ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΛΟΓΙΚΗΣ ΚΑΙ
ΑΛΓΟΡΙΘΜΩΝ

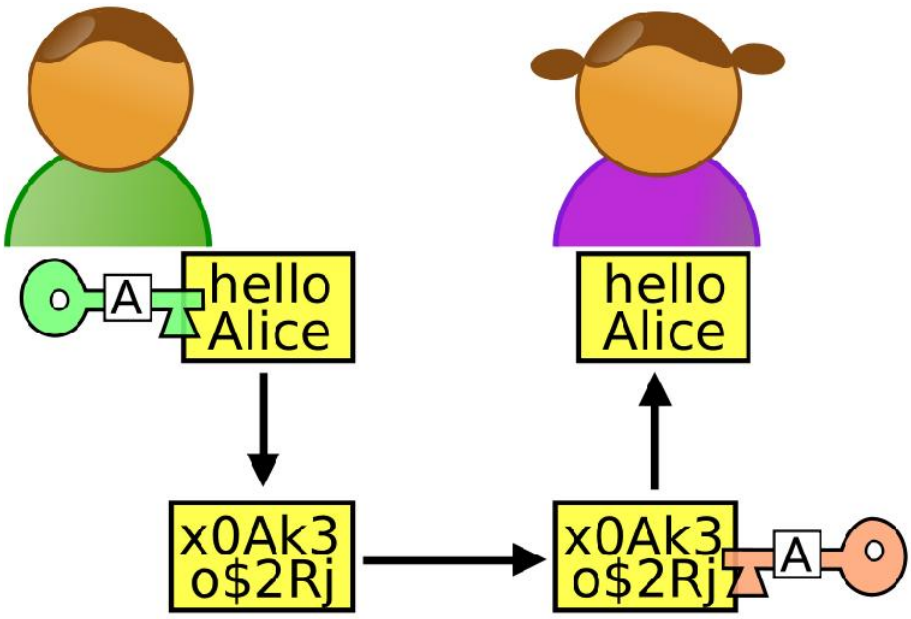
Διπλωματική Εργασία
Μεταπτυχιακού Διπλώματος Ειδίκευσης

«ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RSA»

ΠΕΤΣΗ ΑΙΚΑΤΕΡΙΝΗ

Επιβλέπων Καθηγητής: ΡΑΠΤΗΣ ΕΥΑΓΓΕΛΟΣ

ΑΘΗΝΑ
ΟΚΤΩΒΡΗΣ 2008


A
hello
Alice
hello
Alice
x0Ak3
o$2Rj
x0Ak3
o$2Rj
A

Στην οικογένειά μου

Περιεχόμενα

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον κ. Ράπτη ο οποίος καθ' όλη τη διάρκεια των σπουδών μου, τόσο στο προπτυχιακό όσο και στο μεταπτυχιακό επίπεδο, πίστεψε σε ′μένα και μαζί με τον κ. Μοσχοβάκη και τον κ. Δημητρακόπουλο μου έδωσαν την ευκαιρία να φοιτήσω στο ΜΠΛΑ. Επιπλέον, θα ήθελα να ευχαριστήσω τους καθηγητές μου για όσα αποκόμισα από την παρακολούθηση των μαθημάτων τους. Τέλος, ευχαριστώ τους φίλους και συμφοιτητές μου Τσολακίδη Στράτο και Κούτα Κατερίνα για τις πολύτιμες συμβουλές τους κατά την διάρκεια εκπόνησης της παρούσας εργασίας.

Περίληψη

Η παρούσα εργασία ασχολείται με το κρυπτοσύστημα δημοσίου κλειδιού RSA. Αρχικά, γίνεται μια σύντομη αναφορά στην ιστορία της κρυπτογραφίας καθώς και σε μερικά από τα πιο γνωστά κρυπτοσυστήματα δημοσίου κλειδιού. Έπειτα, αναλύεται ο RSA αλγόριθμος και η πολυπλοκότητά του. Στη συνέχεια αποδεικνύεται το ότι ο υπολογισμός του ιδιωτικού κλειδιού από το δημόσιο είναι ισοδύναμος με την παραγοντοποίηση μεγάλων σύνθετων ακεραίων με δύο πρώτους παράγοντες. Ακόμη, αναφέρονται μερικές από τις πιο γνωστές επιθέσεις στο κρυπτοσύστημα και τέλος εξηγείται ο τρόπος με τον οποίο δημιουργείται μια ψηφιακή υπογραφή με χρήση του συγκεκριμένου κρυπτοσυστήματος.

Κεφάλαιο 1

ΕΙΣΑΓΩΓΗ

1.1 Η ΚΡΥΠΤΟΓΡΑΦΙΑ

Ο όρος **κρυπτογραφία (cryptography)** αναφέρεται στην μελέτη των μεθόδων αποστολής μηνυμάτων με τρόπο ώστε μόνο ο παραλήπτης να μπορεί να διαβάσει το μήνυμα. Αντιθέτως, ο όρος **κρυπτανάλυση (cryptanalysis)** αναφέρεται στις μαθηματικές τεχνικές που χρησιμοποιούνται για το "σπάσιμο" των κρυπτογραφημένων μηνυμάτων. Το 1645 ο James Howell εισήγαγε τον όρο **κρυπτολογία (cryptology)** για να εκφράσει την επιστήμη που ασχολείται με την κρυπτογραφία και την κρυπτανάλυση. Ο όρος αυτός δεν είναι πολύ διαδεδομένος στις μέρες μας, αντί για αυτόν χρησιμοποιείται απλώς η λέξη κρυπτογραφία.

1.2 ΜΙΑ ΣΥΝΤΟΜΗ ΑΝΑΣΚΟΠΗΣΗ ΤΗΣ ΙΣΤΟΡΙΑΣ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Σύμφωνα με τον David Kahn[1] μία μικρή σφηνοειδής επιγραφή, που ανακαλύφθηκε στις όχθες του ποταμού Τίγρη και χρονολογείται από το 1500 π.Χ. θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο. Στην Εβραϊκή λογοτεχνία συναντάμε κρυπτογραφημένα κείμενα με μία μέθοδο που ονομάζεται atbash. Κατά την μέθοδο αυτή γίνεται μια απλή αντιστροφή της αλφαβήτου, δηλ. μια αντικατάσταση του πρώτου γράμματος της αλφαβήτου με το τελευταίο, του δεύτερου με το πρότελευταίο κ.ο.κ. Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Γύρω στον 5ο π.Χ. αιώνα εφεύραν τη "σκυτάλη", την πρώτη κρυπτογραφική συσκευή. Όπως αναφέρει ο Πλούταρχος, η "Σπαρτιατική Σκυτάλη", ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το κλειδί[2] ήταν η διάμετρος της σκυτάλης.

Η πρώτη χρήση κρυπτοσυστήματος με αντικατάσταση[3] χρησιμοποιήθηκε από

[1] Αμερικανός ιστορικός, συγγραφέας και δημοσιογράφος ο οποίος έχει ασχοληθεί εκτεταμένα με την ιστορία της κρυπτογραφίας.

[2] βλ. §§ 2.1

[3] Αντικατάσταση ενός γράμματος από κάποιο άλλο.

Σχήμα 1.1: Η Σπαρτιατική Σκυτάλη

τον Ιούλιο Καίσαρα, από τον οποίο έχει πάρει και το όνομά του, Caesar Cipher. Ο Ιούλιος Καίσαρας έγραφε στον Κικέρωνα και σε άλλους φίλους του, αντικαθιστώντας τα γράμματα του κειμένου, με γράμματα, που βρίσκονται k θέσεις μετά, στο Λατινικό Αλφάβητο, όπου $k \in \mathbb{N}$. Ένα βιβλίο του Valerius Probus, στο οποίο καταγράφονταν και άλλα πιο πολύπλοκα συστήματα που χρησιμοποιούσε ο Καίσαρας και δεν σώζεται σήμερα, θεωρείται το πρώτο βιβλίο κρυπτολογίας.

Στην διάρκεια του Μεσαίωνα, η κρυπτολογία στην Ευρώπη ήταν κάτι το απαγορευμένο και αποτελούσε μια μορφή αποκρυφισμού και μαύρης μαγείας, ενώ την ίδια περίοδο οι Άραβες ανακάλυπταν τις πρώτες μεθόδους κρυπτανάλυσης. Αντιθέτως, κατά την περίοδο της Αναγέννησης και κυρίως για στρατιωτικούς σκοπούς παρατηρείται σημαντική ανάπτυξη της κρυπτολογίας αν και τα κρυπτοσυστήματα που χρησιμοποιούνται είναι σχετικά απλά και βασίζονται στην αντικατάσταση ή μετάθεση γραμμάτων.

Ραγδαία ανάπτυξη της κρυπτογραφίας, και πάλι για στρατιωτικούς σκοπούς, σημειώθηκε κατά το πρώτο μισό του εικοστού αιώνα όπου πλέον η κρυπτογράφηση και η αποκρυπτογράφηση γινόταν μέσω μηχανικών και ηλεκτρομηχανικών κατασκευών όπως π.χ. η Enigma των Γερμανών, η Μηχανή-Μ και η Red των Αμερικανών κ.α. Στην ανάπτυξη αυτή συνετέλεσαν κορυφαίοι μαθηματικοί όπως ο Alan Turing.

Σχήμα 1.2: Η Enigma των Γερμανών

Το 1949 ο Claude Shannon, ο οποίος θεωρείται και ο πατέρας των μαθη-

ματικών συστημάτων κρυπτογραφίας, δημοσίευσε το Communication Theory of Secrecy Systems στο οποίο έθεσε τα θεμέλια για τον σχεδιασμό ενός ασφαλούς αλγορίθμου. Στις 17 Μαρτίου του 1975 δημοσιεύεται το DES (Data Encryption Standard) σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις.

1.3 ΓΙΑΤΙ ΕΙΝΑΙ ΑΝΑΓΚΑΙΑ Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΗ ΣΗΜΕΡΙΝΗ ΕΠΟΧΗ;

Στην εποχή μας, ένα κομμάτι της καθημερινότητάς μας έχει "μεταφερθεί" από τον φυσικό κόσμο στον ηλεκτρονικό. Έτσι, εκτός από την χρήση της για στρατιωτικούς σκοπούς, η κρυπτογραφία χρειάζεται για να μπορούμε να είμαστε σίγουροι οτι ενέργειες που κάνουμε μέσω ηλεκτρονικών συσκευών είναι ασφαλείς. Τέτοιες ενέργειες είναι για παράδειγμα η χρήση των διαφόρων δικτύων, όπως το intenet, για επικοινωνία ή εμπόριο, η χρήση των ATM για συναλλαγή με τις τράπεζες κ.α.

Ίσως το πρώτο πράγμα που μας έρχεται στο μυαλό όταν ακούμε την φράση "ασφάλεια στη χρήση ηλεκτρονικών συσκευών" είναι ο υπολογιστής και το intenet. Όλοι όσοι χρησιμοποιούμε το διαδίκτυο επιθυμούμε οι πληροφορίες που μεταφέρονται μέσω αυτού να μην είναι προσβάσιμες στον καθένα. Τέτοιες πληροφορίες είναι για παράδειγμα στοιχεία που μπορεί να δώσει ένας χρήστης για τις συναλλαγές του με διάφορες υπηρεσίες ή με τις τράπεζες, για αγορές, στα διάφορα chatrooms, στο facebook ή στην επικοινωνία με e-mails.

Σε ορισμένες περιπτώσεις, η κρυπτογραφία μας επιτρέπει να νιώθουμε πιο ασφαλείς όταν χρησιμοποιούμε ηλεκτρονικές μεθόδους για να επισημοποιήσουμε κάποιες ενέργειές μας απ΄ ότι αν το κάναμε με φυσικό τρόπο. Ένα τέτοιο παράδειγμα είναι η υπογραφή κειμένων. Στον πραγματικό κόσμο μία υπογραφή μπορεί εύκολα να πλαστογραφηθεί από κάποιον ειδικό ενώ όσον αφορά στις ψηφιακές υπογραφές (βλ. κεφ. 5) αυτό είναι σχεδόν αδύνατο. Τέλος, κρυπτογράφηση χρησιμοποιούμε σε όλες τις περιπτώσεις που θέλουμε να έχουμε ελεγχόμενη πρόσβαση, δηλαδή σε όλες τις στιγμές της καθημερινότητάς μας που χρησιμοποιούμε κωδικούς, όπως στο κινητό ή στην πιστωτική μας κάρτα.

Κεφάλαιο 2

ΚΡΥΠΤΟΓΡΑΦΗΣΗ

2.1 ΓΕΝΙΚΑ

Όμως, με ποιόν τρόπο μπορούμε να κρυπτογραφίσουμε ένα μήνυμα έτσι ώστε μόνο ο παραλήπτης να μπορεί να το διαβάσει; Έστω οτι ο ο Bob θέλει να στείλει στην Αλίκη το p. Αρχικά, πριν την συγγραφή του κειμένου, ο Bob και η Αλίκη θα πρέπει να έχουν συμφωνήσει το αλφάβητο A με το οποίο θα γράφουν και θα διαβάζουν τα μηνύματα και το αλφάβητο B με βάση το οποίο θα μεταφέρεται το μήνυμα. Στη συνέχεια ο Bob, αφού γράψει το κείμενο p στο αλφάβητο A, το μετασχηματίζει στο αλφάβητο B. Το μετασχηματισμένο κείμενο ονομάζεται **κρυπτοκείμενο**. Ο παραπάνω μετασχηματισμός γίνεται μέσω ενός μονομορφισμού $e_k : \mathbf{M} \to \mathbf{C}$ που εξαρτάται από το k, όπου το $\mathbf{M}$ είναι το σύνολο των κειμένων που μπορούν να σχηματιστούν με το A και $\mathbf{C}$ το σύνολο των κειμένων που μπορούν να σχηματιστούν με το B. Όταν η Αλίκη λάβει το $e_k(p)$ τότε το αποκρυπτογραφεί μέσω ενός μονομορφισμού $d_{k'} : \mathbf{C} \to \mathbf{M}$ που εξαρτάται από το k' και ανακτά το μήνυμα p. Τα k, k' ονομάζονται **κλειδιά** και το σύνολο όλων των κλειδιών συμβολίζεται με το K.

