ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Περιπτώσεις ψηφιακών υπογραφών στην ασύμμετρη κρυπτογραφία

Παναγιώτα Λαμπροπούλου

Επιβλέπων : **Αλέξανδρος Παπαϊωάννου**
Αναπληρωτής Καθηγητής Ε.Μ.Π.

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Περιπτώσεις ψηφιακών υπογραφών στην ασύμμετρη κρυπτογραφία

Παναγιώτα Λαμπροπούλου

Εξεταστική επιτροπή :

1. Α. Παπαϊωάννου, Αναπληρωτής Καθηγητής Ε.Μ.Π. (Επιβλέπων της Δ.Ε.)
2. Π. Στεφανέας, Λέκτορας Ε.Μ.Π.
3. Π. Ψαρράκος, Αναπληρωτής Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2012

Πρόλογος

Η κρυπτογραφία χρησιμοποιείται για πλήθος εφαρμογών, όμως ο βασικός της σκοπός είναι η παραποίηση μιας πληροφορίας έτσι ώστε να μπορεί να γίνει αντιληπτή μόνο από αυτόν στον οποίο απευθύνεται. Οι ψηφιακές υπογραφές είναι μία από τις πιο χρήσιμες ανακαλύψεις της κρυπτογραφίας. Είναι μία μέθοδος να υπογράφουμε ένα μήνυμα που είναι αποθηκευμένο σε ηλεκτρονική μορφή. Το 1978 παρουσιάζεται για πρώτη φορά το RSA, το πρώτο σχήμα που παράγει ψηφιακές υπογραφές. Από τότε μέχρι σήμερα έχουν δημιουργηθεί πάρα πολλά σχήματα.

Η παρούσα διπλωματική εργασία είναι χωρισμένη σε έξι κεφάλαια. Στο πρώτο κεφάλαιο γίνεται μια γενική παρουσίαση της επιστήμης της Κρυπτογραφίας και παρουσιάζονται βασικά στοιχεία από τη θεωρία αριθμών και την άλγεβρα. Το δεύτερο κεφάλαιο είναι μία εισαγωγή στις βασικές έννοιες των ψηφιακών υπογραφών. Στο τρίτο κεφάλαιο παρουσιάζεται το κρυπτοσύστημα και το σχήμα ψηφιακής υπογραφής RSA. Στο τέταρτο κεφάλαιο παρουσιάζονται εφτά σχήματα υπογραφών. Στο πέμπτο κεφάλαιο περιγράφονται τέσσερα σχήματα υπογραφών μιας χρήσης. Τέλος στο έκτο και τελευταίο κεφάλαιο γίνεται αναφορά σε τυφλά σχήματα υπογραφών, αδιαμφισβήτητα σχήματα υπογραφών και σχήματα υπογραφών εύρεσης πλαστογράφησης. Η παρουσίαση κάθε σχήματος περιλαμβάνει την πλήρη περιγραφή των τριών αλγορίθμων που το συνθέτουν, σχόλια για την ασφάλεια του σχήματος και παράδειγμα με μικρές παραμέτρους ώστε να γίνει πιο κατανοητός ο τρόπος λειτουργίας του.

Abstract

Cryptography has many applications, however its basic purpose is information modification such that it can be perceptible only by the one to whom is addressed. The most useful cryptography's discoveries are digital signatures. Digital signature is a method which can be used in order to sign a message which is in an electronic form. The RSA scheme, the first scheme that produces digital signatures, became known in 1978. Since then many schemes have been developed by the scientific community.

This thesis is composed of six chapters. The first chapter presents an overview of cryptography and includes some main theoretical prerequisites from number theory and algebra. The second chapter is an introduction to the main notions of digital signatures. The third chapter describes the RSA cryptosystem and RSA signature scheme. At the fourth chapter, seven digital signature schemes are presented. At the fifth chapter, four one-time digital signature schemes are presented. Finally at the last chapter blind signature schemes, undeniable signature schemes and fail-stop signature schemes are described. The presentation of each scheme includes the full description of their three core algorithms, some comments on its safety, and also an example.

Ευχαριστίες

Ευχαριστώ πάρα πολύ τον επιβλέπων της διπλωματικής μου εργασίας και αναπληρωτή καθηγητή του Ε.Μ.Π. κύριο **Αλέξανδρο Παπαϊωάννου**, που αγαπά, μορφώνει και στηρίζει τους φοιτητές του, για τη συνεχόμενη βοήθεια και καθοδήγησή του. Επίσης ευχαριστώ πολύ τις φίλες και συναδέλφους μου Δήμητρα Λάγιου και Ρέα Αθανασοπούλου για την υποστήριξή τους.

Περιεχόμενα

Αφιερωμένο στη γιαγιά μου
και στον παππού μου

Κεφάλαιο 1

ΕΙΣΑΓΩΓΗ

1.1 Γενικά

1.1.1 Ιστορική αναδρομή κρυπτογραφίας

Η κρυπτογραφία είχε αρχικά μορφή τέχνης που τα μυστικά της γνώριζαν λίγοι. Η ιστορία της ξεκινάει περίπου το 4000 π.Χ. στην αρχαία Αίγυπτο που γραμματείς, όταν ήθελαν να αναγράψουν ένα κείμενο στους αφέντες τους, άλλαζαν κάποιες λέξεις ή φράσεις με παρόμοιες μεταβάλλοντας έτσι το αρχικό κείμενο. Περνά αργότερα στην Ελλάδα με την πρώτη στρατιωτική χρήση της κρυπτογραφίας που αποδίδεται στους Σπαρτιάτες όπου γύρω στον 5ο π.Χ. αιώνα εφηύραν την «σκυτάλη», την πρώτη κρυπτογραφική συσκευή, στην οποία χρησιμοποίησαν για την κρυπτογράφηση τη μέθοδο της αντικατάστασης. Επίσης έχουμε αναφορές της κρυπτογραφίας στον ιστορικό Πολύβιο ο οποίος ανέπτυξε ένα σύστημα που αντιστοιχεί τα γράμματα της αλφαβήτου σε αριθμούς. Αργότερα ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του με μηνύματα που δεν θα ήταν δυνατόν να διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος της αλφαβήτου με κάποιο άλλο όχι όμως τυχαία επιλεγμένο αλλά με απόσταση ορισμένων θέσεων.

Η κρυπτογραφία πέρασε στο πεδίο της επιστήμης όταν άρχισε να χρησιμοποιείται για στρατιωτικούς σκοπούς και για απόκρυψη σημαντικών πληροφοριών. Κρυπτογράφοι και κρυπταναλυτές επιδόθηκαν σε έναν έντονο συναγωνισμό με αποτέλεσμα κάθε πρόοδος της κρυπτογραφίας να συνοδεύεται από μια αντίστοιχη πρόοδο κρυπτανάλυσης. Την περίοδο ποτοαπαγόρευσης στην Αμερική, περίπου το 1920, το FBI χρησιμοποίησε τεχνικές κρυπτογραφίας για να αποκρύπτει από τη μαφία τους τόπους παράδοσης φορτίων ποτών. Στο δεύτερο Παγκόσμιο Πόλεμο οι Γερμανοί

έκαναν εκτενή χρήση ενός συστήματος γνωστού ως Enigma. Ο Marian Rejewski, στην Πολωνία , προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασιζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους. Η προσπάθεια αυτή συνεχίστηκε από τον Alan Turing, τον Gordon Welchman και από πολλούς άλλους στο κέντρο της Βρετανικής Υπηρεσίας απο/κρυπτογράφησης και οδήγησε σε συνεχείς αποκρυπτογραφήσεις των διαφόρων παραλλαγών του Enigma.

Από το 1960 και μετά η κρυπτογραφία γνώρισε μεγάλη ανάπτυξη λόγω της ραγδαίας ανάπτυξης των υπολογιστών αλλά και των τηλεπικοινωνιών. Στα μέσα της δεκαετίας του '70 έγιναν δύο σημαντικές δημόσιες πρόοδοι. Πρώτα ήταν η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES (Data Encryption Standard). Το προτεινόμενο DES υποβλήθηκε από την IBM, στην πρόσκληση του Εθνικού Γραφείου Προτύπων των Η.Π.Α. (σημερινό NIST) σε μια προσπάθεια να αναπτυχθούν ασφαλείς ηλεκτρονικές εγκαταστάσεις επικοινωνίας για επιχειρήσεις όπως τράπεζες και άλλες μεγάλες οικονομικές οργανώσεις.

Η πιο εντυπωσιακή ανάπτυξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν ο Diffie και ο Hellman δημοσίευσαν το “New directions in cryptography”. Αυτή η επιστημονική δημοσίευση εισήγαγε την επαναστατική έννοια της κρυπτογραφίας δημοσίου κλειδιού. Παρόλο που οι συγγραφείς δεν έκαναν πρακτική εφαρμογή του σχήματος που πρότειναν η αρχή είχε γίνει και το θέμα έτυχε μεγάλου ενδιαφέροντος από την κρυπτογραφική κοινότητα.

Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική εφαρμογή του προταθέντος σχήματος. Ήταν το λεγόμενο σχήμα RSA και βασιζόταν σε ένα απλό αλλά δύσκολο μαθηματικό πρόβλημα, αυτό της δυσκολίας παραγοντοποίησης

μεγάλων ακεραίων αριθμών. Όπως ήταν φυσικό οι κρυπταναλυτές άρχισαν να ψάχνουν πιο αποτελεσματικούς τρόπους παραγοντοποίησης αλλά παρά τις μεγάλες προόδους τους, κυρίως τη δεκαετία του ’80 το RSA παρέμενει ακόμα ασφαλές!

Σήμερα η κρυπτογραφία έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών αφού σε νομικό και σε κοινωνικό επίπεδο τίθεται θέμα προστασίας του απορρήτου σ’ όλες τις εκδοχές δικτυακής συναλλαγής. Η εξέλιξη της κρυπτογραφίας καθιστά πλέον αξιόπιστη τη μεταφορά της πληροφορίας για διάφορους λειτουργικούς σκοπούς όπως είναι η κινητή τηλεφωνία, οι συναλλαγές με πιστωτική κάρτα κυρίως εντός Διαδικτύου, το e-mail και άλλα πολλά.

1.1.2 Έννοιες και βασική ορολογία

Η κρυπτογραφία είναι η επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και την αποκωδικοποίηση των δεδομένων. Είναι δηλαδή το σύνολο των μαθηματικων τεχνικών που στοχεύουν στην εξασφάλιση θεμάτων που άπτονται της ασφάλειας μετάδοσης της πληροφορίας, όπως εμπιστευτικότητα, ακεραιότητα δεδομένων, πιστοποίηση ταυτότητας του αποστολέα και διασφάλιση του αδιάβλητου της πληροφορίας. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο σε όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Η αρχική μορφή του μηνύματος, αποτελεί το **απλό κείμενο** (plaintext), ενώ το κρυπτογραφημένο κείμενο αποτελεί το **κρυπτοκείμενο** (ciphertext). Ο μετασχηματισμός του απλού κειμένου σε κρυπτοκείμενο ονομάζεται **κρυπτογράφηση** (encryption) ενώ ο μετασχηματισμός του κρυπτοκειμένου σε απλό κείμενο ονομάζεται **αποκρυπτογράφηση** (decryption). Οι διαδικασίες της κρυπτογράφησης και της αποκρυπτογράφησης υλοποιούνται με αλγόριθμο κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα. Οι δύο αυτοί αλγόριθμοι συνιστούν τον **κρυπταλγόριθμο** (cipher). Η διαδικασία κρυπτογράφησης (και αποκρυπτογράφησης) απαιτεί μια επιπλέον ποσότητα πληροφορίας που την ονομάζουμε **κλειδί** (key). Η ύπαρξη του κλειδιού είναι και η ειδοποιός διαφορά της κρυπτογράφησης με την **κωδικοποίηση** (encoding). Αναλυτικότερα, η

κρυπτογράφηση και αποκρυπτογράφηση ενός κειμένου μπορεί να πραγματοποιηθεί με επιτυχία μόνον από τον κάτοχο του σωστού κλειδιού. Ο όρος «κλειδί» είναι πολύ εύστοχος καθότι το κλειδί παραπέμπει σε κάτι μυστικό, που έχει συγκεκριμένους κατόχους, και είναι αναγκαίο για να κλειδώνει και ξεκλειδώνει κλειδαριές. Έτσι λοιπόν ένας αλγόριθμος κρυπτογράφησης μπορεί να παρομοιαστεί με μια κλειδαριά, η οποία χρησιμοποιείται για να φυλάξει ένα μήνυμα. Όποιος έχει το κλειδί μπορεί χωρίς μεγάλη προσπάθεια να ανοίξει την κλειδαριά και να διαβάσει το μήνυμα.

Η περιγραφή των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης αποτελούν το **κρυπτοσύστημα**. Ο αντίπαλος ενός κρυπτοσυστήματος θα επικεντρωθεί στο να ανακαλύψει το σωστό κλειδί, δηλαδή το κλειδί εκείνο με το οποίο θα μπορέσει να ανοίξει την κλειδαριά και να διαβάσει το μήνυμα.

Κρυπτανάλυση είναι η επιστήμη που ασχολείται με την αποκρυπτογράφηση του κρυπτοκειμένου χωρίς την γνώση του κλειδιού.

Εναλλακτικά, ο αντίπαλος μπορεί να ενδιαφέρεται περισσότερο στο να ανακαλύψει το κλειδί, για να μπορεί να αποκρυπτογραφήσει όλα τα μηνύματα που ενδεχομένως στάλθηκαν με τη χρήση του κλειδιού αυτού. Ο στόχος όμως παραμένει στο να ανακτήσει την πληροφορία που βρίσκεται κρυμμένη στο κρυπτοκείμενο. Σε αυτό το σημείο εύλογα γεννιέται η απορία του πώς είναι δυνατό να μπορούμε να ανακτήσουμε απευθείας το απλό κείμενο από το κρυπτοκείμενο, χωρίς να ανακαλύψουμε πρώτα το κλειδί. Αυτό το θέμα είναι γνωστό ως **αποτυχία πρωτοκόλλου** (protocol failure) όπου ο αντίπαλος «ξεγελάει» ένα κρυπτοσύστημα στο να εκτελέσει την αποκρυπτογράφηση σε ένα κρυπτοκείμενο το οποίο δεν του ανήκει. Ο αντίπαλος μπορεί να μη γνωρίζει το κλειδί, το οποίο μπορεί να είναι πολύ καλά θαμμένο μέσα στο σύστημα, αλλά μπορεί να εκμεταλλευτεί την πρόσβασή του σε αυτό και να επιτύχει την αποκρυπτογράφηση.

1.1.3 Είδη Κρυπτογραφίας

Συμμετρική Κρυπτογραφία (Secret Key Cryptography)

Στη συμμετρική κρυπτογραφία χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Ο αποστολέας χρησιμοποιεί το

μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης για να το αποκρυπτογραφήσει. Η απαίτηση του κρυπτοσυστήματος να χρησιμοποιείται το ίδιο κλειδί στην κρυπτογράφηση και αποκρυπτογράφηση, προϋποθέτει ότι ο αποστολέας και ο παραλήπτης έχουν κάποιον ασφαλή τρόπο να μοιραστούν αυτήν την πληροφορία. Το κλειδί δημιουργείται και βρίσκεται αρχικά στον αποστολέα καθώς η κρυπτογράφηση προηγείται της αποκρυπτογράφησης. Επομένως, ο αποστολέας θα πρέπει να στείλει το κλειδί στον παραλήπτη, χωρίς να πέσει στα χέρια του αντιπάλου. Γιατί όμως να μπούμε στη διαδικασία κρυπτογραφίας εφόσον μπορούμε να έχουμε ασφαλές κανάλι; Θα μπορούσαμε να στέλναμε απ' ευθείας το κείμενο και δεν θα ήταν αναγκαία η κρυπτογράφησή του. Όπως θα διαπιστώσουμε, η κρυπτογραφία στην πραγματικότητα δεν λύνει τα προβλήματα, αλλά απλώς τα μετασχηματίζει σε μορφές τις οποίες μπορούμε πιο εύκολα να ελέγξουμε. Τα ασφαλή κανάλια δεν είναι πάντοτε διαθέσιμα, απαιτούν σχετικά μεγάλη προσπάθεια για να δημιουργηθούν και η μορφή τους είναι ανάλογα με την περίσταση. Για παράδειγμα ο αποστολέας και ο παραλήπτης μπορεί να είχαν συναντηθεί κάποια στιγμή στο παρελθόν και να είχαν μοιραστεί το κλειδί με την προοπτική να το χρησιμοποιήσουν σε μελλοντική επικοινωνία. Το ασφαλές κανάλι ήταν η επαφή τους χωρίς τη μεσολάβηση κάποιου τρίτου (μιας τηλεφωνικής εταιρείας για παράδειγμα). Ένας άλλος τρόπος για τη δημιουργία ασφαλούς καναλιού, είναι να τεμαχιστεί το κλειδί και τα τεμάχια να διαβιβασθούν μέσω διαφορετικών καναλιών, όπως τηλεφωνικά, ταχυδρομικά, ή με κούριερ, έτσι ώστε ο αντίπαλος να μην είναι σε θέση να μπορεί να τα παρακολουθεί όλα και να συλλέξει όλα τα τεμάχια για να χτίσει το κλειδί. Επίσης το κλειδί είναι πολύ μικρότερο σε μέγεθος από το απλό κείμενο και επιπλέον μπορεί να επαναχρησιμοποιηθεί για την κρυπτογράφηση πολλών κειμένων. Αυτό βέβαια είναι και μια πολύ σημαντική κρυπτογραφική αδυναμία που μπορεί να εκμεταλλευτεί ο αντίπαλος και να σπάσει το κρυπτοσύστημα.

Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση αλλά και για πιστοποίηση ταυτότητας. Μια τεχνική είναι η MAC (Message Authentication Code).

Στα πλεονεκτήματα της συμμετρικής κρυπτογραφίας συγκαταλέγονται οι υψηλές ταχύτητες κρυπτογράφησης και αποκρυπτογράφησης καθώς επίσης και οι μικρές απαιτήσεις της σε μνήμη και υπολογιστική ισχύ. Έτσι κάνει δυνατή την εφαρμογή της

σε περιβάλλοντα όπως αυτά ενός κινητού τηλεφώνου ή μιας έξυπνης κάρτας. Επίσης το μέγεθος του κρυπτογραφήματος είναι αρκετά μικρότερο από αυτό του αρχικού κειμένου.

Η ανάγκη της ανταλλαγής του συμμετρικού κλειδιού μεταξύ αποστολέα και παραλήπτη είναι ένας από τους σημαντικότερους περιορισμούς της συμμετρικής κρυπτογραφίας. Η ασφάλειά της βασίζεται αποκλειστικά στο γεγονός ότι ο αποστολέας και ο παραλήπτης μοιράζονται το συμμετρικό κλειδί πριν από την αποστολή του μηνύματος. Έτσι κρίνεται απαραίτητη η επίτευξη μιας ασφαλούς ζεύξης για τη μεταφορά του συμμετρικού κλειδιού. Η διαδικασία της ασφαλούς ανταλλαγής του συμμετρικού κλειδιού γίνεται ακόμα δυσκολότερη όταν ο αποστολέας και ο παραλήπτης είναι άγνωστοι μεταξύ τους. Σε αυτή την περίπτωση προκύπτει η ανάγκη πιστοποίησης της ταυτότητας κάθε οντότητας ώστε να αποφευχθεί η διαβίβαση του κλειδιού σε κάποια μη εξουσιοδοτημένη οντότητα. Συνήθως στη συμμετρική κρυπτογραφία η μεταφορά του κλειδιού γίνεται μέσω μιας φυσικής ζεύξης είτε μέσω μιας έμπιστης τρίτης οντότητας.

Ένας ακόμη σημαντικός περιορισμός αφορά στη δυσκολία της κλιμάκωσης της μεθόδου. Καθώς το πλήθος των χρηστών που θέλουν να επικοινωνήσουν μεταξύ τους μεγαλώνει, μεγαλώνει και το πλήθος των κλειδιών που θα χρησιμοποιηθούν για κάθε επιμέρους επικοινωνία. Για την επίτευξη επικοινωνίας n χρηστών απαιτούνται $\frac{n^2}{2}$ μοναδικά συμμετρικά κλειδιά, συμπεριλαμβανομένου και του κλειδιού που έχει κάθε χρήστης για τον εαυτό του. Τα προβλήματα της διαχείρισης των κλειδιών γίνονται ακόμα μεγαλύτερα γιατί κάθε κλειδί θα πρέπει περιοδικά να αντικαθίσταται από κάποιο καινούριο με σκοπό τη μείωση των δεδομένων που κρυπτογραφούνται με το ίδιο κλειδί.

Γνωστοί αλγόριθμοι συμμετρικής κρυπτογραφίας είναι ο DES (Data Encryption Standard) και οι δυο παραλλαγές του 3DES και DESX, ο AES (Advanced Encryption Standard), ο IDEA, οι RC2, RC4, RC5 και ο Blowfish.

Ασύμμετρη Κρυπτογραφία ή Κρυπτογραφία Δημοσίου Κλειδιού (Public Key Cryptography)

Στα μέσα της δεκαετίας του ’70 οι Whitfield Diffie και Martin Hellman πρότειναν μια νέα τεχνική για τον περιορισμό των προβλημάτων της συμμετρικής κρυπτογραφίας. Η τεχνική αυτή, γνωστή ως κρυπτογραφία δημοσίου κλειδιού ή ασύμμετρη κρυπτογραφία βασίζεται στην ύπαρξη ενός ζεύγους κλειδιών. Το κλειδί για την κρυπτογράφηση ονομάζεται **δημόσιο κλειδί** γιατί μπορεί να διατεθεί ελεύθερα χωρίς να απαιτείται ασφαλές κανάλι για τη μετάδοσή του. Το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση είναι το **ιδιωτικό κλειδί** και παραμένει υπό την κατοχή του παραλήπτη. Το δημόσιο κλειδί δεν μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση διότι εάν χρησιμοποιηθεί το αποτέλεσμα δεν θα είναι το αρχικό απλό κείμενο. Το ιδιωτικό κλειδί είναι γνωστό μόνον στον παραλήπτη του μηνύματος. Έτσι σε αντίθεση με τα συμμετρικά κρυπτοσυστήματα, τα κλειδιά δημιουργούνται στον παραλήπτη, ο οποίος είναι ο μόνος που μπορεί να παράγει και να συσχετίσει ένα ζευγάρι ασύμμετρων κλειδιών.

Έτσι το μοντέλο επικοινωνίας ενός ασύμμετρου κρυπτοσυστήματος δεν περιλαμβάνει ασφαλές κανάλι, αλλά η μετάδοση του μηνύματος περιλαμβάνει τα ακόλουθα στάδια:

1. Ο αποστολέας ζητάει από τον παραλήπτη το δημόσιο κλειδί K_e.
2. Ο παραλήπτης στέλνει το δημόσιο κλειδί μέσω του μη ασφαλούς καναλιού επικοινωνίας.
3. Ο αποστολέας κρυπτογραφεί το μήνυμα P με το δημόσιο κλειδί του παραλήπτη και στέλνει το κρυπτοκείμενο C στον παραλήπτη.
4. Ο παραλήπτης αποκρυπτογραφεί το κρυπτοκείμενο χρησιμοποιώντας το ιδιωτικό κλειδί K_d.

Μια ενδιαφέρουσα και χρήσιμη ιδιότητα του ασύμμετρου κρυπτοσυστήματος είναι ότι ένα ζευγάρι ιδιωτικού/δημόσιου κλειδιού μπορεί να χρησιμοποιηθεί αντίστροφα, δηλαδή το ιδιωτικό κλειδί μπορεί να κρυπτογραφήσει ένα απλό κείμενο, και το δημόσιο κλειδί να αποκρυπτογραφήσει το αντίστοιχο κρυπτοκείμενο. Αυτή η ιδιότητα είναι η αρχή λειτουργίας της **ψηφιακής υπογραφής**. Ο κάτοχος του ιδιωτικού κλειδιού είναι ο μόνος που μπορεί να κρυπτογραφήσει ένα κείμενο με το

ιδιωτικό του κλειδί, ενώ οποιοσδήποτε μπορεί να το αποκρυπτογραφήσει. Εάν το κρυπτογραφημένο κείμενο συνοδεύεται από το απλό κείμενο, τότε ο παραλήπτης μπορεί να συγκρίνει το απλό κείμενο με το αποτέλεσμα της αποκρυπτογράφησης και να επαληθεύσει ότι το κείμενο προέρχεται από τον κάτοχο του ιδιωτικού κλειδιού.

Για μια ακόμη φορά η κρυπτογραφία δεν έχει λύσει το πρόβλημα, αλλά το έχει μετασχηματίσει. Πλέον, δεν τίθεται πρόβλημα της διανομής του κλειδιού, αλλά υπάρχει το πρόβλημα του «ενδιάμεσου ατόμου» (man in the middle). Εφόσον ο αποστολέας και ο παραλήπτης επικοινωνούν με ψηφιακά μέσα στέλνοντας μόνο μηνύματα, ο αντίπαλος έχει τη δυνατότητα στο μοντέλο του ασύμμετρου κρυπτοσυστήματος να συμμετέχει ενεργά, προκειμένου να αποκρυπτογραφήσει το μήνυμα. Ο αντίπαλος παρεμβάλλεται μεταξύ του αποστολέα και του αποδέκτη και αναλαμβάνει να δρομολογεί τα μηνύματα που ανταλλάσσονται μεταξύ του αποστολέα και του αποδέκτη. Έτσι, κατά την περίοδο της αποστολής του δημόσιου κλειδιού, ο αντίπαλος αντικαθιστά το δημόσιο κλειδί του παραλήπτη K_e με το δικό του δημόσιο κλειδί A_e, εφόσον γνωρίζει και το ιδιωτικό του κλειδί A_d. Ο αποστολέας πιστεύει ότι το δημόσιο κλειδί που έλαβε είναι του παραλήπτη του μηνύματος, ενώ το κλειδί αυτό στην πραγματικότητα είναι του αντιπάλου. Συνεπώς, το μήνυμα κρυπτογραφείται (C) με το δημόσιο κλειδί του αντιπάλου. Στη συνέχεια, ο αντίπαλος αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί, το κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη και μεταβιβάζει το νέο κρυπτοκείμενο (C′) στον παραλήπτη, με αποτέλεσμα η παρεμβολή του να μη γίνει αντιληπτή από κανέναν από τους δύο συμμετάσχοντες.

Το σημαντικότερο πλεονέκτημα της ασύμμετρης κρυπτογραφίας είανι ότι δεν απαιτείται ανταλλαγή μυστικού κλειδιού. Το δημόσιο κλειδί είναι ελεύθερα διαθέσιμο κάτι που κάνει τη διαχείριση των κλειδιών ευκολότερη και το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του, καθιστώντας έτσι δυσκολότερη την παραποίησή του. Όμως η κρυπτογραφία δημοσίου κλειδιού έχει μεγάλες απαιτήσεις σε υπολογιστική ισχύ και είναι αρκετά αργή κυρίως στα μεγάλα μηνύματα. Γι’ αυτό το λόγο συνήθως δεν κρυπτογραφούνται δεδομένα αλλά συμμετρικά κλειδιά με τη μέθοδο του ψηφιακού φακέλου.

