή υπογραφή είναι επιθυμητή όταν δεν υπάρχει πλήρης εμπιστοσύνη μεταξύ του αποστολέα και του παραλήπτη, οπότε απαιτείται κάτι περισσότερο από αυθεντικοποίηση.

Η υπηρεσία της μη απάρνησης πηγής συναντάται συχνότερα από τη μη απάρνηση προορισμού, καθώς οι ηλεκτρονικές συναλλαγές ξεκινούν πάντοτε από τον αποστολέα και τις περισσότερες φορές οι ενέργειες του παραλήπτη γίνονται φανερές και αποδεικνύονται έτσι αυτόματα. Η μη απάρνηση της πηγής απαιτείται για να αποδειχθεί ότι ο παραλήπτης δεν ενήργησε αυθαίρετα χωρίς την αίτηση του αποστολέα. Έτσι, η μη απάρνηση προορισμού δεν είναι υποχρεωτική.

Αυτές ήταν οι απαιτήσεις ασφαλείας των ψηφιακών υπογραφών. Παρακάτω ακολουθεί σύγκριση των χειρόγραφων υπογραφών με τις ψηφιακές:

Χειρόγραφες υπογραφές	Ψηφιακές υπογραφές
Αναγνώριση της ταυτότητας του υπογεγραμμένου	Αυθεντικοποίηση της ταυτότητας του υπογεγραμμένου: Η ψηφιακή υπογραφή θα πρέπει να συνδέει την ταυτότητα ενός μέλους με κάποια πληροφορία με τέτοιον τρόπο ώστε να είναι αναμφισβήτητη η αναγνώριση του μέλους.
Αναγνώριση της αυθεντικότητας του υπογεγραμμένου κειμένου	Αυθεντικοποίηση του μηνύματος προορισμού: Η ψηφιακή υπογραφή θα πρέπει να αντιστοιχεί σε πληροφορία η οποία να εξαρτάται από το υπογεγραμμένο μήνυμα και τον υπογεγραμμένο.
Δυνατότητα επαλήθευσης της υπογραφής από	Δυνατότητα επαλήθευσης της ψηφιακής υπογραφής από τρίτους: Η επαλήθευση της

τρίτους	ψηφιακής υπογραφής θα πρέπει να είναι εύκολη διαδικασία και θα πρέπει να μπορεί να εκτελεσθεί από οποιονδήποτε.

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

ΟΡΙΣΜΟΣ: Έστω ένα σύνολο μηνυμάτων M, ένα σύνολο τιμών S και μια συνάρτηση μετασχηματισμού S_A: M→S, μιας οντότητας με ταυτότητα A. Το σύνολο S αποτελεί σύνολο υπογραφών, όταν μόνον η οντότητα A για οποιοδήποτε m ϵ M μπορεί να υπολογίσει "με ευκολία" την $S_A(m) = s \epsilon S$. Η S_A ονομάζεται πράξη υπογραφής.

ΟΡΙΣΜΟΣ: Έστω ένα σύνολο μηνυμάτων M κι έστω η συνάρτηση Boole V_A: S x M → {0, 1}, όπου το 0 αντιστοιχεί στο "ψευδές" και το 1 αντιστοιχεί στο "αληθές". Η συνάρτηση V_A ορίζει την πράξη επαλήθευσης αν μπορεί να υπολογισθεί " με ευκολία" από οποιονδήποτε έτσι ώστε για δεδομένο (s, m) ϵ S x M, είναι:

$$V_A(s, m) = 1, \text{ αν } S_A(m) = s$$

ή $$V_A(s, m) = 0, \text{ αν } S_A(m) \neq s$$

Ο όρος "ευκολία" που περιέχεται στους ορισμούς πιο πάνω αναφέρεται στην πολυπλοκότητα που αντιμετωπίζει η οντότητα η οποία επιχειρεί να υπολογίσει την αντίστοιχη συνάρτηση. Έτσι από το σύνολο των μηνυμάτων στο σύνολο των υπογραφών, μόνο η οντότητα A είναι σε θέση να υπολογίσει s τέτοιο ώστε για δεδομένο m ∈ M, να είναι $S_A(m)$, ενώ για κάποιον αντίπαλο είναι υπολογιστικά αδύνατο να εκτελέσει αυτόν τον υπολογισμό. Εφόσον η οντότητα A αποκαλύψει ένα ζεύγος (s, m) όπου $S_A(m) = s$, θα πρέπει να είναι υπολογιστικά δυνατή η επαλήθευση ότι όντως είναι $S_A(m) = s$, προκειμένου να θεωρηθεί έγκυρη η υπογραφή. Η πράξη επαλήθευσης γίνεται με τη βοήθεια της συνάρτησης επαλήθευσης V_A.

ΟΡΙΣΜΟΣ: Η πράξη ψηφιακής υπογραφής S_A, μαζί με την πράξη επαλήθευσης V_A, αποτελούν ένα σύστημα ψηφιακής υπογραφής για την οντότητα A.

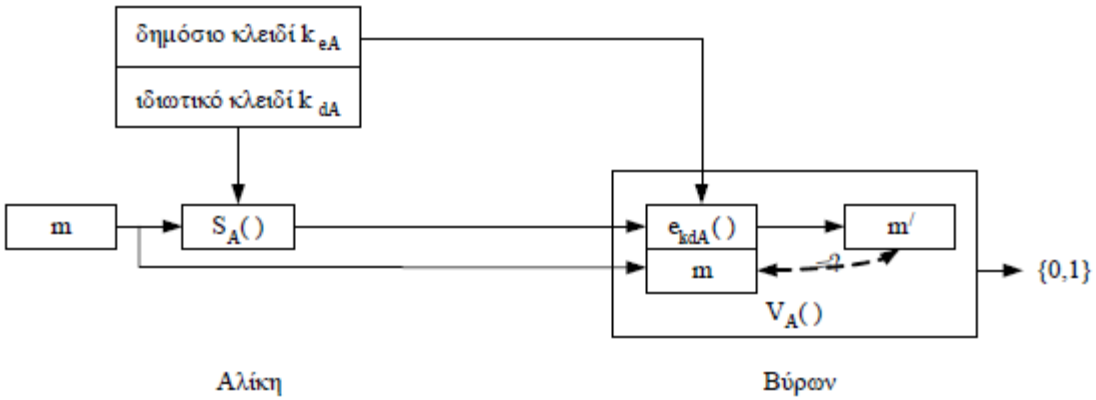
Στην πράξη, το σύνολο των μηνυμάτων είναι μεγαλύτερο από το σύνολο των υπογραφών. Μάλιστα, ο αριθμός των μηνυμάτων είναι κατά πολύ μεγαλύτερος από τον αριθμό των δυνατών υπογραφών. Το σύνολο των μηνυμάτων περιλαμβάνει μηνύματα με διαφορετικό μέγεθος, ενώ οι υπογραφές έχουν συνήθως ένα τυποποιημένο σταθερό μέγεθος. Έτσι, δε μπορούμε να δεχθούμε ότι η πράξη υπογραφής είναι συνάρτηση 1 – 1. Αυτό έχει ως αποτέλεσμα στην ύπαρξη μιας επίθεσης η οποία εκφράζεται στην ακόλουθη επιπρόσθετη απαίτηση:

Αποτροπή πλαστογραφίας. Θα πρέπει να είναι υπολογιστικά αδύνατο σε έναν αντίπαλο ο οποίος έχει στην κατοχή του μια έγκυρη υπογραφή s ενός μηνύματος m, να βρει ένα μήνυμα m', όπου $V_A(m', s) = 1$, με $m \neq m'$.

Η ασύμμετρη κρυπτογραφία είναι ένα αποτελεσματικό μέσο για να πληρούν οι ψηφιακές υπογραφές όλες τις απαιτήσεις. Έτσι, στις ψηφιακές υπογραφές χρησιμοποιείται κατά κόρον η ασύμμετρη κρυπτογραφία. Από την άλλη, έχουν προταθεί λύσεις συστημάτων ψηφιακής υπογραφής με τη χρήση συμμετρικής κρυπτογραφίας, αλλά υπάρχουν αρκετοί περιορισμοί που αντιμετωπίζονται με μη κρυπτογραφικές μεθόδους.

5.3 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΑΣΥΜΜΕΤΡΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Ένα απλό σύστημα ψηφιακής υπογραφής βασισμένο σε ασύμμετρη κρυπτογραφία παρουσιάζεται στο παρακάτω σχήμα:



Σχήμα: Το σύστημα ψηφιακής υπογραφής βασισμένο στην ασύμμετρη κρυπτογραφία

Το μήνυμα απλά κρυπτογραφείται με το ιδιωτικό κλειδί της Αλίκης και το κρυπτοκείμενο που προκύπτει αποτελεί τη ψηφιακή υπογραφή της Αλίκης στο m. Η Αλίκη στέλνει το μήνυμα συνοδευόμενο με τη ψηφιακή υπογραφή στο Βύρωνα. Ο Βύρων, ο οποίος κατέχει το δημόσιο κλειδί της Αλίκης, έχει τη δυνατότητα να επαληθεύσει τη ψηφιακή υπογραφή, εκτελώντας την αποκρυπτογράφηση του κρυπτοκειμένου με το δημόσιο κλειδί της Αλίκης και να ελέγξει αν τα δύο μηνύματα συμπίπτουν.

Αυτό το απλό σύστημα έχει δύο μειονεκτήματα. Πρώτον, ο όγκος των μηνυμάτων που στέλνονται είναι διπλάσιος του μεγέθους του αρχικού μηνύματος m. Το μέγεθος της υπογραφής είναι μεταβλητό και εξαρτάται από το μέγεθος του μηνύματος. Σε δίκτυα όπου ανταλλάσσονται πολλά και μεγάλα μηνύματα, μπορεί να αυξηθεί απαγορευτικά η κίνηση και να μειωθεί η παραγωγή. Αν και το σύστημα της ψηφιακής υπογραφής ορίζει συνάρτηση υπογραφής η οποία είναι 1 – 1, δεν υπάρχει προστασία από επίθεση πλαστογραφίας, που είναι το δεύτερο μειονέκτημα του συστήματος. Η συνάρτηση της ψηφιακής υπογραφής είναι η αποκρυπτογράφηση του μηνύματος με το ιδιωτικό κλειδί. Αυτό σημαίνει ότι αν το μήνυμα έχει μεγαλύτερο μέγεθος από το μέγεθος που δέχεται η πράξη αποκρυπτογράφησης, τότε το μήνυμα θα διαιρεθεί σε μικρότερα τμήματα και θα κρυπτογραφηθεί το κάθε τμήμα χωριστά. Στην περίπτωση που ισχύει η ιδιότητα της αντιμετάθεσης στο ασύμμετρο κρυπτοσύστημα, τότε ο Βύρων μπορεί να κατασκευάσει μηνύματα επιλέγοντας και επαναλαμβάνοντας τμήματα του μηνύματος της αρεσκείας του και ταιριάζοντάς τα με

τα αντίστοιχα τμήματα της ψηφιακής υπογραφής. Δηλαδή, σε αυτήν την επίθεση ο Βύρων μπορεί να κατασκευάσει έναν αριθμό από (m', s'), από το αρχικό (m, s), έτσι ώστε $V_A(m', s') = 1$.

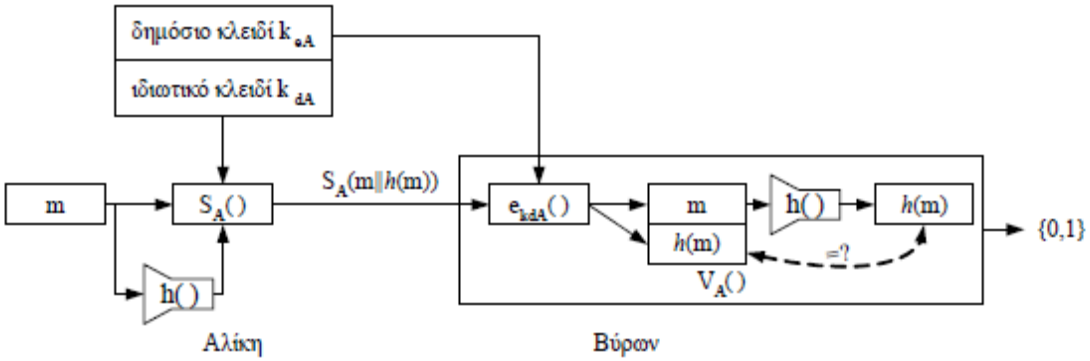
Στην περίπτωση που ο Βύρων έχει κάποια γνώση του μηνύματος, μπορεί η Αλίκη να στείλει μόνο την υπογραφή. Έτσι αν για παράδειγμα το μήνυμα είναι γραμμένο στα ελληνικά, ο Βύρων εφαρμόζοντας την πράξη κρυπτογράφησης (που εδώ λειτουργεί ως αποκρυπτογράφηση) με το δημόσιο κλειδί της Αλίκης, μπορεί εύκολα να διαπιστώσει αν το αποτέλεσμα που προκύπτει είναι ελληνικά. Η ελληνική γλώσσα, όπως και κάθε φυσική γλώσσα, έχει αρκετό πλεονασμό, ώστε οποιαδήποτε τροποποίηση της υπογραφής θα έχει σαν αποτέλεσμα η κρυπτογράφησή του να οδηγήσει σε ασυνάρτητες για την ελληνική γλώσσα λέξεις. Η γνώση του περιεχομένου του μηνύματος από τον παραλήπτη επιτρέπει μια άτυπη επαλήθευση της υπογραφής. Ένα τέτοιο σύστημα ψηφιακής περιγραφής έχει την ιδιότητα της αυτοανάκτησης (self recovery).

Α) ΣΥΣΤΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΜΕ ΑΥΤΟΑΝΑΚΤΗΣΗ

Σε ένα σύστημα ψηφιακής υπογραφής με αυτοανάκτηση, ο πλεονασμός της γλώσσας του μηνύματος θα πρέπει να υπάρχει σε τέτοιο βαθμό, ώστε να είναι δυνατή η επαλήθευση της υπογραφής. Συνεπώς, όταν η γλώσσα του μηνύματος δεν έχει πλεονασμό (ή όταν αυτή είναι μικρή), θα πρέπει με κάποιον τρόπο να προσθέσουμε πλεονασμό. Αυτό έχει ως αποτέλεσμα την αύξηση του μεγέθους του μηνύματος. Η κωδικοποίηση των μηνυμάτων στα δίκτυα υπολογιστών συνήθως είναι τέτοια που ο πλεονασμός είναι ελάχιστος. Μάλιστα, οι αλγόριθμοι συμπίεσης δεδομένων αποβλέπουν στην εξάλειψη του πλεονασμού έτσι ώστε το μήνυμα να καταλαμβάνει το μικρότερο δυνατό χώρο για την αποτελεσματική αποθήκευση και μεταφορά. Έτσι, από τη μια ένας μηχανικός υπολογιστών επιδιώκει να μειώσει τον πλεονασμό, ενώ από την άλλη ένας κρυπτογράφος επιθυμεί να εισάγει πλεονασμό. Συνεπώς, η ισορροπία στη σύγκρουση των ενδιαφερόντων βρίσκεται στο να υπάρχει τόσος πλεονασμός, ώστε να είναι ασφαλές το σύστημα ψηφιακών υπογραφών, όσον αφορά την αξιοπιστία της διαδικασίας επαλήθευσης της υπογραφής.

Οι υποψήφιες κρυπτογραφικές συναρτήσεις που χρησιμοποιούνται για να εισάγουν πλεονασμό στο σύστημα δεν είναι άλλες από τις κρυπτογραφικές μονόδρομες hash. Οι ιδιότητες των κρυπτογραφικών μονόδρομων hash τις καθιστούν ιδανικές για να εισάγουν περίσσεια στο μήνυμα. Ο πλεονασμός εξαρτάται από όλα τα σύμβολα του μηνύματος, έχει σταθερό μέγεθος και είναι ανθεκτική σε συγκρούσεις.

Στο πιο κάτω σχήμα, παρουσιάζεται ένα σύστημα ψηφιακής υπογραφής με αυτοανάκτηση.



Σχήμα: Το σύστημα ψηφιακής υπογραφής με αυτοανάκτηση

Η Αλίκη υπογράφει το μήνυμα m ως εξής: Αρχικά δημιουργεί μια σύνοψη του μηνύματος με τη βοήθεια της κρυπτογραφικής μονόδρομης hash h( ). Στη συνέχεια προσθέτει στο τέλος του μηνύματος m τη σύνοψη h(m) και τροφοδοτεί το συνδυασμό m||h(m) στη συνάρτηση υπογραφής $S_A( )$. Η συνάρτηση υπογραφής αποτελείται από την κρυπτογραφική πράξη της αποκρυπτογράφησης με το ιδιωτικό κλειδί της Αλίκης k_{dA}. Εδώ, η αποκρυπτογράφηση είναι στην πραγματικότητα πράξη κρυπτογράφησης, αλλά για λόγους τυποποίησης δεχόμαστε ότι η κρυπτογραφική πράξη με το ιδιωτικό κλειδί θεωρείται αποκρυπτογράφηση και μπορεί να γίνει μόνο από τον κάτοχο του ιδιωτικού κλειδιού, σε αντίθεση με την πράξη κρυπτογράφησης που μπορεί να γίνει από όλους που έχουν στην κατοχή τους το δημόσιο κλειδί.

Ο Βύρων, μόλις λάβει την υπογραφή, την κρυπτογραφεί εφαρμόζοντας το δημόσιο κλειδί της Αλίκης προκειμένου να ανακτήσει τα δύο τμήματα, το μήνυμα και τη σύνοψη. Στην συνέχεια, υπολογίζει τη σύνοψη του πρώτου τμήματος που αντιστοιχεί στο αρχικό μήνυμα και ελέγχει αν αυτή είναι ίση με τη σύνοψη που έστειλε η Αλίκη. Αν οι δύο συνόψεις είναι ίσες, τότε η υπογραφή είναι έγκυρη.

Ασφάλεια συστήματος ψηφιακής υπογραφής με αυτοανάκτηση

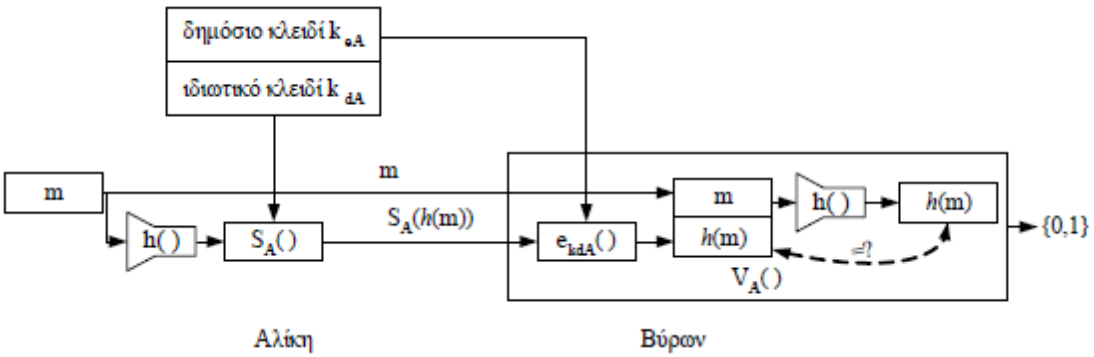
Η επιλογή της κρυπτογραφικής μονόδρομης hash είναι κρίσιμη όσον αφορά την ασφάλεια του συστήματος ψηφιακής υπογραφής με αυτοανάκτηση. Επειδή το μήνυμα είναι μέρος της υπογραφής, η μονόδρομη hash θα πρέπει να έχει ασθενή αντίσταση σε συγκρούσεις.

Το σύστημα είναι ασφαλές σε επίθεση πλαστογραφίας, ακόμα και αν το ασύμμετρο κρυπτοσύστημα που χρησιμοποιείται διατηρεί την ιδιότητα της αντιμετάθεσης. Σε μια κρυπτογραφικά μονόδρομη hash η οποία έχει ασθενή αντίσταση σε συγκρούσεις, δεν ισχύει η αντιμεταθετικότητα, επομένως η σύνοψη ενός πλαστού μηνύματος το οποίο προκύπτει από την αντιμετάθεση των τμημάτων του αρχικού μηνύματος θα είναι διαφορετική από τη σύνοψη του αρχικού μηνύματος.