2.2 ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Μέχρι τα μέσα της δεκαετίας του 1970 όλα τα κρυπτοσυστήματα είχαν το κοινό χαρακτηριστικό οτι γνωρίζοντας ένα από τα k, k' το άλλο μπορούσε να υπολογιστεί πολύ εύκολα. Αυτά τα κρυπτοσυστήματα ονομάζονται **συμμετρικά κρυπτοσυστήματα**. Ένα από τα βασικά μειονεκτήματα αυτών των κρυπτοσυστημάτων είναι οτι απαιτείται επικοινωνία ανάμεσα στον αποστολέα και τον παραλήπτη μέσω ενός ασφαλούς καναλιού με σκοπό την ανταλλαγή των κλειδιών. Στις μέρες μας, λόγω των ταχύτατων Η/Υ, και της εξέλιξης της τεχνολογίας τα συμμετρικά κρυπτοσυστήματα δεν θεωρούνται ασφαλή.

Το 1976 οι Diffie, Hellman δημοσιεύουν το πρώτο **ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού**. Κάθε ένας που συμμετέχει στη διαδικασία κρυπτογράφησης έχει δύο κλειδιά, ένα δημόσιο p και ένα κρυφό s, όπου το ένα εξαρτάται μαθηματικά από το άλλο. Η απαραίτητη προϋπόθεση για τα κρυπτοσυστήματα δημοσίου κλειδιού είναι οτι ενώ είναι σχετικά εύκολο να υπολογιστεί το p αν είναι γνωστό το s, είναι υπολογιστικά αδύνατο να κάνουμε το

αντίθετο δηλαδή να υπολογίσουμε το s αν είναι γνωστό το p.

Η Κρυπτογράφηση Δημοσίου Κλειδιού βασίζεται στην ιδέα της trapdoor μονόδρομης συνάρτησης.

Ορισμός 2.2.1.

Μια συνάρτηση $f : X \to Y$ λέγεται **μονόδρομη συνάρτηση** (**one-way function**) αν το $f(x)$ υπολογίζεται εύκολα για κάθε $x \in X$ αλλά είναι υπολογιστικά ακατόρθωτο να βρεθεί κάποιο $x \in X$ τέτοιο ώστε $f(x) = y$ για σχεδόν όλα τα $y \in f[X]$.

Μια συνάρτηση $f : X \to Y$ λέγεται **trapdoor μονόδρομη συνάρτηση** (**trapdoor one-way function**) αν είναι μονόδρομη και δοσμένης μιας επιπλέον πληροφορίας, η οποία λέγεται **trapdoor πληροφορία**, γίνεται εφικτό να βρούμε ένα $x \in X$ τέτοιο ώστε $f(x) = y$ για κάθε $y \in f[X]$. ◇

Εκεί που υπερέχουν τα κρυπτοσυστήματα δημοσίου κλειδιού σε σχέση με τα συμμετρικά κρυπτοσυστήματα είναι το γεγονός οτι δεν χρειάζεται να γίνει ανταλλαγή κλειδιών ανάμεσα στον αποστολέα και τον παραλήπτη του κρυπτοκειμένου. Αντί γι' αυτήν την ανταλλαγή υπάρχει ένας δημόσιος "τηλεφωνικός αριθμός" τον οποίο μπορεί να χρησιμοποιεί όποιος θέλει να επικοινωνήσει με τον κάτοχό του.

Κάποια από τα πιο γνωστά κρυπτοσυστήματα δημοσίου κλειδιού είναι τα εξής:

RSA
: Είναι το κρυπτοσύστημα με το οποίο ασχολείται εκτενώς αυτή η εργασία.

Merkle-Hellman Knapsack
: Η ασφάλεια αυτού και άλλων παρόμοιων συστημάτων βασίζεται στην δυσκολία του SubSet-Sum problem[1], τό οποίο είναι NP-complete[2].

McEliece
: Βασίζεται στην θεωρία αλγεβρικής κωδικοποίησης.

ElGamal
: Βασίζεται στη δυσκολία του προβλήματος του διακριτού λογαρίθμου για πεπερασμένα σώματα.

Ελλειπτικές Καμπύλες
: Όπως και το ElGamal, βασίζεται στο πρόβλημα του διακριτού λογαρίθμου με τη διαφορά ότι αντί δακτυλίων της μορφής $\mathbb{Z}_p$ χρησιμοποιεί κάποια πεπερασμένα σώματα που έχουν τάξη κάποιο πρώτο αριθμό και βρίσκονται κάτω από μια ελλειπτική καμπύλη[3].

[1] SubSet-Sum problem $= \{< S, t > \in \ \wp(\mathbb{N}) \times \mathbb{N} : \ \exists\ S' \ \subset \ S \ \textit{έτσι ώστε}\ t = \sum_{s \in S'} s\}$

[2] Ένα πρόβλημα είναι NP-complete αν μπορούμε να επιβεβαιώσουμε την λύση του σε πολυωνυμικό χρόνο και είναι ισοδύναμο με κάποιο άλλο γνωστό NP-complete πρόβλημα.

[3] Ελλειπτική καμπύλη ονομάζουμε μια καμπύλη E πάνω από ένα σώμα $\mathbb{F}$ η οποία δίνεται από

την εξίσωση:

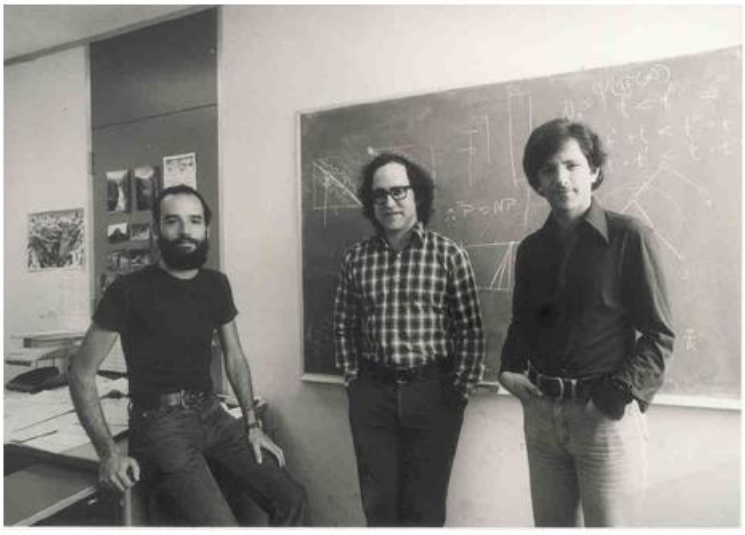
$$Y^2 + \alpha_1 XY + \alpha_3 Y = \alpha_0 X^3 + \alpha_2 X^2 + \alpha_4 X + \alpha_6,\ \alpha_i \in \mathbb{F}$$

Κεφάλαιο 3

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ *RSA*

3.1 ΤΟ *RSA*

Το 1977 οι Ron Rivest, Adi Shamir και Adleman από το MIT δημοσίευσαν ένα μαθηματικό σύστημα κρυπτογράφησης το οποίο ονόμασαν RSA, από τα αρχικά γράμματα των ονομάτων τους. Τα βασικά μαθηματικά εργαλεία του αλγορίθμου είναι η Ευκλείδεια διαίρεση και οι πρώτοι αριθμοί. Το RSA είναι ένα κρυπτοσύστημα δημοσίου κλειδιού και η ασφάλεια του οφείλεται στην δυσκολία παραγοντοποίησης των μεγάλων φυσικών αριθμών.



Σχήμα 3.1: Οι εφευρέτες του RSA από αριστερά Adi Shamir, Ron Rivest και Len Adleman

3.2 Ο ΑΛΓΟΡΙΘΜΟΣ *RSA*

Σύμφωνα με τον Richard A. Mollin [3], μπορούμε να σπάσουμε τον αλγόριθμο σε δύο μέρη, όπως φαίνονται παρακάτω.

Έστω οτι ο Bob θέλει να μπορεί να στέλνει μηνύματα στην Αλίκη, τα οποία να μπορεί να διαβάζει μόνο εκείνη, δηλαδή ακόμα και αν κάποιος κλέψει ένα μήνυμα να μην μπορέσει να το διαβάσει. Τότε θα πρέπει να γίνουν τα εξής βήματα:

1. **Δημιουργία του RSA-Κλειδιού:**
   - (α′) Η Αλίκη, επιλέγει δύο μεγάλους, περίπου ίδιου μεγέθους, τυχαίους πρώτους αριθμούς $p \neq q$.
   - (β′) Υπολογίζει τους $n = pq$, $\phi(n) = (p-1)(q-1)$, όπου ο n ονομάζεται **(RSA)-Συντελεστής**.
   - (γ′) Επιλέγει ένα τυχαίο $e \in \mathbb{Z}$ τέτοιο ώστε $1 < e < \phi(n)$ και ΜΚΔ$(e,\phi(n))$=1. Ο e ονομάζεται **(RSA)-Κρυπτογραφικός Εκθέτης**.
   - (δ′) Χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο υπολογίζει το μοναδικό[1] $d \in \mathbb{Z}$ με $1 < d < \phi(n)$ και $de = 1(mod\phi(n))$.
   - (ε′) Το **(RSA)-Δημόσιο Κλειδί** είναι το (n, e) και το **(RSA)-Ιδιωτικό Κλειδί** είναι το d[2].
2. **Κρυπτογράφηση με το RSA-Δημόσιο Κλειδί:**
   - (α′) Ο Bob μεταφράζει το αρχικό κείμενο σε ένα αριθμητικό σύστημα με βάση το N για κάποιο $N > 1$. Αυτό το ισοδύναμο αριθμητικό μήνυμα χωρίζεται σε ομάδες ίσου μεγέθους $l \in \mathbb{N}$ [3].
   - (β′) Κρυπτογραφεί κάθε ομάδα $m \in \mathbf{M}$ ξεχωριστά υπολογίζοντας το $c = m^e(modn)$, όπου η $f(m) = m^e(modn)$ είναι η trapdoor μονόδρομη συνάρτηση του RSA.
   - (γ′) Στέλνει το $c \in C$ Αλίκη.

Τέλος η Αλίκη υπολογίζει το $c^d(modn)$ και ανακτά το μήνυμα m.

Πιο συνοπτικά:

Ο ΑΛΓΟΡΙΘΜΟΣ RSA
1. Η Αλίκη επιλέγει δύο μεγάλους πρώτους p, q και υπολογίζει το $n = pq$.
2. Η Αλίκη επιλέγει ένα e με ΜΚΔ$(e,\phi(n))$=1.
3. Η Αλίκη υπολογίζει έναν αριθμό d τέτοιο ώστε $de = 1(mod\phi(n))$.
4. Η Αλίκη δημοσιεύει τα n, e και κρατά κρυφά τα p, q, d.
5. Ο Bob υπολογίζει το $c = m^e(modn)$ για κάθε ομάδα m και το στέλνει στην Αλίκη.
6. Η Αλίκη υπολογίζει το $c^d(modn)$ και ανακτά τις ομάδες m.

[1] Το d είναι μοναδικό αφού είναι αυτό για το οποίο ισχύει $de + \lambda\phi(n) = 1$, όπου τα e, $\phi(n)$ είναι ήδη γνωστά.

[2] Η Αλίκη, εκτός του d, πρέπει να κρατά κρυφά και τα p, q (βλ. παράγραφο 3.4.).

[3] π.χ. το l μπορεί να είναι τέτοιο ώστε $N^l < n < N^{l+1}$.

Παρακάτω παρατίθεται ένα παράδειγμα χρήσης του αλγορίθμου με μη ρεαλιστικούς αριθμούς, αφού όλοι είναι πολύ μικροί.

Παράδειγμα 3.2.1.

Έστω οτι η Αλίκη επιλέγει τους πρώτους $p = 31$ και $q = 61$. Τότε θα έχει $n = 1891$ και $\phi(n) = 1800$. Ακόμη, επιλέγει έναν ακέραιο e τέτοιο ώστε $1 < e < \phi(n)$ και ΜΚΔ(e,$\phi(n)$)=1, π.χ. τον $e = 1001$. Στη συνέχεια, χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο υπολογίζει τον μοναδικό $d \in \mathbb{Z}$ με $1 < d < \phi(n)$ και $de = 1(mod\phi(n))$, δηλαδή τον $d = 401$ και τον κρατά κρυφό ενώ δημοσιεύει τους 1891, 1001.

Έστω τώρα οτι ο Bob θέλει να στείλει στην Αλίκη την πρόταση "Σήμερα δεν βρέχει", τότε θα το μεταφράσει σε ένα αριθμητικό σύστημα με βάση το N, π.χ. $N = 24$ και η μετάφραση γίνεται σύμφωνα με τον παρακάτω πίνακα.

Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ
00	01	02	03	04	05	06	07	08	09	10	11
Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
12	13	14	15	16	17	18	19	20	21	22	23

Αν επιπλέον, χωρίσει το αρχικό μήνυμα σε ομάδες των $l = 2$[4], θα πάρει το σύνολο

$$M' = \{17, 06, 11, 04, 16, 00, 03, 04, 12, 01, 16, 04, 21, 04, 08\} \subset \mathbf{M}.$$

Έπειτα, ο Bob, για κάθε $m \in \mathbf{M}'$ υπολογίζει το $c = m^e(modn)$ και παίρνει το σύνολο

$$C' = \{921, 1359, 1109, 66, 574, 0, 1284, 66, 1540, 1, 574, 66, 1066, 66, 8\} \subset \mathbf{C}$$

το οποίο στέλνει στην Αλίκη. Και τέλος η Αλίκη για κάθε $c \in C'$ υπολογίζει το $c^d(modn)$ και ανακτά το μήνυμα. ◇

3.3 ΓΙΑΤΙ Η ΑΛΙΚΗ ΑΝΑΚΤΑ ΤΟ ΜΗΝΥΜΑ m;

Ισχυρισμός 3.3.1.