Συστήματα κρυπτογράφησης με δημόσιο κλειδί είναι το κρυπτοσύστημα Elgamal, το RSA, το κρυπτοσύστημα Diffie-Hellman και το DSA (Digital Signature Algorithm).

Υβριδική Κρυπτογραφία Ψηφιακού Φακέλου

Ιδιαίτερο ενδιαφέρον για την επίτευξη ασφαλούς επικοινωνίας μεταξύ δυο μερών παρουσιάζει η υβριδική κρυπτογραφία που είναι γνωστή και ως ψηφιακός φάκελος η οποία αξιοποιεί ταυτόχρονα τις τεχνικές συμμετρικής και ασύμμετρης κρυπτογραφίας. Η υβριδική κρυπτογραφία μπορεί να χρησιμοποιηθεί για πολλούς παραλήπτες ταυτόχρονα. Τα βήματα που ακολουθούνται για τη δημιουργία ενός ψηφιακού φακέλου είναι :

1. Δημιουργείται ένα συμμετρικό κλειδί με χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας.
2. Η αρχική πληροφορία κρυπτογραφείται με το συμμετρικό κλειδί που έχει δημιουργηθεί.
3. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.
4. Τα δυο κρυπτογραφημένα κείμενα αποτελούν τον ψηφιακό φάκελο του παραλήπτη.

Ο παραλήπτης ανοίγει τον ψηφιακό του φάκελο αποκρυπτογραφώντας με το ιδιωτικό κλειδί του το κρυπτογραφημένο συμμετρικό κλειδί. Με χρήση του συμμετρικού κλειδιού ο παραλήπτης αποκρυπτογραφεί το αρχικό κείμενο. Μετά την επίτευξη μιας ασφαλούς επικοινωνίας μεταξύ αποστολέα και παραλήπτη το συμμετρικό κλειδί καταστρέφεται.

Η υβριδική κρυπτογραφία βοηθά στο να ξεπεραστούν οι σημαντικές δυσκολίες της κρυπτογραφίας δημοσίου κλειδιού που αναφέρθηκαν παραπάνω.

1.1.4 Κρυπτογραφικές υπηρεσίες και Πρωτόκολλα

Οι κρυπτογραφικές υπηρεσίες είναι υπηρεσίες που χρησιμοποιώντας κρυπτογραφία, στοχεύουν στην αντιμετώπιση συγκεκριμένων απειλών. Οι κρυπτογραφικές υπηρεσίες είναι οι ακόλουθες:

- **Εμπιστευτικότητα** (Confidentiality)**.** Είναι η προστασία από τη μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας. Η εμπιστευτικότητα θα πρέπει να προσφέρεται με τέτοιον τρόπο ώστε να είναι αδύνατη η αποκάλυψη και πολλές φορές η ίδια η ύπαρξη της πληροφορίας σε μη εξουσιοδοτημένα άτομα.
- **Ακεραιότητα** (Integrity). Είναι η προστασία από τη μη εξουσιοδοτημένη τροποποίηση των δεδομένων. Η ακεραιότητα θα πρέπει να παρέχει στον παραλήπτη και γενικότερα στον κάτοχο ενός μηνύματος τη δυνατότητα να μπορεί να ανιχνεύσει πιθανές αλλαγές στο μήνυμα από μη εξουσιοδοτημένα άτομα. Στον χώρο των τηλεπικοινωνιών και της θεωρίας της πληροφορίας, η ακεραιότητα είναι γνωστή ως ανίχνευση σφαλμάτων, όπου ένα μήνυμα μπορεί να υποστεί τροποποίηση λόγω του θορύβου του καναλιού επικοινωνίας.
- **Αυθεντικοποίηση** (Authentication). Είναι η εξασφάλιση του ότι γνωρίζουμε το χρήστη ή γενικότερα την οντότητα που επικοινωνούμε (user/entity authentication). Αυθεντικοποίηση δεδομένων (data authentication) είναι η εξασφάλιση ότι ένα μήνυμα προέρχεται πράγματι από τον αποστολέα που πιστεύουμε ότι το έστειλε.
- **Μη-απάρνηση** (Non-repudiation). Είναι η υπηρεσία κατά την οποία ο παραλήπτης δε μπορεί να απαρνηθεί ότι έλαβε το μήνυμα (μη-απάρνηση προορισμού (non-repudiation of destination)), ή η υπηρεσία κατά την οποία ο αποστολέας δεν μπορεί να απαρνηθεί ότι έστειλε το μήνυμα (μη-απάρνηση προέλευσης (non-repudiation of origin)).

Θα πρέπει να σημειωθεί ότι υπάρχει αλληλεξάρτηση της ακεραιότητας και της αυθεντικοποίησης ενός μηνύματος. Δεν είναι δυνατό να προσφέρεται με επιτυχία μόνον ακεραιότητα χωρίς να προσφέρεται αυθεντικοποίηση και αντίστροφα. Σε περίπτωση που προσφέρεται αυθεντικοποίηση χωρίς ακεραιότητα, ο αντίπαλος μπορεί να τροποποιήσει την πληροφορία αυθεντικοποίησης, προσδίδοντας

διαφορετικό κάτοχο στο μήνυμα. Σε περίπτωση που προσφέρεται ακεραιότητα χωρίς αυθεντικοποίηση, ο αντίπαλος μπορεί ανεξέλεγκτα να τροποποιήσει το μήνυμα και να επανυπολογίσει το κρυπτογραφικό άθροισμα ελέγχου που προσδιορίζει την ακεραιότητα του μηνύματος

Κρυπτογραφικό πρωτόκολλο είναι η πλήρως αποσαφηνισμένη διαδικασία που πρέπει να ακολουθήσουν τα επικοινωνούντα μέλη, προκειμένου να επιτύχουν μια συγκεκριμένη κρυπτογραφική υπηρεσία.

Το βασικό χαρακτηριστικό του κρυπτογραφικού πρωτοκόλλου είναι ότι πρέπει το κάθε μέλος να γνωρίζει σε κάθε χρονική στιγμή (κατά τη διάρκεια εκτέλεσης του πρωτοκόλλου) πιο βήμα πρέπει να εκτελεστεί και πως πρέπει να εκτελεστεί. Οποιαδήποτε παρέκκλιση από τη διαδικασία που απαιτεί το κρυπτογραφικό πρωτόκολλο έχει ως αποτέλεσμα την κατάρρευση της επικοινωνίας ή της υποκείμενης κρυπτογραφικής υπηρεσίας.

Παράδειγμα: Απλό πρωτόκολλο ανταλλαγής κλειδιών. Ο Α και ο Β αποφασίζουν να χρησιμοποιήσουν ένα συμμετρικό κρυπτοσύστημα για να ανταλλάξουν εμπιστευτικά μηνύματα. Η διανομή του κλειδιού γίνεται μέσω ασύμμετρου κρυπτοσυστήματος με το ακόλουθο πρωτόκολλο:

1. Ο Α δημιουργεί ένα συμμετρικό κλειδί.
2. Ο Α ζητά το δημόσιο κλειδί του Β.
3. Ο Β στέλνει το δημόσιό του κλειδί στον Α.
4. Ο Α κρυπτογραφεί το συμμετρικό κλειδί με το κλειδί του Β.
5. Ο Α στέλνει το κρυπτογραφημένο κλειδί στον Β σε μορφή κρυπτογραφημένου μηνύματος.
6. Ο Β αποκρυπτογραφεί το κρυπτογραφημένο μήνυμα και ανακτά το συμμετρικό κλειδί.

Με την ολοκλήρωση του πρωτοκόλλου ο Α και ο Β έχουν ένα κοινό συμμετρικό κλειδί το οποίο το μοιράστηκαν με εμπιστευτικότητα.

1.1.5 Αρχές μέτρησης κρυπτογραφικής δύναμης

Το πρώτο στάδιο στην ανάλυση της δύναμης ενός κρυπτοσυστήματος είναι η υπόθεση της ικανότητας του αντιπάλου. Η ικανότητα του αντιπάλου κρίνεται με βάση τους πόρους που διαθέτει, καθώς και με την πρόσβαση που έχει στο κρυπτοκείμενο, στο απλό κείμενο και στο κρυπτοσύστημα. Οι δυνατότητες επίθεσης ενός αντιπάλου σε ένα κρυπτοσύστημα χωρίζονται στις ακόλουθες κατηγορίες:

- Επίθεση στο κρυπτοκείμενο (ciphertext-only). Ο αντίπαλος έχει πρόσβαση μόνο σε ορισμένα κομμάτια του κρυπτοκειμένου και ο αντικειμενικός του σκοπός είναι να αποκρυπτογραφήσει το κρυπτοκείμενο αυτό, ή να ανακαλύψει το αντίστοιχο κλειδί. Ένα κρυπτοσύστημα το οποίο είναι ευάλωτο σε μια τέτοια επίθεση θεωρείται ανασφαλές.
- Επίθεση με γνωστό απλό κείμενο (known-plaintext). Ο αντίπαλος γνωρίζει αντιστοιχίες κρυπτοκειμένου με απλό κείμενο, και ο αντικειμενικός του σκοπός είναι η ανακάλυψη του αντίστοιχου κλειδιού. Πολλές φορές συναντάμε μηνύματα όπως γράμματα, όπου η αρχή και το τέλος τους είναι τυποποιημένα, όπως «αγαπητέ κ.…» και «με εκτίμηση….». Στον κόσμο των δικτύων των υπολογιστών τα πρωτόκολλα επικοινωνίας εμφανίζουν συστηματικά τυποποιημένα μηνύματα. Ένα κρυπτοσύστημα το οποίο υποπίπτει σε επίθεση γνωστού απλού κειμένου θεωρείται ανασφαλές.
- Επίθεση με επιλεγμένο απλό κείμενο (chosen-plaintext). Ο αντίπαλος έχει τη δυνατότητα πρόσβασης στο κρυπτοσύστημα όπου δεν γνωρίζει το κλειδί και μπορεί να ζητά την κρυπτογράφηση μηνυμάτων. Με αυτόν τον τρόπο μπορεί να ανακαλύψει την αντιστοιχία του απλού κειμένου με το άγνωστο κρυπτοκείμενο
- Επίθεση προσαρμόσιμου επιλεγμένου απλού κειμένου (adaptive chosen-plaintext). Ο αντίπαλος είναι σε θέση να πραγματοποιήσει επίθεση με επιλεγμένο απλό κείμενο, αλλά επιπλέον μπορεί να εφαρμόσει μεθοδολογία σύμφωνα με την οποία η επόμενη επιλογή του απλού κειμένου εξαρτάται από τις προηγούμενες, προκειμένου να ανακαλύψει γρηγορότερα το κλειδί, από μια εξαντλητική αναζήτηση (exhaustive search).

- Επίθεση με επιλεγμένο κρυπτοκείμενο (chosen-ciphertext). Υποθέτοντας ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης, ο αντικειμενικός σκοπός του είναι να ανακαλύψει το κλειδί αποκρυπτογράφησης προκειμένου να μπορεί στο μέλλον να αποκρυπτογραφεί τα νέα κρυπτοκείμενα, όταν δεν θα έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης. Στα περισσότερα συμμετρικά κρυπτοσυστήματα η επίθεση αυτή έχει την ίδια ισχύ με την επίθεση του επιλεγμένου απλού κειμένου. Η επίθεση με επιλεγμένο κρυπτοκείμενο θεωρείται ως η πιο αυστηρή επίθεση.
- Επίθεση προσαρμόσιμου επιλεγμένου κρυπτοκειμένου (adaptive chosen-ciphertext). Η επίθεση αυτή είναι αντίστοιχη του προσαρμόσιμου επιλεγμένου απλού κειμένου, με τη διαφορά ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης.

Η αρχή του Kerchoff

Στις παραπάνω δυνατότητες επίθεσης είναι προφανές ότι ο αντίπαλος γνωρίζει πλήρως τον αλγόριθμο κρυπτογράφησης. Αυτό εκτός από απαίτηση είναι και ένα θεμελιώδες κριτήριο στην αντικειμενική μέτρηση της δύναμης ενός κρυπτοσυστήματος το οποίο είναι γνωστό ως η αρχή του Kerchoff:

«Η ασφάλεια ενός κρυπτοσυστήματος δεν εξαρτάται από τη μυστικότητα του αλγόριθμου κρυπτογράφησης. Η ασφάλεια του κρυπτοσυστήματος εξαρτάται μόνον από το να διατηρείται μυστικό το κλειδί»

Η απαίτηση να είναι ο αλγόριθμος κρυπτογράφησης μυστικός υποθάλπει τόσο κινδύνους όσο και προβλήματα. Πρώτον, η αντικειμενική αξιολόγηση του αλγόριθμου δεν θα είναι εφικτή, με αποτέλεσμα να είναι αδύνατον να υπολογισθεί η πραγματική του κρυπτογραφική δύναμη. Δεύτερον, η αντίστροφη ανάλυση (reverse engineering) επέτρεπε στον αντίπαλο να ανακαλύπτει τη δομή και λεπτομέρειες του αλγόριθμου κρυπτογράφησης. Η ιστορία μας έχει διδάξει ότι όποτε η κρυπτογραφία βασιζόταν στη μυστικότητα του αλγόριθμου κρυπτογράφησης, η κατάρρευση του

κρυπτοσυστήματος ήταν σχεδόν βέβαιη. Τρίτον, εάν ένα κλειδί γίνει γνωστό είναι σχετικά εύκολη η αντικατάστασή του, ενώ εάν ο αλγόριθμος κρυπτογράφησης γίνει γνωστός, τότε υπάρχει σοβαρό πρόβλημα στην αποτελεσματικότητα της μυστικής επικοινωνίας.

Τα μέτρα του Shannon

Ο Shannon, ο θεμελιωτής της θεωρίας της πληροφορίας διατύπωσε το 1949 ένα σύνολο από μέτρα τα οποία χαρακτηρίζουν έναν ορθά σχεδιασμένο αλγόριθμο κρυπτογράφησης:

1. Βαθμός απαιτούμενης κρυπτογραφικής ασφάλειας. Το μέτρο αυτό αφορά το κέρδος του αντιπάλου σε πληροφορία, όταν παρατηρεί το κρυπτοκείμενο.
2. Μήκος του κλειδιού. Η ευκολία χειρισμού του κλειδιού εξαρτάται από το μήκος του.
3. Πρακτική εκτέλεση της κρυπτογράφησης και της αποκρυπτογράφησης. Η προσπάθεια που απαιτείται για την κρυπτογράφηση και την αποκρυπτογράφηση, σε χρόνο ή λειτουργίες.
4. Διόγκωση του κρυπτοκειμένου. Είναι επιθυμητό το κρυπτοκείμενο να έχει το ίδιο μήκος (ή συγκρίσιμου μεγέθους) με το απλό κείμενο.
5. Διάδοση των σφαλμάτων κρυπτογράφησης. Είναι επιθυμητό ένα σφάλμα κατά την κρυπτογράφηση να επηρεάζει σε όσον το δυνατόν λιγότερο βαθμό την αποκρυπτογράφηση.

Η ύπαρξη των μέτρων σε ένα κρυπτοσύστημα είναι υποχρεωτική, αλλά συγχρόνως και αντιφατική, με αποτέλεσμα να μην υπάρχει στην πραγματικότητα κρυπτοσύστημα το οποίο να ικανοποιεί όλα τα μέτρα στο μέγιστό τους. Για παράδειγμα, πλήρης έλλειψη του μέτρου 1 σημαίνει ότι ο αντίπαλος μπορεί να ανακτήσει πλήρως το απλό κείμενο, ή ακόμη καλύτερα, το απλό κείμενο είναι ένα αποδεκτό κρυπτοκείμενο. Η πλήρης έλλειψη των μέτρων 3 και 4 επιτρέπει κρυπτοσυστήματα που μπορούν να μεγιστοποιούν όλα τα άλλα μέτρα. Η πλήρης έλλειψη του μέτρου 5 δέχεται ύπαρξη κρυπτοσυστήματος που μεγιστοποιεί όλα τα

άλλα μέτρα, αλλά σε περίπτωση σφάλματος κατά την κρυπτογράφηση, η ανάκτηση του απλού κειμένου θα ήταν αδύνατη, ακόμη και για κάποιο τμήμα αυτού.

Σύγχυση και Διάχυση

Δύο ιδιότητες που χρησιμοποιούνται στην αξιολόγηση της κρυπτογραφικής δύναμης είναι η σύγχυση (confusion) και η διάχυση (diffusion). Έστω ένα απλό κείμενο το οποίο αντιστοιχεί σε ένα κρυπτοκείμενο μέσω ενός κρυπταλγόριθμου. Εάν αντικαταστήσουμε ένα σύμβολο του απλού κειμένου και κρυπτογραφήσουμε το νέο απλό κείμενο, τότε για έναν κρυπταλγόριθμο με υψηλή διάχυση, ο αντίπαλος δεν θα μπορεί να προβλέψει ποια σύμβολα του κρυπτοκειμένου θα μεταβληθούν ή γενικότερα θα επηρεαστούν.

Σύγχυση είναι η ικανότητα του αλγόριθμου κρυπτογράφησης όπου ο αντίπαλος δεν είναι σε θέση να προβλέψει ποιες μεταβολές θα συμβούν στο κρυπτοκείμενο, δεδομένης μιας μεταβολής στο απλό κείμενο.

Δηλαδή, ένας αλγόριθμος έχει υψηλή σύγχυση όταν οι σχέσεις μεταξύ του απλού κειμένου και του κρυπτοκειμένου είναι αρκετά πολύπλοκες, ώστε να χρειάζεται ο αντίπαλος να ξοδέψει σημαντικό χρόνο προκειμένου να τις προσδιορίσει.

Διάχυση είναι η ικανότητα του αλγόριθμου κρυπτογράφησης όπου ένα τμήμα του απλού κειμένου να έχει την ευκαιρία να επηρεάζει όσο το δυνατόν περισσότερα τμήματα του κρυπτοκειμένου.

Ένας αλγόριθμος έχει υψηλή διάχυση όταν ένα στοιχειώδες τμήμα του απλού κειμένου έχει την δυνατότητα να επηρεάσει όλα τα τμήματα του κρυπτοκειμένου, ανεξάρτητα της τοποθεσίας του τμήματος αυτού στο απλό κείμενο.

1.2 Μαθηματικό υπόβαθρο

1.2.1 Συναρτήσεις

Ορισμός 1. Μια συνάρτηση ορίζεται από δυο σύνολα X και Y και έναν κανόνα f όπου απεικονίζει κάθε στοιχείο του X σε μόνο ένα στοιχείο του Y .Το σύνολο X ονομάζεται πεδίο ορισμού της συνάρτησης και το σύνολο Y ονομάζεται σύνολο τιμών της συνάρτησης. Αν x είναι στοιχείο του X $\left(x \in X\right)$ τότε η εικόνα του x είναι ένα στοιχείο του Y που το βρίσκουμε εάν εφαρμόσουμε τον κανόνα f στο x . Η εικόνα y του x ορίζεται ως $f\left(x\right) = y$. Μια συνάρτηση f από το X στο Y συμβολίζεται ως $f : X \to Y$. Το σύνολο όλων των στοιχείων του Y όπου σε κάθε στοιχείο του απεικονίζεται τουλάχιστον ένα στοιχείο του X με τον κανόνα f ονομάζεται εικόνα της f και συμβολίζεται με $\mathrm{Im}\left(f\right)$.

Ορισμός 2. Μια συνάρτηση $f : X \to Y$ λέγεται 1-1 αν κάθε στοιχείο του Y είναι εικόνα το πολύ ενός στοιχείου του X .

Ορισμός 3. Μια συνάρτηση $f : X \to Y$ λέγεται επί αν κάθε στοιχείο του Y είναι εικόνα τουλάχιστον ενός στοιχείου του X .

Ορισμός 4. Μια συνάρτηση $f : X \to Y$ λέγεται 1-1 και επί αν κάθε στοιχείο του Y είναι εικόνα ενός στοιχείου του X .

Ορισμός 5. Μια συνάρτηση $f : X \to Y$ που είναι 1-1 και επί, για κάθε στοιχείο $y \in Y$ ορίζουμε την $g : Y \to X$, με $g\left(y\right) = x$ όπου $x \in X$ και $f\left(x\right) = y$. Η g είναι συνάρτηση που καθορίζεται από την f , λέγεται αντίστροφη της f και συμβολίζεται $g = f^{-1}$.

Υπάρχουν αρκετά είδη συναρτήσεων που έχουν πολύ σημαντικό ρόλο στην κρυπτογραφία και στις ψηφιακές υπογραφές όπως οι one-way, trapdoor one-way και οι hash συναρτήσεις.

Ορισμός 6. Μια συνάρτηση $f : X \to Y$ ονομάζεται one-way συνάρτηση αν το $f(x)$ είναι εύκολα υπολογίσιμο για όλα τα $x \in X$ αλλά και για σχεδόν όλα τα στοιχεία $y \in \mathrm{Im}(f)$ είναι υπολογιστικά ανέφικτο να βρεθεί κάποιο $x \in X$ τέτοιο ώστε $f(x) = y$

Υπάρχουν πολλές συναρτήσεις που πιστεύεται ότι είναι one-way αλλά μέχρι σήμερα δεν έχει αποδειχθεί ότι κάποια συγκεκριμένη συνάρτηση είναι one-way.

Παράδειγμα : Επιλέγουμε δύο πρώτους αριθμούς $p = 48611$ και $q = 53993$, υπολογίζουμε το $n = p \cdot q = 2624652723$ και ορίζουμε το σύνολο $X = \{1, 2, 3, ..., n-1\}$. Ορίζουμε τη συνάρτηση f στο X, όπου $f(x) = r_x$, $\forall x \in X$ και r_x είναι το υπόλοιπο όταν διαιρούμε το x^3 με το n. Για παράδειγμα $f(2489991) = 1981394214$ επειδή $2489991^3 = 5881949859 \cdot n + 1981394214$. Για να βρούμε το $f(x)$ είναι εύκολο αλλά η αντίστροφη διαδικασία είναι αρκετά πιο δύσκολη. Αν οι παράγοντες του n είναι άγνωστοι και μεγάλοι αριθμοί τότε είναι ένα δύσκολο πρόβλημα, αλλά αν οι p και q είναι γνωστοί τότε το πρόβλημα είναι εύκολο.

Ορισμός 7. Μια συνάρτηση $f : X \to Y$ ονομάζεται trapdoor one-way συνάρτηση αν η f είναι μια one-way συνάρτηση με μια επιπλέον ιδιότητα που λέγεται trapdoor πληροφορία και είναι εύκολο να βρούμε για κάθε $y \in \mathrm{Im}(f)$ ένα $x \in X$ τέτοιο ώστε $f(x) = y$

Στις συναρτήσεις one-way και trapdoor one-way στηρίζεται η κρυπτογραφία δημοσίου κλειδιού (public-key cryptography).

Ορισμός 8. Έστω ένα πεπερασμένο σύνολο S. Μια μετάθεση $p : S \to S$ είναι μια συνάρτηση από το S στον εαυτό του.

Ορισμός 9. Έστω ένα πεπερασμένο σύνολο S και f μια 1-1 συνάρτηση από το S στο S. Η f ονομάζεται involution αν $f = f^{-1}$ δηλαδή αν $f\left(f\left(x\right)\right) = x$ για όλα τα $x \in S$.

Hash Functions

Ο όρος hash function υποδηλώνει ένα μετασχηματισμό που παίρνει σαν είσοδο ένα μήνυμα m οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων H περιορισμένου μήκους που καλείται hash value, δηλαδή είναι $H = h(m)$. Οι hash functions είναι συναρτήσεις της μορφής $h(x) = y$, με τις εξής ιδιότητες:

- η είσοδος είναι οποιουδήποτε μήκους
- η έξοδος έχει περιορισμένο μήκος (σταθερό)
- δεδομένου του *x*, ο υπολογισμός του *y* είναι εύκολος
- η $h(x)$ είναι μη αντιστρέψιμη
- η $h(x)$ είναι αμφιμονοσήμαντη (ένα προς ένα συνάρτηση).

Λέγοντας μη αντιστρέψιμη συνάρτηση εννοούμε ότι δεδομένου ενός *y* είναι υπολογιστικά πολύ δύσκολο έως αδύνατο να βρεθεί ο *x*. Λέγοντας αμφιμονοσήμαντη εννοούμε ότι για δύο x_1, x_2 για τα οποία ισχύει ότι $x_1 \neq x_2$ είναι πάντα $h(x_1) \neq h(x_2)$.Σε καμία περίπτωση δεν ισχύει $h(x_1) = h(x_2)$ όταν $x_1 \neq x_2$.

Ορισμός 10. Μία hash συνάρτηση είναι μία εύκολα υπολογίσιμη συνάρτηση που αντιστοιχίζει δυαδικές συμβολοσειρές αυθαίρετου μήκους σε δυαδικές συμβολοσειρές σταθερού μήκους τις hash- τιμές(hash values).

Στις ψηφιακές υπογραφές πολλά προβλήματα που δημιουργούνται επιλύονται με τη χρήση των hash συναρτήσεων. Μερικά από αυτά είναι:

(α). Ένα μεγάλο μήνυμα σε έκταση θα έχει τεράστια ψηφιακή υπογραφή.

(β).Τα πιο «ασφαλή» ψηφιακά σχήματα είναι αργά επειδή χρησιμοποιούν πολύπλοκους υπολογισμούς.

(γ). Αν ένα μήνυμα έχει διασπασθεί σε μπλοκ για να υπογραφεί μπορεί κάποια μπλοκ να αλλάξουν θέση ή να διαγραφούν και η υπογραφή να μπορεί παρ' όλα αυτά να πιστοποιηθεί. Πρέπει να διαφυλάξουμε την ακεραιότητα του μηνύματος και αυτό δεν μπορεί να γίνει με ανεξάρτητες υπογραφές σε κάθε μπλοκ.

Πρέπει να είμαστε πολύ προσεκτικοί στην χρήση των hash συναρτήσεων στις ψηφιακές υπογραφές. Δεν πρέπει σε καμία περίπτωση η χρήση της hash συνάρτησης να επηρεάζει την ασφάλεια του συστήματος.

Για μια hash συνάρτηση όπου η hash value είναι n-bit, η πιθανότητα να επιλεγεί τυχαία μια συγκεκριμένη τιμή είναι 2^{-n} . Οι hash συναρτήσεις που χρησιμοποιούνται στις ψηφιακές υπογραφές είναι επιλεγμένες συναρτήσεις ώστε να είναι υπολογιστικά ανέφικτο να βρούμε δυο διαφορετικά x, y τέτοια ώστε $h(x) = h(y)$ και άρα δοθέντος μίας τιμής y είναι υπολογιστικά ανέφικτο να βρούμε τέτοιο x που $h(x) = y$.