Β) ΣΥΣΤΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΜΕ ΠΑΡΑΡΤΗΜΑ

Το παραπάνω σύστημα ψηφιακής υπογραφής με αυτοανάκτηση έχει το μειονέκτημα ότι το μέγεθος της ψηφιακής υπογραφής δεν είναι σταθερό και εξαρτάται από το μέγεθος του αρχικού μηνύματος. Είναι κοινή πρακτική οι πράξεις στις οποίες εμπλέκεται ασύμμετρη κρυπτογραφία, να είναι όσο το δυνατόν περιορισμένες. Η ασύμμετρη κρυπτογραφία είναι αρκετές τάξεις μεγέθους πιο αργή από τη συμμετρική κρυπτογραφία. Η κρυπτογράφηση (ή αποκρυπτογράφηση) ενός μηνύματος με ασύμμετρη κρυπτογραφία θα πρέπει συστηματικά να αποφεύγεται για καθαρά πρακτικούς λόγους.

Με βάση τα πιο πάνω, ορίζεται το σύστημα ψηφιακής υπογραφής με παράρτημα.



Σχήμα: Το σύστημα ψηφιακής υπογραφής με παράρτημα

Επειδή ο στόχος της ψηφιακής υπογραφής είναι η αυθεντικοποίηση και όχι η εμπιστευτικότητα, η ασύμμετρη κρυπτογραφία είναι προτιμότερο να αποδεσμευτεί από το μήνυμα. Έτσι, η αποκρυπτογράφηση κατά τη διαδικασία της δημιουργίας της ψηφιακής υπογραφής περιορίζεται στη σύνοψη του μηνύματος.

Ο ξεχωριστός χειρισμός της σύνοψης από το μήνυμα έχει σαν αποτέλεσμα να στέλνονται δύο ανεξάρτητα τμήματα, το αρχικό μήνυμα το οποίο δεν έχει υποστεί κανένα μετασχηματισμό και η ψηφιακή υπογραφή που συνήθως ακολουθεί το μήνυμα. Ο όρος "παράρτημα" οφείλεται στην προσκόλληση της ψηφιακής υπογραφής στο τέλος του μηνύματος, ως ανεξάρτητο αντικείμενο.

Ασφάλεια συστήματος ψηφιακής υπογραφής με παράρτημα

Η ασφάλεια του συστήματος ψηφιακής υπογραφής με παράρτημα είναι συγκρίσιμη με αυτήν του συστήματος ψηφιακής υπογραφής με αυτοανάκτηση. Επειδή όμως ο αντίπαλος έχει πρόσβαση σε περισσότερα μηνύματα, η κρυπτογραφική μονόδρομη hash θα πρέπει να παρουσιάζει ισχυρή αντίσταση σε συγκρούσεις. Στην περίπτωση του συστήματος της ψηφιακής υπογραφής με αυτοανάκτηση, ο αριθμός των μηνυμάτων που μπορεί να κατασκευάσει ο αντίπαλος καθορίζεται από το συνδυασμό των τμημάτων του αρχικού μηνύματος. Αντίθετα, στην περίπτωση του συστήματος ψηφιακής υπογραφής με παράρτημα, ο αντίπαλος έχει ολόκληρο το σύνολο των μηνυμάτων στη διάθεσή του.

Στην περίπτωση που απαιτείται εμπιστευτικότητα, το μήνυμα m κρυπτογραφείται είτε με το ιδιωτικό κλειδί του Βύρωνα, είτε με το συμμετρικό κλειδί συνόδου. Αν η επικοινωνία μεταξύ της Αλίκης και του Βύρωνα είναι συχνή ή περιλαμβάνει μεγάλα μηνύματα, τότε προτιμάται η χρήση συμμετρικής κρυπτογραφίας για να κρυπτογραφηθεί το μήνυμα, για λόγους ταχύτητας.

Υπάρχουν δύο συνδυασμοί για την κρυπτογράφηση και την εφαρμογή ψηφιακής υπογραφής:

κρυπτογράφηση του μηνύματος με το συμμετρικό κλειδί συνόδου και στη συνέχεια υπογραφή του κρυπτοκειμένου,

υπογραφή του (απλού κειμένου) μηνύματος και στη συνέχεια κρυπτογράφηση του μηνύματος.

Από τις δύο εναλλακτικές, η πρώτη δεν προτιμάται για δύο βασικούς λόγους. Η ψηφιακή υπογραφή του κρυπτοκειμένου εισάγει και τη μεταβλητή του μυστικού κλειδιού συνόδου. Έτσι, ο Βύρων θα μπορούσε να αποκρυπτογραφήσει το κρυπτοκείμενο με κάποιο άλλο κλειδί και να ισχυριστεί ότι το απλό κείμενο που προκύπτει είναι το μήνυμα το οποίο έστειλε η Αλίκη. Με άλλα λόγια, η ψηφιακή υπογραφή της Αλίκης είναι έγκυρη για 2^n μηνύματα, όπου n το μέγεθος του μυστικού κλειδιού συνόδου σε bits. Έτσι, ο Βύρων έχει τη δυνατότητα να πραγματοποιήσει επιλεκτική πλαστογραφία. Το πρόβλημα μπορεί να λυθεί αν η Αλίκη συμπεριλάβει στο μήνυμα και το μυστικό κλειδί και το υπογράψει. Όμως, σε έναν τέτοιο διακανονισμό, ο κίνδυνος αποκάλυψης του κλειδιού σε τρίτους είναι μεγάλος και μπορεί να δημιουργήσει προβλήματα ασφάλειας, αν το κλειδί αυτό χρησιμοποιείται για περαιτέρω επικοινωνία μεταξύ της Αλίκης και του Βύρωνα.

Ο δεύτερος λόγος είναι καθαρά δεοντολογικός. Η ενέργεια της υπογραφής υποδεικνύει γνώση του περιεχομένου που υπογράφεται. Η ψηφιακή υπογραφή σε κάποιο κρυπτοκείμενο δε στηρίζει την έννοια της υπογραφής, αφού η Αλίκη δε γνωρίζει άμεσα τι υπογράφει.

Γ) ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΜΕ ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RSA

Το κρυπτοσύστημα RSA μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός συστήματος ψηφιακών υπογραφών. Το σύστημα ψηφιακών υπογραφών RSA απαιτεί ότι όλες οι οντότητες έχουν στην κατοχή τους αντίστοιχα ζεύγη δημόσιου και ιδιωτικού κλειδιού.

ΟΡΙΣΜΟΣ: Έστω p και q δύο πρώτοι αριθμοί και n = pq. Το σύστημα ψηφιακών υπογραφών RSA ορίζεται με $M = S = Z_n$, πράξη υπογραφής:

$$S_A(m) = m^{kdA} \bmod n$$

και πράξη επαλήθευσης:

$$V_A(s) = s^{keA} \bmod n,$$

όπου $k_{eA}k_{dA} \equiv 1 \pmod{\varphi(n)}$, με k_{eA} το δημόσιο κλειδί και k_{dA} το ιδιωτικό κλειδί της οντότητας Α.

Επειδή η ψηφιακή υπογραφή αποτελείται από το μήνυμα αποκρυπτογραφημένων με το ιδιωτικό κλειδί του αποστολέα, το παραπάνω σύστημα ψηφιακών υπογραφών RSA μπορεί να λειτουργήσει ως σύστημα ψηφιακής υπογραφής με αυτοανάκτηση αν σταλεί μόνον η ψηφιακή υπογραφή χωρίς το μήνυμα.

Ασφάλεια συστήματος ψηφιακών υπογραφών RSA

Το κρυπτοσύστημα RSA διατηρεί την αντιμεταθετική ιδιότητα που σημαίνει ότι ένας αντίπαλος μπορεί να εκτελέσει ενεργητική επίθεση και να αναδιατάξει το μήνυμα και την υπογραφή του κατά τη μεταφορά τους από τον αποστολέα στον παραλήπτη. Οι αναδιατάξεις πραγματοποιούνται σε τμήματα των $\lfloor \log_2(n) \rfloor$ bits, όπου n το δημόσιο modulus του αποστολέα. Επίσης, ο αντίπαλος έχει τη δυνατότητα να επαναλάβει ορισμένα τμήματα του μηνύματος, σε θέσεις της επιλογής του, κατοπτρίζοντας τις επαναλήψεις και στα αντίστοιχα τμήματα της ψηφιακής υπογραφής.

Μια λύση είναι να κρυπτογραφηθεί η ψηφιακή υπογραφή με το δημόσιο κλειδί του παραλήπτη, εκμεταλλευόμενοι το γεγονός ότι όλα τα επικοινωνούντα μέλη που συμμετέχουν στην υποδομή του RSA θα έχουν δημόσια και ιδιωτικά κλειδιά. Έστω ότι η Αλίκη επιθυμεί να στείλει εμπιστευτικά στο Βύρωνα ένα μήνυμα m το οποίο να είναι συγχρόνως υπογεγραμμένο από την ίδια. Τα στοιχεία τα οποία απαιτούνται για τις κρυπτογραφικές πράξεις είναι οι παράμετροι RSA (k_{eA}, k_{dA}, n_A) της Αλίκης, καθώς και οι παράμετροι RSA (k_{eB}, k_{dB}, n_B) του Βύρωνα. Αρχικά, η Αλίκη υπογράφει ψηφιακά το μήνυμα m:

$$s = S_A(m) = m^{kdA} \bmod n_A.$$

Στη συνέχεια κρυπτογραφεί την υπογραφή με το δημόσιο κλειδί του Βύρωνα:

$$c = s^{keB} \bmod n_B.$$

Έτσι, ο αντίπαλος θα έχει πρόσβαση μόνο στο μήνυμα και δε θα έχει τη δυνατότητα να πραγματοποιήσει τις αλλαγές του μηνύματος στη ψηφιακή υπογραφή.

Ωστόσο, η εξάρτηση του μεγέθους των δεδομένων που κρυπτογραφούνται από τις RSA παραμέτρους των μελών, έχει επιπτώσεις στην αντιστρεψιμότητα της πράξης της κρυπτογράφησης. Πιο συγκεκριμένα, αν τα modulus των δύο μελών είναι διαφορετικά με $n_A > n_B$, τότε υπάρχει πιθανότητα η κρυπτογραφημένη υπογραφή να μη μπορεί να αποκρυπτογραφηθεί σωστά από το Βύρωνα. Για την αποφυγή αυτού του ενδεχομένου υπάρχουν οι εξής τακτικές:

να προηγηθεί η κρυπτογράφηση του μηνύματος με το δημόσιο κλειδί του Βύρωνα της ψηφιακής υπογραφής, στην περίπτωση που $n_A > n_B$. Η τακτική αυτή δε συστήνεται.

να τμηματοποιηθεί η υπογραφή προκειμένου να είναι συμβατή με το n_B. Η τακτική αυτή δημιουργεί προβλήματα υλοποίησης, αυξάνοντας την πολυπλοκότητα και τις απαιτήσεις επεξεργασίας του συστήματος ψηφιακών υπογραφών.

το κάθε μέλος να έχει δύο διαφορετικά ζεύγη κλειδιών, το ένα για ψηφιακή υπογραφή και το άλλο για κρυπτογράφηση, έτσι ώστε το modulus για την κρυπτογράφηση να είναι μεγαλύτερο από όλα τα moduli που χρησιμοποιούνται στις ψηφιακές υπογραφές.

να μειωθεί η πιθανότητα μη αντιστρεψιμότητας της κρυπτογράφησης σε πρακτικώς ανεκτά επίπεδα. Έχει δειχθεί ότι αυτό μπορεί να γίνει αν η δυαδική αναπαράσταση του n έχει τη μορφή:

$$n = (100...01...)_2 \quad \text{(k φορές το 0)}$$

δηλαδή το σημαντικότερο bit θα πρέπει να είναι άσσος και στη συνέχεια να ακολουθήσουν k μηδενικά, όπου k αριθμός επιλογής μας. Επειδή το n είναι γινόμενο δύο αριθμών, υπάρχει τρόπος επιλογής των p και q έτσι ώστε το γινόμενο που προκύπτει να έχει την επιθυμητή μορφή. Έτσι η ψηφιακή υπογραφή θα είναι μικρότερη του n και θα έχει 0 στη θέση του σημαντικότερου bit.

Στην περίπτωση του συστήματος ψηφιακής υπογραφής RSA με παράρτημα, το κατώτατο μέγεθος της κρυπτογραφικής μονόδρομης hash θα πρέπει να είναι ίσο με 128 bits. Τέλος, όσον αφορά το μέγεθος των RSA παραμέτρων, αν το κρυπτοσύστημα RSA χρησιμοποιείται μόνο για ψηφιακές υπογραφές και όχι μόνο για εμπιστευτικότητα, τότε ο δημόσιος εκθέτης k_e μπορεί να έχει οποιαδήποτε τιμή, καθώς δεν έχουν αναφερθεί αδυναμίες για μικρές τιμές του k_e. Ο αριθμός n θα πρέπει να έχει μέγεθος το λιγότερο ίσο με 1024 bits, ενώ σε περιπτώσεις όπου απαιτείται μεγάλη διάρκεια ζωής των κλειδιών, προτείνεται το μέγεθος των 2048 bits.

Δ) ΤΟ ΣΥΣΤΗΜΑ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ ElGamal

Η ασφάλεια του συστήματος των ψηφιακών υπογραφών ElGamal βασίζεται στη δυσκολία του υπολογισμού του διακριτού λογάριθμου από τον αντίπαλο. Για την υλοποίηση του συστήματος ψηφιακών υπογραφών ElGamal απαιτείται κρυπτογραφική μονόδρομη hash της οποίας η σύνοψη είναι στοιχείο του συνόλου Z_p*, όπου p πρώτος αριθμός.

Η υποδομή ενός συστήματος ψηφιακών υπογραφών ElGamal απαιτεί την ακόλουθη διαδικασία δημιουργίας ζεύγους κλειδιών από τα μέλη. Αρχικά επιλέγεται ένας μεγάλος πρώτος αριθμός p και ένας ακέραιος α ο οποίος είναι γεννήτορας του συνόλου Z_p^*. Στη συνέχεια επιλέγεται ένας ακέραιος b τέτοιος ώστε $0 < b < p-1$

και υπολογίζεται το:

$$y \equiv \alpha^b \pmod{p}.$$

Το δημόσιο κλειδί αποτελείται από τους τρεις ακέραιους (p, α, y) ενώ το ιδιωτικό κλειδί είναι ο εκθέτης b. Η παραπάνω διαδικασία εκτελείται από κάθε μέλος.

Κατά τη διαδικασία υπογραφής, εκτελείται το ακόλουθο πρωτόκολλο:

Επιλογή μυστικού ακεραίου k, με $0 < k < p-1$ και $\gcd(k, p-1) = 1$.

Υπολογισμός του $r \equiv \alpha^k \pmod{p}$.

Υπολογισμός του $k^{-1} \bmod p$.

Υπολογισμός του $s \equiv k^{-1} (h(m)-br) \pmod{p-1}$.

Η υπογραφή για το μήνυμα m είναι το ζεύγος (r, s), το οποίο αποστέλλεται μαζί με το μήνυμα στον παραλήπτη.

Η διαδικασία επαλήθευσης πραγματοποιείται με το ακόλουθο πρωτόκολλο:

1. Έλεγχος ότι $0 < r < p-1$. Στην περίπτωση που το r δε βρίσκεται μεταξύ των ενδεδειγμένων ορίων, απορρίπτεται η ψηφιακή υπογραφή.

2. Υπολογισμός του $\nu \equiv y^r r^s \pmod p$.

3. Υπολογισμός της σύνοψης h(m) και υπολογισμός του $\nu' \equiv \alpha^{h(m)} \pmod p$.

4. Η υπογραφή θεωρείται έγκυρη αν και μόνο αν $\nu = \nu'$.

Μπορούμε να επαληθεύσουμε την εγκυρότητα της υπογραφής με την ισοδυναμία του τελευταίου βήματος του πρωτοκόλλου επαλήθευσης ως εξής:

$$s \equiv k^{-1}(h(m) - br) \pmod{p-1} \rightarrow$$

$$ks \equiv h(m) - br \pmod{p-1} \rightarrow$$

$$h(m) \equiv ks + br \pmod{p-1} \rightarrow$$

$$\alpha^{h(m)} \equiv \alpha^{ks+br} \pmod p \rightarrow$$

$$\alpha^{h(m)} \equiv (\alpha^b)^r (\alpha^k)^s \pmod p \rightarrow$$

$$\alpha^{h(m)} \equiv y^r r^s \pmod p$$

ή ισοδύναμα $\nu' = \nu$.

Ασφάλεια του συστήματος ψηφιακών υπογραφών ElGamal

Όπως αναφέρθηκε και νωρίτερα, η ασφάλεια του συστήματος ψηφιακών υπογραφών ElGamal βασίζεται στη δυσκολία υπολογισμού του διακριτού λογάριθμου. Ο αντίπαλος έχει στην κατοχή του το δημόσιο κλειδί (p, α, y) του υπογεγραμμένου και καλείται να ανακαλύψει το ιδιωτικό κλειδί b, το οποίο ικανοποιεί τη σχέση:

$$y \equiv \alpha^b \pmod{p}.$$

Αν θεωρήσουμε ότι το πρόβλημα του διακριτού λογάριθμου είναι υπολογιστικά αδύνατο, τότε αν ο αντίπαλος επιλέξει στην τύχη έναν ακέραιο για υποψήφιο ιδιωτικό κλειδί, η πιθανότητα να επιλέξει το σωστό κλειδί είναι ίση με 1/(p-1), εφόσον οι επιτρεπτές τιμές του ιδιωτικού κλειδιού βρίσκονται στο διάστημα $0 < b < p-1$. Επομένως, το P θα πρέπει να είναι αρκετά μεγάλο ώστε η πιθανότητα εύρεσης του ιδιωτικού κλειδιού να είναι μικρή.

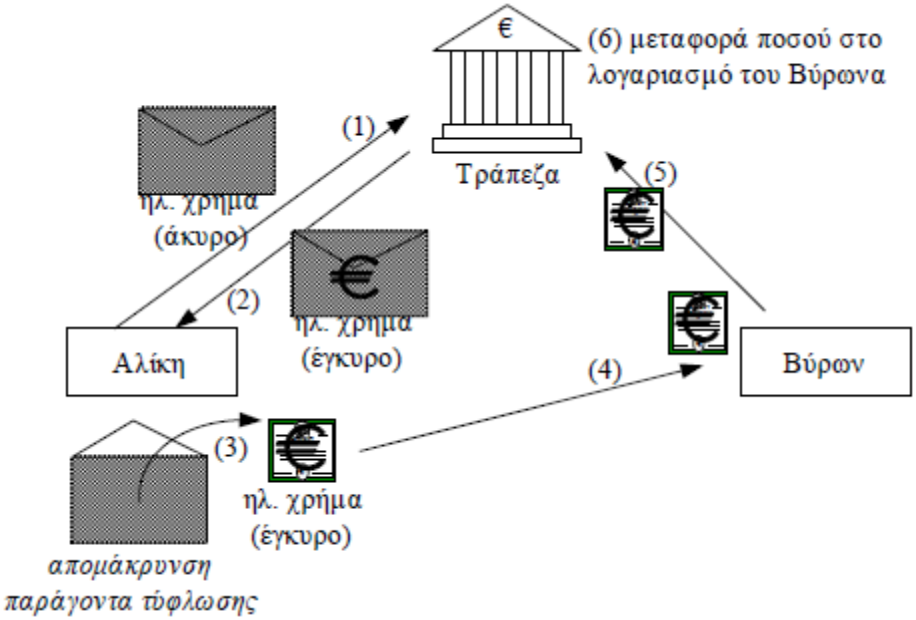
Ένα άλλο σημείο το οποίο θέτει σε κίνδυνο το σύστημα δίνοντας πλεονέκτημα για επιτυχή πλαστογραφία είναι η επιλογή του τυχαίου ακέραιου k, κατά τη διαδικασία δημιουργίας της ψηφιακής υπογραφής. Πιο συγκεκριμένα, ο υπογεγραμμένος θα πρέπει να διατηρεί ιστορικό όλων των τυχαίων αριθμών που έχει επιλέξει, ώστε σε κάθε υπογραφή να χρησιμοποιείται διαφορετικός ακέραιος k.

Ε) ΣΥΣΤΗΜΑΤΑ ΤΥΦΛΩΝ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ

Οι τυφλές ψηφιακές υπογραφές παρουσιάζουν πρακτικό ενδιαφέρον σε πολλές εφαρμογές, όπως στο ηλεκτρονικό χρήμα και στις ηλεκτρονικές εκλογές. Η χαρακτηριστική ιδιότητα που καθιστά μια υπογραφή τυφλή είναι το γεγονός ότι ο υπογράφων δε γνωρίζει το περιεχόμενο του μηνύματος που υπογράφει.