Έστω p, q πρώτοι αριθμοί με $p \neq q$, $n = pq$, $e, d \in \mathbb{Z}$, όπου ΜΚΔ(e,$\phi(n)$)=1 και $de = 1(mod\phi(n))$. Τότε, για κάθε $x \in \mathbb{Z}$ ισχυει

$$x^{ed}(modn) = x(modn).$$

Απόδειξη:
Είναι $de = 1(mod\phi(n)) \iff ed = 1 + \lambda(p-1)(q-1)$, $\lambda \in \mathbb{Z}$.

[4] $24^2 < 1891 < 24^3$.

Διακρίνουμε τις περιπτώσεις:

▷ Το x είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_n$. Τότε, από το θεώρημα του Euler, έχουμε ότι:

$$x^{ed} = x^{1+\lambda(p-1)(q-1)} = x \cdot x^{\lambda(p-1)(q-1)} = x \cdot x^{\lambda\phi(n)} = x \cdot [x^{\phi(n)}]^{\lambda} = x \cdot 1(modn) = x(modn)$$

▷ Το x δεν είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_n$. Τότε το x θα είναι της μορφής κp, κq ή κpq, όπου $\kappa \in \mathbb{Z}$.

∘ Έστω $x = \kappa p$, τότε:

$$x^{ed} = x \cdot x^{\lambda(p-1)(q-1)} = x \cdot [(\kappa p)^{q-1}]^{\lambda(p-1)} = x \cdot 1(modq) = x(modq)$$

και

$$x^{ed} = (\kappa p)^{ed} = 0(modp),$$

από το οποίο παίρνουμε ότι $x^{ed} = x(modp)$, αφού $x = \kappa p = 0(modp)$.

Δηλαδή έχουμε να λύσουμε το σύστημα:

$$\begin{cases} x^{ed} = x(modq) \\ x^{ed} = x(modp) \end{cases}$$

Από το Κινέζικο Θεώρημα υπολοίπων, το σύστημα έχει μοναδική λύση, την

$$x^{ed} = x \cdot \frac{pq}{p}\mu_1 + x \cdot \frac{pq}{q}\mu_2,$$

όπου $q\mu_1 = 1(modp)$ και $p\mu_2 = 1(modp)$. Τα μ_1, μ_2 μπορούμε να τα βρούμε από τον Ευκλείδειο αλγόριθμο για τον ΜΚΔ, αφού $\text{ΜΚΔ}(p, q) = 1$.

Έτσι θα είναι: $x^{ed} = xq\mu_1 + xp\mu_2 = x(q\mu_1 + p\mu_2) = x(modn)$.

∘ Έστω $x = \kappa q$, ομοίως.

∘ Έστω $x = \kappa pq$, τότε: $x^{ed} = 0(modn)$ και αφού είναι και $x = 0(modn)$ παίρνουμε οτι $x^{ed} = x(modn)$. ◇

Παρατήρηση:
Για να μην ψάχνει η Αλίκη όλους τους πιθανούς ακέραιους αριθμούς των οποίων το υπόλοιπο της διαίρεσης με το n είναι $m(modn)$, θα πρέπει ο Bob να διαλέξει το l έτσι ώστε $m < n$.

3.4 ΠΟΣΟ ΓΡΗΓΟΡΟΣ ΕΙΝΑΙ Ο ΑΛΓΟΡΙΘΜΟΣ *RSA*;

Όμως πόσο ρεαλιστικός είναι ο παραπάνω αλγόριθμος; Είναι δυνατόν να εφαρμοστεί με τα σύγχρονα τεχνολογικά μέσα;

Μία (RSA)-διαδικασία είτε αυτή είναι κρυπτογράφηση, είτε αποκρυπτογράφηση, είτε υπογραφή, είτε αυθεντικοποίηση (βλ. §§ 5) είναι μία σειρά από πολλαπλασιασμούς. Στις εφαρμογές είναι συχνό φαινόμενο να επιλέγεται ένας σχετικά μικρός (RSA)-Κρυπτογραφικός Εκθέτης[5]. Επιπλέον, μπορεί μια ομάδα ανθρώπων να χρησιμοποιεί τον ίδιο (RSA)-Κρυπτογραφικό Εκθέτη αλλά το κάθε ένα από τα μέλη της ομάδας να χρησιμοποιεί διαφορετικό (RSA)-Συντελεστή. Αυτό κάνει την διαδικασία κρυπτογράφησης γρηγορότερη από αυτή της αποκρυπτογράφησης και τη διαδικασία αυθεντικοποίησης γρηγορότερη από αυτή της υπογραφής. Χρησιμοποιώντας τον τυπικό RSA αλγόριθμο, οι διαδικασίες δημοσίου κλειδιού χρειάζονται $O(k^2)$ βήματα, οι διαδικασίες ιδιωτικού κλειδιού $O(k^3)$ βήματα και η δημιουργία του κλειδιού $O(k^4)$ βήματα, όπου k είναι ο αριθμός των bits του (RSA)-Συντελεστή. Παρ' όλ' αυτά, υπάρχουν τεχνικές που μειώνουν τα βήματα υπολογισμού. Μία τέτοια φαίνεται στην επόμενη παράγραφο.

3.5 ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ ΜΕ ΧΡΗΣΗ ΤΟΥ ΚΙΝΕΖΙΚΟΥ ΘΕΩΡΗΜΑΤΟΣ ΥΠΟΛΟΙΠΩΝ

Όπως φαίνεται παρακάτω, η χρήση του Κινέζικου θεωρήματος υπολοίπων για την αποκρυπτογράφηση μειώνει τον χρόνο των υπολογισμών. Έστω λοιπόν οτι η Αλίκη θέλει να αποκρυπτογραφήσει το κρυπτοκείμενο c και έστω d το (RSA)-Ιδιωτικό Κλειδί της. Αρχικά, θα πρέπει να υπολογίσει τα

$$m_p = c^{d(modp)-1}(modp), \quad m_q = c^{d(modq)-1}(modq)$$

και στη συνέχεια να βρει το αρχικό κείμενο m λύνοντας το παρακάτω σύστημα με το Κινέζικο θεώρημα υπολοίπων

$$m = m_p(modp)$$

$$m = m_q(modq).$$

Μένει να δείξουμε οτι αυτός ο τρόπος αποκρυπτογράφησης είναι γρηγορότερος από τον κλασσικό για το RSA. Ας υποθέσουμε οτι τόσο ο (RSA)-Κρυπτογραφικός Εκθέτης e όσο και το (RSA)-Ιδιωτικό Κλειδί d αποτελούνται από k bits. Τότε οι p, q θα αποτελούνται από $\frac{k}{2}$ *bits*. Ο πολλαπλασιασμός δύο ακεραίων με δυαδικό μήκος μικρότερο ή ίσο του r χρειάζεται χρόνο το πολύ Cr^2, όπου C είναι μία σταθερά. Τον ίδιο χρόνο χρειάζεται και η διαίρεση με υπόλοιπο δύο αριθμών με δυαδικό μήκος μικρότερο ή ίσο του r. Έτσι, ο υπολογισμός του $m = c^d(modn)$

[5] Αν και αυτό μπορεί να εγκυμονεί κίνδυνους (βλ. §§ 4.3.2.2).

απαιτεί χρόνο το πολύ $C(k+l)k^2$, όπου l είναι το πλήθος των άσσων που περιέχονται στην δυαδική μορφή του d. Αντιθέτως ο υπολογισμός των $m_p,\ m_q$ απαιτεί χρόνο $\frac{2(k+l)Ck^2}{4} = \frac{(k+l)Ck^2}{2}$. Ο χρόνος που χρειάζεται για να υπολογίσουμε τα $y_p,\ y_q$ που χρειάζονται για το Κινέζικο θεώρημα υπολοίπων[6] καθώς και το m είναι αμελητέος αφού είναι της τάξης του k^2. Άρα, η αποκρυπτογράφηση με το Κινέζικο θεώρημα υπολοίπων μειώνει τον χρόνο υπολογισμού σχεδόν στο μισό.

3.6 ΠΩΣ ΧΡΗΣΙΜΟΠΟΙΕΙΤΑΙ Ο ΑΛΓΟΡΙΘΜΟΣ RSA ΣΤΗΝ ΠΡΑΞΗ;

Στην πράξη ο αλγόριθμος χρησιμοποιείται σε συνδυασμό με ένα συμμετρικό κρυπτοσύστημα. Έστω λοιπόν οτι ο Bob θέλει να στείλει το μήνυμα M στην Αλίκη. Αρχικά, κρυπτογραφεί το μήνυμα με το κλειδί του συμμετρικού κρυπτοσυστήματος και έτσι δημιουργεί το m. Στη συνέχεια κρυπτογραφεί το m με το RSA και το στέλνει στην Αλίκη. Προφανώς, η Αλίκη θα πρέπει να κάνει την αντίστροφη διαδικασία για να ανακτήσει το M, δηλαδή πρώτα να αποκρυπτογραφήσει με το RSA και έπειτα με το συμμετρικό κλειδί.

[6] Πρέπει να βρούμε τα $y_p,\ y_q$ έτσι ώστε $y_p p + y_q q = 1$ και στη συνέχεια να υπολογίσουμε το $m = (m_p y_q q + m_q y_p p)(mod n)$.

Κεφάλαιο 4

Η ΑΣΦΑΛΕΙΑ ΤΟΥ *RSA*

Η φράση "μία αλυσίδα δεν είναι πιο δυνατή από τον πιο αδύναμο κρίκο της" είναι η καταλληλότερη για να περιγράψει τις επιθέσεις στα κρυπτοσυστήματα. Αυτό που γίνεται στην πραγματικότητα είναι οτι ο επιτιθέμενος ψάχνει να βρει το πιο αδύναμο σημείο του αλγορίθμου και να το χρησιμοποιήσει προς όφελός του. Κάποιες φορές, αυτή η αδυναμία ήταν γνωστή στον σχεδιαστή του αλγορίθμου και απλώς θεωρήθηκε ασήμαντη, ενώ κάποιες άλλες φορές, η κρυπτανάλυση φέρνει στο φως μια αδυναμία του συστήματος που δεν είχε προσέξει κανείς πιο πριν. Αυτό που πρέπει να έχουν πάντα υπόψιν τους οι σχεδιαστές κρυπτοσυστημάτων, είναι οτι το ενδεχόμενο να υπάρχει στον αλγόριθμό τους μια λεπτομέρεια, η οποία μπορεί να χρησιμοποιηθεί εναντίον του συστήματός τους, έχει μεγάλη πιθανότητα να συμβεί.

4.1 ΠΟΥ ΟΦΕΙΛΕΤΑΙ Η ΑΣΦΑΛΕΙΑ ΤΟΥ ΑΛΓΟΡΙΘΜΟΥ;

Μέχρι στιγμής, το RSA φαίνεται να είναι αρκετά ασφαλές, αφού έχει επιβιώσει 30 χρόνια εξονυχιστικού ελέγχου και χρησιμοποιείται ευρέως σε όλο τον κόσμο. Η πιο συνηθισμένη επίθεση στο RSA είναι η παραγοντοποίηση του n, αφού, όπως αποδεικνύεται παρακάτω, ο υπολογισμός του d από το δημόσιο κλειδί (n, e) είναι ισοδύναμος με την εύρεση των παραγόντων του n.

Έστω οτι γνωρίζουμε το $\phi(n)$ τότε, επειδή είναι $n - \phi(n) + 1 = pq - (p - 1)(q-1) + 1 = p+q$, κατασκευάζοντας το τριώνυμο $x^2 - (n-\phi(n)+1)x+n = 0$ μπορούμε να βρούμε τα p, q τα οποία είναι, προφανώς, οι λύσεις του τριωνύμου.

Αν γνωρίζουμε ένα από τα p, q, π.χ. το p τότε μπορούμε πολύ εύκολα να βρούμε και το άλλο (εδώ $q = n : p$).

Επιπλέον είναι προφανές οτι αν με οποιονδήποτε τρόπο γνωρίζουμε τα p, q μπορούμε πολύ εύκολα να υπολογίσουμε το d με τον ίδιο τρόπο που το υπολογίζει και η Αλίκη.

Αντίστροφα, έστω οτι γνωρίζουμε το d. Θέτουμε $s = max\{t \in \mathbb{N} : 2^t | ed - 1\}$ και $k = \frac{ed-1}{2^s}$.

Λήμμα 4.1.1.

Για κάθε ακέραιο α τέτοιο ώστε $MK\Delta(\alpha, n) = 1$, η τάξη του $\alpha^k + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$ ανήκει στο $\{2^i : 0 \leq i \leq s\}$.

Απόδειξη:
Έστω $\alpha \in \mathbb{Z}$ με $MK\Delta(\alpha, n) = 1$. Από τον ισχυρισμό 3.3.1 έχουμε οτι $\alpha^{ed-1} = 1(modn)$. Όμως ξέρουμε οτι $ed - 1 = k2^s$ και έτσι $(\alpha^k)^{2^s} = 1(modn)$ και έτσι $\alpha^k + n\mathbb{Z}|2^s$. ◇

Θεώρημα 4.1.1.

Έστω $\alpha \in \mathbb{Z}$ τέτοιο ώστε $MK\Delta(\alpha, n) = 1$. Αν οι τάξεις των $\alpha^k + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$ και $\alpha^k + q\mathbb{Z} \in (\mathbb{Z}/q\mathbb{Z})^*$ είναι διαφορετικές τότε για κάποιο $t \in \{0, 1, 2, ..., s-1\}$ είναι $1 < MK\Delta(\alpha^{2^t k} - 1, n) < n$.