Ορισμός 11. Έστω x είναι ένα μήνυμα. Μια hash συνάρτηση h είναι weakly collision free για το x αν είναι υπολογιστικά ανέφικτο να βρούμε ένα μήνυμα $x' \neq x$ τέτοιο ώστε $h(x') = h(x)$.

Ορισμός 12. Μια hash συνάρτηση h είναι strongly collision free αν είναι υπολογιστικά ανέφικτο να βρούμε μηνύματα x' και x τέτοια ώστε $x' \neq x$ και $h(x') = h(x)$.

Ορισμός 13. Μια hash συνάρτηση h είναι one-way αν δοθέντος ενός μηνύματος x είναι υπολογιστικά ανέφικτο να βρούμε ένα μήνυμα x' τέτοιο ώστε $h(x') = x$.

Η hash value παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, για αυτό καλείται και σύνοψη μηνύματος (message digest). Μπορούμε να φανταστούμε την σύνοψη του μηνύματος σαν "ψηφιακό αποτύπωμα" ("digital fingerprint") του εγγράφου. Παραδείγματα γνωστών hash functions είναι οι MD2, MD5 και SHA.

Επειδή οι hash functions είναι πιο γρήγορες από τους αλγόριθμους κρυπτογράφησης και ψηφιακών υπογραφών, συνηθίζεται να παράγεται η υπογραφή των μηνυμάτων με την εφαρμογή κρυπτογραφικών διαδικασιών στο message digest, το οποίο είναι πιο μικρό και εύκολο στην διαχείριση. Επιπλέον ένα message digest μπορεί να δημοσιοποιηθεί χωρίς να αποκαλύπτει τα περιεχόμενα του αυθεντικού κειμένου.

Οι Damgard και Merkle εισήγαγαν την έννοια του compression function. Αυτές οι συναρτήσεις παίρνουν είσοδο καθορισμένου μήκους και δίνουν έξοδο μικρότερου, περιορισμένου μήκους. Δεδομένου, λοιπόν, ενός compression function, ένας hash function μπορεί να πραγματοποιηθεί με την επανειλημμένη εφαρμογή του compression function έως ότου ολόκληρο το μήνυμα έχει επεξεργαστεί. Πιο αναλυτικά, το μήνυμα τεμαχίζεται σε blocks, των οποίων το μέγεθος εξαρτάται από τον compression function, και συμπληρώνεται (padded) για λόγους ασφαλείας, ώστε το μήκος του μηνύματος να είναι πολλαπλάσιο του μήκους του block.

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού (Cryptographic hash functions) ή αλλιώς συναρτήσεις κωδικοποίησης μηνυμάτων (message digest functions) δεν χρησιμοποιούν κλειδιά αλλά είναι ένας σχετικός και σημαντικός κλάδος των αλγορίθμων κρυπτογράφησης . Αυτές αποτελούν ένα είδος αθροίσματος ελέγχου (checksum). Η έξοδος μιας κρυπτογραφικής συνάρτησης κατακερματισμού h είναι πάντα του ίδιου μήκους ανεξαρτήτως του μήκους της εισόδου της. Μια δυνατή κρυπτογραφική συνάρτηση κατακερματισμού θα πρέπει για μια πολύ μικρή αλλαγή της εισόδου της να παρουσιάζει μια τελείως διαφορετική έξοδο, έτσι ώστε να είναι πραγματικά δύσκολο να συμπεράνει κανείς την είσοδο από την έξοδο. Σημαντική ιδιότητα των hash function αποτελεί το γεγονός ότι δεν αντιστρέφονται. Δηλαδή δεν υπάρχει τρόπος κάποιος να βρει μια είσοδο που να αντιστοιχεί σε ένα κατακερματισμό που ήδη έχει.

Παράδειγμα: Ο αλγόριθμος MD5 έχει έξοδο 128 bit και κρυπτογραφικά είναι πολύ δυνατός. Κατά μέσον όρο θα πρέπει κάποιος να δοκιμάσει 2^{127} εισόδους πριν να αρχίσει ο αλγόριθμος να του δίνει ίδιες εξόδους. Ακόμα όμως και αν το καταφέρει αυτό είναι μόνο μια περίπτωση από τις άπειρες εισόδους που θα μπορούσαν να παράξουν το συγκεκριμένο κατακερματισμό μηνύματος.

2^{127} = 170.141.183.460.469.231.731.687.303.715.884.105.728

Όμως με την εξέλιξη της σύγχρονης τεχνολογίας ένας χώρος αναζήτησης της τάξης του 2^{128} δεν είναι πλέον επαρκώς μεγάλος. Οι ερευνητές έχουν δημοσιεύσει αποτελέσματα συγκρούσεων, όπου κατάφεραν χρησιμοποιώντας σύγχρονη τεχνολογία και βρήκαν δύο εισόδους που είχαν τον ίδιο MD5 κατακερματισμό καθώς και μια δεύτερη είσοδο που έχει τον ίδιο MD5 κατακερματισμό με ένα δοσμένο MD5 κατακερματισμό. Για αυτό δημιουργήθηκε ένας άλλος αλγόριθμος κατακερματισμού, ο SHA-1 ο οποίος εμφανίζει έξοδο 160-bit και προς το παρόν θεωρείται περισσότερο ασφαλής.

2^{160} = 1.461.501.637.330.902.918.203.684.832.716.283.019.655.932.542.976

ενώ

2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456

Δημοσιεύσεις από τους Xiaoyun Wang, Yiqun Yin, και Hongbo Yu παρουσίασαν επιθέσεις εναντίον και του SHA-1 και μάλιστα σε μεταγενέστερες αυτών οι ίδιοι ανακοίνωσαν ότι τελικά η χρονική πολυπλοκότητα είναι ακόμη μικρότερη από ότι είχαν αρχικά ανακοινώσει. Όμως το συμπέρασμα ότι ο SHA-1 έχει τελικά “σπαστεί”, είναι σχετικό αφού το να βρει κάποιος μια σύγκρουση στον 160-bit χώρο αναζήτησης του SHA-1 ισοδυναμεί με το εξαντλητικό ψάξιμο 2^{80} συνδυασμών. Οι παραπάνω ερευνητές έδειξαν τελικά ότι αυτό γίνεται σε λιγότερα βήματα και για την ακρίβεια σε 2^{63}. Άρα το συμπέρασμα είναι ότι παρόλο που τελικά ο SHA-1 είναι πιο αδύναμος απ’ ότι είχαμε υπολογίσει αρχικά, ο αριθμός 2^{63} παραμένει αρκετά μεγάλος για να παράσχει σχετική και πρακτική ασφάλεια δεδομένου ακόμη και της σύγχρονης τεχνολογίας. Παρ’ όλα αυτά οι τελευταίες έρευνες επικεντρώνονται γύρω από την ανάπτυξη αλγορίθμων με ακόμη μεγαλύτερο μέγεθος εξόδων όπως οι SHA-256 και SHA-512 οι οποίοι εγγυούνται ακόμη μεγαλύτερη ασφάλεια.

Εν κατακλείδι, μπορούμε να πούμε ότι οι συγκρούσεις είναι απίθανο να συμβούν τυχαία, και πολύ δύσκολο να βρεθούν από κάποιο, αλλά δεν μπορεί κανείς να αποκλείσει αυτήν την πιθανότητα.

1.2.2 Πιθανότητες

Με S συμβολίζουμε το χώρο των γεγονότων και με $E \subseteq S$ ένα σύνολο γεγονότων.

Ορισμός 1. Μια πιθανοτική κατανομή του P στο S είναι μια ακολουθία αριθμών $p_1, p_2, ..., p_n$ τέτοια που όλοι οι p_i είναι μη αρνητικοί και έχουν άθροισμα ίσο με 1. $P(s_i)$ ή p_i είναι η πιθανότητα να συμβεί το γεγονός s_i.

Ορισμός 2. Ένα σύνολο γεγονότων Ε είναι ένα υποσύνολο του S. Η πιθανότητα να συμβεί το S είναι η $P(E)$ και ισούται με το άθροισμα των πιθανοτήτων p_i όλων των γεγονότων s_i που ανήκουν στο Ε. Αν $s_i \in S$ τότε $P(\{s_i\})$ γράφεται $P(s_i)$.

Ορισμός 3. Αν Ε είναι ένα σύνολο γεγονότων , το συμπλήρωμά του είναι ένα σύνολο γεγονότων που δεν ανήκουν στο Ε και συμβολίζεται με $\overline{E}$.

Ιδιότητα 1. Έστω $E \subseteq S$ τότε :

α) $0 \le P(E) \le 1$ με $P(S) = 1$ και $P(\varnothing) = 0$

β) $P(\overline{E}) = 1 - P(E)$

Ορισμός 4. Δυο γεγονότα E_1 και E_2 λέγονται αμοιβαίως αποκλειόμενα αν $P(E_1 \cap E_2) = 0$ δηλαδή δεν μπορούν να συμβούν ταυτόχρονα.

Ιδιότητα 2. Έστω δυο γεγονότα E_1 και E_2 τότε:

α)Αν $E_1 \subseteq E_2$ τότε $P(E_1) \le P(E_2)$

β) $P(E_1 \cup E_2) + P(E_1 \cap E_2) \le P(E_1) + P(E_2)$. Αν E_1 και E_2 είναι αμοιβαίως αποκλειόμενα τότε : $P(E_1 \cup E_2) \le P(E_1) + P(E_2)$

Ορισμός 5. Έστω δυο γεγονότα E_1 και E_2 με $P(E_2) \succ 0$. Η πιθανότητα να συμβεί το γεγονός E_1 δεδομένου ότι έχει συμβεί το γεγονός E_2 ορίζεται ως $P(E_1|E_2)$ και ισούται με :

$$P(E_1|E_2) = \frac{P(E_1 \cap E_2)}{P(E_2)}$$

Ορισμός 6. Δυο γεγονότα E_1 και E_2 λέγονται ανεξάρτητα αν $P(E_1 \cap E_2) \quad P(E_1) \cdot P(E_2)$.

Ιδιότητα 3. (Θεώρημα του Bayes)

Αν E_1 και E_2 είναι δυο γεγονότα με $P(E_2) \succ 0$ τότε:

$$P(E_1|E_2) = \frac{P(E_1) \cdot P(E_2|E_1)}{P(E_2)}$$

Ορισμός 7. Μια τυχαία μεταβλητή X είναι μια συνάρτηση από το S σε ένα σύνολο πραγματικών αριθμών όπου για κάθε γεγονός $s_i \in S$ η X αντιστοιχίζει ένα πραγματικό αριθμό $X(s_i)$.

Ορισμός 8. Έστω μια τυχαία μεταβλητή X στο S. Η αναμενόμενη τιμή της X είναι $E(X) = \sum_{s_i \in S} X(s_i) \cdot P(s_i)$

1.2.3 Θεωρία αριθμών

Η μελέτη της θεωρίας αριθμών έχει παίξει σημαντικό ρόλο στην ανάπτυξη των σχημάτων των ψηφιακών υπογραφών. Τα πιο πολλά σχήματα ψηφιακών υπογραφών στηρίζονται σε ανοικτά προβλήματα της θεωρίας αριθμών.

Ακέραιοι αριθμοί

Ορισμός 1. Έστω α και β ακέραιοι. Ο α διαιρεί τον β $\left(\alpha\middle|\beta\right)$ αν υπάρχει ένας ακέραιος γ έτσι ώστε $\beta=\alpha\cdot\gamma$

Ιδιότητα 1. Για όλους τους $\alpha,\beta,\gamma\in\mathbb{Z}$ ισχύουν τα παρακάτω:

α) $\alpha\middle|\alpha$.

β) Αν $\alpha\middle|\beta$ και $\beta\middle|\gamma$ τότε $\alpha\middle|\gamma$.

γ) Αν $\alpha\middle|\beta$ και $\alpha\middle|\gamma$ τότε $\alpha\middle|\left(\beta\cdot x+\gamma\cdot y\right)$ για όλα τα $x,y\in\mathbb{Z}$.

δ) Αν $\alpha\middle|\beta$ και $\beta\middle|\alpha$ τότε $\alpha=\pm\beta$.

Ορισμός 2. (Αλγόριθμος Διαίρεσης) Αν α και β ακέραιοι με $\beta\geq 1$ τότε η διαίρεση του α με το β δίνει δύο ακέραιους π (πηλίκο) και υ (υπόλοιπο) τέτοιους που $\alpha=\pi\cdot\beta+\upsilon$, όπου $0\leq\upsilon\prec\beta$. Οι π και υ είναι μοναδικοί. Ο υ συμβολίζεται $\alpha \bmod \beta$.

Ορισμός 3. Ένας ακέραιος γ είναι κοινός διαιρέτης των α και β αν $\gamma\middle|\alpha$ και $\gamma\middle|\beta$.

Ορισμός 4. Ένας μη αρνητικός ακέραιος δ είναι μέγιστος κοινός διαιρέτης των ακεραίων α και β $\left(\delta=\gcd\left(\alpha,\beta\right)\right)$ αν ισχύουν:

α) Ο δ είναι κοινός διαιρέτης των α και β.

β) Για κάθε ακέραιο γ που $\gamma\middle|\alpha$ και $\gamma\middle|\beta$ τότε $\gamma\middle|\delta$.

Ορισμός 5. Ένας μη αρνητικός ακέραιος δ είναι ελάχιστο κοινό πολλαπλάσιο των ακεραίων α και β $\left(\delta=lcd\left(\alpha,\beta\right)\right)$ αν ισχύουν:

α) $\alpha\middle|\delta$ και $\beta\middle|\delta$.

β) Για κάθε ακέραιο γ που $\alpha\middle|\gamma$ και $\beta\middle|\gamma$ τότε $\delta\middle|\gamma$.

Ιδιότητα 2. Αν α και β θετικοί ακέραιοι τότε : $lcd(\alpha,\beta)=\alpha\cdot\beta\,|\gcd(\alpha,\beta)$.

Ορισμός 6. Δύο ακέραιοι α και β λέγονται σχετικώς πρώτοι αν $\gcd(\alpha,\beta)=1$.

Ορισμός 7. Ένας ακέραιος $\rho\geq 2$ είναι πρώτος αριθμός αν οι μοναδικοί θετικοί διαιρέτες του είναι ο 1 και ο ρ. Αλλιώς ο ρ λέγεται σύνθετος.

Ιδιότητα 3. Αν ο ρ είναι πρώτος και $\rho\,|\alpha\cdot\beta$ τότε $\rho\,|\alpha$ ή $\rho\,|\beta$ (ή και τα δύο).

Ιδιότητα 4. Υπάρχουν άπειροι στο πλήθος πρώτοι αριθμοί.

Ιδιότητα 5. (Θεμελιώδες θεώρημα Αριθμητικής) Για κάθε ακέραιο $n\geq 2$ υπάρχει μοναδική παραγοντοποίηση του n σε γινόμενο πρώτων αριθμών: $n=\rho_1^{e_1}\cdot\rho_2^{e_2}\cdot\ldots\cdot\rho_k^{e_k}$ όπου ρ_i: μοναδικοί διαφορετικοί πρώτοι αριθμοί και e_i: θετικοί ακέραιοι.

Ορισμός 8. (Euler φ συνάρτηση) Για $n\geq 1$ με $\varphi(n)$ ορίζουμε τον αριθμό των ακεραίων στο διάστημα $[1,n]$ που είναι σχετικώς πρώτοι με τον n.

Ιδιότητα 6. Η συνάρτηση φ έχει τις ακόλουθες ιδιότητες:

α) Αν ο ρ είναι πρώτος τότε $\varphi(\rho)=\rho-1$.

β) Αν $\gcd(\alpha,\beta)=1$ τότε $\varphi(\alpha\cdot\beta)=\varphi(\alpha)\cdot\varphi(\beta)$.

γ) Αν $n=\rho_1^{e_1}\cdot\rho_2^{e_2}\cdot\ldots\cdot\rho_k^{e_k}$ είναι η παραγοντοποίηση του n σε πρώτους αριθμούς τότε:

$$\varphi(n)=n\cdot\left(1-\frac{1}{\rho_1}\right)\cdot\left(1-\frac{1}{\rho_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{\rho_\kappa}\right).$$

Ιδιότητα 7. Αν α και β θετικοί ακέραιοι με $\alpha\succ\beta$ τότε $\gcd(\alpha,\beta)=\gcd(\beta,\alpha \bmod \beta)$.

Ορισμός 9. Αν n, α, β είναι θετικοί ακέραιοι , ο α λέγεται ότι είναι ισοδύναμος με τον $\beta \bmod n$ και γράφουμε $a = \beta \bmod n$, αν ο n διαιρεί τον $(\alpha - \beta)$.

Ιδιότητα 8. Για όλους τους $\alpha, \alpha_1, \beta, \beta_1, \gamma \in \mathbb{Z}$ με $n \succ 0$ ισχύουν τα παρακάτω:

α) $a = \beta \bmod n$ αν και μόνο αν οι α, β έχουν το ίδιο υπόλοιπο όταν διαιρεθούν με το n.

β) $\alpha = \alpha \bmod n$.

γ) Αν $a = \beta \bmod n$ τότε $\beta = \alpha \bmod n$.

δ) Αν $a = \beta \bmod n$ και $\beta = \gamma \bmod n$ τότε $a = \gamma \bmod n$.

ε) Αν $a = \alpha_1 \bmod n$ και $\beta = \beta_1 \bmod n$ τότε $\alpha + \beta \equiv (\alpha_1 + \beta_1) \bmod n$ και $\alpha \cdot \beta \equiv (\alpha_1 \cdot \beta_1) \bmod n$.

Ορισμός 10. Οι ακέραιοι $\bmod n$ ορίζουν το σύνολο $Z_n = \{0, 1, 2, ..., n-1\}$.

Ορισμός 11. Έστω $\alpha \in Z_n$. Ο αντίστροφος του $\alpha \bmod n$ είναι ένας ακέραιος $x \in Z_n$ τέτοιος ώστε $\alpha \cdot x = 1 \bmod n$. Αν υπάρχει τέτοιο x τότε αυτό είναι μοναδικό, συμβολίζεται α^{-1} και θα λέγεται αντιστρέψιμος.

Ορισμός 12. Έστω $\alpha, \beta \in Z_n$. Η διαίρεση του α με το $\beta \bmod n$ είναι το γινόμενο του α και του $\beta^{-1} \bmod n$ και ορίζεται μόνο αν ο $\beta \bmod n$ είναι αντιστρέψιμος.

Ιδιότητα 9. Έστω $\alpha \in Z_n$, ο α είναι αντιστρέψιμος αν και μόνο αν $\gcd(\alpha, n) = 1$.

Ιδιότητα 10. (Κινέζικο Θεώρημα) Αν οι ακέραιοι $n_1, n_2, ..., n_k$ είναι ανά δύο σχετικώς πρώτοι τότε το σύστημα των εξισώσεων :

$$x = a_1 \bmod n_1$$
$$x = a_2 \bmod n_2$$
$$\vdots$$
$$x = a_k \bmod n_k$$

έχει μια μοναδική λύση $\bmod n$ όπου: $n = n_1 \cdot n_2 \cdot ... \cdot n_k$.

Ιδιότητα 11. Αν $\gcd(n_1, n_2) = 1$, τότε το ζευγάρι εξισώσεων $x = a \bmod n_1$ και $x = a \bmod n_2$ έχει μοναδική λύση την $x = a \bmod (n_1 n_2)$.

Ορισμός 13. Η πολλαπλασιαστική ομάδα του Z_n είναι $Z_n^* = \{a \in Z_n \mid \gcd(a, n) = 1\}$. Ειδικά αν n είναι πρώτος αριθμός τότε $Z_n^* = \{a \mid 1 \le a \le n-1\}$.

Ορισμός 14. Τάξη του Z_n^* ορίζεται ο αριθμός των στοιχείων στο Z_n^* και συμβολίζεται με $|Z_n^*|$.

Σχετικά με την συνάρτηση του Euler έχουμε ότι: $\varphi(n) = |Z_n^*|$. Ειδικά αν n πρώτος τότε ισχύει : $\varphi(n) = |Z_{\overline{n}}^*| \quad n-1$.

Ιδιότητα 12. Έστω ένας ακέραιος $n \ge 2$ τότε:

α) **(Θεώρημα Euler)** Αν $a \in Z_n^*$ τότε $a^{\varphi(n)} = 1 \bmod n$.

β) Αν n είναι γινόμενο διαφορετικών πρώτων αριθμών και αν $r = s \bmod \varphi(n)$ τότε $a^r = a^s \bmod n$ για όλους τους ακέραιους a.

Ιδιότητα 13. Έστω ένας πρώτος αριθμός p τότε:

α) **(Θεώρημα Fermat)** Αν $\gcd(a, p) = 1$ τότε $a^{p-1} = 1 \bmod p$.

β) Αν $r = s \pmod{p-1}$ τότε $a^r = a^s \pmod p$ για όλους τους ακέραιους a.

γ) $a^p = a \pmod p$ για όλους τους ακέραιους a.

Ορισμός 15. Έστω $a \in Z_n^*$. Τάξη του a $(ord(a))$ είναι ο ελάχιστος θετικός ακέραιος t τέτοιος ώστε $a^t = 1 \pmod n$.

Ιδιότητα 14. Αν η τάξη του $a \in Z_n^*$ είναι t και $a^s = 1 \pmod n$ τότε ο t διαιρεί τον s.

Ορισμός 16. Έστω $a \in Z_n^*$. Αν η τάξη του a είναι $\varphi(n)$ τότε ο a είναι πρωταρχική ρίζα $\bmod n$. Αν το Z_n^* είναι κυκλική ομάδα οι έννοιες γεννήτορας και πρωταρχική ρίζα συμπίπτουν.

Ιδιότητα 15. Ιδιότητες των πρωταρχικών ριζών του Z_n^*:

α) Το Z_n^* έχει πρωταρχική ρίζα αν και μόνο αν $n = 2$ ή 4 ή p^k ή $2p^k$ όπου p είναι περιττός πρώτος αριθμός και $k \geq 1$.

β) Αν a είναι πρωταρχική ρίζα του Z_n^* τότε $Z_n^* = \left\{ a^i \bmod n \middle| 0 \leq i \leq \varphi(n) - 1 \right\}$.

γ) Έστω a μια πρωταρχική ρίζα του Z_n^*. Τότε $\beta = a^i \bmod n$ είναι επίσης πρωταρχική ρίζα του Z_n^* αν και μόνο αν $\gcd(i, \varphi(n)) = 1$. Αν το Z_n^* είναι κυκλικό τότε ο αριθμός των πρωταρχικών ριζών είναι $\varphi(\varphi(n))$.

δ) Έστω $a \in Z_n^*$, ο a είναι πρωταρχική ρίζα του Z_n^* αν και μόνο αν $a^{\frac{\varphi(n)}{p}} \neq 1 (\bmod n)$ για κάθε πρώτο διαιρέτη p του $\varphi(n)$.

Ορισμός 17. Έστω $a \in Z_n^*$, το a είναι τετραγωνικό υπόλοιπο του modulo n αν υπάρχει $x \in Z_n^*$ τέτοιο που $x^2 = a (\bmod n)$. Αν δεν υπάρχει τέτοιο x τότε το a λέγεται μη τετραγωνικό υπόλοιπο του modulo n. Το σύνολο των τετραγωνικών υπολοίπων του modulo n είναι το Q_n και το σύνολο των μη τετραγωνικών υπολοίπων του modulo n είναι το $\overline{Q_n}$.

Ιδιότητα 16. Έστω p είναι ένας περιττός πρώτος αριθμός και a μια πρωταρχική ρίζα του Z_p^*. Τότε $\beta \in Z_p^*$ είναι τετραγωνικό υπόλοιπο του modulo p αν και μόνο αν $\beta = a^i \bmod p$ όπου i είναι ένας άρτιος ακέραιος αριθμός. Τότε έπεται ότι: $|Q_p| = \frac{p-1}{2}$ και $|\overline{Q_p}| = \frac{p-1}{2}$, δηλαδή τα μισά στοιχεία στο Z_p^* είναι τετραγωνικά υπόλοιπα και τα άλλα μισά δεν είναι.

Παράδειγμα : Έστω $p=17$ ένας περιττός πρώτος αριθμός. Για να βρούμε τα τετραγωνικά υπόλοιπα στο Z_{17}^* εργαζόμαστε ως εξής :

$1^2=1 \bmod 17$, $2^2=4 \bmod 17$, $3^2=9 \bmod 17$, $4^2=16 \bmod 17$, $5^2=8 \bmod 17$, $6^2=2 \bmod 17$, $7^2=15 \bmod 17$, $8^2=13 \bmod 17$, $9^2=13 \bmod 17=8^2$, $10^2=15 \bmod 17=7^2$, $11^2=2 \bmod 17=6^2$, $12^2=8 \bmod 17=5^2$, $13^2=16 \bmod 17=4^2$, $14^2=9 \bmod 17=3^2$, $15^2=4 \bmod 17=2^2$, $16^2=1 \bmod 17=1^2$.

Άρα $Q_{17}=\{1,2,4,8,9,13,15,16\}$ και $\overline{Q_{17}}=\{3,5,6,7,10,11,12,14\}$. Όντως τα μισά στοιχεία στο Z_{17}^* είναι τετραγωνικά υπόλοιπα και τα άλλα μισά μη τετραγωνικά υπόλοιπα.

Ιδιότητα 17. Έστω n είναι το γινόμενο δύο διαφορετικών πρώτων αριθμών p και q, δηλαδή $n=p\cdot q$. Τότε $a\in Z_n^*$ είναι ένα τετραγωνικό υπόλοιπο του modulo n αν και μόνο αν $a\in Q_p$ και $a\in Q_q$.

Ορισμός 18. Έστω $a\in Q_n$. Αν $x\in Z_n^*$ ικανοποιεί την εξίσωση $x^2=a(\bmod n)$ τότε το x λέγεται τετραγωνική ρίζα του $a \bmod n$.

Ιδιότητα 18. Για τον αριθμό των τετραγωνικών ριζών ισχύουν:

α) Αν p είναι περιττός πρώτος και $a\in Q_p$ τότε ο α έχει ακριβώς δυο τετραγωνικές ρίζες $\bmod p$.

β) Έστω $n=p_1^{e_1}\cdot p_2^{e_2}\cdot ...\cdot p_k^{e_k}$ όπου p_i είναι διαφορετικοί περιττοί πρώτοι αριθμοί και $e_i\geq 1$. Αν $a\in Q_n$ τότε ο α έχει ακριβώς 2^k διαφορετικές τετραγωνικές ρίζες $\bmod n$.

Ορισμός 19. Ένας Blum ακέραιος είναι ένας σύνθετος ακέραιος n με $n=p\cdot q$ όπου p,q είναι διαφορετικοί πρώτοι και $p=3 \bmod 4$ και $q=3 \bmod 4$.