Η αναλογία της τυφλής υπογραφής παριστάνεται στο ακόλουθο παράδειγμα. Έστω ότι απαιτείται να υπογραφεί ένα έγγραφο χωρίς να γνωρίζει ο υπογράφων το περιεχόμενό του. Το έγγραφο μπορεί να μπει σε φάκελο, μαζί με ένα φύλλο καρμπόν και να σφραγισθεί. Στη συνέχεια, ο υπογράφων βάζει την υπογραφή του επάνω στο φάκελο και λόγω της παρεμβολής του καρμπόν, η υπογραφή μεταφέρεται στο κλειστό έγγραφο. Στη συνέχεια, ο παραλήπτης του εγγράφου μπορεί να ανοίξει το φάκελο και να παραλάβει το υπογεγραμμένο έγγραφο.

Η παραπάνω αναλογία είναι χρήσιμη στο ηλεκτρονικό χρήμα ως εξής: Ο πελάτης της ηλεκτρονικής τράπεζας ετοιμάζει ηλεκτρονικά χρήματα, τα οποία επικυρώνονται από την ηλεκτρονική τράπεζα. Η επικύρωση πραγματοποιείται όταν η ηλεκτρονική τράπεζα υπογράφει τα ηλεκτρονικά χρήματα του πελάτη, τα οποία αυτόματα μετατρέπονται σε ηλεκτρονικό χρήμα. Μια βασική ιδιότητα του φυσικού χρήματος είναι η ανωνυμία ξοδέματος (anonymity of spending). Η τράπεζα δε μπορεί να ανιχνεύσει που ξοδεύονται τα φυσικά χρήματα τα οποία έχει διανέμει στους πολίτες. Αυτή η ιδιότητα είναι επιθυμητή και στον ηλεκτρονικό κόσμο. Αν η ηλεκτρονική τράπεζα ήταν σε θέση να γνωρίζει τα χρήματα που υπογράφει, τότε θα είχε τη δυνατότητα να αναγνωρίσει τον αγοραστή σε μια συναλλαγή.



Σχήμα: Ο κύκλος του ηλεκτρονικού χρήματος

Η Αλίκη αποφασίζει να αγοράσει ένα σαξόφωνο από το μουσικό οίκο του Βύρωνα. Αρχικά, δημιουργεί ένα ηλεκτρονικό "χαρτονόμισμα" που αναγράφει την αξία του σαξοφώνου. Στη συνέχεια, το τοποθετεί σε ηλεκτρονικό φάκελο, εφαρμόζοντας ένα μυστικό παράγοντα τύφλωσης (blinding factor) και στέλνει το ψηφιακό φάκελο, καθιστώντας έγκυρο το περιεχόμενό του και στέλνει το αποτέλεσμα πίσω στην Αλίκη. Η Αλίκη απομακρύνει τον παράγοντα τύφλωσης, το οποίο ισοδυναμεί με την εξαγωγή του έγκυρου πλέον χαρτονομίσματος από το φάκελο και το μεταβιβάζει στο Βύρωνα. Ο Βύρων ελέγχει την εγκυρότητα της υπογραφής, εφόσον γνωρίζει το αντίστοιχο δημόσιο κλειδί της Τράπεζας και παραδίδει το προϊόν στην Αλίκη. Τέλος, ο Βύρων στέλνει το χαρτονόμισμα στην Τράπεζα η οποία ενημερώνει το λογαριασμό του Βύρωνα με το αναγραφόμενο ποσό.

Η παραπάνω περιγραφή του κύκλου του ηλεκτρονικού χρήματος δίνει μόνον την αρχή λειτουργίας μιας υποδομής ηλεκτρονικού χρήματος. Στην πράξη εφαρμόζονται ποικίλα πρωτόκολλα τα οποία ανταλλάσσονται μεταξύ των επικοινωνούντων μελών, για την προστασία αυτών. Τα πρωτόκολλα απαιτούνται για να μειωθούν ή και να εξαλειφθούν σοβαρές απειλές του συστήματος. Ίσως η σημαντικότερη από αυτές είναι η απειλή του διπλού ξοδέματος (double spending). Καθώς το ηλεκτρονικό χρήμα δεν είναι τίποτα άλλο από μια σειρά δυαδικών ψηφίων, η Αλίκη θα μπορούσε να κρατήσει ένα αντίγραφο του χαρτονομίσματος και να το παρουσιάσει σε κάποιο άλλο κατάστημα για να πραγματοποιήσει αγορά με το ίδιο χαρτονόμισμα. Παρόμοια και ο Βύρων θα μπορούσε να χρησιμοποιήσει το χαρτονόμισμα της Αλίκης για να πραγματοποιήσει δική του αγορά.

ΣΤ) ΣΥΣΤΗΜΑ ΤΥΦΛΩΝ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ RSA

Η ανακάλυψη των τυφλών υπογραφών αποδίδεται στον Chaum[13], ο οποίος είναι και ο βασικός ερευνητής στο συγκεκριμένο χώρο. Το πρώτο και απλούστερο σύστημα ψηφιακών υπογραφών που κατασκευάσθηκε βασίζεται στις κρυπτογραφικές πράξεις του ασύμμετρου κρυπτοσυστήματος RSA.

Έστω ότι η Αλίκη επιθυμεί να παραλάβει υπογεγραμμένο το μήνυμα m από το Βύρωνα, χωρίς αυτός να γνωρίζει το περιεχόμενο του μηνύματος. Θεωρούμε ότι το δημόσιο κλειδί του Βύρωνα είναι (e, m) και το ιδιωτικό του κλειδί είναι το d. Επίσης, για το μήνυμα ισχύει $m < n$.

Αρχικά η Αλίκη επιλέγει τον παράγοντα τύφλωσης ο οποίος είναι ένας μυστικός ακέραιος k, τέτοιος ώστε $0 < k < n$ και $\gcd(k, n) = 1$. Ένα σύστημα τυφλών ψηφιακών υπογραφών αποτελείται από τρεις διαδικασίες: την τύφλωση, την υπογραφή και την απομάκρυνση του παράγοντα τύφλωσης. Στο σύστημά μας, οι τρεις διαδικασίες ορίζονται ως εξής:

τύφλωση. Υπολογισμός του $m' \equiv mk^e \pmod n$ από την Αλίκη.

13 Chaum David: Είναι ο εφευρέτης πολλών κρυπτογραφικών πρωτοκόλλων, συμπεριλαμβανομένων και των σχημάτων τυφλών υπογραφών. Το 1982, ίδρυσε τη Διεθνή Οργάνωση Κρυπτολογικής Έρευνας (IARC – International Association for Cryptologic Research), η οποία συμβάλλει σημαντικά στην έρευνα της κρυπτογραφίας. Οι συνεισφορές του στον τομέα της κρυπτογραφίας συμπεριλαμβάνουν την ανακάλυψη των mix networks (τη βάση για όλα τα μοντέρνα ανώνυμα δίκτυα) και των DC – Nets, των διαφόρων ψηφιακών υπογραφών και των πρώτων τεχνικών για ανώνυμες συναλλαγές ψηφιακών μετρητών.

Αλίκη → Βύρων: m'

υπογραφή. Υπολογισμός του $s \equiv (m')^d \pmod n$ από το Βύρωνα.

Βύρων → Αλίκη: s

απομάκρυνση του παράγοντα τύφλωσης. Υπολογισμός του sk-1 mod n. Το αποτέλεσμα του υπολογισμού θα είναι η υπογραφή του Βύρωνα στο μήνυμα m.

ΚΕΦΑΛΑΙΟ 6

ΕΠΙΛΟΓΟΣ – ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΟΠΤΙΚΕΣ

ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Επί δύο χιλιάδες χρόνια, οι κωδικοπλάστες αγωνίζονταν να προστατεύσουν μυστικά, ενώ οι κωδικοθραύστες έβαζαν τα δυνατά τους για να τα αποκαλύψουν. Ήταν πάντα μία μάχη στήθος με στήθος, με τους δεύτερους να αντεπιτίθενται όταν οι πρώτοι κυριαρχούσαν και με τους πρώτους να επινοούν νέες και ισχυρότερες μορφές κρυπτογράφησης, όταν οι προηγούμενες μέθοδοί τους αποτύγχαναν. Η επινόηση της κρυπτογραφίας δημοσίου κλειδιού και η πολιτική διαμάχη που περιβάλλει τη χρήση ισχυρής κρυπτογραφίας μας φέρνει στο σήμερα και είναι σαφές ότι οι κρυπτογράφοι κερδίζουν τον πόλεμο της πληροφορίας.

Στο τελευταίο αυτό κεφάλαιο εξετάζουμε μερικές από τις φουτουριστικές ιδέες που μπορεί να βελτιώσουν ή να καταστρέψουν το ιδιωτικό απόρρητο κατά τον εικοστό πρώτο αιώνα. Το τμήμα, που ακολουθεί, ρίχνει μια ματιά στο μέλλον της κρυπτανάλυσης και ιδίως σε μια ιδέα που μπορεί να επιτρέψει στους κρυπταναλυτές να σπάσουν όλα τα σημερινά κρυπτογράμματα.

6.1 ΤΟ ΜΕΛΛΟΝ ΤΗΣ ΚΡΥΠΤΑΝΑΛΥΣΗΣ

Παρά την τεράστια ισχύ του RSA και των άλλων σύγχρονων κρυπτογραμμάτων, οι κρυπταναλυτές εξακολουθούν να παίζουν σημαντικό ρόλο στη συλλογή πληροφοριών. Η επιτυχία τους φαίνεται από το γεγονός ότι η ζήτηση κρυπταναλυτών είναι μεγαλύτερη από ποτέ – η NSA (Εθνική Υπηρεσία Ασφάλειας των ΗΠΑ – κρατική κεντρική υπηρεσία του Υπουργείου Άμυνας των ΗΠΑ, ειδικότερα αρμόδια για την ασφάλεια των επικοινωνιών) παραμένει ο μεγαλύτερος εργοδότης μαθηματικών στον κόσμο.

Μόνο ένα μικρό ποσοστό των πληροφοριών που ρέουν ανά τον κόσμο είναι κρυπτογραφημένο με ασφαλή τρόπο, ενώ οι υπόλοιπες πληροφορίες είναι κρυπτογραφημένες ανεπαρκώς ή και καθόλου. Αυτό συμβαίνει επειδή ο αριθμός των χρηστών του Διαδικτύου αυξάνει ραγδαία και ωστόσο ελάχιστοι είναι εκείνοι που παίρνουν τις κατάλληλες προφυλάξεις ως προς την προστασία των προσωπικών τους δεδομένων. Αυτό με τη σειρά του σημαίνει ότι οι οργανώσεις εθνικής ασφάλειας, οι υπεύθυνοι για την επιβολή του νόμου, αλλά και οποιοσδήποτε περίεργος μπορεί να έχει πρόσβαση σε περισσότερες πληροφορίες από όσες είναι σε θέση να διαχειριστεί.

Ακόμη και αν οι χρήστες χρησιμοποιούν σωστά το κρυπτόγραμμα RSA και πάλι οι κωδικοθραύστες διαθέτουν πολλές μεθόδους για να σταχυολογούν πληροφορίες από τα μηνύματα που υποκλέπτουν. Κατ' αρχάς, εξακολουθούν να χρησιμοποιούν τις παραδοσιακές τεχνικές, όπως η ανάλυση κυκλοφορίας: έστω και αν δεν είναι σε θέση να μαντέψουν το περιεχόμενο ενός μηνύματος, μπορούν τουλάχιστον να εντοπίσουν τον αποστολέα και τον αποδέκτη του, πράγμα που από μόνο του μπορεί να είναι αποκαλυπτικό. Μια πιο πρόσφατη εξέλιξη είναι η επίθεση θυέλλης, που στόχο έχει να ανιχνεύει τα ηλεκτρομαγνητικά σήματα, τα οποία εκπέμπονται από τα ηλεκτρονικά κυκλώματα της οθόνης ενός υπολογιστή.

Κάποιες άλλες μορφές επίθεσης περιλαμβάνουν τη χρήση ιών (viruses) και δούρειων ίππων (trojan horses). Μια παραλλαγή του δούρειου ίππου είναι ένα εντελώς καινούριο λογισμικό κρυπτογράφησης, που μοιάζει ασφαλές, αλλά που στην πραγματικότητα περιέχει μια "πίσω πόρτα", κάτι που επιτρέπει στους σχεδιαστές του να αποκρυπτογραφούν τα μηνύματα όλων των χρηστών. Το 1998 ο Ουέιν Μάντσεν αποκάλυψε σε μια αναφορά του ότι η ελβετική κρυπτογραφική εταιρεία Crypto AG είχε ενσωματώσει πίσω πόρτες σε κάποια από τα προϊόντα της και είχε διοχετεύσει στην αμερικανική κυβέρνηση όλες τις λεπτομέρειες για το πώς να τις εκμεταλλεύεται. Αποτέλεσμα; Οι ΗΠΑ ήταν σε θέση να διαβάζουν τις επικοινωνίες αρκετών χωρών. Το 1991, οι δολοφόνοι του Σαπούρ Μπαχτιάρ, του εξόριστου πρώην πρωθυπουργού του Ιράν, συνελήφθησαν χάρη στην υποκλοπή και την αποκρυπτογράφηση, με τη μέθοδο της πίσω πόρτας, ιρανικών μηνυμάτων κρυπτογραφημένων με εξοπλισμό της Crypto AG.

Παρότι η ανάλυση κυκλοφορίας, οι επιθέσεις θυέλλης, οι ιοί και οι δούρειοι ίπποι αποτελούν χρήσιμες τεχνικές για τη συλλογή πληροφοριών, οι κρυπταναλυτές συνειδητοποιούν ότι ο πραγματικός στόχος τους είναι να βρουν έναν τρόπο για να σπάσουν το κρυπτόγραμμα RSA, τον ακρογωνιαίο λίθο της σύγχρονης κρυπτογράφησης. Το κρυπτόγραμμα RSA χρησιμοποιείται για να προστατεύσει τις

πιο σημαντικές στρατιωτικές, διπλωματικές, εμπορικές και εγκληματικές επικοινωνίες – ακριβώς δηλαδή εκείνα τα μηνύματα που επιδιώκουν να αποκρυπτογραφήσουν οι οργανώσεις συλλογής πληροφοριών. Αν, λοιπόν, οι κρυπταναλυτές θέλουν να απειλήσουν την ισχυρή κρυπτογράφηση RSA, θα πρέπει να πραγματοποιήσουν ένα μείζον θεωρητικό ή τεχνολογικό επίτευγμα.

Ένα θεωρητικό επίτευγμα θα ήταν ένας ριζικά νέος τρόπος ανεύρεσης του ιδιωτικού κλειδιού της Αλίκης. Το κλειδί αυτό αποτελείται από τους αριθμούς p και q, οι οποίοι μπορούν να ευρεθούν από την παραγοντοποίηση του N, του δημόσιου κλειδιού. Η κλασική προσέγγιση είναι να ελέγχουμε έναν προς έναν όλους τους πρώτους αριθμούς για να δούμε ποιος διαιρεί τον N, όμως γνωρίζουμε ότι αυτό απαιτεί παράλογα πολύ χρόνο. Οι κρυπταναλυτές προσπάθησαν να βρουν ένα σύντομο δρόμο για την παραγοντοποίηση, μια μέθοδο που να μειώνει δραστικά τα βήματα που χρειάζονται για να βρεθούν οι p και q, όμως μέχρι τώρα όλες οι απόπειρες για την ανάπτυξη μιας τέτοιας μεθόδου έχουν καταλήξει σε αποτυχία. Οι μαθηματικοί μελετούν την παραγοντοποίηση εδώ και αιώνες και οι σύγχρονες τεχνικές στον τομέα αυτό δεν είναι σημαντικά καλύτερες από τις παλιές. Ίσως μάλιστα οι νόμοι των μαθηματικών να αποκλείουν την ύπαρξη ενός ριζικά σύντομου δρόμου για την παραγοντοποίηση.

Μην έχοντας πολλές ελπίδες για μια θεωρητική ανακάλυψη, οι κρυπταναλυτές υποχρεώθηκαν να αναζητήσουν μια τεχνολογική καινοτομία. Αν δεν υπάρχει κανένας προφανής τρόπος μείωσης του αριθμού των βημάτων που απαιτούνται για την παραγοντοποίηση, τότε οι κρυπταναλυτές χρειάζονται μια τεχνολογία που θα εκτελεί αυτά τα βήματα ταχύτερα. Επομένως, αναζητούν μια ριζικά νέα μορφή υπολογιστή, τον κβαντικό υπολογιστή. Αν οι επιστήμονες μπορούσαν να κατασκευάσουν έναν κβαντικό υπολογιστή, αυτός θα είχε τη δυνατότητα να εκτελεί υπολογισμούς με τόσο τεράστια ταχύτητα, που θα έκανε έναν σημερινό υπερυπολογιστή να μοιάζει με σπασμένο αριθμητήριο.

Πριν προχωρήσουμε παρακάτω, καλό είναι να λάβουμε υπόψη την παρακάτω προειδοποίηση: Η κβαντομηχανική εισάγει κάποιες μάλλον αλλόκοτες ιδέες, που με την πρώτη ανάγνωση ίσως προκαλούν ζαλάδα ή σάστισμα. Και για να εξηγήσουμε τις αρχές της κβαντικής υπολογιστικής, είναι χρήσιμο να πάμε πίσω στα τέλη του 18ου αιώνα και στο έργο του Τόμας Γιανγκ, του Άγγλου πανεπιστήμονα που έκανε την πρώτη σημαντική πρόοδο στην αποκρυπτογράφηση των αιγυπτιακών ιερογλυφικών. Όσο ήταν υπότροφος στο Εμμάνουελ Κόλετζ του Κέμπριτζ, ο Γιανγκ συχνά περνούσε τα απογεύματά του χαλαρώνοντας κοντά στη λιμνούλα με τις πάπιες. Μια μέρα, όπως λέγεται, εκεί που παρακολουθούσε δύο πάπιες να κολυμπούν ευτυχισμένες πλάι – πλάι, παρατήρησε ότι άφηναν πίσω τους δύο ίχνη κυματισμών, τα οποία αλληλεπιδρούσαν και σχημάτιζαν ένα ιδιαίτερο σχήμα αποτελούμενο από ταραγμένα και ήρεμα κομμάτια. Οι δύο σειρές κυματισμών απλώνονταν σε σχήμα βεντάλιας πίσω από τις δύο πάπιες και όταν μία κορυφή από μια πάπια συναντούσε ένα βαθούλωμα αλληλοεξουδετερώνονταν. Αντίθετα, όταν συναντιώνταν στο ίδιο σημείο δύο κορυφές, το αποτέλεσμα ήταν μια ακόμα ψηλότερη κορυφή, ενώ όταν συναντιώνταν δύο βαθουλώματα, προέκυπτε ένα ακόμη βαθύτερο. Το θέαμα αυτό σαγήνευε τον Γιανγκ, γιατί του θύμισε ένα πείραμα με αντικείμενο τη φύση του φωτός, το οποίο είχε πραγματοποιήσει το 1799.

Στο πείραμα εκείνο ο Γιανγκ είχε ρίξει φως σε ένα μεσότοιχο, όπου υπήρχαν δύο στενές κάθετες σχισμές. Σε μια οθόνη τοποθετημένη σε κάποια απόσταση πίσω από τις σχισμές, ο Γιανγκ περίμενε να δει δύο φωτεινές λωρίδες, προβολές των σχισμών. Αντ' αυτού παρατήρησε ότι το φως απλωνόταν σε σχήμα βεντάλιας από τις δύο σχισμές και δημιουργούσε στην οθόνη ένα σχήμα αποτελούμενο από φωτεινές και σκοτεινές λωρίδες. Τότε, το ραβδωτό σχήμα του φωτός στην οθόνη τον είχε προβληματίσει, τώρα όμως πίστευε ότι μπορούσε να το εξηγήσει πλήρως με βάση αυτό που είχε δει στη λιμνούλα με τις πάπιες.

Ο Γιανγκ ξεκίνησε με την υπόθεση ότι το φως είναι μια μορφή κύματος. Αν το φως που εκπεμπόταν από τις δύο σχισμές συμπεριφερόταν ως κύματα, τότε ήταν ακριβώς όπως οι κυματισμοί πίσω από τις δύο πάπιες. Επιπλέον, οι φωτεινές και σκοτεινές λωρίδες στην οθόνη δημιουργούνταν από τις ίδιες αλληλεπιδράσεις που έκαναν τα κύματα του νερού να σχηματίζουν ψηλές κορυφές, βαθιές γούβες και ήρεμα τμήματα. Ο Γιανγκ μπορούσε να φαντασθεί πάνω στην οθόνη σημεία όπου ένα βαθούλωμα συναντούσε μια κορυφή, με αποτέλεσμα την αλληλοεξουδετέρωσή τους και τη δημιουργία μιας σκοτεινής λωρίδας και άλλα σημεία όπου δύο κορυφές (ή δύο βαθουλώματα) συναντιώνταν, με αποτέλεσμα την ενίσχυσή τους και τη δημιουργία μιας φωτεινής λωρίδας. Οι πάπιες είχαν χαρίσει στον Γιανγκ μια βαθύτερη κατανόηση της αληθινής φύσης του φωτός.