Απόδειξη:
Ξέρουμε οτι οι τάξεις των $\alpha^k(modp)$, $\alpha^k(modq)$ ανήκουν στο $\{2^i : 0 \leq i \leq s\}$ και επειδή είναι διαφορετικές, χωρίς βλάβη της γενικότητας, θεωρούμε οτι η τάξη του $\alpha^k(modp)$ είναι μεγαλύτερη από την τάξη του $\alpha^k(modq)$. Έτσι, έστω οτι η τάξη του $\alpha^k(modp)$ είναι 2^t, όπου $t < s$. Άρα, έχουμε οτι $\alpha^{2^t k} = 1(modp)$, όμως είναι $\alpha^{2^t k} \neq 1(modq)$. Έτσι προκύπτει οτι $MK\Delta(\alpha^{2^t k} - 1, n) = q$. ◇

Για την παραγοντοποίηση του n ακολουθούμε τον παρακάτω αλγόριθμο:

1. Επιλέγουμε τυχαία ένα $\alpha \in \{1, 2, ..., n-1\}$.

2. Υπολογίζουμε το $g = MK\Delta(\alpha, n)$.

3. Αν $g = 1$ τότε θέτουμε $g = MK\Delta(\alpha^{2^t k} - 1(modn), n)$ και επαναλαμβάνουμε το αυτό το βήμα για κάθε $t \in \{s-1, s-2, ..., 0\}$ μέχρι να προκύψει $g > 1$ ή $t = 0$.

4. Αν $g > 1$ τότε $g = p$ ή $g = q$ και έτσι παραγοντοποιήσαμε το n. Στην περίπτωση που δεν καταλήγουμε σε ένα $g > 1$ ο αλγόριθμος κρίνεται ανεπιτυχής και ο λόγος είναι οτι δεν επιλέχτηκε το κατάλληλο α, αφού μπορεί οι τάξεις των $\alpha^k(modp)$, $\alpha^k(modq)$ να είναι ίδιες. Ξανατρέχουμε τον αλγόριθμο. ◇

Αποδεικνύεται [4] οτι ο παραπάνω αλγόριθμος έχει τουλάχιστον 50% επιτυχία. Έτσι αν τον τρέξουμε r φορές έχουμε τουλάχιστον $1 - \frac{1}{2^r}$ πιθανότητες να παραγοντοποιήσουμε το n.

Επομένως, το να υπολογίσουμε το d από το κλειδί (n, e) είναι τουλάχιστον όσο δύσκολο είναι να παραγοντοποιήσουμε το n. Έτσι, χάριν σ΄ αυτό και στο οτι το να παραγοντοποιήσουμε έναν μεγάλο ακέραιο με τα σύγχρονα μέσα, είναι ένα εξαιρετικά δύσκολο πρόβλημα, το RSA παραμένει ένας ασφαλής αλγόριθμος κρυπτογράφησης. Όμως, πόσο μεγάλο πρέπει να είναι το n έτσι ώστε το σύστημα να είναι ασφαλές;

4.2 ΕΠΙΛΟΓΗ ΤΩΝ $p,\ q,\ e,\ d$

Είναι κοινή αντίληψη οτι τα p, q πρέπει να είναι τυχαίοι πρώτοι, περίπου του ίδιου δοσμένου δυαδικού μήκους και αρκετά μεγάλοι, έτσι ώστε, από την μία να μην μπορούν οι σύγχρονοι υπολογιστές να τους υπολογίσουν παραγοντοποιώντας το n και από την άλλη το μήκος του n να είναι τέτοιο ώστε οι υπολογισμοί να γίνονται μέσα σε λογικό χρονικό διάστημα. Βέβαια, κανείς δεν είναι σε θέση να πει με βεβαιότητα πόσο μεγάλοι πρέπει να είναι, δεδομένου οτι κανείς δεν μπορεί να προβλέψει τις εξελίξεις στην θεωρία αλγορίθμων και στην τεχνολογία των υπολογιστών.

Για την επιλογή του e υπάρχει η εξής δυσκολία. Κατ΄ αρχήν, πρέπει να ισχύει οτι $e \geq 3$ αφού διαφορετικά $\text{ΜΚΔ}(e, \phi(n)) \neq 1$ και επιπλέον, το e πρέπει να είναι ικανοποιητικά μικρό, έτσι ώστε οι υπολογισμοί κρυπτογράφησης να γίνονται σε λογικό χρονικό διάστημα. Όμως, όταν επιλέξουμε μικρό e υπάρχει ο κίνδυνος να δεχτούμε επίθεση μικρού εκθέτη (βλ. §§ 4.3.2.2).

Ένας τρόπος για να καταφέρουμε να διατηρήσουμε μυστικό το (RSA)-Ιδιωτικό Κλειδί d, είναι να το αποθηκεύσουμε σε μία smartcard[1], η οποία μπορεί να εκτελέσει όλους του υπολογισμούς μόνη της, όποτε δεν χρειάζεται να τοποθετήσουμε το d πουθενά αλλού, είτε για φύλαξη είτε για υπολογισμούς σε κάποιο πρόγραμμα (βλ. Παράρτημα Α §§ 8). Το πρόβλημα εδώ έγγυται στο γεγονός οτι η smartcard έχει περιορισμένη μνήμη και επομένως το d πρέπει να είναι σχετικά μικρό. Επειδή όμως, εφόσον έχει γίνει η επιλογή του e, το d είναι ένα και μοναδικό, μπορούμε να κάνουμε την διαδικασία αντίστροφα, δηλαδή, μπορούμε πρώτα να επιλέξουμε το d που μας εξυπηρετεί και στη συνέχεια να βρούμε το μοναδικό e τέτοιο ώστε $de = 1(mod\phi(n))$.

Μία άλλη συσκευή στην οποία θα μπορούσαμε να αποθηκεύσουμε το (RSA)-Ιδιωτικό Κλειδί d είναι μία κρυπτογραφική συσκευή. Μία κρυπτογραφική συσκευή είναι μια ηλεκτρονική συσκευή που μπορεί να εφαρμόσει έναν κρυπτογραφικό αλγόριθμο και να αποθηκεύσει το κρυπτογραφικό κλειδί. Είναι ικανή να εφαρμόσει τον αλγόριθμο χρησιμοποιώντας το αποθηκευμένο κλειδί. Η ασφάλεια μιας τέτοιας συσκευής στηρίζεται στην μυστικότητα του κλειδιού.

[1] Οι smartcards είναι κάρτες αποθήκευσης όπως οι τηλεκάρτες, οι πιστωτικές κάρτς και οι κάρτες sim.

4.3 ΕΠΙΘΕΣΕΙΣ ΣΤΟ *RSA*

Είναι κοινώς αποδεκτό οτι ο λόγος που κρυπτογραφείται ένα κείμενο, είναι για να παραμείνει κρυφό από τουλάχιστον ένα άτομο. Έστω λοιπόν οτι ο Bob έστειλε το κρυπτοκείμενο στην Αλίκη για να μην μπορέσει να μάθει ο Κώστας τις πληροφορίες που περιέχει το αρχικό κείμενο. Υποθέτοντας οτι το κρυπτοκείμενο φτάνει στα χέρια του Κώστα, αυτός θα προσπαθήσει να το "σπάσει" ή αλλιώς να επιτεθεί στο κρυπτοσύστημα.

4.3.1 ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΤΟΥ n

Από όσα έχουν αναφερθεί παραπάνω γίνεται φανερό πως ο οποιοσδήποτε που θα επιδίωκε να επιτεθεί στο RSA θα ήθελε να γνωρίζει το d ή τουλάχιστον κάποιον από τους παράγοντες του n, αφού τότε το d μπορεί να υπολογιστεί πολύ εύκολα. Έτσι, η πιο προφανής προσπάθεια επίθεσης στο RSA είναι η παραγοντοποίηση του n. Από την αρχαιότητα έως σήμερα έχουν προταθεί αρκετοί αλγόριθμοι παραγοντοποίησης ενός ακεραίου. Παραπάνω (βλ. θεώρημα 4.1.1), έχει ήδη αναφερθεί ένας τέτοιος αλγόριθμος. Σε γενικές γραμμές έχουμε δύο μεγάλες κατηγορίες τέτοιων αλγορίθμων, τους αλγόριθμους "ειδικού-σκοπού" και τους αλγόριθμους "γενικού-σκοπού". Ο χρόνος εκτέλεσης των αλγόριθμων της πρώτης κατηγορίας εξαρτάται από τις ιδιότητες των άγνωστων παραγόντων του n όπως το μέγεθος ή η ειδική τους μορφή και διαφέρει από αλγόριθμο σε αλγόριθμο. Κάποιοι από αυτούς είναι η παραγοντοποίηση με δοκιμές, ο rho αλγόριθμος του Pollard, οι αλγόριθμοι παραγοντοποίησης με την χρήση αλγεβρικών ομάδων όπως ο αλγόριθμος $p-1$ του Pollard, ο αλγόριθμος $p+1$ του William και ο αλγόριθμος παραγοντοποίησης με χρήση ελλειπτικών καμπύλων. Άλλοι αλγόριθμοι που ανήκουν σε αυτήν την κατηγορία είναι αυτός του Fermat, αυτός του Euler ο Number field sieve (NFS) και ο Special number field sieve (SNFS). Αντιθέτως, ο χρόνος εκτέλεσης των αλγόριθμων της δεύτερης κατηγορίας εξαρτάται μόνο από το μέγεθος του n. Κάποιοι από αυτούς είναι ο αλγόριθμος του Dixon, ο Continued fraction factorization (CFRAC), το Τετραγωνικό Κόσκινο, ο General number field sieve (GNFS) και ο Shanks' square forms factorization (SQUFOF). Παρακάτω παρατίθενται και κάποιοι από τους αλγορίθμους και των δύο κατηγοριών.

4.3.1.1 ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΜΕ ΔΟΚΙΜΕΣ

Ο συγκεκριμένος αλγόριθμος είναι ένας από τους παλαιότερους αλγορίθμους παραγοντοποίησης αλλά ταυτόχρονα και ένας από τους πιο αργούς για ακεραίους με μεγάλο αριθμό ψηφίων. Κατά την εκτέλεση του αλγορίθμου το n διαιρείται διαδοχικά με όλους του πρώτους αριθμούς που είναι μικρότεροι ή ίσοι με την $\sqrt{n}$. Αν βρεθεί αριθμός που να διαιρεί το n τότε προφανώς αυτός είναι ένας από τους p, q.

Παρόλο που αυτή η μέθοδος εγγυάται οτι θα βρεθεί ένας πρώτος παράγοντας του n, αφού εξετάζει όλους τους αριθμούς που μπορούν να έχουν αυτή την ιδιότητα, είναι μία από τις πιο χρονοβόρες. Στην χειρότερη των περιπτώσεων απαιτεί

περίπου $\frac{2\sqrt{n}}{lnn}$ διαιρέσεις. Στον υπολογισμό αυτόν δεν υπολογίζεται το κόστος εύρεσης όλων των πρώτων που είναι μικρότεροι του ή ίσοι του $\sqrt{n}$. Στην περίπτωση που δεν γνωρίζουμε αυτούς τους πρώτους θα πρέπει να διαιρέσουμε το n διαδοχικά με όλους τους φυσικούς που είναι μικρότεροι του ή ίσοι του $\sqrt{n}$ και τότε απαιτούνται $\frac{\sqrt{n}}{2}$ διαιρέσεις! Αυτό σημαίνει οτι αν οι παράγοντες του n είναι μεγάλοι και ίδιου μεγέθους πρώτοι η παραγοντοποίηση με δοκιμές είναι πρακτικά αδύνατη.

4.3.1.2 Ο RHO ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ POLLARD

Ο αλγόριθμος[2] δημοσιεύτηκε από τον John Pollard το 1975 και στηρίζεται στην ιδέα του cycle-finding αλγόριθμου[3] του Floyd και στην παρατήρηση οτι αν αρχίσουμε να επιλέγουμε τυχαίους αριθμούς $a,\ b$ διάφορους μεταξύ τους, τότε μετά από $1,177\sqrt{p}$ επιλογές έχουμε 50% πιθανότητες να ισχύει $a = b(modp)$. Από την τελευταία σχέση προκύπτει οτι $|a-b| = \mu p$, για κάποιο $\mu \in \mathbb{N}$ και έτσι $MK\Delta(|a-b|, n) = p$. Όμως με ποιον τρόπο θα πρέπει να επιλέξουμε τα $a,\ b$ αφού υπάρχουν $(n-1)(n-2)$ ζευγάρια $0 < a,\ b < n$ με $a \neq b$;

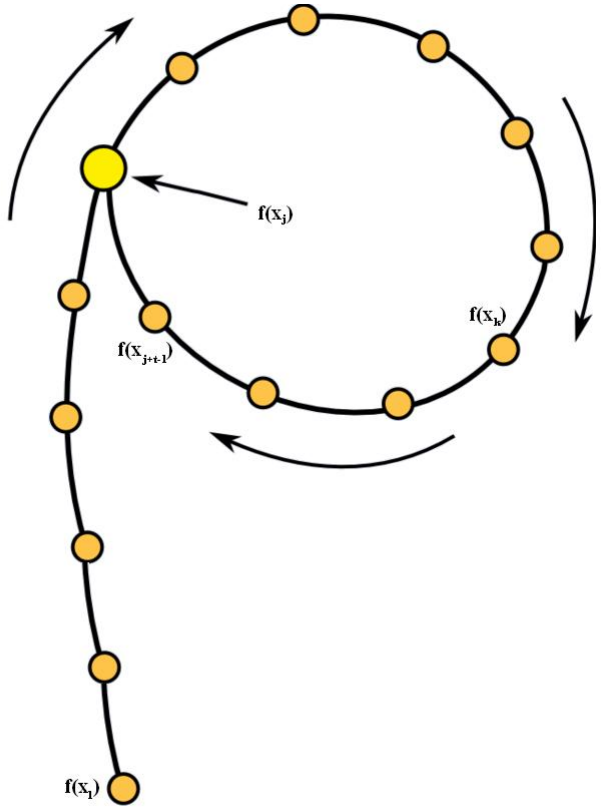
Έστω οτι το $f(x)$ είναι ένα πολυώνυμο το οποίο θα χρησιμοποιήσουμε σε έναν cycle-finding αλγόριθμο, όπου $x_{i+1} = f(x_i)(modn)$. Υποθέτουμε οτι ο κύκλος δημιουργείται στο j-στό βήμα και οτι χρειάζεται t βήματα για να ολοκληρωθεί. Έστω τώρα ο k-στός όρος της ακολουθίας έτσι ώστε $j < k$ $με$ $k = \lambda t$. Προφανώς, αυτός ο όρος βρίσκεται μέσα στον κύκλο και επειδή $t|k$ θα έχουμε οτι $t|2k$. Έτσι θα είναι $x_{2k} = x_k(modp)$ αφού αντιστοιχούν στο ίδιο στοιχείο του κύκλου. Επομένως αν υπολογίζουμε τον $MK\Delta(|x_k - x_{\frac{k}{2}}|, n)$ για κάθε άρτιο k θα βρούμε έναν παράγοντα του n. Το πραγματικό πρόβλημα για τον αλγόριθμο είναι η επιλογή του πολυωνύμου έτσι ώστε να πάρουμε τυχαίους αριθμούς χωρίς να έχουμε πολλές $(modp)$ επιλογές. Η πιο συνηθισμένη επιλογή είναι το $f(x) = x^2 + c,\ c \neq 0, -2(modn)$.