Ιδιότητα 19. Έστω $n=p\cdot q$ είναι ένας Blum ακέραιος και $a\in Q_n$. Τότε ο α έχει ακριβώς τέσσερις τετραγωνικές ρίζες $\bmod n$ και μόνο μια από αυτές ανήκει στο Q_n.

Ορισμός 20. Έστω n είναι ένας Blum ακέραιος και $a \in Q_n$. Τότε η μοναδική τετραγωνική ρίζα του α στο Q_n λέγεται κύρια τετραγωνική ρίζα του $a \bmod n$.

Ιδιότητα 20. Έστω $n = p \cdot q$ είναι ένας Blum ακέραιος, τότε η συνάρτηση $f : Q_n \to Q_n$ ορίζεται από τον τύπο $f(x) = x^2 \bmod n$ και είναι μια μετάθεση. Η αντίστροφη της f είναι $f^{-1}(x) = x^{((p-1)(q-1)+4)/8}$.

Ορισμός 21. Έστω p είναι ένας περιττός πρώτος και a ένας ακέραιος. Το σύμβολο Legendre $\left(\frac{a}{p}\right)$ ορίζεται ως εξής:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \alpha\nu\ p \mid a \\ 1 & \alpha\nu\ \alpha \in Q_p \\ -1 & \alpha\nu\ a \in \overline{Q_p} \end{cases}$$

Ιδιότητα 21. Έστω p είναι ένας περιττός πρώτος και $a, \beta \in \mathbb{Z}$. Τότε το σύμβολο Legendre έχει τις ακόλουθες ιδιότητες:

α) $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p$

β) $\left(\frac{a\beta}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{\beta}{p}\right)$

γ) Αν $a = \beta \pmod p$ τότε $\left(\frac{a}{p}\right) = \left(\frac{\beta}{p}\right)$

δ) Αν q είναι περιττός πρώτος διαφορετικός από τον p τότε: $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$. Η ιδιότητα αυτή λέγεται νόμος τετραγωνικής αντιστροφής (QRL) και πρωτοαποδείχτηκε από τον Gauss.

Ορισμός 22. Έστω $n \geq 3$ περιττός με $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$. Το σύμβολο Jacobi $\left(\frac{a}{n}\right)$ ορίζεται ως εξής: $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \left(\frac{a}{p_2}\right)^{e_2} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{e_k}$.

Ιδιότητα 22. Έστω $m \geq 3, n \geq 3$ περιττοί ακέραιοι και $a, \beta \in \mathbb{Z}$. Τότε το σύμβολο Jacobi έχει τις ακόλουθες ιδιότητες:

α) $\left(\frac{a}{n}\right) = 0, -1, 1$. Ισχύει $\left(\frac{a}{n}\right) = 0$ ανν $\gcd(a, n) \neq 1$.

β) $\left(\frac{a\beta}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{\beta}{n}\right)$

γ) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

δ) Αν $a = \beta \pmod{n}$ τότε $\left(\frac{a}{n}\right) = \left(\frac{\beta}{n}\right)$

ε) $\left(\frac{1}{n}\right) = 1$

στ) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

ζ) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

η) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)^{\frac{(m-1)(n-1)}{4}}$.

1.2.4 Άλγεβρα

1.2.4.1 Ομάδες

Ορισμός 1. Μία ομάδα $(G, *)$ αποτελείται από ένα σύνολο G εφοδιασμένο με τη διμελή πράξη $*$ που ικανοποιεί τα παρακάτω:

(α) Αν $\alpha, \beta \in G$ τότε και $\alpha + \beta \in G$.

(β). Η $*$ είναι προσεταιριστική. Δηλαδή $a*(\beta*\gamma) = (\alpha*\beta)*\gamma$ για όλα τα $\alpha, \beta, \gamma \in G$.

(γ). Υπάρχει ένα στοιχείο $1 \in G$ τέτοιο που $a*1 = 1*a = a$ για όλα τα $a \in G$ και λέγεται ουδέτερο στοιχείο.

(δ). Για κάθε $a \in G$ υπάρχει ένα στοιχείο $a^{-1} \in G$ που λέγεται αντίστροφο του α τέτοιο που $a * a^{-1} = a^{-1} * a = 1$.

$\Rightarrow$Η ομάδα $(G,*)$ είναι αβελιανή αν η $*$ είναι αντιμεταθετική. Δηλαδή $a * \beta = \beta * a$ για όλα τα $\alpha, \beta \in G$.

Ορισμός 2. Μία ομάδα G είναι πεπερασμένη αν $|G|$ είναι πεπερασμένο. Ο αριθμός των στοιχείων μιας πεπερασμένης ομάδας λέγεται τάξη της ομάδας.

Ορισμός 3. Ένα μη κενό υποσύνολο Η της ομάδος G είναι υποομάδα της G αν το Η είναι ομάδα και σέβεται την πράξη $*$ της G. Αν το Η είναι υποομάδα της G και $H \neq G$ τότε το Η λέγεται γνήσια υποομάδα της G . Η υποομάδα που αποτελείται από την ίδια τη G λέγεται μη γνήσια υποομάδα της G. Η υποομάδα $\{e\}$ είναι η τετριμμένη υποομάδα της G. Όλες οι άλλες υποομάδες λέγονται μη τετριμμένες.

Ορισμός 4. Μία ομάδα G είναι κυκλική αν υπάρχει ένα στοιχείο $a \in G$ τέτοιο που για κάθε $\beta \in G$ υπάρχει ακέραιος i με $\beta = \alpha^i$.Το α λέγεται γεννήτορας της G.

Ιδιότητα 1. Αν G είναι μία ομάδα και $a \in G$, τότε το σύνολο των δυνάμεων του a είναι μία κυκλική υποομάδα του G που δημιουργήθηκε από το a και συμβολίζεται (a).

Ορισμός 5. Έστω G είναι μία ομάδα και $a \in G$. Τάξη του α είναι ο ελάχιστος θετικός ακέραιος t τέτοιος που $a^t = 1$ αν υπάρχει τέτοιος t. Αν δεν υπάρχει τότε η τάξη του α είναι άπειρη.

Ιδιότητα 2. Έστω G είναι μία ομάδα και $a \in G$ τάξης t. Τότε $|(\alpha)|$, το μέγεθος της υποομάδας που δημιουργήθηκε από το α είναι ίσο με t.

Ιδιότητα 3. (Θεώρημα Lagrance). Αν G είναι μία πεπερασμένη ομάδα και Η είναι μία υποομάδα του G , τότε $|\mathrm{H}|$ διαιρεί το $|G|$. Αν $a \in G$, η τάξη του a διαιρεί το $|G|$.

Ιδιότητα 4. Κάθε υποομάδα της κυκλικής ομάδας G είναι επίσης κυκλική. Αν G είναι κυκλική ομάδα τάξης n τότε για κάθε θετικό διαιρέτη d του n, η G περιέχει ακριβώς μία υποομάδα τάξης d.

Ιδιότητα 5. Έστω G είναι μία ομάδα.

(α). Αν η τάξη του $\alpha \in G$ είναι t τότε η τάξη του a^{κ} είναι t/gcd (t, κ).

(β). Αν G είναι κυκλική ομάδα τάξης n και $d \mid n$ τότε η G έχει ακριβώς φ(d) στοιχεία τάξης d. Δηλαδή η G έχει φ(n) γεννήτορες.

1.2.4.2 Δακτύλιοι

Ορισμός 1. Ένας δακτύλιος $(R,+,\times)$ αποτελείται από ένα σύνολο R, με τουλάχιστον δύο στοιχεία $\{0,1\}$, με δυο διμελείς πράξεις $+$ και $\times$ που ικανοποιούν τα παρακάτω:

α) Η $(R,+)$ είναι αβελιανή ομάδα με ουδέτερο στοιχείο το 0.

β) Η πράξη $\times$ είναι προσεταιριστική. Δηλαδή $a\times(\beta\times\gamma)=(\alpha\times\beta)\times\gamma$ για όλα τα $\alpha,\beta,\gamma\in R$.

γ) Υπάρχει ουδέτερο στοιχείο στη πράξη $\times$ το 1 με $1\neq 0$ τέτοιο ώστε $1\times\alpha=\ \alpha\times 1=\alpha$ για όλα τα $\alpha\in R$.

δ) Η πράξη $\times$ είναι επιμεριστική στην $+$. Δηλαδή $\alpha\times(\beta+\gamma)=(\alpha\times\beta)+(\alpha\times\gamma)$ και $(\beta+\gamma)\times\alpha\ =(\beta\times\alpha)+(\gamma\times\alpha)$ για όλα τα $\alpha,\beta,\gamma\in R$.

$\Rightarrow$Ο δακτύλιος $(R,+,\times)$ είναι αντιμεταθετικός ή αβελιανός αν $\alpha\times\beta=\beta\times\alpha$ για όλα τα $\alpha,\beta\in R$

Ορισμός 2. Ένα στοιχείο α του δακτυλίου R λέγεται αντιστρέψιμο αν υπάρχει στοιχείο β του R τέτοιο ώστε $\alpha\times\beta=1$.

Ιδιότητα 1. Το σύνολο των αντιστρέψιμων στοιχείων του δακτυλίου R στην πράξη $\times$ είναι ομάδα και λέγεται ομάδα των αντιστρέψιμων στοιχείων του R.

1.2.4.3 Σώματα

Ορισμός 1. Ένα σώμα F είναι ένας μεταβατικός δακτύλιος όπου όλα τα μη μηδενικά στοιχεία είναι αντιστρέψιμα.

Ορισμός 2. Η χαρακτηριστική ενός σώματος είναι m αν η παράσταση $1+1+...+1$ δεν είναι ποτέ 0 για λιγότερους από m προσθετέους. Αλλιώς η χαρακτηριστική του σώματος είναι ο ελάχιστος θετικός ακέραιος m τέτοιος που $\sum_{i=1}^{m} 1 = 0$.

Ιδιότητα 1. Το Z_n είναι σώμα (με τις συνηθισμένες πράξεις της πρόσθεσης και του πολλαπλασιασμού modn) αν και μόνο αν ο n είναι πρώτος αριθμός. Αν ο n είναι πρώτος τότε το Z_n έχει χαρακτηριστική n.

Ιδιότητα 2. Αν η χαρακτηριστική n του σώματος δεν είναι 0 τότε ο n είναι πρώτος αριθμός.

Ορισμός 3. Ένα υποσύνολο F του σώματος E, είναι υποσώμα του E αν το F είναι σώμα και σέβεται τις πράξεις του E. Το σώμα E λέγεται επέκταση του σώματος F.

Ορισμός 4. Ένα πεπερασμένο σώμα F είναι ένα σώμα που έχει πεπερασμένο αριθμό στοιχείων. Τάξη του F είναι ο αριθμός των στοιχείων του F.

Ιδιότητα 3. Αν F είναι πεπερασμένο σώμα τότε περιέχει p^m στοιχεία όπου p είναι πρώτος αριθμός και $m \geq 1$.

Ιδιότητα 4. Για κάθε δύναμη p^m του πρώτου p υπάρχει ένα μοναδικό πεπερασμένο σώμα τάξης p^m. Το σώμα αυτό συμβολίζεται με F_{p^m}. (Το θεώρημα αυτό οφείλεται στον E. Galois)

Ιδιότητα 5. Αν F_q είναι πεπερασμένο σώμα τάξης $q = p^m$ όπου p είναι πρώτος αριθμός τότε η χαρακτηριστική του F_q είναι p. Το F_q περιέχει ένα αντίγραφο του Z_p ως υποσώμα του F_q. Το F_q είναι μία επέκταση του Z_p βαθμού m.

1.2.4.4 Ελλειπτικές Καμπύλες

Ορισμός 1. Έστω $p > 3$ ένας πρώτος αριθμός. Η ελλειπτική καμπύλη E $y^2 = x^3 + ax + \beta$ στο Z_p είναι το σύνολο των λύσεων $(x, y) \in Z_p \times Z_p$ της $y^2 = x^3 + ax + \beta (\text{mod } p)$, όπου $\alpha, \beta \in Z_p$ είναι σταθερές τέτοιες που $4a^3 + 27\beta^2 \neq 0 (\text{mod } p)$ με το ειδικό σημείο O που λέγεται σημείο στο άπειρο.

Ορισμός 2. Έστω E μια ελλειπτική καμπύλη και $P(x, y)$, $Q(x', y')$ δύο σημεία της καμπύλης E. Ορίζουμε το αντίθετο του P και το άθροισμα $P + Q$ σύμφωνα με τους παρακάτω κανόνες:

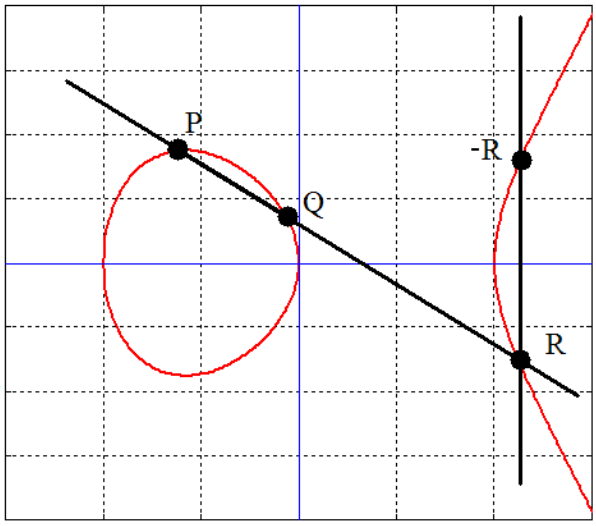
(α). Αν το P είναι το σημείο στο άπειρο O τότε το $-P$ είναι το O. Για οποιοδήποτε σημείο Q ορίζουμε το $O + Q = O$.

Στα παρακάτω θεωρούμε ότι $P, Q \neq O$.

(β). Το $-P$ έχει συντεταγμένες $(x, -y)$ δηλαδή $-(x, y)$ $(x, -y)$ και ανήκει στην ελλειπτική καμπύλη E. Αν $Q = -P$ τότε ορίζουμε $P + Q = O$.

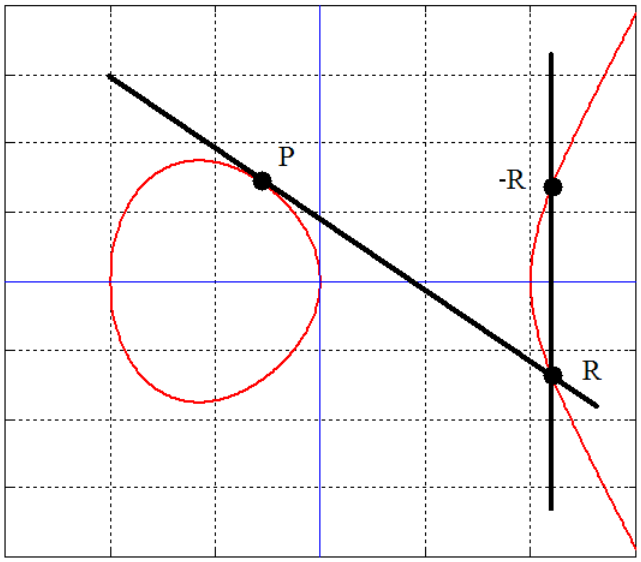
(γ). Αν $x \neq x'$ τότε η ευθεία $\varepsilon = \overline{PQ}$ τέμνει την E και σε ένα άλλο σημείο R (εκτός αν η ε είναι εφαπτομένη στην E στο P όπου παίρνουμε $R = P$ ή στο Q όπου παίρνουμε $R = Q$). Τότε ορίζουμε το $P + Q$ να είναι το $-R$, που είναι η προβολή στον άξονα $x'x$ του R και $-R \in E$.

Στο παρακάτω σχήμα φαίνεται η πρόσθεση σημείου, δηλαδή ισχύει : $-R = P + Q$.



(δ). Αν $P = Q$, τότε η ευθεία $\varepsilon = \overline{PQ}$ είναι εφαπτομένη της Ε στο P και R είναι το μοναδικό άλλο σημείο της Ε και ορίζουμε $2P = -R$

Στο παρακάτω σχήμα φαίνεται ο διπλασιασμός σημείου, δηλαδή ισχύει : $-R = 2P$.



Ιδιότητα 1. Έστω $P=(x_1,y_1)$ και $Q=(x_2,y_2)$ είναι σημεία της ελλειπτικής καμπύλης Ε.

(α). Αν $x_2=x_1$ και $y_2=-y_1$ τότε $P+Q=O$

(β). Αλλιώς P+Q= $P+Q=(x_3,y_3)$ όπου :

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

$$y_3=\lambda(x_1-x_3)-y_1 \qquad \text{με } \lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & \alpha\nu \quad P=Q \\ \dfrac{3x_1^{\,2}+a}{2y_1} & \alpha\nu \quad P\neq Q\end{cases}$$

Ιδιότητα 2. Η παραπάνω ιδιότητα και ο ορισμός του αθροίσματος $P+Q$ κάνει τα σημεία της ελλειπτικής καμπύλης να είναι στοιχεία μιας αβελιανής ομάδας.

1.3 Θεωρία πολυπλοκότητας και αλγόριθμοι

Θα αναφέρουμε βασικές έννοιες της θεωρίας πολυπλοκότητας και ορισμένους αλγορίθμους που θα χρησιμοποιήσουμε στις ψηφιακές υπογραφές. Είναι σημαντικό να γνωρίζουμε τους αλγόριθμους που θα χρησιμοποιήσουμε, σε ποιες κλάσεις πολυπλοκότητας ανήκουν, ποια είναι τα χαρακτηριστικά αυτών των κλάσεων και ποια είναι η εξέλιξη των ανοικτών προβλημάτων στις κλάσεις αυτές.

Όταν αναφέρουμε για ένα πρόβλημα ότι είναι υπολογιστικά ανέφικτο να το λύσουμε εννοούμε ότι δεν μπορούμε να το λύσουμε σε πολυωνυμικό χρόνο ως προς την είσοδο του προβλήματος.

Στόχος αυτού του κεφαλαίου είναι να δούμε την κατάταξη των προβλημάτων ως προς το χρόνο επίλυσης τους που σχετίζονται με τις ψηφιακές υπογραφές και διάφορους χρήσιμους αλγορίθμους.

1.3.1 Θεωρία πολυπλοκότητας

Σε αυτή την παράγραφο θα δούμε τους ασυμπτωτικούς ορισμούς και τις κλάσεις πολυπλοκότητας.

Προβλήματα που είναι εύκολα υπολογίσιμα δεν μας είναι χρήσιμα στις ψηφιακές υπογραφές. Είναι ανοικτό ερώτημα αν $P = NP$ και ότι το πρόβλημα απόφασης αν ένας ακέραιος αριθμός είναι σύνθετος ανήκει στην κλάση NP. Αν για παράδειγμα στο μέλλον αποδειχθεί ότι $P = NP$ τότε πολλά κρυπτοσυστήματα που χρησιμοποιούνται στις ψηφιακές υπογραφές θα είναι πρακτικά άχρηστα(π.χ. το RSA). Έχει λοιπόν μεγάλη σημασία να γνωρίζουμε τις κλάσεις πολυπλοκότητας που ανήκουν οι αλγόριθμοι που χρησιμοποιούμε.

Θα δούμε ότι ακόμα και αν συσχετίσουμε ένα σχήμα ψηφιακής υπογραφής με ένα NP πρόβλημα αυτό δεν θα είναι πολύ χρήσιμο για τις ψηφιακές υπογραφές. Η μελέτη των κλάσεων πολυπλοκότητας δεν έχει την ίδια προσέγγιση στις ψηφιακές υπογραφές (και γενικότερα στην κρυπτογραφία) :

α. Γνωρίζουμε ότι το κρυπτοσύστημα RSA στηρίζει την ασφάλεια του στο πρόβλημα της παραγοντοποίησης ενός ακεραίου που δεν ξέρουμε αν είναι NP-complete και το κρυπτοσύστημα των Merkle και Hellman στο subset sum πρόβλημα που γνωρίζουμε ότι είναι NP-complete. Δηλαδή θα περιμέναμε το δεύτερο κρυπτοσύστημα να είναι πιο ασφαλές από το πρώτο αφού στηρίζεται σε πιο δύσκολο πρόβλημα. Τα αποτελέσματα όμως είναι διαφορετικά. Ο Adi Shamir το 1984 κατάφερε για μία ειδική περίπτωση του subset sum προβλήματος να αποδείξει ότι λύνεται σε πολυωνυμικό χρόνο. Έτσι το κρυπτοσύστημα των Merkle και Hellman κατέρρευσε. Την εξήγηση του παραπάνω αποτελέσματος μας τη δίνει το θεώρημα του Brassard. Το σημαντικό στοιχείο είναι ότι η κρυπτογραφία δεν πρέπει να στηρίζεται σε προβλήματα που είναι NP-complete αλλά σε προβλήματα που η δυσκολία τους βρίσκεται ανάμεσα στις κλάσεις P και NP-complete.

β. Στη θεωρία πολυπλοκότητας μελετάμε τα προβλήματα στη χειρότερη τους περίπτωση (worst case) όπου και υπολογίζουμε τους χρόνους εκτέλεσης και θέλουμε

αλγορίθμους με καλή απόδοση σε αυτή την περίπτωση. Στα σχήματα όμως των ψηφιακών υπογραφών αυτό δεν αρκεί. Για παράδειγμα δεν είναι αποδεκτός αυτός ο αλγόριθμος που δίνει το δικαίωμα στον αντίπαλο να αποκρυπτογραφήσει τα μισά από όλα τα πιθανά μηνύματα ακόμα και αν η αποκρυπτογράφηση των υπολοίπων θέλει εκθετικό χρόνο.

Είναι τώρα ξεκάθαρο ότι η χειρότερη περίπτωση στην πολυπλοκότητα δεν είναι σημαντικό κριτήριο για τις ψηφιακές υπογραφές.

1.3.2 Ασυμπτωτικοί ορισμοί

Ο κύριος στόχος της θεωρίας πολυπλοκότητας είναι να ορίσουμε μηχανισμούς για την ταξινόμηση των προβλημάτων σύμφωνα με τις πηγές που χρειάζονται για την επίλυση τους. Η ταξινόμηση δε βασίζεται σε ένα συγκεκριμένο μοντέλο υπολογισμού αλλά στη μέτρηση της πραγματικής δυσκολίας για την επίλυση του προβλήματος. Οι πηγές που θα μας απασχολήσουν μπορεί να είναι χρόνος(κυρίως), χώρος, τυχαία bits, αριθμός επεξεργαστών κ.λπ.

Ορισμός 1. Ένας αλγόριθμος είναι μία καλά ορισμένη υπολογιστική διαδικασία που έχει μια συγκεκριμένη είσοδο και τερματίζει σε μία έξοδο.

Ορισμός 2. Ο χρόνος εκτέλεσης ενός αλγορίθμου για μια συγκεκριμένη είσοδο είναι ο συνολικός αριθμός πράξεων ή βημάτων που απαιτούνται για την επίλυση του προβλήματος που περιγράφει ο αλγόριθμος.

Ορισμός 3. Ο χειρότερος χρόνος εκτέλεσης ενός αλγορίθμου είναι ένα πάνω όριο του χρόνου εκτέλεσης του αλγορίθμου για οποιαδήποτε είσοδο και εκφράζεται σαν συνάρτηση του μεγέθους της εισόδου.

Επειδή είναι συχνά δύσκολο να βρούμε ακριβώς το χρόνο εκτέλεσης ενός αλγορίθμου, χρησιμοποιούμε τους ασυμπτωτικούς τύπους που θα ορίσουμε παρακάτω. Θεωρούμε ότι το μέγεθος της εισόδου του αλγορίθμου είναι n και ο χρόνος εκτέλεσης του αλγορίθμου είναι $f(n)$.

Ορισμός 4.

α) $f(n)=O(g(n))$ αν υπάρχει θετική σταθερά c και ένας θετικός ακέραιος n_0 τέτοιος που $0\le f(n)\le c\cdot g(n)$ για όλα τα $n\ge n_0$.

β) $f(n)=\Omega(g(n))$ αν υπάρχει θετική σταθερά c και ένας θετικός ακέραιος n_0 τέτοιος που $0\le c\cdot g(n)\le f(n)$ για όλα τα. $n\ge n_0$

γ) $f(n)=\Theta(g(n))$ αν υπάρχουν θετικές σταθερές c_1 και c_2 και ένας θετικός ακέραιος n_0 τέτοιος που $c_1\cdot g(n)\le f(n)\le c_2\cdot g(n)$ για όλα τα $n\ge n_0$.

δ) $f(n)=o(g(n))$ αν για κάθε θετική σταθερά c υπάρχει ένας σταθερός n_0 τέτοιος που $0\le f(n)\le c\cdot g(n)$ για όλα τα $n\ge n_0$.

Ιδιότητα 1. Για οποιεσδήποτε συναρτήσεις $f(n),g(n),h(n),l(n)$ ισχύουν τα παρακάτω :

α) $f(n)=O(g(n))$ αν και μόνο αν $g(n)=\Omega(f(n))$.

β) $f(n)=\Theta(g(n))$ αν και μόνο αν $f(n)=O(g(n))$ και $f(n)=\Omega(g(n))$.

γ) Αν $f(n)=O(h(n))$ και $g(n)=O(h(n))$ τότε $(f+g)(n)=O(h(n))$.

δ) Αν $f(n)=O(h(n))$ και $g(n)=O(l(n))$ τότε $(f\cdot g)(n)\quad \Theta(h(n)\cdot l(n))$.

ε) $f(n)=O(f(n))$.

στ) Αν $f(n)=O(g(n))$ και $g(n)=O(h(n))$ τότε $f(n)=O(h(n))$.

Ιδιότητα 2.

α) Αν $f(n)$ είναι πολυώνυμο βαθμού k με θετικό συντελεστή του μεγιστοβάθμιου όρου τότε $f(n)=\Theta(n^k)$.

β) Για οποιαδήποτε θετική σταθερά c ισχύει $\log_c n=\Theta(\log n)$.

γ) $\log(n!)=\Theta(n\cdot\log n)$.

δ) Για όλους τους ακεραίους $n\ge 1$ ισχύει $\sqrt{2\pi n}\cdot\left(\frac{n}{e}\right)^n\le n!\le\sqrt{2\pi n}\cdot\left(\frac{n}{e}\right)^{n+\left(1/(12n)\right)}$ (τύπος του Stirling).

1.3.3 Κλάσεις πολυπλοκότητας

Ορισμός 1. Ένας αλγόριθμος πολυωνυμικού χρόνου είναι ένας αλγόριθμος του οποίου ο χειρότερος χρόνος εκτέλεσης είναι μία συνάρτηση του τύπου $O(n^k)$, όπου n είναι το μέγεθος της εισόδου του αλγορίθμου και k είναι μία σταθερά. Οποιοσδήποτε αλγόριθμος του οποίου ο χρόνος εκτέλεσης δεν μπορεί να είναι φραγμένος από ένα τέτοιο τύπο λέγεται αλγόριθμος εκθετικού χρόνου.