Σήμερα, γνωρίζουμε ότι το φως όντως συμπεριφέρεται σαν κύμα, ξέρουμε όμως ότι μπορεί να συμπεριφέρεται και σαν σωματίδιο. Το αν αντιλαμβανόμαστε το φως σαν κύμα ή σαν σωματίδιο εξαρτάται από τις συνθήκες και αυτή η διττή φύση του φωτός είναι γνωστή ως δυϊσμός κύματος – σωματιδίου. Μέχρι εδώ δεν υπάρχει τίποτε το παράξενο στο πείραμα του Γιανγκ. Ωστόσο, η σύγχρονη τεχνολογία επιτρέπει στους φυσικούς να το επαναλάβουν χρησιμοποιώντας ένα λεπτό νήμα που είναι τόσο σκοτεινό, ώστε να εκπέμπει μεμονωμένα φωτόνια. Τα φωτόνια παράγονται με ρυθμό ένα το λεπτό και κάθε φωτόνιο ταξιδεύει μόνο του προς το μεσότοιχο. Μερικές φορές, ένα φωτόνιο θα περάσει μέσα από τη μία ή την άλλη σχισμή και θα προσκρούσει στην οθόνη. Παρότι τα μάτια μας δεν είναι αρκετά ευαίσθητα ώστε να δουν τα μεμονωμένα φωτόνια, αυτά μπορούν να παρατηρηθούν με τη βοήθεια ενός ειδικού ανιχνευτή και μετά από παρέλευση κάποιων ωρών μπορούμε να σχηματίσουμε μια γενική εικόνα του πού χτυπούν τα φωτόνια την οθόνη. Εφόσον κάθε φορά περνάει μέσα από τις σχισμές ένα μόνο φωτόνιο, δε θα περιμέναμε να δούμε το ραβδωτό σχήμα που παρατήρησε ο Γιανγκ, επειδή το φαινόμενο μοιάζει να εξαρτάται από το ταυτόχρονο πέρασμα δύο φωτονίων μέσα από διαφορετικές σχισμές και την αλληλεπίδρασή τους στην άλλη πλευρά. Αντ' αυτού, θα περιμέναμε να δούμε μόνο δύο φωτεινές λωρίδες, απλές προβολές στην οθόνη των σχισμών στο μεσότοιχο. Ωστόσο, για κάποιον παράξενο λόγο, ακόμη και με μεμονωμένα φωτόνια το αποτέλεσμα στην οθόνη είναι και πάλι ένα σχήμα με φωτεινές και σκοτεινές λωρίδες, σα να υπήρχε αλληλεπίδραση φωτονίων.

Το αλλόκοτο αυτό αποτέλεσμα αψηφά την κοινή λογική. Δεν υπάρχει κανένας τρόπος να εξηγηθεί το φαινόμενο με όρους των κλασσικών νόμων της Φυσικής και με αυτό εννοούμε τους παραδοσιακούς νόμους που αναπτύχθηκαν για να εξηγήσουν το πώς συμπεριφέρονται τα καθημερινά αντικείμενα. Για να εξηγήσουν τα φωτονικά φαινόμενα, οι επιστήμονες καταφεύγουν στην κβαντική θεωρία, μια ερμηνεία του πώς συμπεριφέρονται τα αντικείμενα στο μικροσκοπικό επίπεδο. Όμως, ούτε οι θεωρητικοί της κβαντικής φυσικής είναι σε θέση να συμφωνήσουν στο πώς να

ερμηνεύσουν το συγκεκριμένο πείραμα, αλλά χωρίζονται σε δύο αντιτιθέμενα στρατόπεδα, που το καθένα προβάλλει τη δική του ερμηνεία.

Το πρώτο στρατόπεδο προωθεί την ιδέα της λεγόμενης υπέρθεσης. Οι οπαδοί της υπέρθεσης δηλώνουν κατ' αρχήν ότι δύο μόνο πράγματα γνωρίζουμε με βεβαιότητα για το φωτόνιο – εγκαταλείπει το νήμα και προσκρούει στην οθόνη. Όλα τα υπόλοιπα είναι ένα απόλυτο μυστήριο, περιλαμβανομένου και του αν το φωτόνιο πέρασε από τη δεξιά ή την αριστερή σχισμή. Επειδή η ακριβής πορεία του φωτονίου δεν είναι γνωστή, οι οπαδοί της υπέρθεσης κάνουν την παράδοξη υπόθεση ότι το φωτόνιο με κάποιον τρόπο διέρχεται ταυτόχρονα και από τις δύο σχισμές, πράγμα που του επιτρέπει να αλληλεπιδρά με τον εαυτό του και να δημιουργεί το ραβδωτό σχήμα που παρατηρούμε στην οθόνη. Πώς όμως είναι δυνατό να περνά το φωτόνιο και από τις δύο σχισμές;

Οι οπαδοί της υπέρθεσης επιχειρηματολογούν ως εξής: Αν δε γνωρίζουμε τι κάνει ένα σωματίδιο, τότε μπορεί να κάνει ταυτόχρονα όλες τις πιθανές ενέργειες. Στην περίπτωση του φωτονίου, δε ξέρουμε αν πέρασε από την αριστερή ή τη δεξιά σχισμή κι έτσι υποθέτουμε ότι πέρασε και από τις δύο ταυτόχρονα. Η κάθε πιθανότητα αποκαλείται κατάσταση κι επειδή το φωτόνιο πληροί και τις δύο πιθανότητες λέγεται ότι βρίσκεται σε μια υπέρθεση καταστάσεων.

Ο Έρβιν Σρέντιγκερ, που κέρδισε το βραβείο Νόμπελ Φυσικής το 1933, επινόησε ένα παράδειγμα γνωστό ως "γάτα του Σρέντιγκερ", το οποίο χρησιμοποιείται συχνά για να εξηγήσει την έννοια της υπέρθεσης.

Φαντασθείτε μια γάτα μέσα σε ένα κουτί. Υπάρχουν δύο πιθανές καταστάσεις για τη γάτα: να είναι νεκρή ή να είναι ζωντανή. Αρχικά, γνωρίζουμε ότι η γάτα βρίσκεται οπωσδήποτε σε μια συγκεκριμένη κατάσταση, επειδή μπορούμε να δούμε ότι είναι ζωντανή. Στο σημείο αυτό, η γάτα δε βρίσκεται σε υπέρθεση καταστάσεων. Στη συνέχεια τοποθετούμε στο κουτί, μαζί με τη γάτα, ένα φιαλίδιο με κυάνιο και κλείνουμε το σκέπασμα. Τώρα εισερχόμαστε σε μια περίοδο άγνοιας, επειδή δε μπορούμε να δούμε ή να μετρήσουμε την κατάσταση της γάτας. Είναι ακόμα ζωντανή ή μήπως πάτησε πάνω στο φιαλίδιο με το κυάνιο και πέθανε; Κατά την παραδοσιακή αντίληψη, θα λέγαμε ότι η γάτα είναι ή ζωντανή ή νεκρή και απλώς δε ξέρουμε τι από τα δύο συμβαίνει. Ωστόσο, η κβαντική θεωρία υποστηρίζει ότι η γάτα βρίσκεται σε ένα στάδιο υπέρθεσης δύο καταστάσεων – είναι ταυτόχρονα νεκρή και ζωντανή, ικανοποιεί και τις δύο πιθανότητες. Η υπέρθεση συμβαίνει μόνο όταν παύουμε να βλέπουμε ένα αντικείμενο και είναι ένας τρόπος να περιγράψουμε ένα αντικείμενο στη διάρκεια μιας περιόδου αμφιβολίας. Όταν τελικά ανοίξουμε το κουτί, μπορούμε να δούμε αν η γάτα είναι ζωντανή ή νεκρή. Η πράξη του να κοιτάξουμε τη γάτα την αναγκάζει να είναι σε μια συγκεκριμένη κατάσταση και αυτή ακριβώς τη στιγμή η υπέρθεση εξαφανίζεται.

Για τους αναγνώστες που νιώθουν άβολα με την υπέρθεση, υπάρχει το δεύτερο κβαντικό στρατόπεδο, που προτιμά μια διαφορετική ερμηνεία του πειράματος του Γιανγκ. Δυστυχώς, η εναλλακτική αυτή άποψη είναι εξίσου αλλόκοτη. Η ερμηνεία των πολλαπλών κόσμων ισχυρίζεται ότι το φωτόνιο, φεύγοντας από το νήμα, έχει δύο επιλογές – να περάσει από την αριστερή ή από τη δεξιά σχισμή – και στο σημείο αυτό το σύμπαν χωρίζεται σε δύο σύμπαντα: στο ένα σύμπαν το φωτόνιο περνά από την αριστερή σχισμή και στο άλλο από τη δεξιά. Τα

δύο αυτά σύμπαντα με κάποιο τρόπο αλληλεπιδρούν, πράγμα που εξηγεί το ραβδωτό σχήμα. Οι οπαδοί της ερμηνείας των πολλαπλών κόσμων πιστεύουν ότι κάθε φορά που ένα αντικείμενο έχει τη δυνατότητα να εισέλθει σε μία από πολλές πιθανές καταστάσεις, το σύμπαν διασπάται σε πολλά σύμπαντα, έτσι ώστε κάθε δυνατότητα να πραγματοποιηθεί σε ένα διαφορετικό σύμπαν. Αυτή η πολλαπλότητα των συμπάντων είναι γνωστή ως πολυσύμπαν.

Ανεξάρτητα από το αν υιοθετήσουμε την υπέρθεση ή την ερμηνεία των πολλαπλών κόσμων, η κβαντική θεωρία είναι μια φιλοσοφία που θέτει πολλά ερωτήματα. Ωστόσο, απέδειξε ότι είναι η πιο επιτυχημένη και πρακτική επιστημονική θεωρία που επινοήθηκε ποτέ. Εκτός από τη μοναδική της δυνατότητα να εξηγεί το αποτέλεσμα του πειράματος του Γιανγκ, η κβαντική θεωρία εξηγεί με επιτυχία και πολλά άλλα φαινόμενα. Μόνον η κβαντική θεωρία επιτρέπει στους φυσικούς να υπολογίζουν τις συνέπειες των πυρηνικών αντιδράσεων στους σταθμούς παραγωγής ενέργειας μόνο η κβαντική θεωρία μπορεί να εξηγήσει τα θαύματα του DNA. Μόνο η κβαντική θεωρία εξηγεί το πώς λάμπει ο ήλιος, μόνο η κβαντική θεωρία μπορεί να χρησιμοποιηθεί για το σχεδιασμό της ακτίνας λέιζερ που διαβάζει τα Cds στο στερεοφωνικό μας συγκρότημα. Έτσι λοιπόν, είτε μας αρέσει είτε όχι, ζούμε σε έναν κβαντικό κόσμο.

Από όλες τις συνέπειες της κβαντικής θεωρίας, η πιο σημαντική από τεχνολογική άποψη είναι εν δυνάμει ο κβαντικός υπολογιστής. Πέραν του ότι θα κατέστρεφε την ασφάλεια όλων των σύγχρονων κρυπτογραμμάτων, ο κβαντικός υπολογιστής θα εγκαινίαζε μια νέα εποχή υπολογιστικής ισχύος. Ένας από τους σκαπανείς της κβαντικής υπολογιστικής είναι ο Ντέιβιντ Ντόιτς, ένας Βρετανός φυσικός που άρχισε να εργάζεται πάνω σε αυτή την ιδέα το 1984, όταν παρακολούθησε ένα συνέδριο για τη θεωρία των υπολογιστών. Ακούγοντας μια διάλεξη στο συνέδριο, ο Ντόιτς επισήμανε κάτι που ως τότε είχε περάσει απαρατήρητο. Η σιωπηρή παραδοχή ήταν ότι όλοι οι υπολογιστές κατά βάση λειτουργούν σύμφωνα με τους νόμους της κλασσικής Φυσικής, όμως ο Ντόιτς ήταν πεπεισμένος για το αντίθετο, ότι δηλαδή οι υπολογιστές θα πρέπει να υπακούουν στους νόμους της κβαντικής Φυσικής, επειδή οι κβαντικοί νόμοι είναι πιο θεμελιώδεις.

Οι συνηθισμένοι υπολογιστές λειτουργούν σε ένα σχετικά μακροσκοπικό επίπεδο και στο επίπεδο αυτό οι κβαντικοί νόμοι σχεδόν δε διαχωρίζονται από τους κλασσικούς. Επομένως, δεν είχε σημασία το ότι οι επιστήμονες είχαν γενικά σκεφτεί τους συνηθισμένους υπολογιστές με όρους κλασσικής Φυσικής.

6.2 ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Ενώ οι κρυπταναλυτές προσδοκούν την έλευση των κβαντικών υπολογιστών, οι κρυπτογράφοι εργάζονται για το δικό τους τεχνολογικό θαύμα – ένα κρυπτογραφικό σύστημα που θα κατοχυρώσει εκ νέου το ιδιωτικό απόρρητο ακόμη

κι όταν θα έχει να αντιμετωπίσει την ισχύ ενός κβαντικού υπολογιστή. Η νέα αυτή μορφή κρυπτογράφησης διαφέρει ριζικά από οτιδήποτε συναντήσαμε πριν, κατά το ότι προσφέρει την ελπίδα της τέλειας προστασίας του ιδιωτικού απορρήτου. Με άλλα λόγια, ένα τέτοιο σύστημα θα ήταν άψογο και θα εγγυάτο απόλυτη ασφάλεια ες αεί. Επιπλέον, βασίζεται στην κβαντική θεωρία, την ίδια θεωρία που αποτελεί το θεμέλιο των κβαντικών υπολογιστών. Έτσι, η κβαντική θεωρία είναι η έμπνευση για έναν υπολογιστή που θα μπορούσε να σπάσει όλα τα σημερινά κρυπτογράμματα και ταυτόχρονα βρίσκεται στην καρδιά ενός νέου, άθραυστου κρυπτογράμματος που αποκαλείται κβαντική κρυπτογραφία.

Η ιστορία της κβαντικής κρυπτογραφίας ανάγεται σε μια παράξενη ιδέα που ανέπτυξε στο τέλος της δεκαετίας του 1960 ο Στέφεν Βίζενερ, μεταπτυχιακός φοιτητής τότε στο Πανεπιστήμιο Κολούμπια. Δυστυχώς, η ατυχία του Βίζενερ ήταν ότι επινόησε μια ιδέα τόσο πρωτοποριακή για την εποχή του, που κανείς δεν την πήρε στα σοβαρά. Ο Βίζενερ πρότεινε την παράξενη έννοια του κβαντικού χρήματος, που παρουσίαζε το μεγάλο πλεονέκτημα του ότι ήταν αδύνατον να παραχαρακτεί.

Ένα άτομο, το οποίο συμμερίστηκε τον ενθουσιασμό του Βίζενερ για την κβαντική φυσική, ήταν ένας παλιός φίλος του ονόματι Τσαρλς Μπένετ. Η ιδέα του Βίζενερ για το κβαντικό χρήμα γοήτευσε αμέσως τον Μπένετ, ο οποίος εξήγησε την όλη ιδέα στον Ζιλ Μπρασάρ κι έτσι άρχισαν να σχεδιάζουν ένα σύστημα βασισμένο στην εξής αρχή.

Φανταστείτε ότι η Αλίκη θέλει να στείλει στον Μπομπ ένα κρυπτογραφημένο μήνυμα που αποτελείται από μια σειρά μονάδων και μηδενικών. Παριστά λοιπόν τις μονάδες και τα μηδενικά στέλνοντας φωτόνια με συγκεκριμένες πολώσεις. Η Αλίκη έχει να επιλέξει ανάμεσα σε δύο σχήματα σύνδεσης των πολώσεων των φωτονίων με το 1 ή το 0. Στο πρώτο σχήμα, το λεγόμενο ευθύγραμμο, ή σχήμα +, στέλνει ένα φωτόνιο πόλωσης ↕ για να εκπροσωπεί το 1 κι ένα πόλωσης ↔ για το 0. Για να στείλει ένα δυαδικό μήνυμα, εναλλάσσει τα δύο σχήματα με απρόβλεπτο τρόπο. Έτσι, το δυαδικό μήνυμα 1101101001 θα μπορούσε να μεταδοθεί ως εξής:

Μήνυμα 1 1 0 1 1 0 1 0 0 1

Σχήμα + x + x x x + + x x

Μετάδοση ↕ / ↔ / / \ ↕↔ \ /

Η Αλίκη μεταδίδει το πρώτο 1 χρησιμοποιώντας το σχήμα + και το δεύτερο 1 χρησιμοποιώντας το σχήμα x. Κατά συνέπεια, το 1 μεταδίδεται και στις δύο περιπτώσεις, αλλά κάθε φορά εκπροσωπείται από διαφορετικής πόλωσης φωτόνια.

Η συνταγή τους για την κβαντική κρυπτογραφία απαιτεί τρία προπαρασκευαστικά στάδια. Παρότι τα στάδια αυτά δεν περιλαμβάνουν αποστολή κρυπτογραφημένου μηνύματος, επιτρέπουν την ασφαλή ανταλλαγή ενός κλειδιού το οποίο στη συνέχεια θα χρησιμοποιηθεί για την κρυπτογράφηση ενός μηνύματος.

Στάδιο 1. Η Αλίκη αρχίζει μεταδίδοντας μια τυχαία ακολουθία μονάδων και μηδενικών (μπιτ), χρησιμοποιώντας μια τυχαία επιλογή ευθύγραμμων (κάθετων και οριζόντιων) και διαγώνιων σχημάτων πόλωσης.

Στάδιο 2. Ο Μπομπ πρέπει να μετρήσει την ποσότητα των φωτονίων. Εφόσον δε γνωρίζει ποιο σχήμα πόλωσης χρησιμοποίησε η Αλίκη για το κάθε φωτόνιο, ανταλλάσσει τυχαία τους δύο ανιχνευτές του, τον + και τον x. Μερικές φορές ο Μπομπ επιλέγει το σωστό ανιχνευτή και κάποιες άλλες όχι. Αν ο Μπομπ χρησιμοποιήσει λάθος ανιχνευτή, μπορεί να ερμηνεύσει εσφαλμένα το φωτόνιο της Αλίκης.

Στάδιο 3. Στο σημείο αυτό, η Αλίκη έχει στείλει μια σειρά από μονάδες και μηδενικά και ο Μπομπ έχει ανιχνεύσει ορισμένα από αυτά σωστά και κάποια άλλα λάθος. Στη συνέχεια, για να ξεκαθαρίσει την κατάσταση, η Αλίκη τηλεφωνεί στον Μπομπ σε μια κοινή, μη ασφαλή γραμμή και του λέει ποιο σχήμα πόλωσης χρησιμοποίησε για το κάθε φωτόνιο – όχι όμως και τι είδους πόλωση του έδωσε. Έτσι θα μπορούσε να του πει ότι έστειλε το πρώτο φωτόνιο χρησιμοποιώντας το ευθύγραμμο σχήμα, αλλά όχι αν έστειλε ↕ ή ↔. Τότε ο Μπομπ λέει στην Αλίκη σε ποιες περιπτώσεις μάντεψε το σωστό σχήμα πόλωσης. Στις περιπτώσεις αυτές μέτρησε σωστά την πόλωση και σημείωσε ορθά το 1 ή το 0. Τέλος, η Αλίκη και ο Μπομπ αγνοούν όλα τα φωτόνια για τα οποία ο Μπομπ χρησιμοποίησε εσφαλμένο σχήμα και συγκεντρώνονται μόνο σε εκείνα για τα οποία μάντεψε το σωστό. Στην πραγματικότητα, δημιούργησαν μια νέα, βραχύτερη ακολουθία μπιτ, αποτελούμενη μόνο από τις σωστές μετρήσεις του Μπομπ.