Το 1980, ο Richard Brent δημοσίευσε μία παραλλαγή του αλγορίθμου. Η διαφορά ήταν οτι χρησιμοποίησε έναν cycle-finding αλγόριθμο που είναι πιο γρήγορος από αυτόν του Floyd. Τέλος, για τον υπολογισμό της πολυπλοκότητας πρέπει να λάβουμε υπ' όψην μας το οτι ο αλγόριθμος συνδυάζει τον χρόνο εκτέλεσης και την πιθανότητα που έχει για να βρει έναν παράγοντα του n. Αν το n είναι γινόμενο δύο διαφορετικών και ίσου μεγέθους πρώτων τότε απαιτούνται περίπου $O(n^{\frac{1}{4}}polylog(n))$ βήματα για να εντοπίσει έναν παράγοντα με πιθανότητα 50%[4].

[2] Ο αλγόριθμος πήρε το όνομά του από το ελληνικό γράμμα P που σχηματίζεται αν καταγράψουμε τα στοιχεία της ακολουθίας που προκύπτει (βλ. σχήμα 4.1).

[3] Έχουμε οτι για κάθε συνάρτηση f που απεικονίζει ένα πεπερασμένο σύνολο S στον εαυτό του και για κάθε τιμή $x_0 \in S$, ένας όρος της ακολουθίας $x_0,\ x_1 = f(x_0),\ x_2 = f(x_1),\ ...,\ x_i = f(x_{i-1}),\ ...$ θα πρέπει να εμφανίζεται δύο φορές. Δηλαδή, πρέπει να υπάρχουν $i \neq j$ τέτοια ώστε $x_i = x_j$. Από εκεί και ύστερα η ακολουθία θα επαναλαμβάνεται και έτσι θα δημιουργείται κύκλος. Κάθε αλγόριθμος που ανιχνεύει έναν τέτοιο κύκλο ονομάζεται cycle-finding αλγόριθμος.

[4] Σημειώνουμε οτι η αυστηρή ανάλυση της πολυπλοκότητας του αλγορίθμου είναι ανοιχτό πρόβλημα.



Σχήμα 4.1: Σχηματικά ο rho αλγόριθμος του Pollard

4.3.1.4 Ο ΑΛΓΟΡΙΘΜΟΣ p - 1 ΤΟΥ POLLARD

Ο αλγόριθμος δημοσιεύτηκε από τον Pollard το 1974. Η βασική υπόθεση για τον συγκεκριμένο αλγόριθμο είναι οτι ο αριθμός $p-1$ είναι γινόμενο σχετικά μικρών πρώτων αριθμών. Ο Κώστας θα πρέπει να επιλέξει έναν αριθμό $\alpha > 1$ και ένα φράγμα B. Στη συνέχεια θα πρέπει να υπολογίσει τον αριθμό $b = \alpha^{B!}(modn)$ καθώς και τον $K = MK\Delta(b-1, n)$. Αν ισχύει η υπόθεση, τότε είναι πιθανό $p-1|B!$ $\Leftrightarrow$ $B! = \lambda(p-1)$ και έτσι $b = \alpha^{B!} = 1(modp)$ $\Leftrightarrow$ $b-1 = 0(modp)$ $\Leftrightarrow$ $b-1 = \mu p$. Επομένως θα είναι $1 < K < n$ και έτσι ο Κώστας θα έχει καταφέρει να βρει έναν από τους $p,\ q$, διαφορετικά μπορεί να επιλέξει μία διαφορετική τιμή για το B και να ξαναπροσπαθήσει.

Παρατηρούμε οτι ο χρόνος εκτέλεσης του αλγορίθμου είναι της τάξης του $O(B \cdot log_\alpha B + log_\alpha^2 n)$. Αυτό σημαίνει οτι τα $\alpha,\ B$ πρέπει να επιλεγούν κατά τέτοιο τρόπο ώστε ο αλγόριθμος να εκτελείται όσο πιο γρήγορα γίνεται. Συνήθως για το α ισχύει $\alpha = 2^k$ για κάποιο μικρό φυσικό αριθμό k ενώ το B πρέπει να επιλεγεί έτσι ώστε το $O(B \cdot log_\alpha B)$ να είναι μικρότερο του 10^4. Όμως, από το τελευταίο προκύπτει ένα πολύ μεγάλο εύρος τιμών, το οποίο επιτρέπει πολύ μεγάλα φράγματα $B!$, και επομένως ο Κώστας έχει πολλές πιθανότητες να πετύχει την παραγοντοποίηση σε λογικό χρονικό διάστημα. Για τον λόγο αυτό, η Αλίκη θα πρέπει να επιλέξει

τους αριθμούς $p,\ q$ έτσι ώστε οι $p-1,\ q-1$ να έχουν τουλάχιστον έναν μεγάλο πρώτο παράγοντα.

4.3.1.3 ΤΕΤΡΑΓΩΝΙΚΟ ΚΟΣΚΙΝΟ

Η μέθοδος πηγάζει από την παρακάτω βασική αρχή.

Βασική Αρχή
Έστω n ένας ακέραιος και έστω οτι υπάρχουν ακέραιοι $x,\ y$ με $x^2 = y^2(modn)$ και $x \neq \pm y(modn)$. Τότε ο n είναι σύνθετος και επιπλέον ο $MK\Delta(x-y,n)$ είναι ένας μη τετριμμένος παράγοντας του n.

Απόδειξη:
Έστω $p = MK\Delta(x-y,n)$. Αν $p = n$ τότε θα πρέπει $x = y(modn)$ που είναι άτοπο. Έστω $p = 1$ δηλαδή $n \not| (x-y)$. Όμως είναι $x^2 = y^2(modn) \Leftrightarrow n|(x^2 - y^2) = (x-y)(x+y)$. Επομένως θα πρέπει να είναι $n|(x+y) \Leftrightarrow x = -y(modn)$ που είναι άτοπο. ◇

Αρχικά ο Κώστας θα φτιάξει ένα σύνολο S από μικρούς πρώτους αριθμούς π.χ. $S = \{2,3,5,7,11,13,17,19\}$ το οποίο ονομάζεται **βάση πρώτων**. Στη συνέχεια, θα ψάξει να βρει ακέραιους αριθμούς α της μορφής $[\sqrt{in}+j]$[5] με μικρά $i,\ j$, τέτοιους ώστε $\alpha^2 = \prod_{m\in S}^{k\in\mathbb{N}} m^k$. Σημειώνουμε οτι επειδή $[\sqrt{in}+j]^2 \simeq in + 2j\sqrt{in} + j^2 \simeq 2j\sqrt{in} + j^2(modn)$ και το i είναι μικρό, ο $[\sqrt{in}+j]^2$ είναι μικρός ακέραιος και έτσι έχει καλές πιθανότητες να είναι γινόμενο μικρών πρώτων. Το πλήθος των ακεραίων αυτών θα πρέπει να είναι περίπου ίσο με την πληθικότητα του S. Έπειτα, ο Κώστας θα κατασκευάσει έναν πίνακα οι γραμμές του οποίου θα αντιστοιχούν στους αριθμούς που βρήκε και οι στήλες του στου πρώτους που ανήκουν στο S. Τα στοιχεία του πίνακα θα είναι οι δυναμεις των πρώτων του S τα γινόμενα των οποίων μας δίνουν τα τετράγωνα των αριθμών της παραπάνω μορφής. Για παράδειγμα, αν $n = 3837523$ τότε έχουμε οτι

$$9398^2 = [\sqrt{23n}+4]^2 = 5^5 \cdot 19(mod 3837523),$$

$$8077^2 = [\sqrt{17n}+1]^2 = 2 \cdot 19(mod 3837523),\ \kappa.o.\kappa$$

και ο πίνακας που κατασκευάζεται είναι ο

	2	3	5	7	11	13	17	19
9398	0	0	5	0	0	0	0	1
19095	2	0	1	0	1	1	0	1
1964	0	2	0	0	0	3	0	0
17078	6	2	0	0	1	0	0	0
8077	1	0	0	0	0	0	0	1
3397	5	0	1	0	0	2	0	0
14262	0	0	2	2	0	1	0	0

[5] Με το $[\sqrt{in}+j]$ εννοείται ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος του $\sqrt{in}+j$.

Τέλος, αφού πρώτα ελέγξει ποιες γραμμές πρέπει να προσθέσει έτσι ώστε τα στοιχεία της καινούριας γραμμής που θα προκύψει να είναι $0(mod2)$, ο Κώστας θα πολλαπλασιάσει τους αριθμούς που αντιστοιχούν στις παραπάνω γραμμές και θα πάρει σχέσεις της μορφής $x^2 = y^2(modn)$ με $x \neq \pm y(modn)$ από τις οποίες, λόγω της παραπάνω αρχής, θα βρει έναν παράγοντα του n. Δηλαδή για το παραπάνω παράδειγμα θα έχουμε:

1. $1\eta + 5\eta + 6\eta = (6, 0, 6, 0, 0, 2, 0, 2)$,

2. $1\eta + 2\eta + 3\eta + 4\eta = (6, 4, 6, 0, 2, 4, 0, 2)$,

3. $3\eta + 7\eta = (0, 2, 2, 2, 0, 4, 0, 0)$.

Επομένως, πολλαπλασιάζοντας παίρνουμε

1. $(9398 \cdot 8077 \cdot 3397)^2 = 2^6 \cdot 5^6 \cdot 13^2 \cdot 19^2 = (2^3 \cdot 5^3 \cdot 13 \cdot 19)^2 \Rightarrow$
   $3590523^2 = 247000^2(mod3837523)$
   όμως $3590523 = -247000(mod3837523)$
   και έτσι αυτή η περίπτωση απορρίπτεται,

2. $(9398 \cdot 19095 \cdot 1964 \cdot 17078)^2 = (2^3 \cdot 3^2 \cdot 5^3 \cdot 11 \cdot 13^2 \cdot 19)^2 \Rightarrow$
   $2230387^2 = 2586705^2(mod3837523)$ και
   $MK\Delta(2230387 - 2586705,\ 3837523) = 1093$,

3. $(1964 \cdot 14262)^2 = (3 \cdot 5 \cdot 7 \cdot 13^2)^2 \Rightarrow$
   $1147907^2 = 17745^2(mod3837523)$ και
   $MK\Delta(1147907 - 17745,\ 3837523) = 1093$

και προκύπτει οτι $3837523 = 1093 \cdot 3511$.

4.3.1.4 NUMBER FIELD SIEVE (NFS) SPECIAL NUMBER FIELD SIEVE (SNFS) GENERAL NUMBER FIELD SIEVE (GNFS)

Είναι οι πιο γρήγοροι αλγόριθμοι παραγοντοποίησης στις μέρες μας. Είναι αρκετά πολύπλοκοι και βασίζονται στο τετραγωνικό κόσκινο και στην θεωρία ομάδων. Δεν θα τους αναλύσουμε γιατί η ανάλυση υπερβαίνει τους σκοπούς αυτής της εργασίας.

4.3.2 ΑΛΛΕΣ ΜΕΘΟΔΟΙ ΕΠΙΘΕΣΗΣ

Αν θεωρήσουμε το RSA σαν μία αλυσίδα, τότε κάποιοι από τους κρίκους της είναι η διαδικασία παραγωγής των κλειδιών, ο τρόπος φύλαξης των κλειδιών, ο αλγόριθμος κρυπτογράφησης κ.α. Έτσι, κάποιος που θέλει να επιτεθεί στο σύστημα δεν είναι απαραίτητο να παραγοντοποιήσει το n. Αρκεί να βρει μια αδυναμία

σε κάποιον άλλο κρίκο της αλυσίδας. Παρακάτω παρατίθονται μερικές, τέτοιου, είδους επιθέσεις στο RSA.

4.3.2.1 ΕΠΙΘΕΣΕΙΣ ΧΡΟΝΟΥ

Το 1995 ο Paul Kocker ανακάλυψε μία μέθοδο επίθεσης στο RSA κατά την οποία δεν χρειάζεται η παραγοντοποίηση του n. Έδειξε οτι μπορούμε να βρούμε το d χρονομετρώντας προσεχτικά μια σειρά από διαφορετικές αποκρυπτογραφήσεις.

Έστω οτι ο Κώστας ξέρει με ποια μηχανή και ποιο λογισμικό κάνει η Αλίκη τους υπολογισμούς και έχει την δυνατότητα να την παρακολουθεί να αποκρυπτογραφεί έναν αριθμό κρυπτοκειμένων y. Αν χρονομετρήσει την διαδικασία για κάθε y, και δεδομένου οτι γνωρίζει τα y, μπορεί, όπως φαίνεται παρακάτω, να υπολογίσει το d.

Υποθέτουμε οτι η αποκρυπτογράφηση γίνεται με τον εξής αλγόριθμο[6]:

Αν $d = b_1 \cdot b_2 \cdot ... \cdot b_w$ είναι η δυαδική ανάλυση του b και $y, n \in \mathbb{Z}$ τότε:

1. Ξεκινάμε με $k = 1$ και $s_0 = 1$.
2. Αν $b_k = 1$ τότε $r_k = s_k \cdot y(modn)$, διαφορετικά, αν $b_k = 0$ τότε $r_k = s_k$.
3. Θέτουμε $s_{k+1} = r_k^2(modn)$.
4. Αν $k = w$ τότε ο αλγόριθμος τελειώνει, διαφορετικά, αν $k < w$ τότε θέτουμε $k = k + 1$ και επαναλαμβάνουμε τη διαδικασία από το βήμα (2).