Για να ορίσουμε τις κλάσεις πολυπλοκότητας θα περιορισθούμε σε προβλήματα απόφασης, δηλαδή προβλήματα που έχουν σαν έξοδο το ΝΑΙ ή το ΟΧΙ σαν απάντηση.

Ορισμός 2. Η κλάση πολυπλοκότητας P περιλαμβάνει το σύνολο των προβλημάτων απόφασης που μπορούν να επιλυθούν σε πολυωνυμικό χρόνο.

Ορισμός 3. Η κλάση πολυπλοκότητας NP περιλαμβάνει το σύνολο των προβλημάτων απόφασης που μία απάντηση ΝΑΙ μπορεί να πιστοποιηθεί σε πολυωνυμικό χρόνο με κάποια επιπλέον πληροφορία που λέγεται πιστοποιητικό.

Ορισμός 4. Η κλάση πολυπλοκότητας $co-NP$ περιλαμβάνει το σύνολο των προβλημάτων απόφασης που μία απάντηση ΟΧΙ μπορεί να πιστοποιηθεί σε πολυωνυμικό χρόνο με κάποια επιπλέον πληροφορία που λέγεται πιστοποιητικό.

Παράδειγμα: Έστω ότι έχουμε το παρακάτω πρόβλημα απόφασης: Μας δίνεται ένας θετικός ακέραιος αριθμός n και θέλουμε να βρούμε αν ο n είναι σύνθετος. Δηλαδή αν υπάρχουν ακέραιοι $a,b \succ 1$ τέτοιοι που $n = a \cdot b$.
Το πρόβλημα αν ένας αριθμός είναι σύνθετος ανήκει στην κλάση NP υπάρχει γιατί αν ο n είναι σύνθετος, τότε αυτό το γεγονός μπορεί να πιστοποιηθεί σε πολυωνυμικό χρόνο αν κάποιος μας δώσει ένα διαιρέτη του n τον a όπου $1 \prec a \prec n$ (το πιστοποιητικό είναι ο α).

Γενικά ισχύει ότι $P \subseteq NP$ και $P \subseteq co-NP$.

1.3.4 Αλγόριθμοι

Θα δούμε πρώτα τον αλγόριθμο του Ευκλείδη που υπολογίζει το μέγιστο κοινό διαιρέτη δύο ακεραίων. Είσοδος του αλγορίθμου είναι δύο μη αρνητικοί ακέραιοι a και b με $a \geq b$ και έξοδος είναι ο μέγιστος κοινός διαιρέτης (gcd) των a και b.

α) Αλγόριθμος του Ευκλείδη

1. Όσο ισχύει $b \neq 0$ κάνε:
   Θέσε $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$.
2. Επέστρεψε το a.

Ο χρόνος του παραπάνω αλγορίθμου είναι $O((\log n)^2)$ δυαδικές πράξεις.

Μπορούμε να γενικεύσουμε τον αλγόριθμο του Ευκλείδη ώστε εκτός από το μέγιστο κοινό διαιρέτη των d των a, b να βρίσκει και δύο ακέραιους x, y τέτοιους που $d = xa + yb$. Είσοδος του αλγορίθμου είναι δύο μη αρνητικοί ακέραιοι a και b με $a \geq b$ και έξοδος είναι $\gcd(a,b) = d$ και ακέραιοι τέτοιοι x, y που $d = xa + yb$. Η επιπλέον αυτή διαδικασία μας δίνει τον Εκτεταμένο Ευκλείδειο Αλγόριθμο (Ε.Ε.Α.)

β) Εκτεταμένος Ευκλείδειος αλγόριθμος

1. Αν $b = 0$ τότε θέσε $d \leftarrow a, x \leftarrow 1, y \leftarrow 0$ και επέστρεψε (d, x, y).
2. Θέσε $x_2 \leftarrow 1, x_1 \leftarrow 0, y_2 \leftarrow 0, y_1 \leftarrow 1$.
3. Όσο ισχύει $b \succ 0$ κάνε: $q \leftarrow \lfloor a/b \rfloor, r \leftarrow a - q \cdot b, x \leftarrow x_2 - q \cdot x_1, y \leftarrow y_2 - q \cdot y_1$.
   $a \leftarrow b, b \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1, y_1 \leftarrow y$.
4. Θέσε $d \leftarrow a, x \leftarrow x_2, y \leftarrow y_2$ και επέστρεψε (d, x, y).

Ο χρόνος του παραπάνω αλγορίθμου είναι $O((\log n)^2)$ δυαδικές πράξεις.

Με τη βοήθεια του εκτεταμένου αλγορίθμου του Ευκλείδη μπορούμε να βρούμε το αντίστροφο στοιχείο σε μια πολλαπλασιαστική ομάδα αν υπάρχει. Είσοδος του αλγορίθμου είναι ένα στοιχείο $a \in Z_n$ και έξοδος το a^{-1} αν υπάρχει.

γ) Αλγόριθμος εύρεσης αντίστροφου στοιχείου

1. Χρησιμοποίησε τον εκτεταμένο αλγόριθμο του Ευκλείδη για να βρεις ακέραιους x και y τέτοιους που $d = xa + yb$ με $\gcd(a,b) = d$.
2. Αν $d \succ 1$ τότε δεν υπάρχει a^{-1}, αλλιώς επέστρεψε το (x).

Ο χρόνος του παραπάνω αλγορίθμου είναι $O((\log n)^2)$ δυαδικές πράξεις.

δ) Αλγόριθμος υπολογισμού $a^k \bmod n$

Είσοδος είναι $a \in Z_n$ και ένας ακέραιος k με $0 \le k \le n$ όπου η δυαδική αναπαράσταση είναι $k = \sum_{i=0}^{t} k_i \cdot 2^i$ και έξοδος $a^k \bmod n$.

1. Θέσε $b \leftarrow 1$. Αν $k = 0$ τότε επέστρεψε (b) .
2. Θέσε $A \leftarrow a$.
3. Αν $k_0 = 1$ τότε θέσε $b \leftarrow a$.
4. Για $i = 1$ έως t κάνε:

   Θέσε $A \leftarrow A^2 \bmod n$.

   Αν $k_i = 1$ τότε θέσε $b \leftarrow A \cdot b \bmod n$.
5. Επέστρεψε (b).

Ο χρόνος του παραπάνω αλγορίθμου είναι $O((\log n)^3)$ δυαδικές πράξεις.

Θα δούμε τώρα ένα αλγόριθμο για να υπολογίζουμε το σύμβολο Jacobi και την ειδική του μορφή το σύμβολο Legendre. Είσοδος του αλγορίθμου είναι ένας περιττός ακέραιος $n \ge 3$ και ένας ακέραιος a με $0 \le a \le n$ και έξοδος είναι $(J(a,n))$ (Αν ο n είναι πρώτος έχουμε το σύμβολο Legendre).

ε) Αλγόριθμος υπολογισμού συμβόλου Jacobi και Legendre

1. Αν $a = 0$ τότε επέστρεψε (0).
2. Αν $a = 1$ τότε επέστρεψε (1).
3. Γράψε τον $a = 2^e a_1$, όπου a_1 είναι περιττός.
4. Αν e είναι περιττός τότε θέσε $s \leftarrow 1$.
   Αλλιώς θέσε $s \leftarrow 1$ αν $n = 1$ ή $7 \pmod 8$ ή θέσε $s \leftarrow -1$ αν $n = 3$ ή $5 \pmod 8$.
5. Αν $n = 3 \pmod 4$ και $a_1 = 3 \pmod 4$ τότε θέσε $s \leftarrow -s$.
6. Θέσε $n_1 \leftarrow n \bmod a_1$.
7. Αν $a_1 = 1$ τότε επέστρεψε (s). Αλλιώς επέστρεψε $(s \cdot J(n_1, a_1))$.

Ο χρόνος του παραπάνω αλγορίθμου είναι $O((\log n)^2)$ δυαδικές πράξεις.

Θα εξετάσουμε αλγορίθμους που υπολογίζουν τετραγωνικές ρίζες στο Z_n. Αν ο n είναι πρώτος έχουμε καλά αποτελέσματα αλλά το πρόβλημα είναι δύσκολο όταν ο n είναι σύνθετος και δε γνωρίζουμε τους πρώτους παράγοντες του.

στ) Αλγόριθμος υπολογισμού τετραγωνικών ριζών

Είσοδος είναι ένας περιττός πρώτος a με $1 \le a \le p-1$ και p πρώτος αριθμός και έξοδος οι δύο τετραγωνικές ρίζες του $a \bmod p$ αν βέβαια a είναι τετραγωνικό υπόλοιπο στο Z_p^*.

1. Υπολόγισε το σύμβολο Legendre $(L(a, p))$ με τον αλγόριθμο (ε). Αν $L(a, p) = -1$ τότε επέστρεψε ότι ο a δεν έχει τετραγωνική ρίζα και σταμάτα.
2. Επέλεξε ακεραίους b με $1 \le b \le p-1$ τυχαία μέχρι να βρεις κάποιον με $L(b, p) = -1$ (Ο b δεν είναι τετραγωνικό υπόλοιπο).
3. Με επαναλαμβανόμενες διαιρέσεις με το 2 , γράψε $p-1 = 2^s \cdot t$ όπου t είναι περιττός.
4. Υπολόγισε το $a^{-1} \bmod p$ με τον αλγόριθμο (γ).

5. Θέσε $c \leftarrow b^t \bmod p$ και $r \leftarrow a^{(t+1)/2} \bmod p$ (Με τον αλγόριθμο (δ)).

6. Για $i = 1$ έως $s-1$ κάνε :

Υπολόγισε $d = \left(r^2 \cdot a^{-1}\right)^{2^{s-i-1}} \bmod p$.

Αν $d = -1 (\bmod p)$ τότε θέσε $r \leftarrow r \cdot c \bmod p$.

Θέσε $c \leftarrow c^2 \bmod p$.

7. Επέστρεψε $(r, -r)$.

Ο παραπάνω αλγόριθμος είναι πιθανοτικός και ο αναμενόμενος χρόνος εκτέλεσης είναι $O((\log n)^4)$ δυαδικές πράξεις.

ζ) Αλγόριθμος υπολογισμού τετραγωνικών ριζών με $p = 3 (\bmod 4)$

Είσοδος του αλγορίθμου είναι ένας περιττός πρώτος p με $p = 3 (\bmod 4)$ και ο $a \in Q_p$ και έξοδος δύο τετραγωνικές ρίζες του $a \bmod p$.

1. Υπολόγισε $r = a^{(p+1)/4} \bmod p$ (Με τον αλγόριθμο (δ)).
2. Επέστρεψε $(r, -r)$.

Ο χρόνος του παραπάνω αλγορίθμου είναι $O((\log p)^3)$ δυαδικές πράξεις.

η) Αλγόριθμος υπολογισμού τετραγωνικών ριζών με $p = 5 (\bmod 8)$

Είσοδος του αλγορίθμου είναι ένας περιττός πρώτος p με $p = 5 (\bmod 8)$, ο $a \in Q_p$ και έξοδος δύο τετραγωνικές ρίζες του $a \bmod p$.

1. Υπολόγισε $d = a^{(p-1)/4} \bmod p$ (Με τον αλγόριθμο (δ)).
2. Αν $d = 1$ τότε υπολόγισε $r = a^{(p+3)/8} \bmod p$.
3. Αν $d = p-1$ τότε υπολόγισε $r = 2a(4a)^{(p-5)/8} \bmod p$
4. Επέστρεψε $(r, -r)$.

Ο χρόνος του παραπάνω αλγορίθμου είναι $O((\log p)^3)$ δυαδικές πράξεις.

θ) Αλγόριθμος υπολογισμού τετραγωνικών ριζών

Ο αλγόριθμος αυτός έχει το ίδιο αποτέλεσμα με τον (στ) αλλά είναι καλύτερος όταν $p-1=2^s t$ και το s είναι μεγάλος αριθμός.

1. Επέλεξε τυχαία $b \in Z_p$ μέχρι ο b^2-4a να μην είναι τετραγωνικό υπόλοιπο του $\bmod p$.
2. Έστω f είναι πολυώνυμο $x^2-b\cdot x+a$ στο $Z_p[x]$.
3. Υπολόγισε $r=x^{(p+1)/2} \bmod f$.
4. Επέστρεψε $(r,-r)$.

Ο αναμενόμενος χρόνος του αλγορίθμου είναι $O((\log p)^3)$ δυαδικές πράξεις.

ι) Αλγόριθμος υπολογισμού τετραγωνικών ριζών όπου n είναι σύνθετος αριθμός και $n=p\cdot q$ με p,q πρώτοι αριθμοί.

Είσοδος του αλγορίθμου είναι ένας ακέραιος n, οι πρώτοι παράγοντες του p,q και $a \in Q_n$ και έξοδος οι 4 τετραγωνικές ρίζες του $a \bmod n$.

1. Υπολόγισε τις 2 τετραγωνικές ρίζες $r,-r$ του $a \bmod p$ (Χρησιμοποιώντας τον αλγόριθμο (στ) ή (ζ) ή (η) ή (θ)).
2. Υπολόγισε τις 2 τετραγωνικές ρίζες $s,-s$ του $a \bmod q$ (Χρησιμοποιώντας τον αλγόριθμο (στ) ή (ζ) ή (η) ή (θ)).
3. Βρες δύο ακέραιους c,d τέτοιους που $c\cdot p+d\cdot q=1$ (Χρησιμοποιώντας τον αλγόριθμο (β)).
4. Θέσε $x \leftarrow (rdq+scp) \bmod n$ και $y \leftarrow (rdq-scp) \bmod n$.
5. Επέστρεψε $(\pm x \bmod n, \pm y \bmod n)$.

Ο αναμενόμενος χρόνος του παραπάνω αλγορίθμου είναι $O((\log p)^3)$ δυαδικές πράξεις.

1.4 Παράδοξο των Γενεθλίων και Επίθεση Γενεθλίων

Το παράδοξο των γενεθλίων (**birthday paradox**) είναι ένα κλασικό πρόβλημα στη θεωρία των πιθανοτήτων το οποίο χρησιμοποιείται για να δώσει διάσταση στο πρόβλημα της επιλογής του μεγέθους της σύνοψης. Στη βιβλιογραφία έχει επικρατήσει ο όρος «παράδοξο» που αναφέρεται στη διαστρεβλωμένη αντίληψη που έχουμε για την εκτίμηση ορισμένων μεγεθών. Συνήθως το μέγεθος που επιλέγουμε με βάση την αντίληψή μας είναι πολύ μικρότερο από την πραγματικότητα.

Για παράδειγμα έστω ότι 30 άτομα παρευρίσκονται σε μια συγκέντρωση. Αν αναλογισθούμε την πιθανότητα δύο από αυτά να έχουν την ίδια ημέρα γενέθλια (σε διαφορετικό ή ίδιο έτος), τότε μάλλον εκτιμάμε ότι η πιθανότητα αυτή βρίσκεται κοντά στην τιμή 30/365 δηλαδή λίγο παραπάνω από 8%. Στην πραγματικότητα, η πιθανότητα να έχουν δύο από τα 30 άτομα γενέθλια την ίδια ημέρα είναι μεγαλύτερη του 50%. Αυτό υπολογίζεται (θεωρώντας χάριν απλότητας ότι δεν υπάρχουν δίσεκτα έτη και ότι όλες οι ημέρες του χρόνου είναι ισοπίθανο να είναι μέρες γενεθλίων) ως εξής:

Παραμετροποιούμε το πρόβλημα θεωρώντας n άτομα σε ένα χώρο και θέλουμε να υπολογίσουμε την πιθανότητα να έχουν οποιαδήποτε 2 άτομα γενέθλια την ίδια ημέρα. Αν η πιθανότητα αυτή είναι p_n, τότε η πιθανότητα να μην έχουν οποιαδήποτε 2 άτομα γενέθλια την ίδια μέρα θα είναι $p_n' = 1 - p_n$. Αρκεί λοιπόν να υπολογίσουμε την p_n'.

Έστω ότι τα άτομα εισέρχονται διαδοχικά στην αίθουσα της δεξίωσης. Η πιθανότητα του πρώτου ατόμου να μην έχει γενέθλια με κανένα από τα άτομα της αίθουσας είναι 1 ή 365/365, αφού δεν υπάρχει κανένα άλλο. Στη συνέχεια εισέρχεται το δεύτερο άτομο. Η πιθανότητα του δεύτερου ατόμου να μην έχει γενέθλια με το πρώτο, είναι (365-1)/365. Θα πρέπει δηλαδή τα γενέθλιά του να είναι μια από τις υπόλοιπες 364 μέρες του χρόνου. Παρόμοια, το τρίτο άτομο θα πρέπει να «επιλέξει» μεταξύ των 365-2 διαθέσιμων τιμών που δεν αντιστοιχούν στα γενέθλια των δύο προηγουμένων. Επομένως η πιθανότητα θα είναι ίση με : $p_3' = \frac{365}{365} \cdot \frac{(365-1)}{365} \cdot \frac{(365-2)}{365}$.

Όταν το *n*-στό άτομο εισέλθει στην αίθουσα, η πιθανότητα να μην έχει γενέθλια με κανένα από τα προηγούμενα άτομα, θα δίνεται από την : $p_n' = \frac{365}{365} \cdot \frac{(365-1)}{365} \cdot \ldots \cdot \frac{(365-n+1)}{365} = \frac{365!}{365^n (365-n)!}$.

Επομένως $p_n = 1 - \frac{365!}{365^n (365-n)!}$.

Από την παραπάνω σχέση προκύπτει ότι για $n = 23$ [Ή διαφορετικά αρκεί να προσδιορίσουμε εκείνο το n για το οποίο να ισχύει η σχέση : $\left(1-\frac{1}{365}\right) \cdot \left(1-\frac{2}{365}\right) \cdot \ldots \cdot \left(1-\frac{n}{365}\right) \geq \frac{1}{2}$. Αξιοποιώντας τη σχέση $1 + x \leq e^x$,που ισχύει $\forall x \in \mathbb{R}$, προκύπτει η ισοδύναμη σχέση : $e^{-\frac{1}{365}} \cdot e^{-\frac{2}{365}} \cdot \ldots \cdot e^{-\frac{n}{365}} \geq \frac{1}{2} \Rightarrow$ $e^{-\frac{1}{365}} \cdot \sum_{i=1}^{n} n \geq \frac{1}{2} \Rightarrow \quad -\frac{1}{365} \cdot \sum_{i=1}^{n} n \geq \ln\frac{1}{2} \Rightarrow \quad \frac{1}{365} \cdot \frac{n(n+1)}{2} \leq \ln 2$. Λύνοντας την τετραγωνική εξίσωση καταλήγουμε στο συμπέρασμα ότι η ζητούμενη τιμή είναι $n = 23$], η πιθανότητα είναι $p_{23} = 0,507$. Δηλαδή για 23 άτομα (πόσο μάλλον για 30) η πιθανότητα είναι μεγαλύτερη του 50% να έχουν γενέθλια δύο από αυτά την ίδια μέρα. Αυτός ο αυστηρός μαθηματικός υπολογισμός έρχεται αντίθετος με την αντίληψή μας γι' αυτό θεωρείται και «παράδοξο»!!!.

Από το παράδοξο μπορούμε να σκεφτούμε και την αναλογία σε σχέση με τον κατακερματισμό. Δηλαδή ότι οι 365 μέρες αντιστοιχούν σε θέσεις ενός πίνακα, ενώ τα άτομα αντιστοιχούν σε κλειδιά που εισάγονται στο πίνακα. Με βάση τη δυωνυμική κατανομή προκύπτει ότι η πιθανότητα κατά την εισαγωγή n κλειδιών, k από αυτά θα συμπέσουν στην ίδια θέση, θα είναι : $\left(\frac{1}{n}\right)^k \left(1-\frac{1}{n}\right)^{n-k} \left(\frac{n}{k}\right)$. Για n αρκετά μεγάλο η προηγούμενη σχέση προσεγγίζεται από $\frac{1}{ek!}$. Άρα συνεπάγεται ότι αν σε πίνακα 1000 θέσεων εισαχθούν $n = 1000$ κλειδιά, τότε η πιθανότητα σε μία θέση του πίνακα να αντιστοιχηθούν k κλειδιά προκύπτει ως εξής :

k	Πιθανότητα k συγκρούσεων %
0	37
1	37
2	18
3	6
4	1,5
5	0,3

Το παράδοξο των γενεθλίων πρέπει να λαμβάνεται υπόψη στην επιλογή του μεγέθους της σύνοψης. Είναι καλό να το έχει στο μυαλό του όποιος σχεδιάζει κρυπτογραφική hash συνάρτηση. Μπορεί δηλαδή διαισθητικά να πιστεύουμε ότι είναι αρκετά απίθανο διαφορετικές είσοδοι σε μια hash συνάρτηση να δίνουν ίδια έξοδο, αλλά παρόλα αυτά η πιθανότητα τελικά είναι πολύ μεγαλύτερη από ότι δείχνει φαινομενικά. Ανάλογη με την πιθανότητα των γενεθλίων δύο ατόμων, είναι και η πιθανότητα δύο μηνύματα να έχουν το ίδιο αποτέλεσμα σε μια συνάρτηση hash. Αντιπροσωπευτικά μεγέθη σύνοψης των κρυπτογραφικών hash είναι 128- bit και 160- bit (και όχι ένα hash των 64- bit που θα μπορούσε να θεωρήσει κάποιος). Σε πολλές εφαρμογές 128- bit θεωρούνται αρκετά, λαμβάνοντας υπόψη ότι το μήνυμα που συνοψίζεται έχει αρκετή περίσσεια, ώστε οι τυχόν συγκρούσεις να αντιστοιχούν σε μη έγκυρα μηνύματα. Ωστόσο, τα 160- bit είναι η αποδεκτή τιμή για την αποφυγή συγκρούσεων.

Οι επιθέσεις γενεθλίων μπορούν να εφαρμοστούν επιτυχώς για την κρυπτανάλυση των συναρτήσεων σύνοψης (one-way hash functions). Ανήκουν στις επιθέσεις ωμής βίας και βασίζονται στο παράδοξο των γενεθλίων το οποίο προσαρμόζεται στην αναζήτηση των «συγκρούσεων» (collisions) όταν προσπαθούμε να κάνουμε επίθεση στις συναρτήσεις σύνοψης. Αντί λοιπόν να ψάχνουμε για συγκρούσεις για κάποια συγκεκριμένη είσοδο, είναι ευκολότερο να ψάξουμε για ένα τυχαίο ζευγάρι εισόδων που δίνει την ίδια σύνοψη.

Η επίθεση γενεθλίων (**birthday attack)** λειτουργεί ως εξής:

– Αν ο χρήστης ετοιμάζεται να υπογράψει ένα έγκυρο μήνυμα x παράγοντας το hash του, μεγέθους m bits και κρυπτογραφώντας το με το ιδιωτικό κλειδί του.

– Ο αντίπαλος δημιουργεί $2^{\frac{m}{2}}$ παραλλαγές x' του x (όλες με ουσιαστικά το ίδιο νόημα) και τις αποθηκεύει.

– Ο αντίπαλος δημιουργεί $2^{\frac{m}{2}}$ παραλλαγές y' ενός επιθυμητού πλαστού μηνύματος y.

– Τα δυο σύνολα μηνυμάτων συγκρίνονται για να βρεθεί ένα ζεύγος με το ίδιο hash (μεγάλη πιθανότητα, λόγω του παραδόξου των γενεθλίων).

– Ο αντίπαλος δίνει στον Α να υπογράψει το έγκυρο μήνυμα που έχει ίδιο hash με το πλαστό. Όταν ο χρήστης δημιουργήσει hash για το έγκυρο μήνυμα, τότε ο αντίπαλος το αντικαθιστά με το πλαστό μήνυμα που όμως έχει έγκυρο hash.

Άρα πρέπει να χρησιμοποιούμε hash μεγάλου μεγέθους (Το 160- bit message digest του DSS είναι πιο ασφαλές σε τέτοιου είδους επίθεση).

Κεφάλαιο 2

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

2.1 Εισαγωγή

Σε πολλές περιπτώσεις στην καθημερινή μας ζωή χρειάζεται να υπογράψουμε ένα έγγραφο π.χ. ένα γράμμα, ένα συμβόλαιο ή μια ανάληψη χρημάτων στην τράπεζα, δηλώνοντας έτσι ότι είμαστε υπεύθυνοι για το περιεχόμενό του. Ψηφιακή υπογραφή είναι μία μέθοδος να υπογράφουμε ένα μήνυμα που βρίσκεται σε ηλεκτρονική μορφή.

Η ιδέα της ψηφιακής υπογραφής εμφανίσθηκε το 1976 από τους Diffie και Hellman. Η πρώτη προσέγγιση ήταν ψηφιακές υπογραφές με ανάκτηση του μηνύματος. Οι ψηφιακές υπογραφές με συνημμένο το μήνυμα ανακαλύφθηκαν από τους Merkle και Hellman. Μέχρι το 1978 δεν είχε γίνει κάποια εφαρμογή στις ψηφιακές υπογραφές, η πρώτη έγινε από τους Rivest, Shamir και Adleman.

Η απαίτηση για τη δημιουργία μιας τέτοιας υπογραφής έρχεται ως λογική συνέπεια της τεράστιας ποσότητας πληροφορίας που διακινείται πλέον μέσω του διαδικτύου. Οι ψηφιακές υπογραφές χρησιμοποιούνται σε ηλεκτρονικές συναλλαγές, στην επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, σε ηλεκτρονικές δημοπρασίες και γενικά σε δραστηριότητες κατά τις οποίες απαιτείται επιβεβαίωση της ταυτότητας της μιας πλευράς στην άλλη. Όπως και η απλή υπογραφή σε κάποιο έγγραφο, χρησιμοποιείται για να προσδιορίσει το άτομο που είναι υπεύθυνο για αυτό. Ένα τέτοιο μήνυμα (με ψηφιακή υπογραφή) μπορεί να μεταδοθεί μέσω ενός δικτύου υπολογιστών. Ο παραλήπτης του μηνύματος πρέπει να μπορεί να πιστοποιήσει αν η υπογραφή είναι αληθινή ή πλαστή. Το μοντέλο της ψηφιακής υπογραφής περιλαμβάνει τη δημιουργία των κλειδιών και της υπογραφής και την πιστοποίηση της υπογραφής. Τα σχήματα ψηφιακών υπογραφών βασίζονται σε hash συναρτήσεις και κρυπτογραφία δημοσίου κλειδιού.

Η ηλεκτρονική υπογραφή παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσης του περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά. Τα συστήματα κρυπτογράφησης δημόσιου κλειδιού επιτρέπουν στον καθένα να στείλει ένα μήνυμα χρησιμοποιώντας το δημόσιο κλειδί. Η υπογραφή επιτρέπει στο δέκτη του μηνύματος να έχει την πεποίθηση ότι ο αποστολέας είναι αυτός που υποστηρίζει ότι είναι. Ασφαλώς ο δέκτης δεν μπορεί να 100% σίγουρος ότι είναι πράγματι αυτός που υποστηρίζει, αφού αυτά τα συστήματα μπορούν να παραβιαστούν. Η σημασία της αυθεντικότητας είναι ιδιαίτερα φανερή σε οικονομικό περιεχόμενο. Για παράδειγμα, μια τράπεζα θέλει να στείλει οδηγίες από ένα παράρτημά της στα κεντρικά γραφεία σε μια φόρμα (a,b), όπου a είναι ο αριθμός λογαριασμού και b είναι το ποσό που πρέπει να πιστωθεί στο λογαριασμό. Ένας πελάτης που σκοπό έχει να παραπλανήσει, μπορεί να καταθέσει 100 ευρώ , να παρατηρήσει το αποτέλεσμα της μεταφοράς και αμέσως να βρει το (a,b) .