Ένας άλλος τρόπος να σκεφτούμε την κβαντική κρυπτογραφία είναι με όρους μιας τράπουλας, αντί για τα πολωμένα φωτόνια. Κάθε χαρτί της τράπουλας έχει ένα φύλλο και ένα χρώμα, όπως βαλές κούπα ή έξι μπαστούνι και συνήθως κοιτάζοντας ένα χαρτί βλέπουμε ταυτόχρονα το φύλλο και το χρώμα του. Φαντασθείτε, ωστόσο, ότι μπορούμε να μετρήσουμε μόνο το φύλλο ή μόνο το χρώμα. Ας υποθέσουμε ότι επιλέγει να μετρήσει το χρώμα, που είναι "σπαθί", το οποίο και καταγράφει. Το χαρτί τυχαίνει να είναι το τέσσερα σπαθί, όμως η Αλίκη ξέρει μόνο ότι είναι σπαθί. Στη συνέχεια μεταδίδει το χαρτί μέσω μιας τηλεφωνικής γραμμής στον Μπομπ. Ενώ γίνεται αυτό, η Εύα προσπαθεί να μετρήσει το χαρτί, δυστυχώς όμως γι' αυτή, επιλέγει να μετρήσει το φύλλο του, που είναι "τέσσερα". Όταν το χαρτί φτάνει στον Μπομπ, εκείνος αποφασίζει να μετρήσει το χρώμα του, που είναι πάντα "σπαθί", το οποίο και σημειώνει. Κατόπιν η Αλίκη τηλεφωνεί στον Μπομπ και τον ρωτάει αν μέτρησε το χρώμα, πράγμα που έκανε κι έτσι τώρα η Αλίκη και ο Μπομπ ξέρουν ότι μοιράζονται μια κοινή γνώση – και οι δύο τους έχουν γραμμένο στο σημειωματάριό τους "σπαθί". Αντίθετα, η Εύα έχει γραμμένο στο σημειωματάριό της "τέσσερα", που της είναι εντελώς άχρηστο.

Στη συνέχεια, η Αλίκη παίρνει από την τράπουλα άλλο ένα χαρτί, ας πούμε τον ρήγα καρό και πάλι όμως μπορεί να μετρήσει μόνο μία από τις δύο ιδιότητες. Τη φορά αυτή επιλέγει να μετρήσει το φύλλο, που είναι "ρήγας" και μεταδίδει το χαρτί μέσω μιας τηλεφωνικής γραμμής στον Μπομπ. Η Εύα επιχειρεί να μετρήσει το χαρτί και επιλέγει και αυτή να μετρήσει το φύλλο: "ρήγας". Όταν το χαρτί φτάνει στον Μπομπ, εκείνος αποφασίζει να μετρήσει το χρώμα, που είναι "καρό". Κατόπιν η Αλίκη τηλεφωνεί στον Μπομπ και τον ρωτάει αν μέτρησε το φύλλο του χαρτιού. Εκείνος τότε παραδέχεται ότι μάντεψε λάθος και μέτρησε το χρώμα του. Η Αλίκη και ο Μπομπ δεν ενοχλούνται, επειδή μπορούν να αγνοήσουν εντελώς το συγκεκριμένο χαρτί και να δοκιμάσουν με κάποιο άλλο, επιλεγμένο στην τύχη από την τράπουλα. Στην περίπτωση αυτή η Εύα μάντεψε σωστά και μέτρησε την ίδια ιδιότητα με την Αλίκη, "ρήγας", όμως το χαρτί ακυρώθηκε επειδή ο Μπομπ δεν το μέτρησε σωστά. Έτσι ο Μπομπ δε χρειάζεται να ανησυχεί για τα λάθη του, επειδή ο ίδιος και η Αλίκη μπορούν να συμφωνήσουν να τα αγνοούν, ενώ η Εύα είναι παγιδευμένη στα δικά της. Στέλνοντας αρκετές κάρτες, η Αλίκη και ο Μπομπ μπορούν να συμφωνήσουν σε μια ακολουθία φύλλων και χρωμάτων, η οποία στη συνέχεια μπορεί να χρησιμοποιηθεί ως βάση για ένα είδος κλειδιού.

Η κβαντική κρυπτογραφία επιτρέπει στην Αλίκη και τον Μπομπ να συμφωνήσουν σε ένα κλειδί, το οποίο η Εύα δε μπορεί να υποκλέψει χωρίς να κάνει λάθη. Η κβαντική κρυπτογραφία έχει και ένα επιπλέον πλεονέκτημα: επιτρέπει στην Αλίκη και τον Μπομπ να καταλάβουν αν η Εύα κρυφακούει. Η παρουσία της Εύας στη γραμμή γίνεται εμφανής επειδή κάθε φορά που μετράει ένα φωτόνιο, κινδυνεύει να το αλλοιώσει και οι αλλοιώσεις αυτές γίνονται αντιληπτές από την Αλίκη και τον Μπομπ.

Ο έλεγχος σφαλμάτων διενεργείται μετά τα τρία προκαταρκτικά στάδια μέσω των οποίων η Αλίκη και ο Μπομπ θα έπρεπε να έχουν ταυτόσημες ακολουθίες από μονάδες και μηδενικά. Φαντασθείτε ότι έχουν καταλήξει σε μια ακολουθία που έχει μήκος 1.075 δυαδικά ψηφία. Ένας τρόπος για να ελέγξουν αν οι ακολουθίες τους ταιριάζουν θα ήταν να τηλεφωνήσει η Αλίκη στον Μπομπ και να του διαβάσει την πλήρη της ακολουθία. Δυστυχώς, αν η Εύα κρυφακούει, θα είναι σε θέση να υποκλέψει όλο το κλειδί. Το να ελέγξουν όλη την ακολουθία είναι σαφώς απερίσκεπτο, αλλά και περιττό. Αντ' αυτού, η Αλίκη δεν έχει παρά να επιλέξει στην τύχη 75 ψηφία και να ελέγξει μόνο αυτά. Αν ο Μπομπ επιβεβαιώσει και τα 75 ψηφία, τότε είναι άκρως απίθανο να κρυφάκουγε η Εύα κατά τη διάρκεια της αρχικής μετάδοσης. Πράγματι, οι πιθανότητες να ήταν η Εύα στη γραμμή και ωστόσο να μην επηρέασε τις μετρήσεις του Μπομπ για τα 75 αυτά ψηφία είναι λιγότερες από μία στο δισεκατομμύριο. Επειδή τα 75 συγκεκριμένα ψηφία συζητήθηκαν ανοιχτά από την Αλίκη και τον Μπομπ, θα πρέπει να αποκλειστούν και το μπλοκ τους της μιας χρήσης μειώνεται από 1.075 σε 1.000 δυαδικά ψηφία. Από την άλλη, αν η Αλίκη και ο Μπομπ διαπιστώσουν μια ασυμφωνία ανάμεσα στα 75 ψηφία, τότε θα γνωρίζουν ότι η Εύα κρυφάκουγε και θα πρέπει να εγκαταλείψουν ολόκληρο το μπλοκ μιας χρήσης, να περάσουν σε άλλη γραμμή και να ξαναρχίσουν από την αρχή.

Για να συνοψίσουμε, η κβαντική κρυπτογραφία είναι ένα σύστημα που εγγυάται την ασφάλεια ενός μηνύματος καθιστώντας δύσκολο για την Εύα να διαβάσει με ακρίβεια μια επικοινωνία ανάμεσα στην Αλίκη και τον Μπομπ. Επιπλέον, αν η Εύα επιχειρήσει να κρυφακούσει, τότε η Αλίκη και ο Μπομπ θα είναι σε θέση να ανιχνεύσουν την παρουσία της. Συνεπώς, η κβαντική κρυπτογραφία

επιτρέπει στην Αλίκη και τον Μπομπ να ανταλλάξουν ένα μπλοκ μιας χρήσης και να συμφωνήσουν σ' αυτό κάτω από συνθήκες απόλυτης ασφάλειας και στη συνέχεια να το χρησιμοποιήσουν ως κλειδί για την κρυπτογράφηση ενός μηνύματος. Η διαδικασία αυτή περιλαμβάνει πέντε βασικά βήματα:

Η Αλίκη στέλνει στον Μπομπ μια σειρά από φωτόνια και ο Μπομπ τα μετράει.

Η Αλίκη λέει στον Μπομπ σε ποιες περιπτώσεις οι μετρήσεις του ήταν σωστές.

Η Αλίκη και ο Μπομπ απορρίπτουν τις εσφαλμένες μετρήσεις του δεύτερου και συγκεντρώνονται στις σωστές, ώστε να δημιουργήσουν δύο ταυτόσημα μπλοκ μιας χρήσης.

Η Αλίκη και ο Μπομπ ελέγχουν την ορθότητα των μπλοκ τους δοκιμάζοντας ένα μικρό ποσοστό των ψηφίων.

Αν η διαδικασία της επιβεβαίωσης είναι ικανοποιητική, τότε μπορούν να χρησιμοποιήσουν το μπλοκ μιας χρήσης για να κρυπτογραφήσουν ένα μήνυμα. Αν πάλι η επιβεβαίωση αποκαλύψει σφάλματα, γνωρίζουν ότι τα φωτόνια παγιδεύτηκαν από την Εύα και θα πρέπει να ξαναρχίσουν από την αρχή.

Δεκατέσσερα χρόνια αφότου τα επιστημονικά περιοδικά απέρριψαν το άρθρο του Βίζενερ για κβαντικό χρήμα, η ιδέα του ενέπνευσε ένα απόλυτα ασφαλές σύστημα επικοινωνίας. Ο Βίζενερ, που τώρα ζει στο Ισραήλ, νιώθει ανακούφιση που επιτέλους η εργασία του αναγνωρίζεται.

Οι κρυπτογράφοι χαιρέτισαν την κβαντική κρυπτογραφία των Μπένετ και Μπρασάρ με ενθουσιασμό. Ωστόσο, πολλοί πειραματιστές πρόβαλαν το επιχείρημα ότι το σύστημα λειτουργούσε καλά στη θεωρία, αλλά στην πράξη θα αποτύγχανε. Πίστευαν ότι η δυσκολία χειρισμού μεμονωμένων φωτονίων θα καθιστούσε το σύστημα ανεφάρμοστο. Όμως, παρά τις επικρίσεις, οι Μπένετ και Μπρασάρ ήταν πεπεισμένοι ότι η κβαντική κρυπτογραφία μπορούσε να λειτουργήσει στην πράξη. Μάλιστα είχαν τόση πίστη στο σύστημά τους, που δε μπήκαν καν στον κόπο να κατασκευάσουν τον αντίστοιχο εξοπλισμό. Όπως το έθεσε κάποτε ο Μπένετ, “δεν υπάρχει λόγος να πας στο Βόρειο Πόλο, αν ξέρεις ότι είναι εκεί”.

Ωστόσο, ο αυξανόμενος σκεπτικισμός τελικά παρακίνησε τον Μπένετ να αποδείξει ότι το σύστημα μπορούσε όντως να λειτουργήσει. Το 1988 άρχισε να συγκεντρώνει τα υλικά που θα χρειαζόταν για ένα κβαντικό κρυπτογραφικό σύστημα και ανέθεσε σε έναν φοιτητή, τον Τζον Σμόλιν, να τον βοηθήσει στη συναρμολόγηση του μηχανισμού. Ύστερα από προσπάθειες ενός χρόνου, ήταν έτοιμοι να επιχειρήσουν να στείλουν το πρώτο μήνυμα στην Ιστορία, το οποίο θα προστατευόταν από την κβαντική κρυπτογραφία. Ήταν αργά το απόγευμα όταν αποσύρθηκαν στο ανήλιαγο εργαστήριό τους, ένα κατασκότεινο περιβάλλον, ασφαλές από τα αδέσποτα φωτόνια που θα μπορούσαν να παρεμβληθούν στο πείραμα. Έχοντας δειπνήσει πλούσια, ήταν προετοιμασμένοι για μια μακριά νύχτα

πειραματισμών με τον εξοπλισμό. Επιδίωξή τους ήταν να προσπαθήσουν να στείλουν πολωμένα φωτόνια διαμέσου του δωματίου και στη συνέχεια να τα μετρήσουν χρησιμοποιώντας έναν ανιχνευτή + και έναν x. Ένας υπολογιστής με το όνομα Αλίκη έκανε τον τελικό έλεγχο της μετάδοσης φωτονίων και ένας υπολογιστής με το όνομα Μπομπ αποφάσιζε ποιος ανιχνευτής θα χρησιμοποιείτο για τη μέτρηση του κάθε φωτονίου.

Ύστερα από προσπάθειες ωρών, γύρω στις 3 τα χαράματα, ο Μπένετ παρακολούθησε την πρώτη κβαντική κρυπτογραφική αλλαγή. Η Αλίκη και ο Μπομπ κατόρθωσαν να στείλουν και να λάβουν φωτόνια, συζήτησαν τα σχήματα πόλωσης που είχε χρησιμοποιήσει η Αλίκη, απέρριψαν τα φωτόνια που είχε μετρήσει ο Μπομπ με λάθος ανιχνευτή και συμφώνησαν σε ένα μπλοκ της μιας χρήσης αποτελούμενο από τα εναπομείναντα φωτόνια. Το πείραμα του Μπένετ είχε αποδείξει ότι δύο υπολογιστές, η Αλίκη και ο Μπομπ, μπορούσαν να επικοινωνήσουν με απόλυτη μυστικότητα. Ήταν ένα ιστορικό πείραμα, παρά το γεγονός ότι στους δύο υπολογιστές τους χώριζε μια απόσταση μόλις 12 εκατοστών.

Μετά το πείραμα του Μπένετ, η πρόκληση είναι να κατασκευαστεί εάν κβαντικό κρυπτογραφικό σύστημα που να λειτουργεί σε χρήσιμες αποστάσεις. Το έργο αυτό δεν είναι εύκολο, επειδή τα φωτόνια δεν ταξιδεύουν καλά. Αν η Αλίκη μεταδώσει ένα φωτόνιο με μια συγκεκριμένη πόλωση μέσω του αέρα, τα μόρια του αέρα θα το επηρεάσουν, επιφέροντας μια απαράδεκτη αλλαγή στην πόλωσή του. Ένα αποτελεσματικότερο μέσο μετάδοσης φωτονίων είναι οι οπτικές ίνες και οι ερευνητές κατόρθωσαν πρόσφατα να χρησιμοποιήσουν αυτή την τεχνική για να κατασκευάσουν κβαντικά κρυπτογραφικά συστήματα, τα οποία λειτουργούν σε σημαντικές αποστάσεις. Το 1995, ερευνητές του Πανεπιστημίου της Γενεύης κατάφεραν να εφαρμόσουν την κβαντική κρυπτογραφία σε μια οπτική ίνα μήκους 23 χιλιομέτρων, από τη Γενεύη ως τη Νιόν.

Πιο πρόσφατα, μια ομάδα επιστημόνων στο Εθνικό Εργαστήριο του Λος Άλαμος, στο Νέο Μεξικό, άρχισε και πάλι να πειραματίζεται με την κβαντική κρυπτογραφία διαμέσου του αέρα. Ο τελικός τους στόχος είναι να δημιουργήσουν ένα κβαντικό κρυπτογραφικό σύστημα που να λειτουργεί μέσω δορυφόρων. Αν οι προσπάθειές τους πετύχουν, θα οδηγήσουν σε απολύτως ασφαλείς παγκόσμιες επικοινωνίες. Μέχρι τώρα η ομάδα του Λος Άλαμος κατόρθωσε να μεταδώσει ένα κβαντικό κλειδί διαμέσου του αέρα σε απόσταση ενός χιλιομέτρου.

Οι ειδικοί επί της ασφάλειας διερωτώνται τώρα σε πόσον καιρό θα εξελιχθεί η κβαντική κρυπτογραφία σε πρακτικά εφαρμόσιμη τεχνολογία. Προς το παρόν το να διαθέτουμε την κβαντική κρυπτογραφία δεν προσφέρει κανένα πλεονέκτημα, επειδή το κρυπτόγραμμα RSA ήδη μας εξασφαλίζει πρόσβαση σε μια άθραυστη στην πράξη κρυπτογράφηση. Ωστόσο, αν οι κβαντικοί υπολογιστές γίνουν πραγματικότητα, τότε το RSA και όλα τα σύγχρονα κρυπτογράμματα θα είναι άχρηστα και η κβαντική κρυπτογραφία θα καταστεί αναγκαία. Έτσι ο αγώνας δρόμου έχει ήδη αρχίσει. Το πραγματικά σημαντικό ερώτημα είναι αν η κβαντική κρυπτογραφία θα έλθει εγκαίρως για να μας σώσει από την απειλή των κβαντικών υπολογιστών ή αν θα υπάρξει ένα χάσμα ιδιωτικού απορρήτου, μια περίοδος ανάμεσα στην ανάπτυξη των κβαντικών υπολογιστών και την έλευση της κβαντικής κρυπτογραφίας. Μέχρι τώρα, η κβαντική κρυπτογραφία είναι η πιο εξελιγμένη τεχνολογία. Το ελβετικό πείραμα με τις οπτικές ίνες αποδεικνύει ότι είναι εφικτό να κατασκευασθεί ένα σύστημα που να

επιτρέπει την ασφαλή επικοινωνία μεταξύ οικονομικών οργανισμών μέσα στην ίδια πόλη. Πράγματι, σήμερα είναι δυνατό να κατασκευαστεί ένας κβαντικός κρυπτογραφικός σύνδεσμος μεταξύ του Λευκού Οίκου και του Πενταγώνου. Ίσως μάλιστα να υπάρχει ήδη.

Η κβαντική κρυπτογραφία θα σημάνει το τέλος της μάχης μεταξύ των κωδικοπλαστών και των κωδικοθραυστών και νικητές αναδεικνύονται οι πρώτοι. Η κβαντική κρυπτογραφία είναι ένα άθραυστο σύστημα κρυπτογράφησης. Ίσως η δήλωση αυτή να φαίνεται υπερβολική, ιδίως αν λάβουμε υπόψη προηγούμενους ανάλογους ισχυρισμούς. Τις δύο τελευταίες χιλιετίες σε διάφορες χρονικές στιγμές, οι κρυπτογράφοι πίστεψαν ότι το μονοαλφαβητικό κρυπτόγραμμα, το πολυαλφαβητικό κρυπτόγραμμα και τα μηχανικά κρυπτογράμματα, όπως το Αίνιγμα ήταν όλα τους άθραυστα. Σε όλες αυτές τις περιπτώσεις οι κρυπτογράφοι τελικά διαψεύσθηκαν, επειδή οι ισχυρισμοί τους βασίζονταν απλώς στο γεγονός ότι η πολυπλοκότητα των κρυπτογραμμάτων υπερτερούσε σε μια δεδομένη ιστορική στιγμή της ευφυΐας και της τεχνολογίας των κρυπταναλυτών. Εκ των υστέρων, μπορούμε να δούμε ότι οι κρυπταναλυτές αναπόφευκτα εύρισκαν έναν τρόπο να σπάσουν το εκάστοτε ισχυρό κρυπτόγραμμα ή ανέπτυσσαν μια τεχνολογία που το έσπαζε για λογαριασμό τους.

Ωστόσο, ο ισχυρισμός ότι η κβαντική κρυπτογραφία είναι ασφαλής διαφέρει ποιοτικά από όλους τους προηγούμενους. Η κβαντική κρυπτογραφία δεν είναι απλώς άθραυστη στην πράξη, αλλά απολύτως άθραυστη. Η κβαντική θεωρία, η πιο επιτυχημένη στην ιστορία της Φυσικής, σημαίνει ότι είναι αδύνατο να υποκλέψει με ακρίβεια η Εύα το κλειδί του μπλοκ μιας χρήσης στο οποίο έχουν συμφωνήσει η Αλίκη και ο Μπομπ. Δε μπορεί καν να επιχειρήσει να το υποκλέψει χωρίς να αντιληφθούν η Αλίκη και ο Μπομπ την παρέμβασή της. Πράγματι, αν ένα μήνυμα προστατευμένο από την κβαντική κρυπτογραφία μπορέσει ποτέ να αποκρυπτογραφηθεί, αυτό θα σημαίνει ότι η κβαντική θεωρία είναι ατελής, κάτι που θα είχε καταστροφικές συνέπειες για τους φυσικούς, μιας και θα τους υποχρέωνε να αναθεωρήσουν τις απόψεις τους για το πώς λειτουργεί το σύμπαν στο πιο θεμελιώδες επίπεδο.

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 εταιρείες 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.

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 Άντον Τσάιλιγκερ 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 ασφαλείας 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 και μεγάλη υπολογιστική δύναμη.

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) δε 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 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 να 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 εταιρείες. 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.