Έτσι προκύπτει οτι το $r_w = y^d(modn)$ είναι το αρχικό κείμενο.

Έστω οτι ο Κώστας γνωρίζει τα κρυπτοκείμενα y_1, y_2, ..., y_n που έχουν σταλεί στην Αλίκη, καθώς και τους χρόνους στους οποίους υπολογίζονται τα $y_i^d(modn)$ και έστω οτι με κάποιον τρόπο[7] έχει μάθει τα πρώτα $k-1$ bits b_1, b_2, ..., b_{k-1} του d. Ακόμη, λόγω του οτι ξέρει τη μηχανή και το λογισμικό που χρησιμοποιεί η Αλίκη, μπορεί να βρει τους χρόνους υπολογισμού των r_1, r_2, ..., r_{k-1}. Άρα, για κάθε y_i ξέρει το t_i που χρειάζεται για να υπολογιστούν τα r_k, ..., r_w.

Αν t_i' είναι ο χρόνος υπολογισμού του $s_k y(modn)$ τότε θέτοντας $t_i'' = t_i - t_i'$ προκύπτουν οι περιπτώσεις:

1. Αν $b_k = 1$ τότε $t_i' > 0$ και το t_i'' είναι ο χρόνος που χρειάζεται για να γίνουν οι υπολογισμοί μετά το $s_k y(modn)$. Άρα, τα ενδεχόμενα $\{t_i'\}$, $\{t_i''\}$ είναι ανεξάρτητα. Συνεπάγεται οτι ισχύει η σχέση

$$V(\{t_i\}) \approx V(\{t_i'\}) + V(\{t_i''\}) > V(\{t_i''\}),$$

[6] Ολόκληρος ο κώδικας σε C (βλ. ΠΑΡΑΡΤΗΜΑ Α [8]).
[7] Υπονοείται επαγωγή

2. Αν $b_k = 0$ τότε δεν θα γίνει ο υπολογισμός του $s_k y(modn)$. Αυτό δείχνει οτι, και σ΄ αυτή την περίπτωση, τα $\{t_i'\}$, $\{t_i''\}$ είναι ανεξάρτητα και έτσι προκύπτει η σχέση

$$V(\{t_i''\}) \approx V(\{t_i\}) + V(\{-t_i'\}) > V(\{t_i\}).$$

Έτσι, αν $V(\{t_i\}) > V(\{t_i''\})$ τότε ο Κώστας θέτει $b_k = 1$ ενώ διαφορετικά θέτει $b_k = 0$ και με αυτό τον τρόπο ανακτά το αρχικό κείμενο m.

Σημειώνουμε οτι η παραπάνω διαδικασία είναι μια απλουστευμένη μορφή της μεθόδου. Στην πραγματικότητα, είναι πιο πολύπλοκη και κάθε φορά εξαρτάται από τα δεδομένα μας.

4.3.2.2 ΕΠΙΘΕΣΗ ΜΙΚΡΟΥ ΕΚΘΕΤΗ

Αν το e είναι μικρό, τότε ο Κώστας μπορεί να χρησιμοποιήσει τη μέθοδο του μικρού εκθέτη. Αυτή η μέθοδος δουλεύει αν το ίδιο μήνυμα m κρυπτογραφηθεί e φορές, επιλέγοντας κάθε φορά ένα από τα δημόσια κλειδιά (e, n_i), όπου οι e, n_i είναι πρώτοι μεταξύ τους και $1 \leq i \leq e$.

Για παράδειγμα, έστω οτι η X τράπεζα στέλνει το ίδιο μήνυμα m σε e πελάτες της χρησιμοποιώντας τα διαφορετικά κλειδιά τους (e, n_i), όπου $1 \leq i \leq e$. Επειδή τα n_i κατασκευάζονται ως γινόμενα μεγάλων πρώτων, είναι σχετικά πρώτοι μεταξύ τους, και έστω οτι τα $c_i = m^e(modn_i)$, όπου $1 \leq i \leq e$ είναι τα κρυπτοκείμενα που προκύπτουν.

Υποθέτουμε οτι, με κάποιον τρόπο, ο Κώστας γνωρίζει αυτά τα c_i. Έτσι, υπολογίζει, από το Κινέζικο θεώρημα υπολοίπων, τον ακέραιο $c = c_i(modn_i)$, όπου $1 \leq i \leq e$ και $0 \leq c \leq \prod_{i=1}^{e} n_i$. Στη συνέχεια, βρίσκει το m ως την e-οστή ρίζα του c στο $\mathbb{Z}$. Σημειώνουμε, οτι είναι απλό να αποδείξουμε οτι $c = m^e$.

Προφανώς, από τα παραπάνω συμπεραίνουμε οτι πρέπει να επιλέξουμε όσο είναι δυνατό πιο μεγάλο e. Επιπλέον, επίσης από τα προηγούμενα, προκύπτει οτι πρέπει να αποφεύγεται η κρυπτογράφηση του ίδιου μηνύματος με τον ίδιο (RSA)-Κρυπτογραφικό Εκθέτη, και αν για κάποιο λόγο, αυτό είναι απαραίτητο, μπορούμε να αλλάξουμε λιγάκι το m διαφοροποιώντας κάποια από τα bits του.

4.3.2.3 ΕΠΙΘΕΣΕΙΣ ΚΟΙΝΟΥ (RSA)-ΣΥΝΤΕΛΕΣΤΗ

Υποθέτουμε οτι μια ομάδα w ανθρώπων χρησιμοποιεί τον ίδιο (RSA)-συντελεστή n αλλά διαφορετικούς (RSA)-κρυπτογραφικούς εκθέτες e_1, e_2, ..., e_w. Παρακάτω αποδεικνύεται οτι το σύστημα αυτό είναι ευάλωτο τόσο και σε έναν εξωτερικό εχθρό, εφ΄ όσον τουλάχιστον δύο από τα μέλη της ομάδας δέχονται το ίδιο κρυπτοκείμενο, όσο και σε κάποιο από τα μέλη της ομάδας το οποίο θα θελήσει να πλαστογραφήσει τις ψηφιακές υπογραφές ή να κλέψει τα μηνύματα κάποιων άλλων μελών της ομάδας.

4.3.2.3.1 ΠΡΩΤΗ ΕΠΙΘΕΣΗ ΚΟΙΝΟΥ (RSA)-ΣΥΝΤΕΛΕΣΤΗ

Έστω τώρα οτι η X τράπεζα στέλνει το μήνυμα m στους πελάτες της Π_1 και Π_2 κρυπτογραφώντας το με τα δημόσια κλειδιά τους (n, e_1) και (n, e_2) αντίστοιχα, όπου $\text{ΜΚΔ}(e_1, e_2) = 1$.Έτσι, οι Π_1 και Π_2 θα λάβουν τα κρυπτοκείμενα $c_1 = m^{e_1}(modn)$ και $c_2 = m^{e_2}(modn)$ αντίστοιχα, και έστω οτι με κάποιο τρόπο ο Κώστας μαθαίνει τα c_1, c_2. Τότε, όπως φαίνεται παρακάτω, είναι πολύ εύκολο για αυτόν να ανακτήσει το m.

Επειδή $\text{ΜΚΔ}(e_1, e_2) = 1$, από τον ευκλείδειο αλγόριθμο, υπάρχουν $\alpha,\ \beta \in \mathbb{Z}$ τέτοια ώστε $\alpha e_1 + \beta e_2 = 1$, το ένα από τα οποία είναι θετικό και το άλλο αρνητικό. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε οτι $\alpha < 0$, τότε ο Κώστας υπολογίζει τον $\text{ΜΚΔ}(c_1, n)$. Αν $\text{ΜΚΔ}(c_1, n) \neq 1$, δηλαδή αν $\text{ΜΚΔ}(c_1, n) = p$ ή $\text{ΜΚΔ}(c_1, n) = q$, τότε είναι τυχερός και παραγοντοποιώντας το n βρίσκει το d_1 ή το d_2 και επομένως και το μήνυμα m. Αν $\text{ΜΚΔ}(c_1, n) = 1$, τότε με τον Ευκλείδειο αλγόριθμο βρίσκει το c_1^{-1} και όπως φαίνεται παρακάτω, εκτελώντας τον υπολογισμό $[c_1^{-1}]^{|\alpha|}[c_2]^{\beta}$ ανακτά το m

$$[c_1^{-1}]^{|\alpha|}[c_2]^{\beta} = [[m^{e_1}]^{-1}]^{|\alpha|}[m^{e_2}]^{\beta} = m^{\alpha e_1 + \beta e_2} = m(modn).$$

Ομοίως αν έχουμε $\beta < 0$. Στο σημείο αυτό παρατηρούμε οτι τα μόνα στοιχεία που χρειάστηκαν για την παραπάνω διαδικασία ήταν τα $n,\ e_1,\ e_2,\ c_1,\ c_2$ τα οποία υποτίθεται οτι είναι δημόσια.

4.3.2.3.2 ΔΕΥΤΕΡΗ ΕΠΙΘΕΣΗ ΚΟΙΝΟΥ (RSA)-ΣΥΝΤΕΛΕΣΤΗ

Έστω οτι οι A και B είναι μέλη της παραπάνω ομάδας, τα (n, e_A) και (n, e_B) είναι τα δημόσια κλειδιά τους και τα d_A και d_B τα ιδιωτικά κλειδιά τους αντίστοιχα. Παρακάτω φαίνεται με ποιο τρόπο μπορεί ο B να βρει το ιδιωτικό κλειδί του A.

Έχουμε $\text{ΜΚΔ}(e_A, \phi(n)) = 1$ και

$$e_B d_B = 1(mod\phi(n)) \ \Leftrightarrow\ e_B d_B - 1 = \kappa\phi(n),\ \kappa \in \mathbb{Z}^+.$$

Παρατηρούμε οτι αν ο B βρει[8] ένα $f \in \mathbb{Z}^+$ με $\text{ΜΚΔ}(f, \phi(n)) = 1$ τέτοιο ώστε

$$\frac{\kappa}{f} \in \mathbb{Z}^+,$$

τότε μπορεί να θέσει

$$M = \frac{e_B d_B - 1}{f} = \frac{\kappa\phi(n)}{f} = \frac{\kappa}{f}\phi(n)$$

και να ισχύει $\text{ΜΚΔ}(M, e_A) = 1$. Άρα προκύπτει οτι $M = \lambda\phi(n),\ \lambda \in \mathbb{Z}^+$ και έτσι

$$MK\Delta(M, e_A) = 1 \Leftrightarrow \alpha M + \beta e_A = 1,\ \gamma\iota\alpha\ \kappa\acute{\alpha}\pi o\iota o\ \beta \in \mathbb{Z}^+$$

[8] Για τον αλγόριθμο εύρεσης του f βλ. παρακάτω σελ. 16 (21).

$$\begin{aligned}
&\Leftrightarrow 1-\beta e_A = \alpha M \\
&\Leftrightarrow 1-\beta e_A = \alpha\lambda\phi(n) \\
&\Leftrightarrow 1-\beta e_A = 0(mod\phi(n)) \\
&\Leftrightarrow \beta e_A = 1(mod\phi(n)) \\
&\Leftrightarrow \beta = d_A(mod\phi(n)) \\
&\Leftrightarrow \beta = \mu\phi(n) + d_A,\ \gamma\iota\alpha\ \kappa\acute{\alpha}\pi o\iota o\ \mu \in \mathbb{Z}^+
\end{aligned}$$

Έτσι, έστω οτι ο Α δέχεται το μήνυμα $c = m^{e_A}(modn)$ το οποίο, με κάποιον τρόπο, μαθαίνει ο Β, ο οποίος ακολουθώντας την παρακάτω διαδικασία υποκλέπτει το μήνυμα

$$c^\beta = (m^{e_a})^\beta = m^{\mu e_A\phi(n)}m^{e_A d_A} = m(modn)^{9}.$$

Ομοίως, αν ο Β υπογράψει ένα μήνυμα m με τον εκθέτη β θα δημιουργήσει την υπογραφή $c = m^\beta(modn)$. Έτσι, αν κάποιος θέλει να βεβαιώσει την υπογραφή οτι η υπογραφή ανήκει στον Α, θα χρησιμοποιήσει τον δημόσιο εκθέτη του Α e_A ως εξής $c^{e_A} = m^{\beta e_A} = m(modn)$. Επομένως ο Β θα έχει πλαστογραφήσει την υπογραφή του Α στο μήνυμα m επιτυχώς. Παρακάτω παρατίθεται ο αλγόριθμος εύρεσης του f.

Αλγόριθμος Εύρεσης Του f

$int\ \ e_A,\ e_B,\ d_B,\ i,\ j,\ k[2],\ l,\ h[i],\ w,\ f$
$i = 0$
$j = 0$
$f = 1$
$for\ (w = 1; w \leq 2; ++w)$
  $k[w] = 0$
$l = e_B * d_B - 1$
$h[i] = MK\Delta(l, e_A)$
$while\ (h[i] \neq 1)$
  $k[1] = h[i]$
  $k[2] = l$
  $l = l/k[1]$
  $i = i + 1$
  $h[i] = MK\Delta(k[2], e_A)$
$for\ (j = 1; j \leq i; ++j)$
  $f = f * h[j]$

Ο παραπάνω αλγόριθμος χρειάζεται $i + 1$ Ευκλείδειους αλγόριθμους ο καθένας από τους αποίους έχει πολυπλοκότητα $O(logn)$ και επιπλέον πολυπλοκότητα $O[log(e_B d_B - 1)] \simeq O(logn)$ για τις υπόλοιπες διαδικασίες.

[9] Είναι $m^{\mu e_A\phi(n)} = 1(modn)$. Για την απόδειξη βλ. την απόδειξη του ισχυρισμού στην §§ 3.3.