Έχει επιβεβαιωτική λειτουργία καθώς εξασφαλίζει ότι το μήνυμα που λαμβάνει ο παραλήπτης ανήκει όντως στον αποστολέα και ότι είναι ακέραιο, δηλαδή όχι αλλοιωμένο. Τέλος έχει και εμπιστευτική λειτουργία καθώς μόνο ο παραλήπτης είναι σε θέση να διαβάσει το μήνυμα και κανένας άλλος. Και τα δυο μέρη θέλουν να πιστεύουν πάντα ότι το μήνυμά τους δεν έχει υποστεί καμιά μετατροπή κατά τη διάρκεια της μετάδοσης. Η κρυπτογράφηση δυσκολεύει σε κάποιον τρίτο να διαβάσει το μήνυμα, χωρίς όμως να του απαγορεύει να το τροποποιήσει ώστε να το κάνει περισσότερο χρήσιμο. Ένα παράδειγμα που επεξηγεί τα παραπάνω είναι η επίθεση homomorphism στην τράπεζα του παραπάνω παραδείγματος και ένα πελάτη που καταθέτει 100 ευρώ, παρεμποδίζει την μεταφορά και αμέσως μετά μεταφέρει (a,b^3) ώστε να γίνει εκατομμυριούχος.

Σε ένα κρυπτογραφημένο περιβάλλον (context), η λέξη repudiation αναφέρεται στην πράξη της «άρνησης» από τον υποτιθέμενο αποστολέα, της οποιασδήποτε σχέσης με κάποιο μήνυμα. Ο αποδέκτης του μηνύματος μπορεί να επιμένει σχετικά με την ταυτότητα του αποστολέα μόνο στην περίπτωση που ο τελευταίος επισυνάπτει μια υπογραφή. Με τον τρόπο αυτό αποφεύγεται οποιαδήποτε μελλοντική άρνηση του αποστολέα, καθώς ο αποδέκτης έχει τη δυνατότητα να δείξει το μήνυμα σε κάποιον τρίτο για να αποδείξει την προέλευσή του.

Μια ψηφιακή υπογραφή εξυπηρετεί τον ίδιο σκοπό με μια χειρόγραφη υπογραφή. Ωστόσο μια χειρόγραφη υπογραφή είναι εύκολο να πλαστογραφηθεί και μόνο ο γραφολόγος μπορεί να επιβεβαιώσει με ανάλογη ασφάλεια. Μια ηλεκτρονική υπογραφή είναι ανώτερη από μια χειρόγραφη υπογραφή δεδομένου ότι είναι σχεδόν αδύνατο να πλαστογραφηθεί και επιπλέον ότι βεβαιώνει το περιεχόμενο των πληροφοριών καθώς επίσης και την ταυτότητα του υπογράφοντος. Το μόνο πρόβλημα είναι ότι η ψηφιακή υπογραφή είναι δυνατό να αφαιρεθεί από το αρχικό μήνυμα σε αντίθεση με τη χειρόγραφη που επισυνάπτεται φυσικά σε ένα μήνυμα έτσι που κάθε γνήσιο αντίγραφο την περιέχει. Το πρόβλημα αυτό λύνεται με τον αλγόριθμο υπογραφής που συνδέει το μήνυμα με την υπογραφή. Ένας τρόπος για να γίνει αυτό είναι να κρυπτογραφήσουμε πρώτα το υπογεγραμμένο μήνυμα και έπειτα να το στείλουμε εκεί που θέλουμε.

Στην ηλεκτρονική υπογραφή ακολουθείται το σύστημα ασύμμετρης κρυπτογράφησης (δημόσιο κλειδί). Μια ηλεκτρονική υπογραφή αποτελείται από ένα συνδυασμό (ζεύγος) κλειδιών, δηλαδή από ένα δημόσιο κλειδί (public key), το οποίο μπορεί να αποκτήσει ο καθένας και από ένα ιδιωτικό κλειδί (private key), το οποίο είναι αυστηρά προσωπικό για τον κάτοχό του και δεν πρέπει να κοινοποιηθεί σε κανέναν άλλο. Ακόμα κι αν γνωρίζει κάποιος το ένα κλειδί, είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Τα κλειδιά αυτά λειτουργούν πάντα σε ζεύγος και το ένα κλειδί μπορεί να αποκρυπτογραφήσει ότι έχει κρυπτογραφηθεί με το άλλο κλειδί και αντίστροφα.

Πρέπει να τονίσουμε ότι κατά τη **δημιουργία** μιας ψηφιακής υπογραφής δεν κρυπτογραφούνται τα " προς υπογραφή" δεδομένα, αλλά μια μικρή μαθηματική **σύνοψή** τους (digest), η οποία παράγεται από τη χρήση μονόδρομων αλγορίθμων κατακερματισμού δεδομένων (π.χ. MD5, SHA-1, κ.ά.). Αυτή η σύνοψη των δεδομένων κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντα και επισυνάπτεται μαζί με άλλες χρήσιμες πληροφορίες (π.χ. χρησιμοποιούμενοι αλγόριθμοι, εφαρμοζόμενη πολιτική υπογραφής, κ.ά.), στα αρχικά δεδομένα αποτελώντας την «προηγμένη ηλεκτρονική υπογραφή» τους.

Αν για παράδειγμα ένα μήνυμα ή ένα αρχείο που έχει κρυπτογραφηθεί με το δημόσιο κλειδί ενός κατόχου, μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί του ίδιου κατόχου, που σημαίνει ότι μόνο ο κάτοχος ενός δημοσίου κλειδιού μπορεί να διαβάσει τα μηνύματα που έχουν κρυπτογραφηθεί με το κλειδί αυτό καθώς μόνο αυτός γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Η διαδικασία αυτή εξασφαλίζει ότι το μήνυμα ή το αρχείο δεν μπορεί να αλλοιώνεται ή να παρακολουθείται από κάποιον τρίτο που δεν κατέχει το αντίστοιχο ιδιωτικό κλειδί του δημοσίου κλειδιού με το οποίο κρυπτογραφήθηκε το μήνυμα ή το αρχείο. Άρα στην περίπτωση αυτή θα έχουμε κρυπτογραφημένο μήνυμα!

Κατά την αντίστροφη διαδικασία της **επαλήθευσης** (verification) μιας ηλεκτρονικής υπογραφής, εφαρμόζεται στα υπό εξέταση δεδομένα ο ίδιος αλγόριθμος κατακερματισμού που χρησιμοποιήθηκε κατά την υπογραφή τους. Έτσι η νέα σύνοψη που παράγεται, συγκρίνεται με την αντίστοιχη σύνοψη που προέρχεται από την από την αποκρυπτογράφηση της προηγμένης ηλεκτρονικής υπογραφής με το υποδεικνυόμενο δημόσιο κλειδί του υπογράφοντα. Εάν ταυτίζονται οι δύο συνόψεις τότε η υπογραφή **επαληθεύεται** και επιβεβαιώνεται ότι:

α) Τα δεδομένα υπογράφηκαν από τον κάτοχο του σχετικού ιδιωτικού κλειδιού.
β) Τα αρχικά δεδομένα δεν έχουν αλλοιωθεί.

2.2 Βασικοί ορισμοί και συμβολισμοί

ΟΡΙΣΜΟΙ:

α) Ψηφιακή υπογραφή (ή υπογραφή) είναι μία συμβολοσειρά που συνδυάζει ένα μήνυμα με μία αυθεντική οντότητα.
β) Αλγόριθμος δημιουργίας υπογραφής είναι μια μέθοδος παραγωγής μιας υπογραφής.
γ) Αλγόριθμος πιστοποίησης υπογραφής είναι μια μέθοδος που πιστοποιεί αν η υπογραφή είναι αυθεντική για το συγκεκριμένο μήνυμα.
δ) Μηχανισμός υπογραφής αποτελείται από τους αλγόριθμους δημιουργίας και πιστοποίησης υπογραφής.

ε) Διαδικασία υπογραφής αποτελείται από τον αλγόριθμο δημιουργίας υπογραφής και από μία μέθοδο τυποποίησης των δεδομένων σε μηνύματα ώστε να μπορούν να υπογραφούν.

στ) Διαδικασία πιστοποίησης της υπογραφής αποτελείται από τον αλγόριθμο πιστοποίησης υπογραφής και από μία μέθοδο ανάκτησης των δεδομένων από το μήνυμα.

ΣΥΜΒΟΛΙΣΜΟΙ:

- M : είναι ένα σύνολο στοιχείων που λέγεται «χώρος μηνυμάτων» (message space). Είναι το πεπερασμένο σύνολο όλων των πιθανών μηνυμάτων που μπορούν να υπογραφούν.
- M_s: είναι ένα σύνολο στοιχείων που λέγεται «χώρος υπογραφής» (signing space). Είναι το σύνολο των στοιχείων στα οποία εφαρμόζονται οι μετασχηματισμοί υπογραφής. Οι μετασχηματισμοί υπογραφής δεν εφαρμόζονται άμεσα στο σύνολο M .
- S: είναι ένα σύνολο στοιχείων που λέγεται «χώρος των υπογραφών» (signature space). Τα στοιχεία του σχετίζονται με τα στοιχεία του χώρου μηνυμάτων M και χρησιμοποιούνται για τη δέσμευση του υπογράφοντος με ένα μήνυμα.
- R: είναι μια 1-1, αντιστρέψιμη συνάρτηση με $R: M \to M_s$ που ονομάζεται συνάρτηση αναγωγής (ή συνάρτηση πλεονάζουσας πληροφορίας (redundancy function)) .
- M_R: είναι η εικόνα της R ($M_R = \mathrm{Im}(R)$). Δηλαδή $R: M \to M_R$. Ο χώρος M_R λέγεται «χώρος των μηνυμάτων με πλεονασμό» και είναι $M_R \subseteq M_s$.
- R^{-1}: είναι η αντίστροφη συνάρτηση της R. Δηλαδή $R^{-1}: M_R \to M$.
- P: είναι ένα σύνολο στοιχείων που ονομάζεται «πλήθος υπογραφών» και χρησιμοποιείται για να προσδιορίσουμε συγκεκριμένους μηχανισμούς υπογραφής.
- h: είναι μια one-way συνάρτηση με πεδίο ορισμού το M και λέγεται συνάρτηση κατακερματισμού (hash function).

- M_h: είναι η εικόνα της h. Δηλαδή $h: M \to M_h$ και $|M_h| \prec |M|$. Ο χώρος M_h λέγεται «χώρος των τιμών κατακερματισμού» (hash value space) και είναι $M_h \subseteq M_s$.
- Q_n: είναι το σύνολο στοιχείων των τετραγωνικών υπολοίπων του $\bmod n$.

2.3 Σχήμα Ψηφιακής Υπογραφής

Ένα σχήμα ψηφιακής υπογραφής είναι μια τριάδα (M, S, K), όπου:

α) M, S: όπως ορίσθηκαν παραπάνω.

β) K: είναι το πεπερασμένο σύνολο όλων των πιθανών κλειδιών που μπορούν να χρησιμοποιηθούν για την υπογραφή.

γ) Υπάρχει ένας μετασχηματισμός $S_k: M \to S, \forall k \in K$. Είναι γνωστός μόνο στον υπογράφοντα και ονομάζεται συνάρτηση υπογραφής (signing function).

δ) Υπάρχει ένας μετασχηματισμός $V_k: M \times S \to \{true, false\}, \forall k \in K$. Είναι δημόσια γνωστός και ονομάζεται συνάρτηση επαλήθευσης (verification function). Χρησιμοποιείται για να επαληθεύσει ότι η υπογραφή s έχει όντως προκύψει από εφαρμογή του S_k στο μήνυμα m. Για κάθε μήνυμα $m \in M$ και για κάθε υπογραφή $s \in S$ ισχύει:

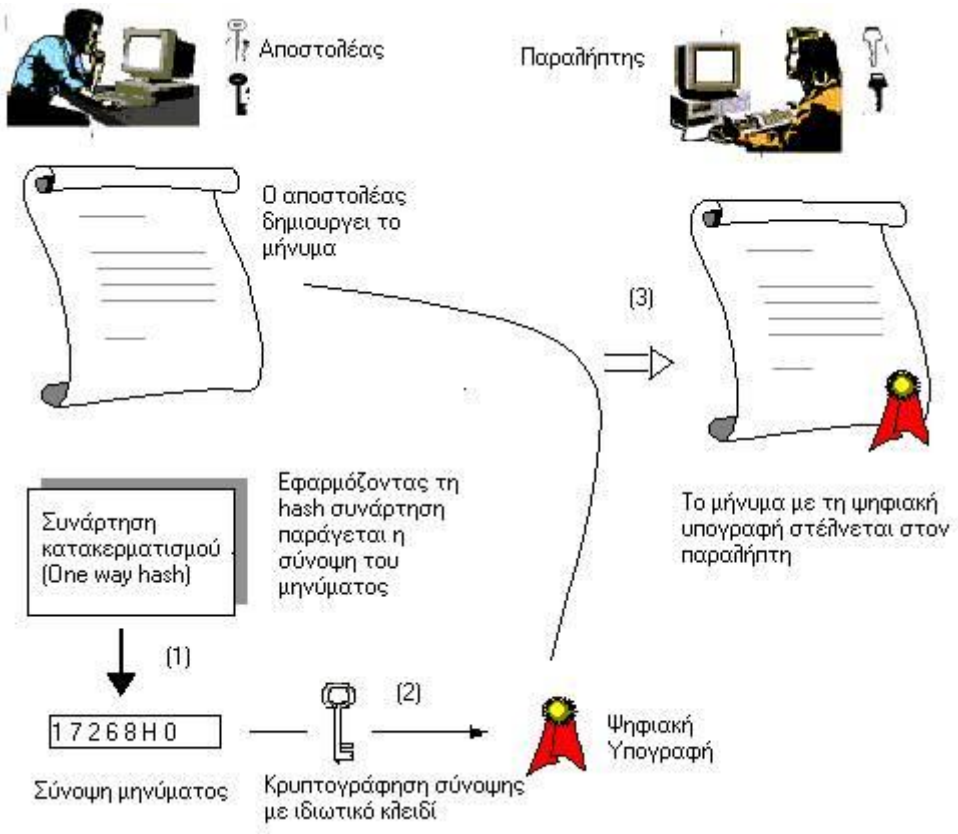
$$V_k(m,s) = \begin{cases} true & \alpha\nu \ \ s = S_k(m) \\ false & \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

<u>Αλγόριθμος Δημιουργίας Υπογραφής</u>

1. Ο αποστολέας χρησιμοποιώντας κάποιο αλγόριθμο κατακερματισμού δημιουργεί τη σύνοψη $h(m)$ του μηνύματος που θέλει να στείλει (message digest). Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μια συγκεκριμένου μήκους συμβολοακολουθία.
2. Ο αποστολέας με το ιδιωτικό του κλειδί κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή $s = S_k(h(m))$ για το μήνυμα m. Η υπογραφή είναι μια σειρά ψηφίων συγκεκριμένου μήκους.

3. Η κρυπτογραφημένη σύνοψη, δηλαδή η ψηφιακή υπογραφή, προσαρτάται στο κείμενο και το ζεύγος μήνυμα – ψηφιακή υπογραφή (m, s) μεταδίδονται μέσω του δικτύου στον παραλήπτη.

Το παρακάτω σχήμα μας δείχνει τη δημιουργία της ψηφιακής υπογραφής:



<u>Αλγόριθμος Επαλήθευσης Υπογραφής</u>

1. Ο παραλήπτης αποσπά από το ζεύγος (m, s) την ψηφιακή υπογραφή s.

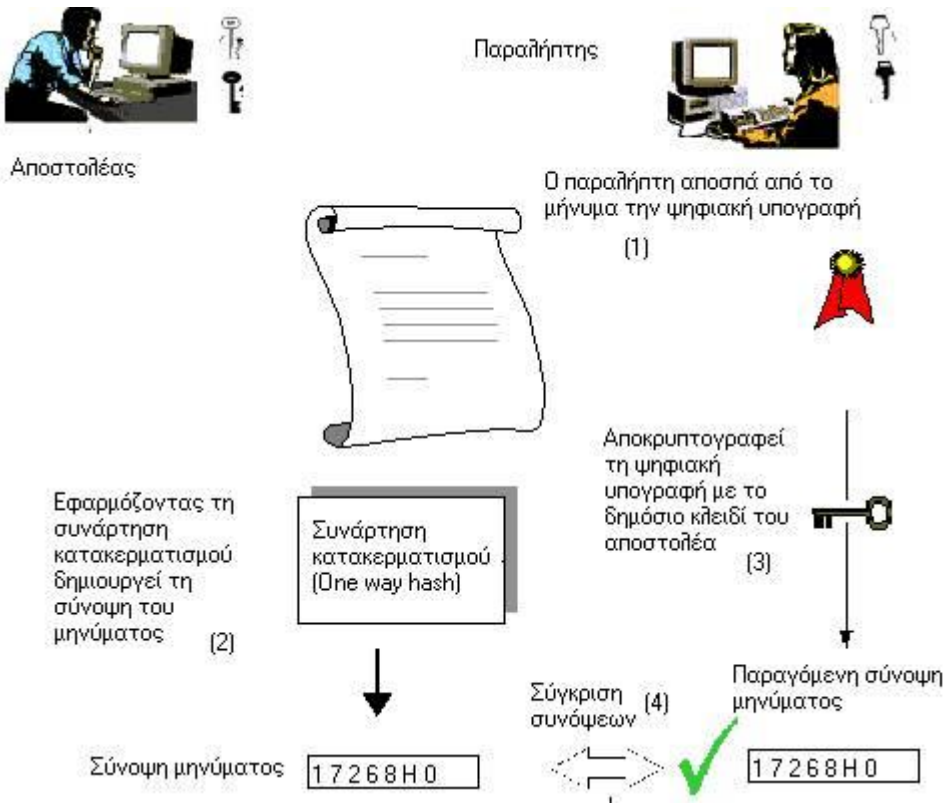
2. Ο παραλήπτης με το δημόσιο κλειδί του αποστολέα αποκρυπτογραφεί την ψηφιακή υπογραφή και καταλήγει στη σύνοψη $h(m)$ του μηνύματος.

3. Εφαρμόζοντας στο μήνυμα που έλαβε, τον δημόσια γνωστό αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη $h^*(m)$.

4. Αν οι δύο συνόψεις βρεθούν ίδιες μετά από σύγκρισή τους, τότε το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί τότε η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από τη σύνοψη που έχει

κρυπτογραφηθεί. Υπολογίζεται δηλαδή το $v = V_k(h^*(m), s)$ και αν $v = true \Leftrightarrow s = S_k(h^*(m)) \Leftrightarrow h(m) = h^*(m)$ και η υπογραφή γίνεται αποδεκτή. Αν $v = false$ η υπογραφή απορρίπτεται.

Το παρακάτω σχήμα μας δείχνει την επαλήθευση της ψηφιακής υπογραφής:



Γενικές Παρατηρήσεις:

1. Για κάθε κλειδί $k \in K$, οι συναρτήσεις υπογραφής και επαλήθευσης πρέπει να είναι πολυωνυμικού χρόνου.

2. Όταν γράφουμε $m \in M$ αναφερόμαστε στη δυαδική ή δεκαδική αναπαράστασή του και όχι στο μήνυμα με την καθημερινή του έννοια. Ένα μήνυμα κειμένου Μ προτού υπογραφεί και αποσταλεί μετατρέπεται σ' έναν θετικό ακέραιο στο δυαδικό ή δεκαδικό σύστημα. Όταν λέμε «μήνυμα» εννοούμε αυτόν ακριβώς τον ακέραιο m. Άρα είναι κατανοητό ότι για το χώρο μηνυμάτων ισχύει: $M \subseteq Z$.

3. Με $k \in K$ συμβολίζεται γενικά το κλειδί που παράγει ο αποστολέας, χωρίς όμως να διευκρινίζεται πάντα αν αναφερόμαστε στο ιδιωτικό ή στο δημόσιο κλειδί. Η

διαδικασία υπογραφής που αφορά τον αποστολέα κάνει χρήση του ιδιωτικού κλειδιού, ενώ η διαδικασία επαλήθευσης που αφορά τον παραλήπτη κάνει χρήση του δημοσίου κλειδιού. Αντίστοιχα, ο μετασχηματισμός υπογραφής S_k καθορίζεται από το κλειδί k_{pr}, γνωστό μόνο στον αποστολέα (private) και ο μετασχηματισμός επαλήθευσης V_k καθορίζεται από το κλειδί k_{pc} το οποίο γίνεται δημοσίως γνωστό (public).

2.4 Κατηγορίες Υπογραφών

Α) Σχήματα ψηφιακής υπογραφής με παράρτημα (Digital Signature Schemes with Appendix)

Τα σχήματα που ανήκουν σε αυτή την κατηγορία απαιτούν το αρχικό μήνυμα ως είσοδο στον αλγόριθμο επαλήθευσης. Το αρχικό μήνυμα είναι δηλαδή απαραίτητο για την πιστοποίηση γνησιότητας της αντίστοιχης υπογραφής. Τα σχήματα ψηφιακής υπογραφής με παράρτημα χρησιμοποιούνται περισσότερο στην πράξη και βασίζονται περισσότερο σε κρυπτογραφικές συναρτήσεις κατακερματισμού (hash functions) παρά σε συναρτήσεις αναγωγής. Τέτοια σχήματα είναι τα ElGamal, DSS και Schnorr.

Έστω ότι ο Α θέλει να στείλει ένα μήνυμα στον Β. Ο Α θα πρέπει να δημιουργήσει ένα μυστικό κλειδί για να υπογράψει το μήνυμα και ένα αντίστοιχο δημόσιο κλειδί για να χρησιμοποιηθεί από τον Β για να πιστοποιήσει ότι η υπογραφή είναι αυθεντική.

α) Αλγόριθμος δημιουργίας κλειδιών

1. Ο Α επιλέγει ένα μυστικό κλειδί και ορίζει το σύνολο $S_A = \{S_{A,k} : k \in P\}$ των μετασχηματισμών. Κάθε $S_{A,k}$ είναι μία 1-1 απεικόνιση από το M_h στο S και ονομάζεται μετασχηματισμός υπογραφής.
2. Το S_A ορίζει μία αντίστοιχη απεικόνιση V_A από το $M_h \times S$ στο $\{true, false\}$ έτσι ώστε: $V_A(m', s^*) = \begin{cases} true \ \alpha\nu \ S_{A,k}(m') = s^* \\ false \ \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$ για όλα τα $m' \in M_h$, $s^* \in S$. Επίσης εδώ

έχουμε ότι $m' = h(m)$ για όλα τα $m \in M$. Ο V_A λέγεται μετασχηματισμός πιστοποίησης και είναι έτσι κατασκευασμένος ώστε να μπορεί να υπολογισθεί χωρίς τη γνώση του μυστικού κλειδιού του Α.

3. Το δημόσιο κλειδί του Α είναι το V_A και το μυστικό κλειδί είναι το σύνολο S_A.

β) Αλγόριθμος δημιουργίας υπογραφής

Ο Α παράγει μία υπογραφή $s \in S$ για το μήνυμα $m \in M$.

1. Επιλέγει ένα στοιχείο $k \in P$.

2. Υπολογίζει $m' = h(m)$ και $s^* = S_{A,k}(m')$. (Η h πρέπει να είναι collision free hash συνάρτηση).

3. Η υπογραφή για το μήνυμα m είναι το s^*. Το ζευγάρι (m, s^*) είναι διαθέσιμο στον Β.

γ) Αλγόριθμος πιστοποίησης της υπογραφής

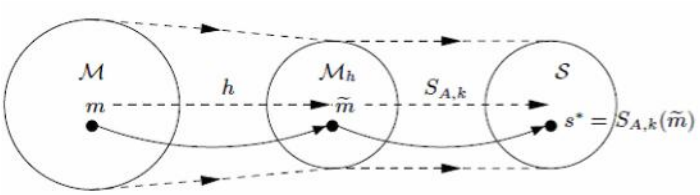
Ο Β πιστοποιεί ότι η υπογραφή είναι αυθεντική.

1. Εξασφαλίζει το δημόσιο κλειδί του Α το V_A.

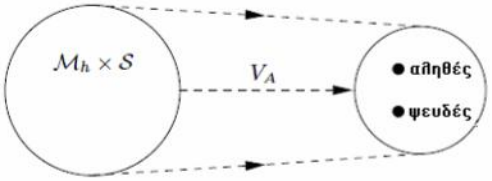
2. Υπολογίζει $m' = h(m)$ και $u = V_A(m', s^*)$.

3. Δέχεται την υπογραφή ως αυθεντική αν και μόνο αν $u = true$.

Το επόμενο είναι ένα σχήμα ψηφιακής υπογραφής με παράρτημα:



(α) Η διεργασία υπογραφής



(β) Η διεργασία επαλήθευσης

Για τους μετασχηματισμούς της υπογραφής και της πιστοποίησης θα πρέπει να ισχύουν οι παρακάτω ιδιότητες:

1. Για κάθε $k \in P$, το $S_{A,k}$ θα πρέπει να υπολογίζεται εύκολα.

2. Το V_A θα πρέπει να υπολογίζεται εύκολα.

3. Θα πρέπει να είναι υπολογιστικά ανέφικτο για κάποιον τρίτο να βρει ένα $m \in M$ και ένα $s^* \in S$ τέτοια που $V_A(m', s^*) = true$ με $m' = h(m)$.

Β) <u>Σχήματα ψηφιακής υπογραφής με ανάκτηση μηνύματος</u> (Digital Signature Schemes with Message Recovery)

Τα σχήματα που ανήκουν σε αυτή την κατηγορία δεν απαιτούν το αρχικό μήνυμα ως είσοδο στον αλγόριθμο επαλήθευσης. Το αρχικό μήνυμα μπορεί να ανακτηθεί από την ίδια την υπογραφή. Στην πράξη το χαρακτηριστικό αυτό χρησιμοποιείται για μικρά μηνύματα. Τέτοια σχήματα είναι τα RSA, Rabin και Nyberg – Rueppel.

Έστω ότι ο Α θέλει να στείλει ένα μήνυμα στον Β. Ο Α θα πρέπει να δημιουργήσει ένα μυστικό κλειδί για να υπογράψει το μήνυμα και ένα αντίστοιχο δημόσιο κλειδί για να χρησιμοποιηθεί από τον Β για να πιστοποιήσει ότι η υπογραφή είναι αυθεντική.