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

Αν καταστεί δυνατό να κατασκευαστούν κβαντικά κρυπτογραφικά συστήματα, τα οποία θα μπορούν να λειτουργούν σε μεγάλες αποστάσεις, η εξέλιξη των κρυπτογραμμάτων θα σταματήσει. Η αναζήτηση για την προστασία του ιδιωτικού απορρήτου θα έχει λήξει. Παράλληλα, όμως, η ανάπτυξη ενός πλήρως λειτουργικού κβαντικού υπολογιστή θα έθετε σε κίνδυνο το ιδιωτικό μας απόρρητο, θα κατάστρεφε το ηλεκτρονικό εμπόριο και θα κατεδάφιζε την έννοια της εθνικής ασφάλειας. Ένας κβαντικός υπολογιστής θα απειλούσε την παγκόσμια σταθερότητα. Όποια χώρα φτάσει πρώτη εκεί, θα έχει τη δυνατότητα να παρακολουθεί τις επικοινωνίες των πολιτών της, να διαβάζει τις σκέψεις των εμπορικών της ανταγωνιστών και να υποκλέπτει τα σχέδια των εχθρών της. Η κβαντική υπολογιστική συνιστά εν δυνάμει απειλή για το άτομο, τις διεθνείς επιχειρήσεις και την παγκόσμια ασφάλεια, αλλά και ένα θαυμάσιο επίτευγμα της σύγχρονης επιστήμης.

ΠΑΡΑΡΤΗΜΑ Α

Τυπική Απόδειξη Ορθότητας του RSA – PSS

Α.1 Κίνητρα

Ένα από τα βασικά πεδία της επιστήμης των υπολογιστών αποτελεί η αλγεβρική προδιαγραφή αλγορίθμων. Όμως έως τώρα δεν έχει γίνει προσπάθεια να προσεγγίσουμε τους κρυπτογραφικούς αλγορίθμους με αλγεβρικές προδιαγραφές, ώστε να αποδείξουμε την ορθότητα τους. Εδώ θα προσπαθήσουμε να αναλύσουμε την αλγεβρική προδιαγραφή (formal specification) για το RSA-RSS (probabilistic signature scheme) που χρησιμοποιείται ως αλγόριθμος για τις ψηφιακές προδιαγραφές στο PKCS, ώστε να δημιουργηθεί η βάση που χρειάζεται για να εφαρμόσουμε αλγεβρικές μέθοδοι (formal methods) σε κάθε τομέα της κρυπτογραφίας. Εκτός από την ορθότητα του RSA-PSS αποδεικνύεται η ορθότητα του RSA, της κρυπτογραφικής μεθόδου του PSS. Επίσης, αναλύονται τεχνικές προδιαγραφής για έναν συγκεκριμένο αλγόριθμο υπογραφής.

Στις μέρες μας το λογισμικό (software) εμπεριέχει σφάλματα, τα οποία δεν είναι δυνατό να ανακαλυφθούν κατά τη δημιουργία του. Εκτός του ότι αυτό είναι ενοχλητικό, τα λεγόμενα σφάλματα κώδικα (bugs) μπορεί να προκαλέσουν προβλήματα ασφαλείας. Επιπλέον, τα σφάλματα κώδικα (bugs) μπορούν να έχουν σοβαρές συνέπειες, αν βρεθούν σε λογισμικό (software) που χρησιμοποιείται για παράδειγμα σε κρίσιμες εφαρμογές, όπως ο έλεγχος πυρηνικών κεφαλών (nuclear power plants). Υπάρχουν πολλά παραδείγματα που ο υπολογιστής σχετίζεται με θανατηφόρα ατυχήματα, όπως για παράδειγμα η σύγκρουση του Korean Air Lines B747 στη Guam το 1997 ή η μηχανή ραδιο-θεραπείας Therac-25 που έδινε πολύ μεγαλύτερες δόσεις ραδιενέργειας στους ασθενείς από το επιτρεπόμενο όριο από το 1985 έως το 1987. Ο λόγος που χρειάζονται οι αποδείξεις ορθότητας του software είναι επειδή δε μπορούν όλα τα λάθη να ανακαλυφθούν μέσω των τεστ. Ακόμα και αν ένα πρόγραμμα εξεταστεί εξονυχιστικά με διάφορα τεστ μπορεί και πάλι να περιέχει πλειάδα από περισσότερο ή λιγότερο επικίνδυνα σφάλματα κώδικα (bugs).

Μια πιθανή λύση σ' αυτό το δίλημμα είναι η αλγεβρική προδιαγραφή των αλγορίθμων. Ο στόχος των εφαρμογών των αλγεβρικών μεθόδων είναι η

προδιαγραφή προγραμμάτων, έτσι ώστε να αποδειχθεί η ορθότητα του software, δηλαδή να δοθεί μια μαθηματική απόδειξη ότι το λογισμικό ικανοποιεί την προδιαγραφή του. Αν δοθεί η αλγεβρική απόδειξη για την ορθότητα ενός προγράμματος, τότε δεν χρειάζεται να το τεστάρουμε. Τα συστήματα που έχουν προδιαγραφεί έχουν υψηλή ποιότητα, όπως απαιτείται σε πολλούς τομείς της βιομηχανίας, όπως για παράδειγμα στην ασφάλεια και στα αυτοματοποιημένα μηχανικά συστήματα. Όμως, για να δοθεί μια αλγεβρική απόδειξη, χρειαζόμαστε μια αλγεβρική προδιαγραφή του προγράμματος ως ερώτηση.

Για την αλγεβρική προδιαγραφή του RSA-PSS, που χρησιμοποιείται ως αλγόριθμος για την ψηφιακή υπογραφή στο PKCS standard, χρησιμοποιήσαμε τον theorem prover Isabelle/HOL, ο οποίος αναπτύχθηκε στο Cambridge University και το TU Munich. Θα μπορούσαμε να πούμε ότι ένας theorem prover είναι μια υπολογιστική βοήθεια για μια αλγεβρική απόδειξη.

Το βασικό πλεονέκτημα του RSA-PSS σε σχέση με το παλαιότερο PKCS #1 v1.5 standard, που απλά χρησιμοποιεί ένα επικαλυμμένο συνοπτικό μήνυμα ως είσοδο στον αλγόριθμο υπογραφής είναι ότι μπορεί να αποδειχθεί η ασφάλεια του σε ένα τυχαίο μοντέλο, δηλαδή σε ένα Τυχαίο Μοντέλο Επιλογής (Random Oracle Model). Επίσης, δεν περιλαμβάνει κάποια κρίσιμα σημεία(certain critic points) του παλαιότερου standard. Ακόμα, οι νέες εφαρμογές υπογραφών θα πρέπει να χρησιμοποιούν σχήμα πιθανοτικής υπογραφής. Βασική επιδίωξη είναι να προσφέρουμε μια βάση αυστηρής "θεραπείας" στο RSA-PSS με τη βοήθεια των αλγεβρικών μεθόδων. Γι' αυτό παρουσιάζεται μια απόδειξη ορθότητας του RSA-PSS. Αυτό καταδεικνύει ότι κάθε υπογραφή πάντα μπορεί να "λειτουργεί ορθά". Η παρακάτω εργασία αποδεικνύει ότι η εφαρμογή του RSA-PSS είναι σωστή μέσω της προδιαγραφής, κάτι το οποίο δεν ισχύει για το PKCS από μόνο του. Επιπρόσθετα, αυτή η εργασία δείχνει ότι είναι δυνατό να χρησιμοποιηθούν αλγεβρικές μέθοδοι στην κρυπτογραφία, άρα δίνεται η προοπτική για εξιχνίαση και δημιουργία νέων μονοπατιών στον τομέα της κρυπτογραφίας. Βέβαια, δεν είναι δυνατό να φανεί καθαρά η σύνδεση ανάμεσα στην κρυπτογραφία και τις αλγεβρικές μεθόδους. Παρόλ' αυτά μια γεύση μπορούμε να πάρουμε, αφού κατά την απόδειξη χρειάστηκε να αποδείξουμε κάποια θεωρήματα της συνάρτησης του RSA.

Καθώς γίνεται όλο και πιο σημαντική η προδιαγραφή στους αλγορίθμους, η προδιαγραφή στην κρυπτογραφία παραμένει ακόμα στα πρώτα βήματα. Η ανάγκη για καθοριστικά βήματα στη δημιουργία ενός συνόλου από αλγεβρικές θεωρίες, ώστε οι "μέθοδοι" να αποδεικνύουν την ορθότητα των κρυπτοσυστημάτων προκύπτει από τη συνεχή απαίτηση να διασφαλίζεται η ασφάλεια των συστημάτων. Η παρακάτω εργασία προσφέρει ένα "κουτί" από εργαλεία που θα επιτρέψουν την εφαρμογή των αλγεβρικών προδιαγραφών στην κρυπτογραφία.

Α.2 Σχήμα Ψηφιακής Υπογραφής του SA-PSS και η Τυπική του Προδιαγραφή

A.2.1 Εισαγωγή

Σε αυτό το σημείο, θα δοθεί μια σύντομη ανάλυση των RSA και RSA-PSS, καθώς επίσης θα παρουσιαστεί και η αλγεβρική προδιαγραφή των RSA και PSS. Ένα από τα σημαντικότερα στοιχεία για μια ασφαλή βάση επικοινωνίας είναι οι ψηφιακές υπογραφές. Διασφαλίζει την αυθεντικότητα, την άδεια και τη μη αποκήρυξη. Η ψηφιακή υπογραφή που εξετάζεται εδώ είναι η RSA-PSS, είναι σχήμα υπογραφής με προσάρτηση. Ένα τέτοιο σχήμα αποτελείται από μια λειτουργία υπογραφής - γεννήτορα και μια λειτουργία υπογραφής - προδιαγραφής. Μια υπογραφή για ένα κείμενο παράγεται από το ιδιωτικό κλειδί του υπογράφοντος. Για να αποδειχθεί η αυθεντικότητα χρειαζόμαστε την υπογραφή, το μήνυμα για το οποίο παρήχθη και το δημόσιο κλειδί του αποστολέα. Το σχήμα υπογραφής με προσάρτηση θεωρείται αόρατο από την υπογραφή με επικαλυμμένο μήνυμα.

A.2.2 Υπογραφές Δημοσίου Κλειδιού

Μια υπογραφή δημοσίου κλειδιού αποτελείται από μια διαδικασία υπογραφής και μια διαδικασία απόδειξης. Για ένα μήνυμα m ο υπογράφων δημιουργεί μια υπογραφή s με το ιδιωτικό του κλειδί. Στη συνέχεια στέλνει το ζεύγος (m,s) σε κάποιο άτομο που θέλει να δείξει την υπογραφή. Ο παραλήπτης (verifier) χρησιμοποιεί το δημόσιο κλειδί ώστε να τσεκάρει ότι η s υπογραφή είναι η επιτρεπτή υπογραφή για το m μήνυμα. Αντίθετα με την αποκρυπτογράφηση του μηνύματος, ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να παράγει μια υπογραφή s από το μήνυμα m. Έτσι τώρα ο παραλήπτης χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα μπορεί να "τσεκάρει" την υπογραφή. Αν η αποκρυπτογράφηση της s είναι ίδια με του m, τότε η s υπογραφή "ταιριάζει" με το μήνυμα m.

A.2.3 Ασύμμετρο κρυπτογραφικό σύστημα – RSA

Στα ασύμμετρα συστήματα κρυπτογραφίας, κάθε χρήστης έχει ένα δημόσιο κλειδί και ένα ιδιωτικό που ανταποκρίνεται. Το δημόσιο κλειδί είναι προσβάσιμο από όλους, ενώ το ιδιωτικό μένει μυστικό. Φυσικά είναι πάρα πολύ δύσκολο να υπολογιστεί το ιδιωτικό κλειδί από το δημόσιο. Με έναν κρυπτογραφικό αλγόριθμο και ένα δημόσιο κλειδί μπορεί οποιοσδήποτε χρήστης να κρυπτογραφήσει ένα μήνυμα. Η αποκρυπτογράφηση μπορεί να επιτευχθεί μόνο από το χρήστη που γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Η χρήση συστήματος δημοσίου κλειδιού, μαθηματικά, προϋποθέτει την ύπαρξη "καταπακτής" με μονής κατεύθυνσης συνάρτηση.

Το δημοφιλέστερο κρυπτοσύστημα δημόσιου κλειδιού είναι το RSA που επινοήθηκε από τους R. Rivest, A. Shamir and L. Adleman το 1987. Από τότε έχει αναλυθεί από πολλούς ειδικούς απ' όλο τον κόσμο. Παρόλ' αυτά δεν έχει αποδειχθεί η ασφάλειά του, αλλά ούτε και το αντίθετο. Το τεράστιο πλεονέκτημα του κρυπτοσυστήματος είναι η απλότητά του στην κατανόηση, καθώς και οι εφαρμογές του. Η ασφάλεια του RSA στηρίζεται στη μη δυνατότητα επίλυσης του προβλήματος παραγοντοποίησης ακέραιων αριθμών σε πολυωνυμικό χρόνο.

Σε αυτό το σημείο καλό θα ήταν να δώσουμε ένα σκαρίφημα του RSA.

Έστω p και q τυχαίοι πρώτοι αριθμοί, με $p \neq q$. Υπολογίζουμε το $n = pq$ και επιλέγουμε τυχαία έναν αριθμό e για τον οποίο ισχύει: $1 < e < (p-1)(q-1)$, έτσι ώστε $\gcd(e, (p-1)(q-1)) = 1$. Επίσης, υπολογίζουμε το μοναδικό ακέραιο d, $1 < d < (p-1)(q-1)$ έτσι ώστε:

$ed \equiv 1 \bmod (p-1)(q-1)$. Το δημόσιο κλειδί είναι το (n,e) και το ιδιωτικό το d. Ο ακέραιος e λέγεται εκθέτης (exponent) κρυπτογράφησης, ο d εκθέτης αποκρυπτογράφησης και το n modulus. Η κρυπτογράφηση ενός μηνύματος m υπολογίζεται από τον τύπο $c = m^e \bmod n$ και το c ονομάζεται κρυπτογράφημα του m. Για να επανακτήσουμε το μήνυμα, πρέπει να υπολογίσουμε το $m = c^d \bmod n$.

Για την προδιαγραφή της RSA συνάρτησης θα χρησιμοποιηθεί ι ίδια "δυαδική μέθοδος", όπου:

$$m^e \bmod n = \begin{cases} (m^{e/2})^2 \bmod n & : \text{ if } e \text{ is even} \\ m(m^{e/2})^2 \bmod n & : \text{ if } e \text{ is odd} \end{cases}$$

A.2.4 Ο Ασφαλής Αλγόριθμος Κατακερματισμού

Στη διαδικασία κρυπτογράφησης στην PSS είναι απαραίτητο να χρησιμοποιήσουμε μια συνάρτηση κατακερματισμού. Η συνάρτηση κατακερματισμού λαμβάνει μια είσοδο μεταβλητού μήκους και την χαρτογραφεί σε ένα μήνυμα σταθερού μεγέθους. Μία κρυπτογραφική συνάρτηση κατακερματισμού πρέπει να ικανοποιεί τρεις ιδιότητες ασφάλειας. Αρχικά, πρέπει να είναι ανθεκτική στις συγκρούσεις. Δηλαδή πρέπει να είναι υπολογιστικά αδύνατο να βρούμε δύο μηνύματα, τα οποία να οδηγούν στην ίδια τιμή κατακερματισμού. Κατά δεύτερον, δεδομένης μίας τιμής κατακερματισμού, πρέπει να είναι ανέφικτο να βρούμε το μήνυμα που αντιστοιχεί σε αυτή την τιμή (first preimage resistance) και τρίτον πρέπει να είναι δύσκολο να δοθεί ένα μήνυμα με το οποίο θα βρούμε κάποιο άλλο μήνυμα, με το οποίο έχουν την ίδια τιμή κατακερματισμού (second preimage resistance).

Σε αυτήν την εργασία χρησιμοποιήθηκε ο Δεύτερος Αλγόριθμος Κατακερματισμού (Secure Hash Algorithm) SHA-1. Υπήρχε διαδεδομένη πίστη ότι ο SHA-1 υπάκουε στις παραπάνω ιδιότητες ασφάλειας, όμως η τεχνική έκθεση των

Wang, Yin καιYu που δημοσιεύτηκε τελευταία υποστηρίζει ότι μπορούν να "σπάσουν" την ιδιότητα της αντίστασης στη σύγκρουση. Αφού η συνάρτηση κατακερματισμού μετατράπηκε, στη δομή του PSS τα συμπαγή εσωτερικά τμήματα του SHA-1 είναι άσχετα με την απόδειξη της ορθότητας του συστήματος. Βέβαια είναι σημαντικό για την αλγεβρική προδιαγραφή, αν θέλει για παράδειγμα να επαληθεύσει το λογισμικό μιας εφαρμογής. Θα ήταν δυνατό με συγκεκριμένες τεχνικές να αλλάξουμε τη συνάρτηση κατακερματισμού στην αλγεβρική απόδειξη, έτσι ώστε να ανταποκρίνεται στην προαναφερόμενη επίθεση. Όμως, η SHA-1 είναι η πιο συνήθης χρησιμοποιημένη συνάρτηση κατακερματισμού, γι' αυτό και διατηρήθηκε αυτούσια.

Η προδιαγραφή της SHA-1 είναι μια απευθείας εφαρμογή του FIPS προτύπου. Το βασικό πρόβλημα εφαρμογής σε ένα αλγεβρικό σύστημα απόδειξης είναι ότι η SHA-1 δεν έχει μια απλή μαθηματική δομή, αλλά ενεργεί σε επίπεδο bit. Επομένως, με κάποιον τρόπο πρέπει τα διανύσματα των bit να ενταχθούν στο σύστημα απόδειξης. Καταρχήν θα χρειαστεί να προσθέσουμε στο σύστημα απόδειξης μια "στήριξη" για το δεκαεξαδικό σύστημα, καθώς και μεθόδους που θα τα μετατρέπουν σε διανύσματα έτσι ώστε να προσφέρουν έναν εύκολο τρόπο να μοντελοποιούμε τις σταθερές που χρησιμοποιούνται στη κρυπτογράφηση της SHA-1. Επίσης, πρέπει να καθοριστούν η λογική συνάρτηση του αποκλεισμού και του μη αποκλεισμού ή οι πράξεις στα διανύσματα, καθώς και η μετάθεση. Επιπλέον, χρειάζεται να βρούμε έναν τρόπο να "σπάμε" ένα διάνυσμα σε επιμέρους συστατικά, ένα επιπλέον modulo 2^{32} και να κατασκευάσουμε ένα αυθαίρετο διάνυσμα με πολλά bit που θα είναι μόνο 0.

Χρησιμοποιώντας αυτές τις επεκτάσεις είναι δυνατό να καθορίσουμε το μήνυμα "γεμίσματος" που χρησιμοποιεί η SHA-1, που προκύπτει από την επέκταση του 0 και την 64-bit μορφή του αρχικού μήκους του μηνύματος, έτσι ώστε το μήνυμα γεμίσματος να είναι πολλαπλάσιο των 512 bits.

Η θεωρία της SHA-1 συνάρτησης κατακερματισμού στην πραγματικότητα είναι η προδιαγραφή της SHA-1. Αυτή η προδιαγραφή διαχωρίζεται σε πολλές παρόμοιες συναρτήσεις της περιγραφής στο FIPS αρχείο.

A.2.5 Η μέθοδος κωδικοποίησης PSS

Η PSS μέθοδος κωδικοποίησης αναπτύχθηκε από τους Bellare και Rogaway. Μια μεταβλητή αυτού του σχήματος περιγράφεται από το αρχείο του PKCS v.1.5 προτύπου. Η προδιαγραφή είναι μια απευθείας εφαρμογή του παραπάνω προτύπου και κάνει χρήση του μήκους που χρησιμοποιεί η συνάρτηση κατακερματισμού. Έχουμε εφαρμόσει την συνάρτηση SHA-1, αφού είναι αυτή που χρησιμοποιείται συχνότερα ως συνάρτηση κατακερματισμού. Βέβαια, είναι δυνατό να αλλάξουμε τη χρησιμοποιημένη συνάρτηση κατακερματισμού χωρίς μεγάλες και σημαντικές αλλαγές στην προδιαγραφή και στην απόδειξη του συστήματος. Βασικά, η PSS χρησιμοποιεί δυο συναρτήσεις. Η πρώτη ενεργοποιεί την κωδικοποίηση αποτυπώματος από το δοθέν μήνυμα. Η άλλη ελέγχει το κωδικοποιημένο αποτύπωμα

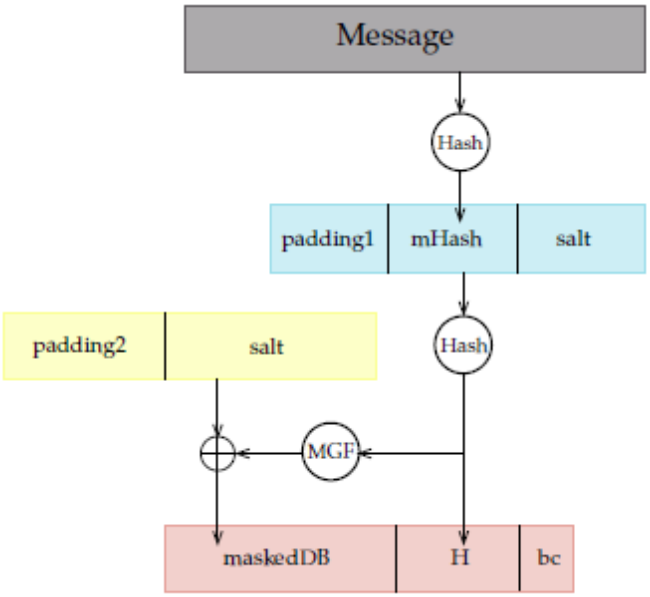
και το μήνυμα, ώστε να καταλήξει στο αν το κωδικοποιημένο αποτύπωμα είναι το κατάλληλο και το σωστό για το συγκεκριμένο μήνυμα.