4.3.2.4 ΥΠΟΚΛΕΠΤΙΚΟΙ (RSA) ΑΛΓΟΡΙΘΜΟΙ

Οι κρυπτογραφικές συσκευές μπορούν να θεωρηθούν κάτι σαν "μαύρα κουτιά" με την έννοια οτι οι χρήστες τα εμπιστεύονται απόλυτα χωρίς να μπορούν να ελέγξουν το λογισμικό τους. Απ΄ την άλλη οι κατασκευαστές τέτοιων συσκευών κρατάνε κρυφό τον κώδικά τους, προκειμένου να προστατέψουν την πνευματική τους ιδιοκτησία. Πάνω σ΄ αυτή τη λογική μπορούν να στηριχτούν κάποιοι κατασκευαστές και να φτιάξουν κρυπτογραφικές συσκευές που στόχο θα έχουν να υποκλέπτουν πληροφορίες από τους χρήστες τους.

Πράγματι, είναι δυνατό να κατασκευάσουμε κρυπτοσυστήματα που "χάνουν" πληροφορίες έτσι ώστε ο κατασκευαστής να μπορεί να επιτεθεί στον χρήστη ανακτώντας τις πληροφορίες από τα εξαγόμενα του κρυπτοσυστήματος. Τέτοια κρυπτοσυστήματα ονομάζονται **Secretly Embedded Trapdoor with Universal Protection** (SETUP) **Mechanism**. Για αυτά τα κρυπτοσυστήματα απαιτείται από τον κατασκευαστή να δημιουργήσει το λογισμικό του έτσι ώστε να μην μπορεί κανείς να αντιληφθεί τον setup μηχανισμό. Δηλαδή ο setup μηχανισμός πρέπει να σχεδιαστεί έτσι ώστε να δίνει το πλεονέκτημα μόνο στον κατασκευαστή. Κάποιοι από τους πιο γνωστούς setup μηχανισμούς είναι αυτοί των Anderson, Young and Yung [7] καθώς επίσης και οι Hidden Prime Factor, Hidden Small Private Exponent δ , Hidden Small Public Exponent ε [7]. Οι τρεις πρώτοι μηχανισμοί δημιουργούν το δημόσιο κλειδί με τέτοιο τρόπο ώστε να μπορεί να παραγοντοποιηθεί από τον κατασκευαστή, ενώ στους δύο τελευταίους τα p, q επιλέγονται με τέτοιο τρόπο ώστε ο κατασκευαστής να μπορεί να παραγοντοποιήσει το n μόνο από το δημόσιο κλειδί (n, e).

4.4 ΑΣΦΑΛΕΣ *RSA*

Μέχρι στιγμής έχουμε περιγράψει διάφορες μεθόδους επίθεσης στο RSA. Όμως ακόμα και αν η Αλίκη επιλέξει όλες τις παραμέτρους του αλγορίθμου έτσι ώστε όλες οι προαναφερθείσες επιθέσεις, και όχι μόνο αυτές, να είναι αδύνατον να υλοποιηθούν υπάρχουν επιθέσεις που δεν μπορούν να ελεγχτούν αφού δεν έχουν να κάνουν με τα p, q, n, e, d. Μία από αυτές είναι η επίθεση επιλεγμένου κρυπτογραφημένου κειμένου (chosen ciphertext attack). Για να χρησιμοποιήσει ο Κώστας αυτήν τη μέθοδο επίθεσης θα πρέπει με κάποιο τρόπο να αποκτήσει πρόσβαση στον μηχανισμό αποκρυπτογράφησης έτσι ώστε να μπορέσει να κλέψει το αρχικό κείμενο. Στη συνέχεια, ο στόχος του θα είναι, ακόμα και αν δεν έχει ξανά πρόσβαση στον μηχανισμό, να μπορεί να ανακτήσει το αρχικό κείμενο γνωρίζοντας μόνο το κρυπτοκείμενο.

Για να αποφευχθούν αυτού του είδους οι επιθέσεις, το 1991 τα RSA Laboratories[10] σε συνεργασία με επιστήμονες που ασχολούνται με τα κρυπτοσυστημάτα παγκοσμίως θέσπισε τα Public-Key Cryptography Standards (PKCS). Μέχρι στιγμής έχουν εκδοθεί 15 τέτοια πρωτόκολλα. Στο RSA αναφέρονται τα PKCS#1,

[10] Τα RSA Laboratories είναι το κέντρο έρευνας για το RSA. Ιδρύθηκε το 1991 στη θέση του RSA Data Security από του εφευρέτες του αλγορίθμου.

PKCS#2 και PKCS#4. Το PKCS#1 ορίζει τις μαθηματικές ιδιότητες και τη μορφή του ιδιωτικού και του δημοσίου κλειδιού καθώς επίσης και τους αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης. Επιπλέον, δημιουργεί και πιστοποιεί ψηφιακές υπογραφές (βλ. §§5). Το PKCS#2 δεν ισχύει πλέον. Κάλυπτε τον αλγόριθμο κρυπτογράφησης μηνυμάτων αλλά συγχωνεύτηκε με το PKCS#1 με το οποίο συγχωνεύτηκε και το PKCS#4 το οποίο κάλυπτε την σύνταξη των κλειδιών. Τέλος, σημειώνουμε οτι τα RSA Laboratories δέχονται παρατηρήσεις και βελτιώσεις των πρωτοκόλλων τους, με σκοπό την εξέλιξή τους, στην ηλεκτρονική διεύθυνση pkcs-editor@rsa.com.

Σχήμα 4.2: Το λογότυπο των RSA Laboratories

Κεφάλαιο 5

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Όπως έχει ήδη αναφερθεί η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων κάνουν επιτακτική την ανάγκη ασφάλειας στις συναλλαγές. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα που στέλνει από τη μια να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι' αυτό άτομα και από την άλλη να μην αλλοιωθούν κατά την μετάδοσή τους. Επιπλέον, ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει. Ακόμη, σε μία τέτοια συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα. Δηλαδή, να γνωρίζει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ. Χ, είναι όντως από τον κ. Χ και όχι από κάποιον που παριστάνει τον Χ. Η διαδικασία με την οποία πιστοποιείται η ταυτότητα του αποστολέα ονομάζεται **αυθεντικότητα (authentication)**. Τέλος εξίσου σημαντικό είναι και το να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή.

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

5.1 ΟΡΙΣΜΟΣ

Μία ψηφιακή υπογραφή είναι ένα είδος ασύμμετρης κρυπτογραφίας που χρησιμοποιείται για να μιμηθεί τις ασφαλείς ιδιότητες της χειρόγραφης υπογραφής στο χαρτί. Η διαφορά από την ασύμμετρη κρυπτογράφηση, βρίσκεται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Στη διαδικασία της δημιουργίας και αυθεντικότητας της υπογρα-

φής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (hash function).

Ορισμός 5.1.1.

Μια συνάρτηση ονομάζεται **μονόδρομη συνάρτησης κατακερματισμού (one way hash function)** όταν μετατρέπει δεδομένα σε σχετικά μικρούς ακεραίους. ◇

Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου μεγέθους, παράγεται το **αποτύπωμά του (fingerprint)**, το οποίο είναι μία σειρά από bits συγκεκριμένου μεγέθους. Το αποτύπωμα του μηνύματος είναι μία ψηφιακή αναπαράστασή του και είναι μοναδική για κάθε μήνυμα, δηλαδή το αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από το αποτύπωμα που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν το ίδιο αποτύπωμα είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποιο συγκεκριμένο αποτύπωμα και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετικό αποτύπωμα, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί. Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικού αποτυπώματος. Άρα, η ψηφιακή υπογραφή, στην ουσία είναι το κρυπτογραφημένο με το ιδιωτικό κλειδί του αποστολέα αποτύπωμα. Δηλαδή, η ψηφιακή υπογραφή (σε αντίθεση με την ιδιόχειρη υπογραφή) είναι διαφορετική για κάθε μήνυμα!!

Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα. Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος. Τέλος, μία ψηφιακή υπογραφή μπορεί να "πλαστογραφηθεί" όταν με κάποιο τρόπο γίνει γνωστό το ιδιωτικό κλειδί του αποστολέα.

5.2 ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ

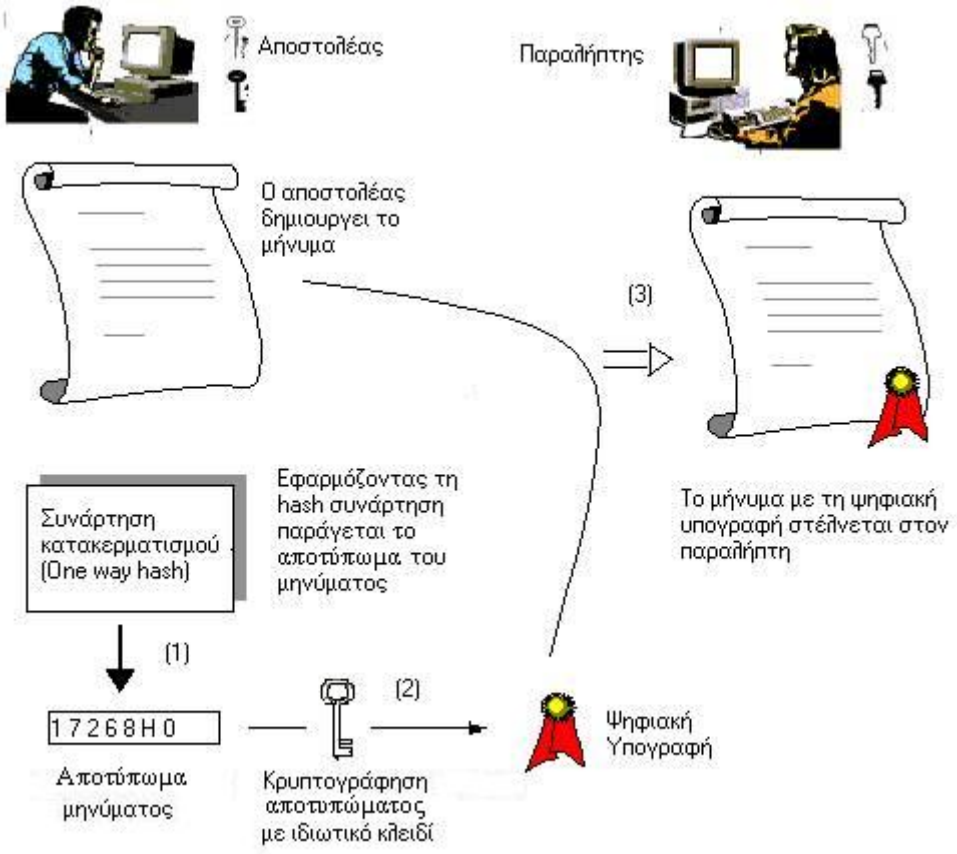
Η χρήση της ψηφιακής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της υπογραφής και την επαλήθευσή της. Παρακάτω, αναφέρονται οι ενέργειες του αποστολέα και του παραλήπτη ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής.

Αποστολέας

1. Ο αποστολέας χρησιμοποιώντας κάποια συνάρτηση κατακερματισμού δημιουργεί το αποτύπωμα του μηνύματος που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων.

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

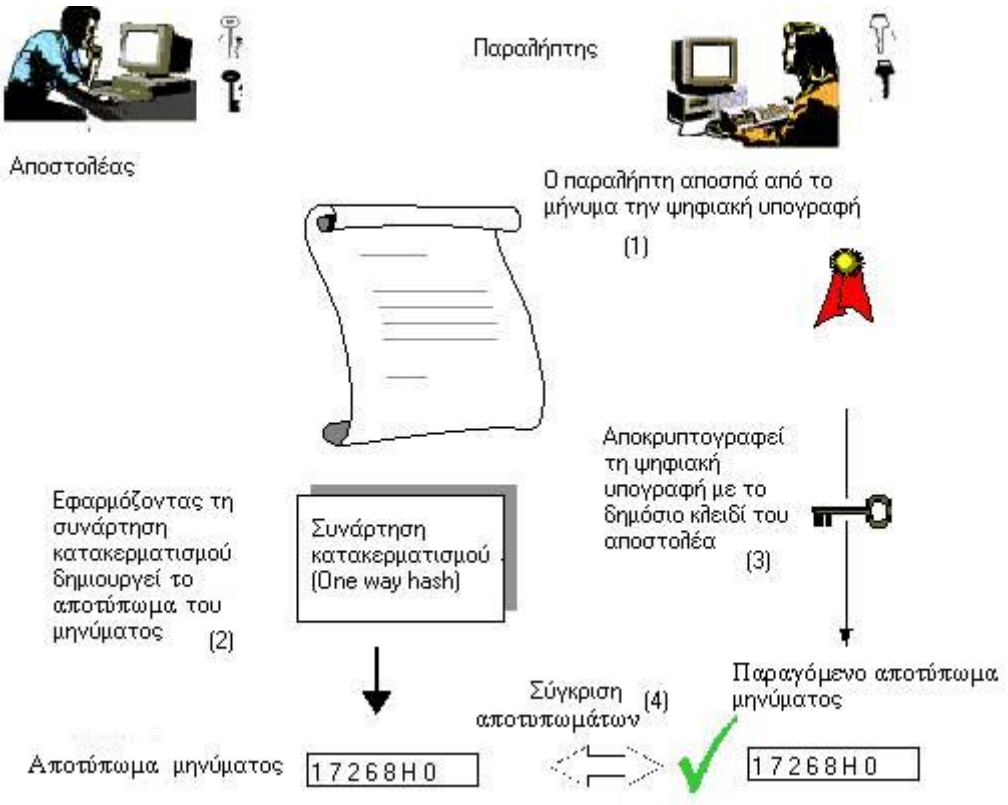
3. Το κρυπτογραφημένο αποτύπωμα, δηλαδή η ψηφιακή υπογραφή, προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου (σημειώνεται ότι ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη).



Σχήμα 5.1: Η δημιουργία της ψηφιακής υπογραφής γίνεται από το ανάλογο λογισμικό στον υπολογιστή του χρήστη.