α) Αλγόριθμος δημιουργίας κλειδιών

1. Ο Α επιλέγει ένα σύνολο $S_A = \{S_{A,k} : k \in P\}$ των μετασχηματισμών. Κάθε $S_{A,k}$ είναι μία 1-1 απεικόνιση από το M_h στο S και ονομάζεται μετασχηματισμός υπογραφής.
2. Το S_A ορίζει μία αντίστοιχη απεικόνιση V_A με την ιδιότητα ότι η $V_A \times S_{A,k}$ είναι ταυτοτική απεικόνιση στο M_S για όλα τα $k \in P$. Ο V_A λέγεται μετασχηματισμός πιστοποίησης και είναι έτσι κατασκευασμένος ώστε να μπορεί να υπολογισθεί χωρίς τη γνώση του μυστικού κλειδιού του Α.
3. Το δημόσιο κλειδί του Α είναι το V_A και το μυστικό κλειδί είναι το σύνολο S_A.

β) Αλγόριθμος δημιουργίας υπογραφής

Ο Α παράγει μία υπογραφή $s \in S$ για το μήνυμα $m \in M$.

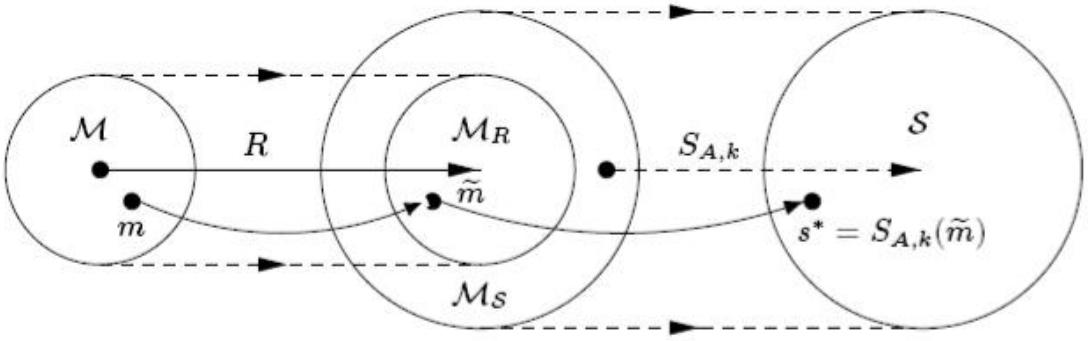
1. Επιλέγει ένα στοιχείο $k \in P$.
2. Υπολογίζει $m' = R(m)$ και $s^* = S_{A,k}(m')$. (Η R είναι η συνάρτηση αναγωγής).
3. Η υπογραφή για το μήνυμα m είναι το s^*. Το s^* είναι διαθέσιμο στον Β για την πιστοποίηση της υπογραφής και την ανάκτηση του μηνύματος.

γ) Αλγόριθμος πιστοποίησης της υπογραφής και ανάκτηση του μηνύματος

Ο Β πιστοποιεί ότι η υπογραφή είναι αυθεντική.

1. Εξασφαλίζει το δημόσιο κλειδί του Α το V_A.
2. Υπολογίζει $m' = V_A(s^*)$.
3. Πιστοποιεί ότι $m' \in M_R$ (Αν $m' \notin M_R$ τότε απορρίπτει την υπογραφή.)
4. Ανακτά το από το m από το m' υπολογίζοντας $R^{-1}(m')$.

Το παρακάτω είναι ένα σχήμα ψηφιακής υπογραφής με ανάκτηση μηνύματος:



Για τους μετασχηματισμούς της υπογραφής και της πιστοποίησης θα πρέπει να ισχύουν οι παρακάτω ιδιότητες:

1. Για κάθε $k \in P$, το $S_{A,k}$ θα πρέπει να υπολογίζεται εύκολα.

2. Το V_A θα πρέπει να υπολογίζεται εύκολα.

3. Θα πρέπει να είναι υπολογιστικά ανέφικτο για κάποιον τρίτο να βρει ένα οποιοδήποτε $s^* \in S$ τέτοιο που $V_A(s^*) \in M_R$.

Η συνάρτηση αναγωγής R και η αντίστροφη της R^{-1} είναι δημόσια γνωστή. Η επιλογή κατάλληλης R έχει σημαντικό ρόλο στην ασφάλεια του συστήματος. Ας υποθέσουμε ότι $M_R = M_S$. Έστω ότι R και $S_{A,k}$ είναι απεικονίσεις από το M στο M_R και από το M_S στο S αντίστοιχα. Δηλαδή τα σύνολα M και S έχουν τον ίδιο αριθμό στοιχείων. Τότε για οποιοδήποτε $s^* \in S$, $V_A(s^*) \in M_R$ είναι προφανές ότι μπορώ να βρω μηνύματα m και αντίστοιχες υπογραφές s^* οι οποίες θα γίνουν αποδεκτές από τον αλγόριθμο πιστοποίησης όπως φαίνεται παρακάτω:

1. Επέλεξε τυχαία $k \in P$ και τυχαία $s^* \in S$.

2. Υπολόγισε $m' = V_A(s^*)$.

3. Υπολόγισε $m = R^{-1}(m')$.

Το στοιχείο s^* είναι μία νόμιμη υπογραφή για το μήνυμα m και δημιουργήθηκε χωρίς να γνωρίζουμε το μετασχηματισμό της υπογραφής S_A.

Παράδειγμα: Έστω $M = \left\{ m : m \in \{0,1\}^n \right\}$ για κάποιο σταθερό n και $M_S = \left\{ t : t \in \{0,1\}^{2n} \right\}$. Ορίζουμε $R : M \to M_S$ με τύπο $R(m) = m \| m$, όπου με $\|$ συμβολίζουμε τη συνένωση συμβολοσειρών. Έτσι θα έχουμε $M_R = \left\{ m \| m : m \in M \right\} \subseteq M_S$. Για μεγάλες τιμές του n η ποσότητα $\frac{|M_R|}{|M_S|} = \left(\frac{1}{2}\right)^n$ παίρνει μηδαμινή τιμή. Αυτή η συνάρτηση αναγωγής είναι κατάλληλη ώστε καμία επιλογή του s^* από το μέρος του αντιπάλου να έχει μη μηδαμινή πιθανότητα να ισχύει $V_A(s^*) \in M_R$.

Οι δύο παραπάνω κατηγορίες υπογραφών μπορούν να χωρισθούν ανάλογα με το πλήθος του P:

α) Πιθανοτική υπογραφή αν $|P| \succ 1$.

β) Ντετερμινιστική υπογραφή αν $|P| = 1$. Τα ντετερμινιστικά σχήματα υπογραφών διακρίνονται σε σχήματα υπογραφών μιας χρήσης (one time signature schemes) και σε σχήματα υπογραφών πολλαπλής χρήσης (multiple use signature schemes).

Σχήματα με παράρτημα που προκύπτουν από σχήματα με ανάκτηση μηνύματος

Ένα σχήμα υπογραφής με ανάκτηση μηνύματος μπορεί να μετατραπεί σε σχήμα με παράρτημα αν χρησιμοποιήσουμε μία συνάρτηση κατακερματισμού. Κατακερματίζουμε δηλαδή το απλό μήνυμα και κατόπιν υπογράφουμε το message digest που προκύπτει.

Ο αλγόριθμος υπογραφής S_k πρέπει να συνδέει με κάποιο τρόπο το μήνυμα με την υπογραφή κι αυτό επιτυγχάνεται πρώτα με κρυπτογράφηση του υπογεγραμμένου μηνύματος και κατόπιν την αποστολή του. Εδώ όμως απαιτείται προσοχή γιατί η διαδικασία πρέπει να γίνει με τη σειρά υπογραφή $\to$ κρυπτογράφηση. Σε αντίθετη περίπτωση, αν ο αποστολέας κρυπτογραφήσει το προς αποστολή μήνυμα και μετά το

υπογράψει, τότε ένας αντίπαλος μπορεί πολύ εύκολα να πάρει τη θέση του αφαιρώντας την υπογραφή από το μήνυμα και προσθέτοντας τη δική του. Η συνάρτηση αναγωγής R τώρα δεν παίζει κανένα ρόλο για την ασφάλεια του συστήματος και μπορεί να είναι οποιαδήποτε 1-1 συνάρτηση από το M_h στο M_S.

Παρατήρηση: Γενικά δε πρέπει να ξεχνάμε πως είναι απαραίτητο το μήνυμα να περιέχει πληροφορίες όπως ημερομηνία και ώρα για να αποφεύγεται η επαναχρησιμοποίησή του αφού η ψηφιακή υπογραφή δεν αποτελεί τμήμα του μηνύματος.

2.5 Ασφάλεια ψηφιακών υπογραφών

Εδώ θα αναφέρουμε πότε ένα κρυπτοσύστημα είναι ασφαλές. Επειδή οι ψηφιακές υπογραφές είναι τμήμα της κρυπτογραφίας και όπως είδαμε σε προηγούμενη παράγραφο το σχήμα της υπογραφής με ανάκτηση του μηνύματος δε διαφέρει ουσιαστικά από τα συστήματα κρυπτογράφησης.

Πλήρη ασφάλεια

Υπάρχουν δύο προσεγγίσεις για την ασφάλεια ενός κρυπτοσυστήματος:

α) Υπολογιστική ασφάλεια.
Η υπολογιστική ασφάλεια μετράει την υπολογιστική δύναμη που απαιτείται για να σπάσει ένα κρυπτοσύστημα. Μπορούμε να πούμε ότι ένα κρυπτοσύστημα είναι ασφαλές αν ο βέλτιστος αλγόριθμος για να το σπάσει χρειάζεται να εκτελέσει N τουλάχιστον πράξεις όπου N είναι ένας συγκεκριμένος πολύ μεγάλος αριθμός. Το πρόβλημα είναι ότι δε γνωρίζουμε κανένα πρακτικό κρυπτοσύστημα που να είναι ασφαλές, δηλαδή δεν μπορούμε να το αποδείξουμε σύμφωνα με τον παραπάνω ορισμό. Πρακτικά λέμε ότι ένα κρυπτοσύστημα είναι υπολογιστικά ασφαλές αν χρειάζεται τεράστιο υπολογιστικό χρόνο (βέβαια αυτό διαφέρει πολύ από την απόδειξη).
Μία άλλη προσέγγιση για την υπολογιστική ασφάλεια είναι να ανάγουμε την ασφάλεια του κρυπτοσυστήματος σε κάποιο γνωστό πρόβλημα που το γνωρίζουμε

και ξέρουμε ότι είναι δύσκολο να επιλυθεί. Για παράδειγμα μπορούμε να αποδείξουμε την πρόταση « ένα κρυπτοσύστημα είναι ασφαλές αν δοθέντος ενός ακεραίου n δεν μπορούμε να βρούμε τους παράγοντές του». Κρυπτοσυστήματα αυτού του τύπου λέγονται και «αποδεικτικά ασφαλή» (provably secure), αλλά πρέπει να σημειωθεί ότι με αυτό τον τρόπο η απόδειξη της ασφάλειας γίνεται σε σχέση με κάποιο άλλο πρόβλημα και όχι ανεξάρτητα.

β) Απεριόριστη ασφάλεια.
Αναφέρεται στην ασφάλεια των κρυπτοσυστημάτων όπου ο αντίπαλος δεν έχει περιορισμό στις πράξεις που μπορεί να εκτελέσει. Ένα κρυπτοσύστημα είναι απεριόριστα ασφαλές αν ο αντίπαλος δε μπορεί να το σπάσει ακόμα και με απεριόριστο υπολογιστικό χρόνο.

2.6 Τύποι επιθέσεων σε συστήματα υπογραφών

Στόχος του αντιπάλου είναι η πλαστογράφηση των υπογραφών, δηλαδή η αποστολή μηνύματος με πλαστή υπογραφή και ο παραλήπτης να νομίσει ότι είναι αυθεντική. Για να το πετύχουμε αυτό σε οποιοδήποτε μήνυμα θα πρέπει να βρούμε το μυστικό κλειδί του υπογράφοντα. Έκτος από την εύρεση του μυστικού κλειδιού υπάρχουν και άλλοι ενδιαφέροντες τρόποι, αλλά λιγότερο ισχυροί, για να βλάψουμε την ασφάλεια ενός συστήματος υπογραφών.

Υπάρχουν οι παρακάτω τύποι επιθέσεων:
α) Κατάρρευση του συστήματος ή ολικό σπάσιμο (total break). Ο αντίπαλος είναι ικανός να υπολογίσει το μυστικό κλειδί του αποστολέα ή να βρει ένα αποδοτικό αλγόριθμο ισοδύναμο με τον αυθεντικό αλγόριθμο δημιουργίας υπογραφής.
β) Ολική πλαστογράφηση (universal forgery). Ο αντίπαλος αν και δεν μπορεί να βρει το μυστικό κλειδί του αποστολέα, μπορεί να πλαστογραφήσει οποιοδήποτε μήνυμα.
γ) Επιλεκτική πλαστογράφηση (selective forgery). Ο αντίπαλος μπορεί να δημιουργήσει νόμιμες υπογραφές για ένα συγκεκριμένο μήνυμα ή για μια κατηγορία μηνυμάτων που έχουν επιλεγεί εκ των προτέρων. Δημιουργώντας τις υπογραφές δεν επιδρά άμεσα στο νόμιμο υπογράφοντα.

δ) Υπαρξιακή πλαστογράφηση (existential forgery). Ο αντίπαλος είναι ικανός να πλαστογραφήσει τουλάχιστο ένα μήνυμα. Έχει λίγο ή καθόλου τον έλεγχο στο μήνυμα όπου πλαστογράφησε και ο νόμιμος υπογράφων μπορεί να εμποδίσει την απάτη.
Δεν μπορούμε ποτέ να αποδείξουμε ότι ένα σχήμα ψηφιακής υπογραφής είναι απόλυτα ασφαλές. Ωστόσο ορίζουμε σαν την πιο ασφαλή υπογραφή, με την έννοια ότι μπορεί να χρησιμοποιηθεί παρέχοντας ασφάλεια σε ένα μεγάλο εύρος εφαρμογών, να είναι αυτή που ορίστηκε από τους Goldwasser, Micali και Rivest.

Δε πρέπει να ξεχνάμε πως: Μία ψηφιακή υπογραφή είναι υπαρξιακά απρόσβλητη κάτω από μία επίθεση προσαρμόσιμα επιλεγμένου μηνύματος αν για οποιονδήποτε προσβολέα που γνωρίζει το δημόσιο κλειδί είναι υπολογιστικά αδύνατο να παράγει μία έγκυρη υπογραφή ενός μηνύματος ακόμα και αν έχει στην κατοχή του αριθμήσιμου πλήθους υπογραφές μηνυμάτων της επιλογής του.

Υπάρχουν δύο είδη επιθέσεων στα σχήματα υπογραφών δημοσίου κλειδιού:

α) Επιθέσεις μόνο στο κλειδί (key-only attacks). Ο αντίπαλος γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντα.
β) Επιθέσεις στο μήνυμα (message attacks). Ο αντίπαλος μπορεί να εξετάσει υπογραφές που αντιστοιχούν σε γνωστά ή σε επιλεγμένα μηνύματα και διακρίνονται σε :

1) Επίθεση σε γνωστά μηνύματα (known message attack). Ο αντίπαλος έχει υπογραφές για ένα σύνολο μηνυμάτων που είναι γνωστά σε αυτόν αλλά όχι επιλεγμένα από αυτόν.
2) Επίθεση σε επιλεγμένο μήνυμα (chosen message attack). Ο αντίπαλος καταφέρνει να έχει νόμιμες υπογραφές για ένα επιλεγμένο σύνολο μηνυμάτων πριν προσπαθήσει να πετύχει κατάρρεύση του συστήματος. Αυτή η επίθεση είναι μη προσαρμόσιμη (non-adaptive) με την έννοια ότι τα μηνύματα επιλέγονται πριν από τις υπογραφές.
3) Επίθεση προσαρμόσιμου επιλεγμένου μηνύματος (adaptive chosen message attack). Ο αντίπαλος μπορεί να χρησιμοποιήσει τον υπογράφοντα ως μαντείο, δηλαδή μπορεί να ζητήσει νόμιμες υπογραφές μηνυμάτων που εξαρτώνται από το δημόσιο

κλειδί του υπογράφοντα ή να ζητήσει νόμιμες υπογραφές μηνυμάτων που εξαρτώνται από προηγούμενες υπογραφές ή μηνύματα.

Η επίθεση προσαρμόσιμου επιλεγμένου μηνύματος είναι ο πιο δύσκολος τύπος επίθεσης. Αν ο αντίπαλος γνωρίζει αρκετά μηνύματα με τις αντίστοιχες υπογραφές τους μπορεί να εξάγει κάποιο τύπο για τον τρόπο υπογραφής και μετά να μπορεί να πλαστογραφήσει ένα μήνυμα της επιλογής του. Άρα ένα καλά σχεδιασμένο σχήμα υπογραφής πρέπει να προστατεύεται από αυτή την περίπτωση.

Το επίπεδο ασφάλειας που απαιτείται για κάθε σχήμα υπογραφής εξαρτάται από τις απαιτήσεις της εφαρμογής που χρησιμοποιείται. Σημαντικό ρόλο στην ασφάλεια του συστήματος έχει και η επιλογή της hash συνάρτησης όπου θα πρέπει να είναι τέτοια ώστε ο αντίπαλος να μη μπορεί να την αντικαταστήσει με κάποια άλλη hash συνάρτηση πιο αδύναμη και να επιδιώξει να κάνει επίθεση επιλεκτικής πλαστογράφησης.

Τέλος, τύπος επίθεσης σε συστήματα υπογραφών είναι και η birthday attack η οποία ανήκει στις επιθέσεις ωμής βίας (επιθέσεις που δοκιμάζουν κάθε δυνατό κλειδί ως προς το αν η κωδικοποίηση έχει γίνει με αυτό το κλειδί ή όχι) και στηρίζεται στο «παράδοξο των γενεθλίων». Ο τύπος αυτός επίθεσης αναπτύχθηκε στο προηγούμενο κεφάλαιο.

Κεφάλαιο 3

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ ΚΑΙ ΤΟ ΣΧΗΜΑ ΥΠΟΓΡΑΦΗΣ RSA

3.1 Το κρυπτοσύστημα RSA

Τα αρχικά του κρυπτοσυστήματος RSA προέρχονται από τα ονόματα των μελετητών R.L.Rivest, A.Shamir και L.Adleman οι οποίοι το δημοσίευσαν το 1978. Το κρυπτοσύστημα RSA είναι κρυπτοσύστημα δημοσίου κλειδιού, δηλαδή ο μετασχηματισμός κρυπτογράφησης αποτελεί δημόσια πληροφορία σε αντίθεση με το μετασχηματισμό αποκρυπτογράφησης που παραμένει κρυφός και είναι γνωστός μόνο στον παραλήπτη (ή στον υπογράφοντα στην περίπτωση του σχήματος υπογραφής). Ο αλγόριθμος RSA είναι ένας από τους πιο διαδεδομένους και περισσότερο χρησιμοποιημένους αλγόριθμους στην κρυπτογραφία δημοσίου κλειδιού. Είναι κατάλληλος για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων για τη δημιουργία ψηφιακών υπογραφών και την επαλήθευσή τους καθώς και για την ασφαλή μεταφορά κλειδιών.

Περιγραφή RSA

Το κρυπτοσύστημα αυτό χρησιμοποιεί υπολογισμούς στο σύνολο $Z_n = \{0,1,2,...,n-1\}$, όπου n είναι το γινόμενο δύο μεγάλων, διακεκριμένων, πρώτων αριθμών p,q. Για ένα τέτοιο n σημειώνουμε και τη συνάρτηση Euler $\varphi(n) = (p-1)\cdot(q-1)$.

α) Αλγόριθμος παραγωγής κλειδιού

Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί RSA και ένα αντίστοιχο ιδιωτικό κλειδί. Ο Α ενεργεί ως εξής:

1. Παράγει δύο μεγάλους, διακεκριμένους, πρώτους αριθμούς p, q περίπου ίδιου μεγέθους.

2. Υπολογίζει $n = p \cdot q$ και $\varphi(n) = (p-1) \cdot (q-1)$.

3. Επιλέγει ένα τυχαίο ακέραιο αριθμό e με $1 \prec e \prec \varphi(n)$ τέτοιο που $\gcd(e, \varphi(n)) = 1$.

4. Χρησιμοποιώντας τον Εκτεταμένο Ευκλείδειο Αλγόριθμο υπολογίζει το μοναδικό ακέραιο d με $1 \prec d \prec \varphi(n)$ τέτοιο που $e \cdot d = 1 \bmod \varphi(n)$.

5. Το δημόσιο κλειδί του Α είναι το ζευγάρι (n, e) και το μυστικό κλειδί είναι το d.

Παρατήρηση: Οι ακέραιοι e και d λέγονται εκθέτης κρυπτογράφησης και εκθέτης αποκρυπτογράφησης αντίστοιχα.

β) Αλγόριθμος κρυπτογράφησης

Ο Β κρυπτογραφεί ένα μήνυμα m για τον Α και ενεργεί ως εξής:

1. Αποκτά το αυθεντικό δημόσιο κλειδί (n, e) του Α.

2.Αναπαριστά το μήνυμα ως έναν ακέραιο m στο διάστημα $[0, n-1]$.

3.Υπολογίζει $c = m^e \bmod n$.

4. Στέλνει το κρυπτοκείμενο c στον Α.

γ) Αλγόριθμος αποκρυπτογράφησης

Ο Α για να ανακτήσει το απλό κείμενο m από το c ενεργεί ως εξής:

1. Χρησιμοποιεί το δημόσιο κλειδί d για να ανακτήσει το $m = c^d \bmod n$.

Παρατηρήσεις :

i. Αφού το n είναι το γινόμενο των δύο πρώτων p, q θα ισχύει: $\varphi(n) = (p-1) \cdot (q-1)$. Έτσι αν κάποιος γνωρίζει τους p, q μπορεί εύκολα να υπολογίσει το $\varphi(n)$ και άρα το d.

ii. Καλή επιλογή για δημόσιο εκθέτη e είναι κάποιος πρώτος αριθμός μεγαλύτερος από $\max\{p,q\}$.

iii. Το πρόβλημα υπολογισμού του εκθέτη αποκρυπτογράφησης d στο RSA από το δημόσιο κλειδί (n,e) και το πρόβλημα παραγοντοποίησης του n, είναι υπολογιστικά ισοδύναμα. Όταν λοιπόν παράγονται τα κλειδιά, είναι πολύ σημαντικό οι πρώτοι p,q να επιλέγονται κατά τέτοιο τρόπο ώστε να επιτυγχάνεται το δυσεπίλυτο της παραγοντοποίησης του $n = p \cdot q$.

iv. Στο RSA ισχύει: $E(D(m)) = m$. Το κρυπτοσυστήμα RSA βασίζεται στη συνάρτηση $E(m) = m^e \bmod n$ η οποία δεχόμαστε ότι είναι one-way συνάρτηση. Δεν υπάρχει γνωστός αλγόριθμος που να αντιστρέφει αυτή τη συνάρτηση χωρίς τη γνώση του κρυφού εκθέτη αποκρυπτογράφησης d. Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης είναι αντίστροφες διαδικασίες. Δηλαδή η συνάρτηση $D(c) = c^d \bmod n$ είναι αντίστροφη της $E(m) = m^e \bmod n$, δηλαδή ότι $D(E(m)) = m$ (**Απόδειξη**: Αφού $e \cdot d = 1 \bmod \varphi(n)$, θα υπάρχει ακέραιος k, τέτοιος ώστε $e \cdot d = 1 + k\varphi(n)$. Έτσι έχουμε $D(E(m)) = m^{ed} \bmod n$. Άρα (χρησιμοποιώντας και το θεώρημα Euler) $D(E(m)) = m^{1+k\varphi(n)} \bmod n = m m^{k\varphi(n)} \bmod n = m(m^{\varphi(n)})^k \bmod n$ $= m \bmod n$.)

<u>Παράδειγμα 1</u>:

Ο Α επιλέγει δυο πρώτους $p = 101$ και $q = 113$ και υπολογίζει $n = p \cdot q = 11413$ και $\varphi(n) = (p-1) \cdot (q-1) = 100 \cdot 112 = 11200$. Αφού $11200 = 2^6 \cdot 5^2 \cdot 7$ ο Α πρέπει να επιλέξει εκθέτη κωδικοποίησης που να μη διαιρείται από τους $2, 5, 7$ (Στην πραγματικότητα ο Α δε θα παραγοντοποιήσει το $\varphi(n)$, απλά θα επιλέξει ένα e, θα επιβεβαιώσει με τον εκτεταμένο Ευκλείδειο αλγόριθμο ότι $\gcd(e, \varphi(n)) = 1$). Επιλέγει $e = 3533$ και βρίσκει ότι $e \cdot d = 3533 \cdot d = 1 \bmod 11200$ με $d = 6597$.

Ο μυστικός εκθέτης κωδικοποίησης του Α είναι ο $d = 6597$ και δημοσιοποιεί τους $n = 11413$ και $e = 3533$ σε έναν κατάλογο. Υποθέτουμε ότι ο Β θέλει να

κρυπτογραφήσει το μήνυμα $m = 9726$ και να το στείλει στον Α. Υπολογίζει το $m^e \bmod n = 9726^{3533} \bmod 11413 \equiv 5761$ c και μεταδίδει μέσω του καναλιού το κρυπτοκείμενο $c = 5761$. Όταν ο Α το λάβει χρησιμοποιεί το ιδιωτικό του κλειδί και υπολογίζει $c^d \bmod n = 5761^{6597} \bmod 11413 \equiv 9726$ m ανακτώντας έτσι το μήνυμα m.

<u>Παράδειγμα 2</u>:

Ο Α επιλέγει δυο πρώτους $p = 2357$ και $q = 2551$ και υπολογίζει $n = p \cdot q = 6012707$ και $\varphi(n) = (p-1) \cdot (q-1) = 2356 \cdot 2550 = 6007800$. Επιλέγει $e = 3674911$ και βρίσκει ότι $e \cdot d = 3674911 \cdot d = 1 \bmod 6007800$ με $d = 422191$. Ο μυστικός εκθέτης κωδικοποίησης του Α είναι ο $d = 422191$ και δημοσιοποιεί τους $n = 6012707$ και $e = 3674911$ σε έναν κατάλογο. Υποθέτουμε ότι ο Β θέλει να κρυπτογραφήσει το μήνυμα $m = 5234673$ και να το στείλει στον Α. Υπολογίζει το $m^e \bmod n = 5234673^{3674911} \bmod 6012707 \equiv 3650502$ c και μεταδίδει μέσω του καναλιού το κρυπτοκείμενο $c = 3650502$. Όταν ο Α το λάβει χρησιμοποιεί το ιδιωτικό του κλειδί και υπολογίζει $c^d \bmod n = 3650502^{422191} \bmod 6012707 = 5234673 = m$ ανακτώντας έτσι το μήνυμα m.