EMSA-PSS-Encoding Operation (Διεργασία Κωδικοποίησης). Η μέθοδος κωδικοποίησης της PSS περιγράφεται στον αλγόριθμο 1 και στο σχέδιο 1. Η προδιαγραφή είναι μια απευθείας εφαρμογή αυτού του αλγορίθμου. Συγκεκριμένα στην προδιαγραφή salt είναι το άδειο αλφαριθμητικό που έχει το μήκος του 0. Ως συνάρτηση κατακερματισμού χρησιμοποιούμε την sha1, που προδιαγράφεται στο A.2.4.

EMSA-PSS-Decoding Operation (Διεργασία Αποκωδικοποίησης). Αν η υπογραφή είναι έγκυρη για το μήνυμα, τότε μπορεί να διαγραφεί από τον αλγόριθμο 2.

Mask Generation Function (Συνάρτηση Παραγωγής – Δημιουργίας της Μάσκας). Η γεννήτρια συνάρτηση λαμβάνει μια αυθαίρετη αξία x και το επιθυμητό μήκος l. Το αποτέλεσμα είναι ο υπολογισμός μιας αξίας κατακερματισμού για το μήκος l.

Η συνάρτηση είναι ντετερμινιστική, δηλαδή η έξοδος είναι απόλυτα εξαρτημένη από την τιμή της εισόδου. Ακόμα, η έξοδος πρέπει να είναι ψευδο-τυχαία, δηλαδή δοθέντος ενός τμήματος της εξόδου και μη δοθέντος της εισόδου να είναι ανέφικτο να υπολογίσουμε άλλο τμήμα της εξόδου.



Σχήμα 1. Διαδικασία Κρυπτογράφησης

Algorithm 1 EMSA-PSS-Encode

Input: message m to be encoded, an octet string
maximal bit length $emBits$ of the output message, at least $8hLen + 8sLen + 9$

Options: Hash function ($hLen$ is the length in octets of the hash function output)
$sLen$ intended length in octets of the salt

Output: encoded message em, an octet string of length $emLen = \lceil emBits/8 \rceil$

1: if length of m is greater than input limitation for the hash function output "error"
2: $mHash \leftarrow \text{Hash}(m)$
3: if $emLen < hLen + sLen + 2$ output "error"
4: generate a random octet string $salt$ of length $sLen$
5: $m' \leftarrow$ (0x)00 00 00 00 00 00 00 00 $\|$ $mHash$ $\|$ $salt$
6: $H \leftarrow \text{Hash}(m')$
7: generate a octet string PS consisting of $emLen - sLen - hLen - 2$ zero octets, the length may be 0
8: $DB \leftarrow PS \| 0\text{x}01 \| salt$
9: $dbMask \leftarrow \text{MGF}(H, emLen - hLen - 1)$
10: $maskedDB \leftarrow DB \oplus dbMask$
11: set the leftmost $8emLen - emBits$ bits of the leftmost octet in $maskedDB$ to zero
12: $em \leftarrow maskedDB \| H \| 0\text{xBC}$

Η γεννήτρια συνάρτηση μπορεί να κατασκευαστεί από μια συνάρτηση κατακερματισμού, που σε αυτή την περίπτωση είναι η SHA-1. Η ασφάλεια της RSA-PSS στηρίζεται στην τυχαιότητα της γεννήτριας συνάρτησης και αυτή με τη σειρά της στην τυχαιότητα της συνάρτησης κατακερματισμού. Η χρησιμοποίηση της γεννήτριας συνάρτησης περιγράφεται στον αλγόριθμο 3.

Algorithm 2 EMSA-PSS-Decoding

Input: message m to be verified, an octet string
encoded message em, an octet string of length $emLen = \lceil emBits/8 \rceil$
maximal bit length $emBits$ of the output message, at least $8hLen + 8sLen + 9$
Options: Hash function ($hLen$ is the length in octets of the hash function output)
$sLen$ intended length in octets of the salt
Output: "valid" or "invalid"

1: if length of m is greater than the input limitation for the hash function output "invalid"
2: $mHash \leftarrow \text{Hash}(m)$
3: if $emLen < hLen + sLen + 2$ output "invalid"
4: if the rightmost octet of em does not have hexadecimal value 0xBC, output "invalid"
5: $maskedDB \leftarrow$ the leftmost $emLen - hLen - 1$ octets of em and
6: $H \leftarrow$ the next $hLen$ octets
7: if the $8emLen - emBits$ bits of the leftmost octet in $maskedDB$ are not all equal to zero, output "invalid"
8: $dbMask \leftarrow \text{MGF}(H, emLen - hLen - 1)$
9: $DB \leftarrow maskedDB \oplus dbMask$
10: set the leftmost $8emLen - emBits$ bits of the leftmost octet in DB to zero
11: if the $emLen - hLen - sLen - 2$ leftmost octets of DB are not zero or if the octet at position $emLen - hLen - sLen - 1$ does not have hexadecimal value 0x01, output "invalid"
12: $salt \leftarrow$ the last $sLen$ octets of DB
13: $m' \leftarrow$ (0x)00 00 00 00 00 00 00 00 $\|$ $mHash$ $\|$ $salt$
14: $H' \leftarrow \text{Hash}(m')$
15: if $H = H'$ then output "valid", otherwise output "invalid"

Algorithm 3 MGF1

Input: $mgfSeed$: seed from which the mask is generated, an octet string
$maskLen$: intended length in octets of the mask, at most $2^{32}hLen$
Output: $mask$: an octet sting of length $maskLen$

1: if $maskLen > 2^{32}hLen$ then output "error"
2: $T \Longleftarrow \epsilon$
3: **for** $counter = 0$ $to \lceil \frac{maskLen}{hLen} \rceil - 1$ **do**
4: $T \Longleftarrow T \| Hash(mgfSeed \| C)$, where C is the counter converted to an octet string of length 4
5: **end for**
6: $mask \Longleftarrow$ the leading $maskLen$ octets of T

A.2.6 Κατασκευή του RSA-PSS

Η RSA-PSS είναι ένας συνδυασμός των αρχέτυπων που περιγράφονται παραπάνω, συγκεκριμένα χρησιμοποιεί την συνάρτηση RSA με είσοδο τα κωδικοποιημένα δεδομένα της PSS. Η προδιαγραφή πέτυχε να χρησιμοποιεί το δημόσιο κλειδί ώστε να "κωδικοποιεί" την υπογραφή, που αποδίδει ξανά το κωδικοποιημένο αποτύπωμα της PSS. Μετά το αποτύπωμα ελέγχεται ως προς τη συνοχή του με τη χρήση της διαδικασίας κωδικοποίησης που περιγράφεται

παραπάνω. Η ολοκληρωμένη λειτουργία του RSA-PSS σχήματος υπογραφής είναι οι παρακάτω συναρτήσεις:

RSASP1((n, d), m) The RSA signature-primitive computes for the input private key (n, d) and a message m, $0 \leq m < n$ the signature $s = m^d \bmod n$.

RSAVP1((n, e), s) The RSA verification-primitive computes for the input public-key (n, e)

and the signature s the corresponding message $m = s^e \bmod n$.

Hash(m) A hash function (e.g. SHA-1) which computes for a message m with arbitrary length a hash value of fixed length.

Επίσης καθορίζουμε δυο συναρτήσεις, (emsapss_encode m emBits), που κωδικοποιεί το αποτύπωμα του μηνύματος m σε ένα διάνυσμα από bit με μέγιστο μήκος emBits και (emsapss_decode m em emBits), που αποφασίζει για το μήνυμα m, ένα κωδικοποιημένο αποτύπωμα em και το μέγιστο μήκος emBits για το em, αν το em είναι έγκυρη κωδικοποίηση για το m.

Signature-Generation Operation (Διεργασία Παραγωγής – Δημιουργίας της Υπογραφής). Στον αλγόριθμο 4 περιγράφεται η δημιουργία μιας RSA-PSS υπογραφής. Αυτός ο αλγόριθμος είναι η βάση της αλγεβρικής προδιαγραφής.

Algorithm 4 RSA-PSS signature generation

Input: signer's RSA private key (n, d)
message m to be signed, an octet string
Output: signature s, an octet string
1: $modBits \leftarrow$ bit length of the RSA modulus n
2: $em \leftarrow$ emsapss_encode$(m, modBits - 1)$
3: $s \leftarrow$ RSASP1 $((n, d), em)$

Signature-Verification Operation (Διεργασία Επαλήθευσης της Υπογραφής). Η προδιαγραφή της RSA-PSS υπογραφής έγινε σε δύο βήματα. Πρώτον, η συνάρτηση RSAVP1 εφαρμόζεται στην υπογραφή ώστε να πάρουμε το

κωδικοποιημένο μήνυμα. Μετά η λειτουργία emsapss_decode εφαρμόζεται στο μήνυμα και το κωδικοποιημένο μήνυμα καθορίζει αν είναι συνεπής ή όχι. Αυτό φαίνεται καλύτερα στον αλγόριθμο 5.

Α.3 Απόδειξη Ορθότητας

Είναι αρκετά δύσκολο και πολύπλοκο να δείξουμε κατευθείαν την ορθότητα ολόκληρης της μεθόδου κωδικοποίησης RSA-PSS. Βέβαια, υπάρχει η δυνατότητα να χωρίσουμε σε μικρότερα κομμάτια την εργασία, πράγμα το οποίο διευκολύνει την προδιαγραφή. Ο σκοπός είναι αρχικά να δοθεί μια απόδειξη της "καθαρής" συνάρτησης RSA, με το όνομα $(m^e)^d$ mod n = m. Δεύτερον να αποδειχθεί ότι: (emsapss_decode m (emsapss_encode m emBits) emBits) = Αληθές. Το τελευταίο βήμα για την ολοκλήρωση της απόδειξης είναι να συνδυαστούν τα μεμονωμένα κομμάτια. Αν και φαίνεται απλό εκ πρώτης όψεως, υπάρχουν διάφορα εμπόδια τα οποία θα ξεκαθαρίσουμε παρακάτω.

Algorithm 5 RSA-PSS signature verification

Input: signer's RSA private key (n, d)
message m whose signature is to be verified, an octet string
signature s to be verified, an octet string

Output: valid or invalid signature

1: $modBits \longleftarrow$ bit length of the RSA modulus n
2: $em \longleftarrow$ RSAVP1 $((n, e), s)$
3: $Result \longleftarrow$ emsapss_decode$(m, em, modBits - 1)$
4: if $Result$ = "valid" then output "valid signature" otherwise "invalid signature"

Α.3.1 Ορθότητα του RSA

Η απόδειξη της ορθότητας της συνάρτησης του RSA κάνει χρήση του μικρού θεωρήματος του Fermat. Για να οριοθετηθεί η απόδειξη, σε αυτό το σημείο

παραλείπεται η αλγεβρική προδιαγραφή του θεωρήματος και αναφέρεται απλά το θεώρημα που χρησιμοποιείται στην μετέπειτα απόδειξη.

lemma *fermat*: $[\![p \in prime;\ m\ mod\ p \neq 0]\!] \Longrightarrow m\hat{}(p-(1::nat))\ mod\ p = 1$

Η απόδειξη της ορθότητας του RSA σύμφωνα με τη γλώσσα Isabelle είναι:

lemma *cryptinverts*:
$[\![p \in prime;\ q \in prime;\ p \neq q;\ n = p*q;\ m < n;$
$e*d\ mod\ ((pred\ p)*(pred\ q)) = 1]\!] \Longrightarrow$
$rsa\text{-}crypt\ (rsa\text{-}crypt\ (m,e,n),\ d\ ,\ n) = m$

που βασικά αναφέρει ότι εάν κάποιος κάνει χρήση του ιδιωτικού κλειδιού, ώστε να κωδικοποιήσει (i.e. sign) ένα μήνυμα m και μετά να χρησιμοποιήσει το δημόσιο κλειδί για να κωδικοποιήσει (i.e. verify) το αποτέλεσμα από την αρχική κωδικοποίηση, τότε θα λάβει πάλι το m.

Από τη στιγμή που η ορθότητα του RSA στηρίζεται στη θεωρία αριθμών, είναι εύκολο να προσαρμοστεί στο πεδίο των αλγεβρικών αποδείξεων. Τα βασικά εργαλεία που χρειάζονται είναι λήμματα από τα αριθμητικά modular και κάποιες ιδιότητες των πρώτων αριθμών. Έτσι, το μικρό θεώρημα του Fermat κατοχυρώνεται με τη χρήση κάποιων θεωρημάτων περί αντιμετάθεσης φυσικών αριθμών.

A.3.2 Μήκος του SHA-1

Σε αυτό το σημείο θα παρουσιαστεί η απόδειξη για το μήκος της συνάρτησης κατακερματισμού SHA-1, που είναι απαραίτητη για την απόδειξη της ορθότητας του σχήματος υπογραφής RSA-PSS. Καταρχάς θα ήταν δυνατό να προσδιορίσουμε μια αφηρημένη συνάρτηση κατακερματισμού και να δοθεί μια απόδειξη ορθότητας για κάθε τέτοια συνάρτηση, η οποία θα έχει ένα συγκεκριμένο ελάχιστο μήκος. Όμως, αφού αποφασίστηκε να δοθεί προδιαγραφή που θα χρησιμοποιηθεί για την επαλήθευση συγκεκριμένης εφαρμογής, θα καταγραφεί η προδιαγραφή της SHA-1 συνάρτησης κατακερματισμού. Γι' αυτό το λόγο, πρέπει να δοθεί η απόδειξη για το μήκος της συγκεκριμένης συνάρτησης. Ολόκληρη η απόδειξη είναι σχετικά εύκολη, επειδή το μήκος της SHA-1 είναι ένας συνδυασμός πέντε μπλοκ των 32-bit, όπως φαίνεται από τον ορισμό της SHA-1.

Α.3.3 Ορθότητα της Μεθόδου Κωδικοποίησης του PSS

Σε αυτό το κομμάτι θα δώσουμε την αλγεβρική απόδειξη ότι για ένα μήνυμα m και το κωδικοποιημένο μήνυμα em του m, η συνάρτηση emsapss_decode επιστρέφει αποτέλεσμα αληθές.

Η απόδειξη κυρίως επαληθεύεται κοιτάζοντας το κωδικοποιημένο μήνυμα, το οποίο δείχνει ότι το μήνυμα έχει συγκεκριμένη μορφή. Το πρώτο βήμα είναι να δείξουμε ότι τα λιγότερα οχτώ σημαντικά bits του κωδικοποιημένου μηνύματος είναι 0xBC. Μετά πρέπει να δείξουμε ότι τα "πιο αριστερά" bits είναι ίσα με το μηδέν. Αυτή είναι μια σημαντική ιδιότητα για ολόκληρη την απόδειξη, επειδή διασφαλίζει ότι το κωδικοποιημένο μήνυμα, όταν θεωρηθεί σαν φυσικός αριθμός, είναι μικρότερο από το RSA modulus, που μας επιτρέπει να εφαρμόσουμε την απόδειξη της ορθότητας του RSA.

Ακόμα ένα σημαντικό εργαλείο είναι να δείξουμε ότι η εφαρμογή της xor δυο φορές με την ίδια μάσκα αφήνει ένα διάνυσμα από bit αναλλοίωτο. Οπότε είναι δυνατό να αναιρέσουμε την επίδραση της διεργασίας της μάσκας. Αυτό αποφέρει το αλφαριθμητικό padding2, που μπορεί να ελεγχθεί για την ορθότητα του. Στη συνέχεια μπορεί να χρησιμοποιηθεί μαζί με το αλφαριθμητικό padding1 για να εξακριβωθεί το πραγματικό αποτύπωμα.

Το υπόλοιπο κομμάτι της απόδειξης μπορεί να δειχθεί από ευθέα υποκατάστατα και την εφαρμογή των θεωρημάτων που αναφέρθηκαν παραπάνω. Τα βασικά προβλήματα σε αυτό το σημείο υπόκεινται σε τεχνικά θέματα. Εξαιτίας της πολυπλοκότητας των εκφράσεων γίνεται δύσκολη η στενή παρακολούθηση της απόδειξης. Εδώ πρέπει να αναφερθεί ότι οι γλώσσες αλγεβρικών προδιαγραφών που χρησιμοποιούνται στις αποδείξεις της ορθότητας των κρυπτογραφικών αλγορίθμων πρέπει με κάποιο τρόπο να απλοποιήσουν τις πολύπλοκες εκφράσεις.

Α.3.4 Συνδυασμός των απλών αποδείξεων

Εδώ θα δειχθεί ότι η RSA-PSS υπογραφή s για ένα μήνυμα m μπορεί να επαληθευθεί από την RSA-PSS προδιαγραφή από το τμήμα Α.2.6. Θα αποδειχθεί το παρακάτω:

lemma *rsa-pss-verify*:
$[\![p \in prime;\ q \in prime;\ p \neq q;\ n = p*q;$
$e*d\ mod\ ((pred\ p)*(pred\ q)) = 1;\ rsapss\text{-}sign\ m\ e\ n \neq [];$
$s = rsapss\text{-}sign\ m\ e\ n]\!]$
$\Longrightarrow rsapss\text{-}verify\ m\ s\ d\ n = True.$

Στη συνέχεια θα χρησιμοποιούμε το | • | για να δηλώνουμε το μήκος του διανύσματος των bit που αντιπροσωπεύει τον αριθμό •.

Για να εφαρμόσουμε την ορθότητα του λήμματος για το RSA, που μας δίνει το em στο βήμα της επαλήθευσης, θα πρέπει να δειχθεί ότι em < n. Αυτό πράγματι είναι το βασικό εμπόδιο για τον συνδυασμό των επιμέρους αποδείξεων που περιγράφονται παραπάνω.

Για να δειχθεί ότι em < n, θα γίνει χρήση των ιδιοτήτων - προϋποθέσεων των πρώτων p, q, όπου $p \neq q$ και $n = p \bullet q$. Η πρόθεση είναι να δειχθεί ότι δεν παίζει ρόλο αν το em ξεκινά με 0 ή 1 bit. Στην πρώτη περίπτωση είναι εύκολο, αφού θα δειχθεί ότι προηγούμενα μηδενικά δεν αλλάζουν την τιμή ενός διανύσματος bit. Με άλλα λόγια, αν σημειώσουμε με em* την τιμή του em με τα αρχικά μηδενικά αφαιρεμένα, μπορεί να δειχθεί ότι $em^* = em$ και $|em^*| < |n|$. Αφού $|em^*| < |n| \rightarrow em^* < n$, άρα εδείχθη η πρώτη περίπτωση (Σημείωση: το n πάντα ξεκινά με πρώτο bit το 1 λόγω της προδιαγραφής)

Στη δεύτερη περίπτωση μπορεί να δειχθεί ότι $|em| = |p \bullet q| - 1$ και $0 < p \bullet q - 1$. Επιπλέον, έχουμε ότι $0 < p \bullet q - 1 \rightarrow 2^{|p \bullet q| - 1} \leq p \bullet q$. Τώρα το μόνο που μένει να δειχθεί είναι ότι $2^{|p \bullet q| - 1} \neq p \bullet q$. Αυτό ισχύει, αφού η μοναδική περίπτωση που μπορεί ο πολλαπλασιασμός δύο πρώτων να δώσει δύναμη του 2 είναι $2 \bullet 2$, πράγμα το οποίο απορρίπτεται αφού έχει ορισθεί η συνθήκη $p \neq q$.