Παραλήπτης

1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή.
2. Εφαρμόζοντας στο μήνυμα που έλαβε την ίδια συνάρτηση κατακερματισμού, ο παραλήπτης δημιουργεί το αποτύπωμα του μηνύματος.
3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την ψηφιακή υπογραφή.
4. Συγκρίνονται τα δύο αποτυπώματα και αν βρεθούν ίδια, τότε το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, το αποτύπωμα που θα παράγει ο παραλήπτης θα είναι διαφορετικό από το αποτύπωμα που έχει κρυπτογραφηθεί.



Σχήμα 5.2: Η διαδικασία αυθεντικοποίησης.

5.2.1 ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ΜΕ ΧΡΗΣΗ ΤΟΥ *RSA*

Έστω οτι η Αλίκη θέλει να στείλει ένα μήνυμα m στον Bob με τέτοιο τρόπο ώστε αυτός να μπορεί να γνωρίζει με σιγουριά οτι το μήνυμα είναι αυθεντικό και οτι έχει σταλεί από την Αλίκη. Αρχικά δημιουργεί το αποτύπωμα του a μέσω της συνάρτησης κατακερματισμού $f(m) = a$. Στη συνέχεια, δημιουργεί μία ψηφιακή υπογραφή $s = a^d(modn)$, όπου το d είναι το (RSA)-Ιδιωτικό Κλειδί της και στέλνει τα $m,\ s$ στον Bob. Ο Bob, για να πιστοποιήσει την υπογραφή αρχικά υπολογίζει το a μέσω της f. Στη συνέχεια, ξαναυπολογίζει το αποτύπωμα με τη χρήση του δημόσιου κλειδιού της Αλίκης $a = s^e(modn)$. Αν από τους δύο υπολογισμούς προκύψει το ίδιο αποτέλεσμα τότε τόσο το μήνυμα όσο και η υπογραφή είναι αυθεντικά.

Κεφάλαιο 6

RSA ΠΡΟΚΛΗΣΗ

Η RSA πρόκληση παραγοντοποίησης θεσμοθετήθηκε από τα RSA Laboratories στις 18 Μαρτίου του 1991 και είχε στόχο να ενισχύσει την έρευνα στην υπολογιστική θεωρία αριθμών, στην πρακτική δυσκολία παραγοντοποίησης μεγάλων πρώτων και στο σπάσιμο των RSA-κλειδιών. Δημοσιεύτηκε μία λίστα ακεραίων οι οποίοι έχουν ακριβώς δύο πρώτους παράγοντες, οι γνωστοί και ως **RSA-αριθμοί**. Η παραγοντοποίηση κάποιων από αυτούς τους αριθμούς συνοδευόταν από ένα υψηλό χρηματικό έπαθλο. Ο μικρότερος από τους RSA-αριθμούς είχε εκατό ψηφία[1] παραγοντοποιήθηκε μετά από μερικές μέρες αλλά οι περισσότεροι από αυτούς δεν έχουν παραγοντοποιηθεί ακόμα. Ο παραπάνω διαγωνισμός τελείωσε το 2007 με μια ανακοίνωση των RSA Laboratories που σε γενικές γραμμές έλεγε οτι τώρα που έχει φανεί η χρησιμότητα των συμμετρικών κλειδιών και των αλγορίθμων δημοσίου κλειδιού, οι RSA προκλήσεις δεν είναι πλέον ενεργές. Ο τελευταίος από τους RSA-αριθμούς που παραγοντοποιήθηκαν ήταν ο RSA-640 στις 2 Νοεμβρίου του 2005. Στο παράρτημα Β (βλ. 9) φαίνεται ο πίνακας με τους RSA-αριθμούς.

Ένας άλλος διαγωνισμός που θεσμοθετήθηκε από τα RSA Laboratories στις 28 Ιανουαρίου του 1997 ήταν η RSA-ιδιωτικό κλειδί πρόκληση. Για κάθε διαγωνισμό δημοσιευόταν στην ιστοσελίδα της εταιρίας ένα κρυπτοκείμενο και ο στόχος ήταν να βρεθεί το αρχικό κείμενο καθώς και το κλειδί από το οποίο προκύπτει το κρυπτοκείμενο. Και αυτός ο διαγωνισμός είναι πλέον ανενεργός.

[1] Αυτός ήταν και ο λόγος που ονομάστηκε RSA-100.

Κεφάλαιο 7

ΣΥΜΠΕΡΑΣΜΑΤΑ

Από τα παραπάνω συμπεραίνουμε οτι όσο αναπτύσσεται η τεχνολογία τόσο πιο ευάλωτα γίνονται τα κρυπτοσυστήματα και όσο εξελίσσεται η επιστήμη σε συνεργασία με τις νέες τεχνολογίες τόσο πιο έξυπνα και πολύπλοκα κρυπτοσυστήματα δημιουργούνται. Το μέλλον θα δείξει μέχρι σε πιο σημείο θα φτάσει αυτή η κόντρα.

Είδαμε ότι όπως όλα τα επιστημονικά επιτεύγματα, έτσι και η κρυπτογραφία έχει θετικές και αρνητικές εφαρμογές. Στις θετικές συγκαταλέγονται η ασφάλεια της επικοινωνίας και των συναλλαγών. Στις αρνητικές συγκαταλέγεται κυρίως η κατασκοπία, είτε για στρατιωτικούς, είτε για οικονομικούς λόγους. Δυστυχώς, δεν ζούμε στον ιδανικό κόσμο στον οποίο ισχύει ο σεβασμός στα προσωπικά δεδομένα, σε έναν κόσμο όπου η δημοκρατία εφαρμόζεται απόλυτα και οι λαοί έχουν το δικαίωμα να αυτοδιαχειρίζονται. Έτσι, για όσο οι κοινωνίες μας λειτουργούν όπως σήμερα η κρυπτογραφία είναι απαραίτητη για να αισθανόμαστε πιο ασφαλείς. Ας ελπίσουμε οτι κάποια στιγμή στο μέλλον θα μας είναι άχρηστη.

Κεφάλαιο 8

ΠΑΡΑΡΤΗΜΑ Α

ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ ΣΤΗ C:

```
#include <stdio.h>
#include <math.h>
#include <stdlib.h>
int main(void)
{
  int d,w,y,n,p,k,s,r,b[w],e,c;
  double q;
  printf("\n Give me the message y and the number n: \n\n");
  scanf("%d %d", &y, &n);
  printf("\nYou gave me y = %d and n = %d. \n", y, n);
  printf("\n Do you want to continue? Press 1 for yes or 0 for no. \n");
  scanf("%d", &e);
  switch(e)
  {
    case 1:
    {
      printf("\n Give me your secret key d: \n\n");
      scanf("%d", &d);
      printf("\n You gave me d = %d. \n", d);
      printf("\nDo you want to continue? Press1 for yes or 0 for no. \n");
      scanf("%d", &c);
      switch(c)
      {
        case 1:
        {
          p = d;
          w = 0;
          while(p > 0)
          {
            q = p/2;
            p = floor(q);
            w = w + 1;
```

```
        }
        p = d;
        k = w;
        while(p > 0)
        {
          q = p/2;
          b[k] = p − (floor(q) ∗ 2);
          p = floor(q);
          k = k − 1;
        }
        k = 1;
        s = 1;
        while(k <= w)
        {
          if(b[k] == 1)
            r = (s ∗ y) − (floor((s ∗ y)/n)) ∗ n;
          else
            if(b[k] == 0)
              r = s;
          s = (r ∗ r) − (floor((r ∗ r)/n)) ∗ n;
          k = k + 1;
        }
        printf(" \n The original message is the %d(mod %d). \n", r, n);
      }
      break;
      case 0 :
      break;
    }
  }
    break;
  case 0 :
    break;
}
return 0;
}
```

Κεφάλαιο 9

ΠΑΡΑΡΤΗΜΑ Β

RSA-Αριθμοί	**Δεκαδικά Ψηφία**	**Δυαδικά Ψηφία**	**Χρηματικό Έπαθλο**	**Παραγοντοποιήθηκε Στις**	**Παραγοντοποιήθηκε Από**
RSA-100	100	330	-	Απρίλιος 1991	Arjen K. Lestra
RSA-110	110	364	-	Απρίλιος 1992	Arjen K. Lestra και M.S Manasse
RSA-120	120	397	-	Ιούνιος 1993	T. Denny
RSA-129	129	426	$ 100	Απρίλιος 1994	Arjen K. Lestra
RSA-130	130	430	-	10 Απριλίου 1996	Arjen K. Lestra
RSA-140	140	463	-	2 Φεβρουαρίου 1999	Herman J. J. te Riele
RSA-150	150	496	-	16 Απριλίου 2004	Kazumaro Aoki
RSA-155	155	512	-	22 Αυγούστου 1999	Herman J. J. te Riele
RSA-160	160	530	-	1 Απριλίου 2003	Jens Franke Πανεπιστήμιο του Bonn
RSA-170	170	563	-	-	-
RSA-576	174	576	$ 10.000	3 Δεκεμβρίου 2003	Jens Franke Πανεπιστήμιο του Bonn
RSA-180	180	596	-	-	-
RSA-190	190	629	-	-	-
RSA-640	193	640	$ 20.000	2 Νοεμβρίου 2005	Jens Franke Πανεπιστήμιο του Bonn
RSA-200	200	663	-	9 Μαΐου 2005	Jens Franke Πανεπιστήμιο του Bonn
RSA-210	210	696	-	-	-
RSA-704	212	704	$ 30.000	-	-
RSA-220	220	729	-	-	-
RSA-230	230	762	-	-	-
RSA-232	232	768	-	-	-
RSA-768	232	768	$ 50.000	-	-
RSA-240	240	795	-	-	-
RSA-250	250	829	-	-	-
RSA-260	260	862	-	-	-
RSA-270	270	895	-	-	-

RSA-Αριθμοί	**Δεκαδικά Ψηφία**	**Δυαδικά Ψηφία**	**Χρηματικό Έπαθλο**	**Παραγοντοποιήθηκε Στις**	**Παραγοντοποιήθηκε Από**
RSA-896	270	896	$ 75.000	-	-
RSA-280	280	928	-	-	-
RSA-290	290	962	-	-	-
RSA-300	300	995	-	-	-
RSA-309	309	1024	-	-	-
RSA-1024	309	1024	$ 100.000	-	-
RSA-310	310	1028	-	-	-
RSA-320	320	1061	-	-	-
RSA-330	330	1094	-	-	-
RSA-340	340	1128	-	-	-
RSA-350	350	1161	-	-	-
RSA-360	360	1194	-	-	-
RSA-370	370	1227	-	-	-
RSA-380	380	1261	-	-	-
RSA-390	390	1294	-	-	-
RSA-400	400	1327	-	-	-
RSA-410	410	1360	-	-	-
RSA-420	420	1393	-	-	-
RSA-430	430	1427	-	-	-
RSA-440	440	1460	-	-	-
RSA-450	450	1493	-	-	-
RSA-460	460	1526	-	-	-
RSA-1536	463	1536	$ 150.000	-	-
RSA-470	470	1559	-	-	-
RSA-480	480	1593	-	-	-
RSA-490	490	1626	-	-	-
RSA-500	500	1659	-	-	-
RSA-617	617	2048	-	-	-
RSA-2048	617	2048	$ 200.000	-	-

Στον παραπάνω πίνακα φαίνονται οι RSA-αριθμοί, το πλήθος των ψηφίων τους, το χρηματικό έπαθλο για όσο ο διαγωνισμός βρισκόταν σε εξέλιξη καθώς και το πότε και ποιος παραγοντοποίησε τους αριθμούς που παραγοντοποιήθηκαν.

Βιβλιογραφία

[1] *A Further Weakness In The Common Modulus Protocol For The RSA Cryptoalgorithm*, John M. DeLaurentis, 1-06-1984, Cryptologia, Taylor & Fransis.

[2] *A "Weak" Privacy Protocol Using The RSA Crypto Algorithm*, Gustavus J. Simmons, 1-03-1983, Cryptologia, Taylor & Fransis.

[3] *An Introduction To Cryptography, Richard A. Mollin, 2001, Chapman & Hall.*

[4] *Introduction to Cryptography 2nd edition, Johannes A. Buckmann, 2004, Springer Verlag NY, LLC.*

[5] *Introduction to Cryptography with Coding Theory, Wade Trappe, Lawrence C. Washington, 2002, Prentice-Hall.*

[6] *Introduction To Power Analisis*, Elisabeth Oswalt.

[7] *Ten Years Of RSA Cheating Cryptosystems*, Jihoon Cho.

[8] *Μαθηματικά και Κρυπτογραφία: Τρόποι Επίθεσης Σε Δημοφιλή Κρυπτοσυστήματα*, Δημήτρης Διώχνος, Εργασία για το Μεταπτυχιακό Πρόγραμμα Λογικής και Αλγορίθμων, Ιούλιος 2005.

[9] *Πλεξίδες και Κρυπτογραφία*, Χρήστος Τζέτζιας, Διπλωματική Εργασία για το Μεταπτυχιακό Πρόγραμμα Λογικής και Αλγορίθμων, 2003.

[10] *Σημειώσεις του Ε. Κρανάκη για το Μάθημα Network Security and Cryptography του Μεταπτυχιακού Προγράμματος Λογικής και Αλγορίθμων που δόθηκε το εαρινό εξάμηνο του Ακαδημαϊκού Έτους 2005-2006.*

Links

[1] http://en.wikipedia.org/wiki

[2] http://members.tripod.com/irish_ronan/rsa/attacks.html

[3] http://www.csh.rit.edu/~pat/math/quickies/rho/

[4] http://www.eett.gr/gr_pages/telec/eSign/IntroEsign.htm

[5] http://web.ew.usna.adu/~wdj/book/node45.html

[6] http://www.maths.mq.edu.au/~steffen/old/PCry/report/node8.html

[7] http://www.rsa.com

Κεφάλαιο 10

ΕΥΡΕΤΗΡΙΟ ΟΡΩΝ

A

B

Δ

E

K

M

N

O

Π

P

Σ

T

Υ