Ακόμα ένα πρόβλημα σχετικό με την πολυπλοκότητα των τρεχουσών εκφράσεων είναι ότι σ' αυτό το βήμα πρέπει να κινούμαστε ανάμεσα σε φυσικούς αριθμούς και την περιγραφή των αριθμών του διανύσματος, τα οποία πάντα εισάγουν ένα επίπεδο αστάθειας. Αυτό το θέμα είναι τυπικό στην αλγεβρική προδιαγραφή των κρυπτογραφικών αλγόριθμων, αφού συνδυάζονται διαδικασίες από διαφορετικά πεδία, όπως GF(2) και Z_n με στόχο την προστασία από επιθέσεις. Μια δυνατή λύση είναι να καταγράψουμε τα θεωρήματα, που επιτρέπουν την ακύρωση στις μετατρεπόμενες συναρτήσεις. Βέβαια, θα πρέπει να μας ενδιαφέρει η σειρά των εφαρμογών των συναρτήσεων, γιατί για παράδειγμα η μετατροπή από τα διανύσματα των bit στους φυσικούς αριθμούς και πίσω διώχνει το αρχικό μηδέν από τα διανύσματα.

Α.4 Συμπεράσματα

Σ' αυτό το παράρτημα παρουσιάστηκε η αλγεβρική προδιαγραφή του πιθανοτικού σχήματος υπογραφής του RSA. Επιπλέον, επαληθεύθηκε η συναρτησιακή ορθότητα της RSA-PSS με τη χρήση αλγεβρικών μεθόδων. Ακόμα, η έρευνα αυτή σε αυτόν τον τομέα είναι πολύ σημαντική, λόγω της έλλειψης εργαλείων που μπορούν να χρησιμοποιηθούν για την επαλήθευση κρυπτογραφικών αλγορίθμων. Ο στόχος ήταν να τυποποιηθεί η απόδειξη της ασφάλειας του RSA-PSS. Προς αυτήν την κατεύθυνση πρέπει να γίνουν πολλά ακόμη. Ένα πολύ σημαντικό σημείο είναι η τυπική περιγραφή ενός μοντέλου τυχαίου μαντείου. Επιπλέον, δεν υπάρχει αρκετή θεωρία στο πως να αναλυθεί ένα πρόγραμμα με σεβασμό προς τη χωρική και χρονική πολυπλοκότητα, που θα επιτρέψει το "αντίπαλο"(adversaries) μοντέλο για δημιουργία ενός θεωρητικού περιβάλλοντος.

Με την παρουσίαση της προδιαγραφής του RSA-PSS γίνεται δυνατό να επαληθευθεί η ορθότητα της εφαρμογής του μοντέλου αυτού (RSA-PSS). Μέχρι στιγμής αυτό μπορούσε να γίνει μόνο με τη χρήση διανυσμάτων ελέγχου, το οποίο είναι μια ένδειξη ορθότητας, όμως δεν αποτελεί απόδειξη. Αν και η δουλειά που έγινε είναι μόλις μόνο ένα βήμα προς την αλγεβρική επεξεργασία του RSA-PSS, αυτές οι αποδείξεις θα δώσουν το θάρρος για περαιτέρω έρευνα σε αυτόν τον τομέα, αφού είναι εφικτό να προδιαγράφουν πολύπλοκα κρυπτογραφικά πρωτόκολλα, όπως το RSA-PSS.

Πριν κλείσουμε αυτήν την έρευνα, θα πρέπει να αναφερθεί ότι υπάρχει η πεποίθηση πως οι αλγεβρικές μέθοδοι είναι ένα χρήσιμο εργαλείο για την κατανόηση των αποδείξεων. Χρησιμοποιώντας περιβάλλοντα θεωρητικών μπορούμε να αποφύγουμε κινδύνους που μπορεί να εμφανιστούν κατά την απόδειξη, και συνήθως τους παραβλέπουμε, όταν γράφουμε αποδείξεις με χαρτί και μολύβι.

Τέλος, παραθέτουμε ένα πολύ μικρό κομμάτι της συνολικής απόδειξης. Συγκεκριμένα το κομμάτι της προδιαγραφής του RSA , καθώς και της αποδείξεως της ορθότητάς του.

Formal Specification of RSA

```
theory Crypt = Mod:

constdefs
  even :: nat ⇒ bool
  even n == 2 dvd n

consts
  rsa-crypt :: nat × nat × nat => nat

recdef rsa-crypt measure(λ(M,e,n).e)
  rsa-crypt (M,0,n) = 1
  rsa-crypt (M,Suc e,n) = (if even (Suc e) then
  ((rsa-crypt (M, (Suc e) div 2,n))^2 mod n) else
  (M * ((rsa-crypt (M, Suc e div 2,n))^2 mod n)) mod n)

lemma div-2-times-2:
  (if (even m) then (m div 2 * 2 = m) else (m div 2 * 2 = m - 1))


 by (simp add: even-def dvd-eq-mod-eq-0 mult-commute mult-div-cancel)

theorem cryptcorrect [rule-format]:
 ((n ≠ 0) & (n ≠ 1)) ⟶ (rsa-crypt(M,e,n) = M^e mod n)
 apply (induct-tac M e n rule: rsa-crypt.induct)
 by (auto simp add: power-mult [THEN sym] div-2-times-2 remainderexp
   timesmod1)

end
```

Correctness Proof for RSA

theory *Cryptinverts* = *Fermat* + *Crypt*:

lemma *cryptinverts-hilf1*:
⟦*p* ∈ *prime*⟧ ⟹ (*m* ∗ *m* ^(*k* ∗ *pred p*)) *mod p* = *m mod p*
apply (*case-tac m mod p* = *0*)
apply (*simp add*: *mod-mult1-eq'*)
apply (*simp only*: *mult-commute* [*of k pred p*] *power-mult mod-mult1-eq*
[*of m* (*m*^*pred p*) ^*k p*] *remainderexp*
[*of m*^*pred p p k*, *THEN sym*])
apply (*insert fermat* [*of p m*])
apply (*simp add*: *predd*)
apply (*subst sucis*)
apply (*subst oneexp*)
apply (*subst onemodprime*)
by (*auto*)

lemma *cryptinverts-hilf2*:
⟦*p* ∈ *prime*⟧ ⟹ *m*∗(*m*^(*k* ∗ (*pred p*) ∗ (*pred q*))) *mod p* = *m mod p*
apply (*simp add*: *mult-commute* [*of k* ∗ *pred p pred q*] *mult-assoc*
[*THEN sym*])
apply (*rule cryptinverts-hilf1* [*of p m* (*pred q*) ∗ *k*])
by (*simp*)

lemma *cryptinverts-hilf3*:
⟦*q* ∈ *prime*⟧ ⟹ *m*∗(*m*^(*k* ∗ (*pred p*) ∗ (*pred q*))) *mod q* = *m mod q*
apply (*simp only*: *mult-assoc*)
apply (*simp add*: *mult-commute* [*of pred p pred q*])
apply (*simp only*: *mult-assoc* [*THEN sym*])
apply (*rule cryptinverts-hilf2*)
by (*simp*)

lemma *cryptinverts-hilf4*: ⟦*p* ∈ *prime*; *q* ∈ *prime*; *p* ≠ *q*; *m* < *p*∗*q*;
x mod ((*pred p*)∗(*pred q*)) = *1*⟧ ⟹ *m*^*x mod* (*p*∗*q*) = *m*
apply (*frule cryptinverts-hilf2* [*of p m k q*])
apply (*frule cryptinverts-hilf3* [*of q m k p*])
apply (*frule mod-eqD*)
apply (*elim exE*)
apply (*rule specializedtoprimes1a*)
by (*simp add*: *cryptinverts-hilf2 cryptinverts-hilf3 mult-assoc*
[*THEN sym*])+

lemma *primmultgreater*:
[$p \in prime$; $q \in prime$; $p \neq 2$; $q \neq 2$] $\Longrightarrow$ $2 < p*q$
apply (*simp add:prime-def*)
apply (*insert mult-le-mono* [*of 2 p 2 q*])
by (*auto*)

lemma *primmultgreater2*: [$p \in prime$; $q \in prime$; $p \neq q$] $\Longrightarrow$ $2 < p*q$
apply (*case-tac p=2*)
apply (*simp*)+
apply (*simp add*: *prime-def*)
apply (*case-tac q=2*)
apply (*simp add*: *prime-def*)
apply (*erule primmultgreater*)
by (*auto*)

lemma *cryptinverts*: [$p \in prime$; $q \in prime$; $p \neq q$; $n = p*q$; $m < n$;
$e*d$ *mod* ((*pred p*)*(*pred q*)) = *1*] $\Longrightarrow$
rsa-crypt (*rsa-crypt* (*m*,*e*,*n*), *d* , *n*) = *m*
apply (*insert cryptinverts-hilf4* [*of p q m e*d*])
apply (*insert cryptcorrect* [*of p*q rsa-crypt* (*m*, *e*, *p* * *q*) *d*])
apply (*insert cryptcorrect* [*of p*q m e*])
apply (*insert primmultgreater2* [*of p q*])
apply (*auto simp add*: *prime-def*)
by (*auto simp add*: *remainderexp* [*of m^e p*q d*] *power-mult*
[*THEN sym*])

end

ΠΑΡΑΡΤΗΜΑ Β

ΤΟ RSA ΣΤΟ ... ΠΑΡΑΣΚΗΝΙΟ

"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 δε 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 μια 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, επίσης 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 μη 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 έρευνάς τους, καθώς τους οδηγούσε σε πιο γόνιμα εδάφη. Τελικά, οι προσπάθειές 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, μη 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 δε θα ήταν δυνατή χωρίς αυτούς. Ο Ρίβεστ τελείωσε το άρθρο αναγράφοντας 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 δε βρήκε κανένα λάθος. Η μόνη του κριτική αφορούσε στον 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 στο 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 δε θα μπορούσε να πέσει περισσότερο έξω. Το σύστημα, που ονομάστηκε RSA (Rivest, Shamir, Adleman) και όχι ARS, αναδείχθηκε στο πιο σημαντικό κρυπτόγραμμα στη σύγχρονη κρυπτογραφία.

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

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

Ωστόσο, η Αλίκη χρειάζεται να αποκρυπτογραφεί τα μηνύματα που της στέλνουν. Θα πρέπει, επομένως, να κατέχει 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. 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. Δε θα περιγράψουμε λεπτομερώς τη μονοσήμαντη

συνάρτηση του Ρίβεστ, αλλά θα εξηγήσουμε 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 τη μονάδα. Για παράδειγμα, το 7 είναι πρώτος αριθμός, επειδή κανείς άλλος αριθμός εκτός από το 1 και το 7 δε 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 N = 17.159 x 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 δε 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 τη 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 τη 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 γινόμενό τους δίνει το Ν. Αν και η Αλίκη έχει πει σε όλον τον κόσμο ότι η τιμή της για 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 λαβαίνει.

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 από την Αλίκη, την πληροφορία που χρειάζεται για την αποκρυπτογράφηση των μηνυμάτων.

Υπάρχει ωστόσο ένα ερώτημα που θα πρέπει να απαντηθεί αμέσως. Αν όλοι γνωρίζουν το N, το δημόσιο κλειδί, τότε δε μπορούν να συμπεράνουν τα p και q, το ιδιωτικό κλειδί και να διαβάσουν τα μηνύματα που απευθύνονται στην Αλίκη; Στο κάτω κάτω, το N δημιουργήθηκε από τα p και q. Στην πραγματικότητα αποδεικνύεται ότι αν το N είναι αρκετά μεγάλο, είναι ουσιαστικά αδύνατο 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 N επιλέγοντας τα p και q και στη συνέχεια πολλαπλασιάζοντάς 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 παράγουμε τον αριθμό 1.709.023, όμως θα μας πάρει σχεδόν ένα απόγευμα για να βρούμε, με μια αριθμομηχανή, τους πρώτους παράγοντες.

Το σύστημα της ασύμμετρης κρυπτογραφίας, γνωστό ως RSA, λέγεται ότι είναι μια μορφή κρυπτογραφίας δημοσίου 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_B και q_B, και τους πολλαπλασίασε για να προκύψει το N_B. Τους p_B και q_B τους κράτησε μυστικούς, γιατί αυτοί αποτελούν το ιδιωτικό του κλειδί της αποκρυπτογράφησης, ενώ δημοσιοποίησε το N_B, που ισούται με 408.508.091. Έτσι η Αλίκη εισάγει το δημόσιο κλειδί του Μπομπ, το N_B, 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_B και q_B, 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_B και q_B. Ο Μπομπ έχει κρατήσει μυστικές τις αριθμητικές αξίες των p_B και q_B, αλλά η Εύα γνωρίζει, όπως όλος ο κόσμος, ότι το N_B είναι 408.508.091. Επιχειρεί λοιπόν να συναγάγει τις τιμές των p_B και q_B 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 N_B. 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_B χωρίς να αφήνουν υπόλοιπο. Για παράδειγμα, το 3 είναι πρώτος αριθμός, αλλά δεν είναι παράγοντας του N_B, επειδή δεν το διαιρεί τέλεια. Έτσι η Εύα προχωρεί στον επόμενο πρώτο αριθμό, το 5. Ούτε και το 5 είναι παράγοντας, οπότε η Εύα φτάνει στο δισχιλιοστό πρώτο αριθμό, το 18.313, που όντως είναι παράγοντας του 408.508.091. Έχοντας βρει τον έναν 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_B και q_B. Με άλλα λόγια, η Εύα θα μπορούσε να ανακαλύψει το ιδιωτικό κλειδί του Μπομπ σε λιγότερο από μια 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 N μια τιμή της τάξης περίπου του 10^{130} (10^{65} x 10^{65}). Ένας υπολογιστής θα μπορούσε να πολλαπλασιάσει τους δύο πρώτους αριθμούς και να παραγάγει το N μέσα σε ένα δευτερόλεπτο, όμως αν η Εύα ήθελε να αναστρέψει τη διαδικασία και να βρει τις τιμές των p_B και q_B, 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 100 MHz, με 8 MB 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.

Η μόνη επιφύλαξη για την ασφάλεια της κρυπτογραφίας δημοσίου κλειδιού τύπου RSA είναι ότι κάποια στιγμή στο μέλλον κάποιος μπορεί να βρει ένα 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 δε χρειαζόταν 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 – όσο περισσότεροι, τόσο καλύτερα, εφόσον το δημόσιο κλειδί βοηθά μόνο την κρυπτογράφηση, 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 χρειαζόταν εκατομμύρια χρόνια για να σπάσει", για τη στήλη του Μαθηματικά παιχνίδια στο περιοδικό Scientific American. Αφού εξηγούσε πώς λειτουργεί η κρυπτογραφία δημοσίου 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=
114.381.625.757.888.867.669.235.779.976.146.612.010.218.296.721.242.362.562.561.842.935.706.935.245.733.897.830.597.123.563.958.705.058.989.075.147.599.290.026.879.543.541.

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 δε 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 δέχθηκαν. Ωστόσο, δεν απάντησαν αμέσως, επειδή ανησυχούσαν μήπως η δημόσια διανομή της ιδέας τους θέσει σε κίνδυνο τις πιθανότητές τους να πάρουν αριθμό ευρεσιτεχνίας. Όταν τελικά λύθηκαν τα ζητήματα της ευρεσιτεχνίας, οι τρεις τους οργάνωσαν ένα πάρτι για να το γιορτάσουν. Εκεί, καθηγητές και φοιτητές κατανάλωσαν πίτσες και μπίρα, ενώ ταυτόχρονα γέμιζαν φακέλους 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 10^{129}. Σήμερα οι χρήστες του RSA επιλέγουν πολύ μεγαλύτερες τιμές για να διασφαλίζουν σημαντικές πληροφορίες. Είναι πλέον συνηθισμένη υπόθεση να κρυπτογραφούνται μηνύματα με τόσο μεγάλη τιμή του N, ώστε όλοι οι υπολογιστές του πλανήτη να χρειάζονται περισσότερο χρόνο από την ηλικία του σύμπαντος για να σπάσουν το κρυπτόγραμμα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Κώδικες και Μυστικά, Simon Singh, Εκδόσεις Τραυλός, 2003

Κρυπτογραφία, Κώδικες και Κρυπτογράμματα, Stephen Pincock, Εκδόσεις Τραυλός, 2010

Κρυπτογραφία, Χ. Κουκουβίνος, Α. Παπαϊωάννου, Εκδόσεις ΕΜΠ, 2007

Σημειώσεις στη Θεωρία Αριθμών και την Κρυπτογραφία, Ε. Ζάχος, Εκδόσεις ΕΜΠ, 2007

Cryptography, Theory and Practice, Douglas R. Stinson, Chapman & Hall/Crc, Third Edition

Guide to Elliptic Curve Cryptography, Darrel Hankerson, Alfred J. Menezes, Scott Vanstone, Springer Publications

Elliptic Curve Cryptography, Number Theory and Cryptography, Lawrence C. Washington, CRC Press

Θεωρία Αριθμών, Δημήτριος Μ. Πουλάκης, Εκδόσεις Ζήτη, 2001

Σύγχρονη Κρυπτογραφία, Παναγιώτης Ε. Νάστου, Παύλος Γ. Σπυράκης, Γιάννης Κ. Σταματίου, Εκδόσεις Ελληνικά Γράμματα, 2003

Θεωρία Αριθμών, Π.Γ. Τσαγκάρης, Εκδόσεις Συμμετρία, 2005

Μαθήματα Αριθμοθεωρίας, Adolph Hurwitz, Νικ. Κριτικός, Επιστημονικές και Τεχνικές Εκδόσεις Γ. Α. Πνευματικού, 1981

Μεταπτυχιακή εργασία: "Ελλειπτικές Καμπύλες και Πιστοποίηση Πρώτου", Ψαρίσιος Λαμπρόπουλος, Οκτώβριος 2008

Μεταπτυχιακή εργασία: "Κρυπτοσυστήματα Ελλειπτικών Καμπύλων Τύπου RSA", Ντούρου Βαρβάρα, Νοέμβριος 2007

Διδακτορική Διατριβή: "Θεωρία και εφαρμογές κρυπτογραφικών συστημάτων δημοσίου κλειδιού βασισμένων σε ελλειπτικές καμπύλες", Ελισάβετ Κωνσταντίνου, Ιούνιος 2005

Μεταπτυχιακή εργασία: "Κβαντική Κρυπτογραφία", Καραγεώργης Βασίλειος, 2006-2007

Quantum Cryptography, A study into the present technologies and future applications, Bill Grind lay, 2003

Μια επισκόπηση της Κρυπτογραφίας, Gary C. Kessler, Σεπτέμβριος 2010

www.google.gr

www.wikipedia.gr

Διαχείριση Κλειδιού, Πρωτόκολλα Εγκαθίδρυσης Κλειδιού, Μάγκος, 2008

Ασφάλεια Διαδικτυακής Διακίνησης Πληροφοριών, ΤΕΙ Πειραία, 1998

Μέθοδος και κρυπτοσύστημα των ελλειπτικών καμπυλών, Ν. Λυγερός

www.lib.ntua.gr

STANDARDS FOR EFFICIENT CRYPTOGRAPHY, SEC 1: Elliptic Curve Cryptography, Certicom Research

A Survey of Public-Key Cryptosystems, Neal Koblitz

Menezes, Oorschot, Vanstone, Scott: Handbook of Applied Cryptography

Introduction to Elliptic Curve Cryptography, Elisabeth Oswald

Διπλωματική εργασία: «e – αξιολόγηση: Εφαρμογές της Κρυπτογραφίας στην Αξιολόγηση μέσω Τεχνολογιών Πληροφορικής και Επικοινωνιών», Γαλάνης Βασίλειος

8η διάλεξη, Κρυπτογραφία: Αρχές και πρωτόκολλα, Καθηγητής Α. Καγιάς, Φθινόπωρο 2008

Andreas V. Meier, Joint Advanced Students Seminar 2005, The ElGamal Cryptosystem

Taher ElGamal, A Public key cryptosystem and a signature scheme based on discrete logarithms

IEEE P1363/D13, Standard Specifications for Public – Key Cryptography, ballot draft, 1999

D. Johnson and A. Menezes, The Elliptic Curve Digital Signature Algorithm, Technical report CORR 99-06, Department of Combinatorics and Optimization, University of Waterloo, 1999

E. Konstantinou, Y. Stamatiou, C. Zaroliagis, On the Construction of Prime Order Elliptic Curves, in Progress in Cryptology – Lecture Notes in Cimputer Science, 2003

E. Konstantinou, Y. Stamatiou, C. Zaroliagis, On the Use of Weber Polynomials in Elliptic Curve Cryptography, in Public Key Infrastructure, 2004

V. Muller and S. Paulus, On the Generation of Cryptographically Strong Elliptic Curves, 1997