3.2 Το Πρόβλημα RSA

Η δυσκολία του προβλήματος RSA αποτελέι τη βάση για την ασφάλεια της κρυπτογραφίας δημοσίου κλειδιού RSA και της ψηφιακής υπογραφής RSA.

Το πρόβλημα RSA (RSAP) είναι το ακόλουθο: έχοντας ένα θετικό ακέραιο, που προκύπτει από δύο ευδιάκριτους περιττούς πρώτους αριθμούς p και q, ένα θετικό ακέραιο e τέτοιο ώστε $\gcd(e,(p-1)\cdot(q-1)) = 1$ και έναν ακέραιο c, βρίσκουμε έναν ακέραιο m έτσι ώστε $m^e = c \bmod n$.

Με άλλα λόγια το RSAP είναι ότι βρίσκοντας τις e-ιοστές ρίζες διαμορφώνεται ένας σύνθετος ακέραιος n. Οι συνθήκες που επιβάλλονται στις παραμέτρους n, e του προβλήματος, επιβεβαιώνουν ότι για κάθε ακέραιο $c \in \{0,1,2,...,n-1\}$ υπάρχει

ακριβώς ένας ακέραιος $m \in \{0,1,2,...,n-1\}$ τέτοιος ώστε $m^e = c \bmod n$. Ισοδύναμα η συνάρτηση $f : Z_n \to Z_n$ ορίζεται ως $f(m) = m^e \bmod n$ και είναι μια αντιμετάθεση.

3.3 Πλεονεκτήματα RSA

Ο RSA παρέχει μερικά πλεονεκτήματα τα οποία βοήθησαν στην υλοποίηση πιο ασφαλών και ευκολότερα διαχειρίσιμων συναλλαγών. Τα πλεονεκτήματα αυτά περιλαμβάνουν:

- Απλοποίηση του προβλήματος της διαχείρισης κλειδιών: στην συμμετρική κρυπτογραφία ο αριθμός των κλειδιών που απαιτείται για την επικοινωνία n οντοτήτων σε ένα κρυπτοσύστημα είναι ανάλογος του n^2. Στην ασύμμετρη κρυπτογραφία όμως κάθε χρήστης χρειάζεται δύο κλειδιά, έτσι ο απαιτούμενος αριθμός κλειδιών είναι απλά $2n$. Άρα είναι κατανοητό ότι σε ένα κρυπτοσύστημα δημοσίου κλειδιού η σχέση που συνδέει τον αριθμό των χρηστών με τον αριθμό των κλειδιών είναι γραμμική και γι' αυτό το λόγο εύκολα διαχειρίσιμη ακόμα και όταν ο αριθμός των χρηστών είναι αρκετά μεγάλος.
- Ενισχυμένη ασφάλεια των συναλλαγών: κάθε χρήστης παράγει μόνος του και για δική του χρήση ένα ζεύγος κλειδιών. Το ιδιωτικό κλειδί θα πρέπει να μένει μυστικό και κρυφό από οποιαδήποτε μη εξουσιοδοτημένη οντότητα εξαλείφοντας έτσι όχι μόνο το πρόβλημα της μεταφοράς του αλλά και την απαίτηση για την εγκατάσταση ενός ασφαλούς διαύλου επικοινωνίας. Το δημόσιο κλειδί από την άλλη είναι ευρέως διαθέσιμο και άρα μπορεί να μεταφερθεί με οποιαδήποτε βολική μέθοδο σε ένα δίκτυο χωρίς να τίθεται θέμα για τη διατήρηση της μυστικότητάς του.

3.4 Σχήμα υπογραφής RSA

Η υπογραφή RSA παρουσιάστηκε και αυτή το 1978. Η ασφάλεια του σχήματος υπογραφής RSA στηρίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακέραιων

αριθμών. Ο χώρος των μηνυμάτων και ο χώρος των κλειδιών είναι $Z_n = \{0,1,2,...,n-1\}$, όπου $n = p \cdot q$ είναι το γινόμενο δύο τυχαίων επιλεγμένων πρώτων αριθμών. Επειδή ο μετασχηματισμός κρυπτογράφησης είναι αντιστρέψιμη συνάρτηση, οι υπογραφές μπορούν να δημιουργηθούν αντιστρέφοντας τους κανόνες κρυπτογράφησης και αποκρυπτογράφησης.

Τα σύνολα M_S και S είναι το Z_n. Επιλέγεται μία συνάρτηση αναγωγής $R: M \to Z_n$ η οποία είναι δημοσίως γνωστή.

α) Αλγόριθμος δημιουργίας κλειδιού

1. Ο Α παράγει δυο μεγάλους τυχαίους πρώτους αριθμούς p και q.
2. Υπολογίζει $n = p \cdot q$ και $\varphi(n) = (p-1) \cdot (q-1)$.
3. Επιλέγει ένα τυχαίο ακέραιο αριθμό e με $1 \prec e \prec \varphi(n)$ τέτοιο που $\gcd(e, \varphi(n)) = 1$.
4. Χρησιμοποιώντας τον Εκτεταμένο Ευκλείδειο Αλγόριθμο υπολογίζει το μοναδικό ακέραιο d με $1 \prec d \prec \varphi(n)$ τέτοιο που $e \cdot d = 1 \bmod \varphi(n)$.
5. Το δημόσιο κλειδί του Α είναι το ζευγάρι (n, e) και το μυστικό κλειδί είναι το d.

β) Αλγόριθμος δημιουργίας υπογραφής

1. Ο Α υπολογίζει $m' = R(m)$, ένας ακέραιος στο διάστημα $[0, n-1]$.
2. Υπολογίζει $s = (m')^d \bmod n$.
3. Η υπογραφή του Α για το μήνυμα m είναι το s.

γ) Αλγόριθμος πιστοποίησης της υπογραφής

1. Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το (n, e).
2. Υπολογίζει $m' = s^e \bmod n$.
3. Πιστοποιεί ότι $m' \in M_R$, αλλιώς απορρίπτει την υπογραφή.
4. Ανακτά το $m = R^{-1}(m')$.

Απόδειξη του αλγόριθμου πιστοποίησης : Αν s είναι η υπογραφή για το μήνυμα m τότε $s = (m')^d \bmod n$ με $m' = R(m)$. Επειδή $e \cdot d = 1 \bmod \varphi(n)$, $s^e = (m')^{ed} = m' \bmod n$, τελικά θα έχουμε ότι $R^{-1}(R(m)) = m$.

Παράδειγμα 1: (Επαλήθευση υπογραφής)

Επιλέγουμε δυο πρώτους $p = 7$ και $q = 11$ και υπολογίζουμε $n = p \cdot q = 77$ και $\varphi(n) = (p-1) \cdot (q-1) = 6 \cdot 10 = 60$. Επιλέγουμε $e = 13$ (ισχύει $1 \prec e \prec 60$ και $\gcd(e, 60) = 1$). Βρίσκουμε ότι $e \cdot d = 13 \cdot d = 1 \bmod 60$ με $d = 37$. Το δημόσιο κλειδί είναι το $(n, e) = (77, 13)$ και το ιδιωτικό κλειδί το $d = 37$.

Για να υπογράψουμε το μήνυμα $m = 57$ υπολογίζουμε το $m^d = 57^{37} = 29 \bmod 77$. Η υπογραφή του μηνύματος m είναι η $s = 29$.

Για να επαληθεύσουμε την υπογραφή s του μηνύματος m ελέγχουμε αν $s^e = m (\bmod n)$. Όντως $29^{13} = 57 \bmod 77$.

Παράδειγμα 2: Θα δούμε ένα παράδειγμα για το RSA με ανάκτηση του μηνύματος.

Παραγωγή κλειδιού:

Ο Α επιλέγει πρώτους αριθμούς $p = 7927$, $q = 6997$ και υπολογίζει $n = p \cdot q = 55465219$ και $\varphi(n) = (p-1) \cdot (q-1)$ $7926 \cdot 6996 = 55450296$. Ο Α επιλέγει $e = 5$ και βρίσκει ότι $e \cdot d = 5 \cdot d = 1 \bmod 55450296$ με $d = 44360237$. Το δημόσιο κλειδί του Α είναι το ζευγάρι $(n, e) = (55465219, 5)$ και το μυστικό κλειδί το $d = 44360237$.

Παραγωγή υπογραφής:

Για λόγους απλότητας θεωρούμε ότι $M = Z_n$ και η συνάρτηση αναγωγής $R : M \to Z_n$ είναι η ταυτοτική συνάρτηση $R(m) = m$ για όλα τα $m \in M$. Έστω ότι το μήνυμα μας είναι $m = 31229978$. Ο Α υπολογίζει $m' = R(m) = 31229978$ και την υπογραφή $s = (m')^d \bmod n$ $31229978^{44360237} \bmod 55465219$ 30729435. =

Πιστοποίηση υπογραφής:

Ο Β υπολογίζει $m' = s^e \bmod n$ $30729435^5 \bmod 55465219$ 31229978. Τελικά ο Β δέχεται την υπογραφή επειδή $m' \in M_R$ και ανακτά το $m' = R^{-1}(m') = 31229978$.

3.5 Δυνατές επιθέσεις και Ασφάλεια του σχήματος RSA

Ένας τρόπος εξαπάτησης είναι η κατάλληλη επιλογή ενός $s \in \{0,1,2,...,n-1\}$ τέτοιο ώστε το μήνυμα $m \in \{0,1,2,...,n-1\}$ που προκύπτει ως $m = s^d \bmod n$ να έχει κάποια σημασία. Αν καταφέρει κάποιος να βρει τέτοιο s τότε έχει την υπογραφή του μηνύματος m. Επιπλέον αν κάποιος θέλει την υπογραφή για ένα μήνυμα m ένας τρόπος για να την αποσπάσει είναι να υπολογίσει $m_1, m_2 \in \{0,1,2,...,n-1\}$ τέτοια ώστε $m = m_1 m_2$ και να προσπαθήσει να αποσπάσει τις υπογραφές των μηνυμάτων m_1, m_2. Έστω λοιπόν ότι $s_1, s_2 \in \{0,1,2,...,n-1\}$ είναι οι ζητούμενες υπογραφές. Τότε η $s_1 s_2$ είναι η υπογραφή του μηνύματος m. Πράγματι $s_1 s_2 = m_1^d m_2^d = m^d \bmod n$.

Παρακάτω θα περιγράψουμε κάποιες γνωστές επιθέσεις καθώς και κάποια μέτρα που πρέπει να λαμβάνονται υπόψη κατά την επιλογή των παραμέτρων της υπογραφής RSA ώστε να αποφεύγονται οι προσβολές.

1. **Παραγοντοποίηση του** n

Κατ' αρχάς για την ασφάλεια του σχήματος η παραγοντοποίηση του n θα πρέπει να είναι πρακτικά ανέφικτη αφού η εύρεση των πρώτων p, q ισοδυναμεί με την εύρεση του ιδιωτικού κλειδιού d που καθιστά τον κάτοχο ικανό να υπογράφει οποιοδήποτε μήνυμα επιθυμεί. Συγκεκριμένα η εύρεση της παραγοντοποίησης του n ισοδυναμεί με την εύρεση του $\varphi(n)$.

Πράγματι γνωρίζοντας τους p, q μπορούμε να υπολογίσουμε το $\varphi(n) = (p-1)\cdot(q-1)$ γιατί η συνάρτηση φ του Euler είναι πολλαπλασιαστική και αντιστρόφως γνωρίζοντας το $\varphi(n)$ έχουμε ότι $n = p \cdot q$ και $p + q = n + 1 - \varphi(n)$ και

επομένως τα p,q είναι λύσεις της εξίσωσης $T^2-(n+1-\varphi(n))T+n=0$ δηλαδή είναι τα $p,q=\dfrac{n+1-\varphi(n)\pm\sqrt{(n+1-\varphi(n))^2-4n}}{2}$.

Επομένως γνωρίζοντας την παραγοντοποίηση του n, επιλύοντας την ισοτιμία $e\cdot d=1\bmod\varphi(n)$ μπορούμε να υπολογίσουμε το d.

Προκύπτει λοιπόν ότι οι p,q θα πρέπει να πληρούν μερικούς περιορισμούς. Πρώτα οι $p-1,q-1$ δεν πρέπει να είναι γινόμενο μικρών πρώτων αριθμών γιατί σ' αυτή την περίπτωση ο αλγόριθμος παραγοντοποίησης $p-1$ του J.Pollard δίνει σχετικά εύκολα την παραγοντοποίηση του n. Επιπλέον οι πρώτοι p,q πρέπει να να μην είναι κάποιας ειδικής μορφής όπως οι πρώτοι του Fermat ή οι πρώτοι του Mersenne και να έχουν περίπου το ίδιο μήκος το οποίο θα πρέπει να τέτοιο ώστε το n να έχει μήκος ≥ 1024 δυαδικά ψηφία. Ακόμη θα πρέπει να τηρείται κάποιο μέτρο για το ιδιωτικό κλειδί d. Παρακάτω θα αναφέρουμε κάποιες επιθέσεις οι οποίες απευθύνονται γενικά στο κρυπτοσύστημα RSA αλλά με τις οποίες μπορεί να προσβληθεί και μία υπογραφή αφού οι επιθέσεις έχουν σαν σκοπό την παραγοντοποίηση του n και την εύρεση του κλειδιού d.

Επίθεση του **Wiener**

Μία γνωστή επίθεση είναι αυτή που οφείλεται στον M.Wiener και η οποία για να αποφευχθεί θα πρέπει το ιδιωτικό κλειδί d να είναι $\succ\dfrac{n^{1/4}}{3}$. Η μέθοδος του Wiener βασίζεται στον υπολογισμό του συνεχούς κλάσματος $\dfrac{e}{n}$ και των συγκλίνοντων σε αυτόν ρητών. Γνωρίζουμε ότι ισχύει η σχέση $e\cdot d=1\bmod\varphi(n)$. Άρα υπάρχει ακέραιος k με $e\cdot d=1+k(n+1-(p+q))$. Διαιρούμε και τα δύο μέλη με dn και παίρνουμε: $\left|\dfrac{e}{n}-\dfrac{k}{d}\right|=\dfrac{|1+k(1-p-q)|}{dn}\prec\dfrac{k(p+q)}{dn}$.

Επειδή ισχύει ότι $ed-k\varphi(n)=1$ και $e\prec\varphi(n)$, θα ισχύει $d\succ k$. Άρα θα έχουμε: $\left|\dfrac{e}{n}-\dfrac{k}{d}\right|\prec\dfrac{p+q}{n}$.

Αν οι πρώτοι p,q έχουν μήκος ίσο με l και $p \prec q$ θα έχουμε $q \le 2^{l-1}+...+1$ και $p \ge 2^{l-1}+1$ απ' όπου προκύπτει ότι $p-q \prec 2^{l-1} \prec p$. Έτσι έχουμε τις εξής σχέσεις: $p \prec q \Leftrightarrow p^2 \prec n \Leftrightarrow p \prec \sqrt{n}$ και $q-p \prec p \Leftrightarrow q \prec 2p$. Επομένως $p+q \prec 3\sqrt{n}$. Άρα $\left|\frac{e}{n}-\frac{k}{d}\right| \prec \frac{3}{\sqrt{n}}$ και αν $d \prec \frac{n^{1/4}}{3}$ τότε $\left|\frac{e}{n}-\frac{k}{d}\right| \prec \frac{1}{3d^2} \prec \frac{1}{2d^2}$.

σύμφωνα με γνωστή πρόταση (Αν $\frac{p}{q}$ είναι ένας θετικός ρητός τέτοιος ώστε $\left|\rho-\frac{p}{q}\right| \prec \frac{1}{2q^2}$ τότε ο $\frac{p}{q}$ είναι συγκλίνων ρητός στο ρ .) το ανάγωγο κλάσμα $\frac{k}{d}$ είναι ένας από τους συγκλίνοντες ρητούς στο $\frac{e}{n}$ και υπολογίζεται σε χρόνο $O((\log e)(\log n))$.

Παράδειγμα: Ας υποθέσουμε ότι το δημόσιο κλειδί είναι $(n,e)=(160523347,60728973)$. Θα ελέγξουμε αν για το κλειδί αποκρυπτογράφησης d ισχύει $d \le \left[\frac{n^{1/4}}{3}\right]=37$. Είδαμε ότι $ed-k\varphi(n)=1$ και $\frac{k}{d}$ είναι ένας από τους συγκλίνοντες ρητούς στο $\frac{e}{n}$. Το ανάπτυγμα σε συνεχές κλάσμα του $\frac{e}{n}$ είναι $\frac{e}{n}=<0,2,1,1,1,4,12,102,1,1,2,3,2,2,36>$. Οι συγκλίνοντες ρητοί στο $\frac{e}{n}$ με ≤ 37 είναι οι : $0,\frac{1}{2},\frac{1}{3},\frac{2}{5},\frac{3}{8},\frac{14}{37}$.

Καθώς ο ακέραιος n είναι το γινόμενο δύο περιττών πρώτων, ο $\varphi(n)$ θα διαιρείται με το 4. Αν $d=2,8$, τότε η σχέση $ed-k\varphi(n)=1$ δίνει ότι $2|1$, δηλαδή άτοπο. Αν $\frac{k}{d}=\frac{2}{5}$ τότε $\varphi(n)=\frac{ed-1}{k}=151822432$ και συνεπώς οι παράγοντες p,q του n είναι οι λύσεις της εξίσωσης $T^2-(n+1-\varphi(n))T+n=0$ όπου $n+1-\varphi(n)=8700916$. Η διακρίνουσα της εξίσωσης είναι $\Delta=75705297145668$ και αφού η τετραγωνική της ρίζα δεν είναι ακέραιος, οι λύσεις της εξίσωσης δε δίνουν τους παράγοντες του n και

επομένως $\frac{k}{d} \neq \frac{2}{5}$. Αν υποθέσουμε ότι $\frac{k}{d} = \frac{14}{37}$ θα έχουμε $\varphi(n) = 160498000$ και θα προκύψει η εξίσωση $T^2 - 25348T + 160523347 = 0$ που δίνει λύσεις $p = 12347$ και $q = 13001$. Άρα το κλειδί αποκρυπτογράφησης είναι $d = 37$.

Επίθεση **Verheul-Van Tilborg**

Το 1997 οι Verheul και Van Tilborg παρουσίασαν μία επέκταση της επίθεσης του Wiener η οποία βασίζεται στα συνεχή κλάσματα. Για $d \prec n^{1/4}$ δίνει τα ίδια αποτελέσματα με τη μέθοδο του Wiener. Για r παραπάνω ψηφία όμως στο ιδιωτικό κλειδί d απαιτείται η εξαντλητική αναζήτηση σχεδόν $2r$ ψηφίων αφού η μέθοδος αυτή δίνει σαν αποτέλεσμα το d ως συνάρτηση άλλων άγνωστων παραμέτρων, $2r$ ψηφίων συνολικά, που πρέπει να τις βρούμε δοκιμάζοντας όλες τις πιθανές επιλογές. Ωστόσο για $n^{1/4} \prec d \prec n^{1/2}$ έδειξαν ότι υπάρχει τρόπος να υπολογίσουμε το d αλλά με έναν αλγόριθμο εκθετικού χρόνου.

Επίθεση **Boneh-Durfee**

Η πρώτη ουσιαστική επέκταση της επίθεσης του Wiener είναι αυτή που παρουσιάστηκε το 2000 από τους Boneh και Durfee η οποία έδειξαν ότι για $d \prec n^{0.292}$ η υπογραφή RSA μπορεί να προσβληθεί σε πολυωνυμικό χρόνο. Η επίθεσή τους βασίζεται στις μεθόδους του Coppersmith για την εύρεση μικρών ριζών πολυωνυμικών ισοτιμιών.

Λόγω των παραπάνω επιθέσεων συμπεραίνουμε ότι δεν μπορούμε να χρησιμοποιούμε μικρού μεγέθους ιδιωτικό κλειδί d. Ωστόσο για να επιταχύνουμε την διαδικασία υπογραφής μπορούμε να χρησιμοποιήσουμε d έτσι ώστε οι ακέραιοι $d_p \in \{1, 2, \ldots p-2\}$ με $d_p = d \bmod (p-1)$ και $d_q \in \{1, 2, \ldots q-2\}$ με $d_q = d \bmod (q-1)$ να είναι μικρού μεγέθους. Ένας τέτοιος εκθέτης d καλείται CRT-εκθέτης (Chinese Remainder Theorem). Για να υπογράψουμε λοιπόν ένα μήνυμα m υπολογίζουμε τα $m^{d_p} \bmod p$, $m^{d_q} \bmod q$ και έπειτα χρησιμοποιώντας το Κινέζικο θεώρημα υπολοίπων υπολογίζουμε την υπογραφή $s = m^d \bmod n$ του μηνύματος m. Οι προηγούμενες

επιθέσεις παύουν να είναι αποτελεσματικές αφού το ιδιωτικό κλειδί d είναι μεγάλου μεγέθους. Μέχρι το 2002 όλες οι γνωστές μέθοδοι επίθεσης της υπογραφής RSA όταν τα d_p, d_q είναι μικρά ήταν εκθετικού χρόνου. Το 2002 όμως ο Alexander May παρουσίασε μία επίθεση πολυωνυμικού χρόνου η οποία εφαρμόζεται όμως μόνο στην περίπτωση που οι πρώτοι p, q έχουν μεγάλη διαφορά μεγέθους.

2. **Χρήση του ίδιου ακεραίου** n

Αν υπάρχει μία ομάδα χρηστών της υπογραφής RSA η οποία χρησιμοποιεί τον ίδιο ακέραιο n αλλά διαφορετικά κλειδιά (e_i, d_i) τότε καθένας από τους χρήστες μπορεί να υπολογίσει το ιδιωτικό κλειδί οποιουδήποτε άλλου χρήστη και να υπογράψει για αυτόν ακολουθώντας την παρακάτω διαδικασία.

Κατ' αρχάς σύμφωνα με το παρακάτω λήμμα καθένας από τους χρήστες μπορεί να παραγοντοποιήσει το n.

Λήμμα: Αν κάποιος γνωρίζει το ιδιωτικό κλειδί d μίας υπογραφής *RSA* τότε χρησιμοποιώντας το δημόσιο κλειδί (n, e) μπορεί να παραγοντοποιήσει το n.

Απόδειξη: Από τη σχέση $e \cdot d = 1 \bmod \varphi(n)$ προκύπτει ότι υπάρχει ακέραιος k τέτοιος ώστε να ισχύει $ed - 1 \quad k \not\in p-1)(q-1)$. Επιλέγουμε ακέραιο $x \neq 0$, με $(x, n) = 1$. Θα ισχύει ότι $x^{ed-1} = 1 \bmod n$. Υπολογίζουμε μία τετραγωνική ρίζα y_1 της μονάδος modulo n και έχουμε $y_1 = \sqrt{x^{ed-1}} = x^{\frac{ed-1}{2}}$, το οποίο μπορούμε να το κάνουμε αφού γνωρίζουμε το $ed-1$ και ότι είναι άρτιος. Έτσι έχουμε $y_1^{\,2} - 1 = 0 \bmod n$ την οποία μπορούμε να τη χρησιμοποιήσουμε για να βρούμε τον $(y_1 - 1, n)$. Έτσι θα έχουμε βρει έναν παράγοντα του n. Για να συμβεί βέβαια αυτό θα πρέπει $y_1 \neq \pm 1 \bmod n$.
Στην περίπτωση όμως που ισχύει ότι $y_1 = \pm 1 \bmod n$ έχουμε δύο περιπτώσεις:

α) Αν $y_1 = -1 \bmod n$, τότε επιστρέφουμε στην αρχή και επιλέγουμε νέο ακέραιο x.

β) Αν $y_1 = 1 \bmod n$, τότε υπολογίζουμε μία νέα τετραγωνική ρίζα $y_2 = \sqrt{y_1} = x^{\frac{ed-1}{4}} \bmod n$. Έτσι έχουμε πάλι ότι $y_2{}^2 - 1 = y_1 - 1 = 0 \bmod n$. Υπολογίζουμε λοιπόν τον $(y_2 - 1, n)$ ο οποίος αν $y_2 \neq \pm 1 \bmod n$, μας δίνει έναν παράγοντα του n, διαφορετικά ακολουθούμε πάλι την προηγούμενη διαδικασία!!!

Επαναλαμβάνουμε την παραπάνω διαδικασία μέχρι να βρούμε κάποιον παράγοντα του n ή μέχρι ο αριθμός $\frac{ed-1}{2^t}$ να μην διαιρείται από το 2. Σ' αυτήν την τελευταία περίπτωση επιλέγουμε νέο ακέραιο x και επαναλαμβάνουμε την διαδικασία από την αρχή. □

Χρησιμοποιώντας λοιπόν ο χρήστης με ιδιωτικό κλειδί d_1 τον παραπάνω αλγόριθμο παραγοντοποιεί το n, δηλαδή υπολογίζει τα p, q. Έτσι υπολογίζοντας το $\varphi(n) = (p-1)\cdot(q-1)$ και επιλύοντας τη σχέση $e \cdot d = 1 \bmod \varphi(n)$ υπολογίζει το ιδιωτικό κλειδί του m-χρήστη.

Επίθεση **Coron-May**

Το 2006 ο Jean-Sébastien Coron και ο Alexander May απέδειξαν το παρακάτω θεώρημα:

Θεώρημα: Έστω $n = p \cdot q$ το γινόμενο δύο πρώτων αριθμών ίδιου μεγέθους και e, d ακέραιοι, τέτοιοι ώστε $e \cdot d = 1 \bmod \varphi(n)$. Αν $1 \prec ed \leq n^{\frac{3}{2}}$, τότε μπορούμε να υπολογίσουμε την παραγοντοποίηση του n σε χρόνο $O(\log^2 n)$.

Απόδειξη: Θεωρούμε ότι $p \prec q$ (χωρίς βλάβη της γενικότητας). Τότε $p \prec n^{\frac{1}{2}} \prec q \prec 2p \prec 2n^{\frac{1}{2}}$ από το οποίο προκύπτει ότι $p + q \prec 3n^{\frac{1}{2}}$ καθώς και ότι $\varphi(n) = n + 1 - (p+q) \succ \frac{1}{2}n$. Επίσης από την σχέση $e \cdot d = 1 \bmod \varphi(n)$ προκύπτει ότι υπάρχει $k \in N$ τέτοιο ώστε $ed = 1 + k\varphi(n)$.

Θα δείξουμε τώρα ότι για $ed \le n^{\frac{3}{2}}$, το k μπορεί εύκολα να βρεθεί. Πράγματι, θέτοντας $k' = \frac{ed-1}{n}$, παρατηρούμε ότι :

$$k - k' = \frac{ed-1}{\varphi(n)} - \frac{ed-1}{n} = \frac{n(ed-1) - (n-p-q+1)(ed-1)}{\varphi(n)n} = \frac{(p+q-1)(ed-1)}{\varphi(n)n}.$$

Χρησιμοποιώντας τις παραπάνω ανισότητες καταλήγουμε στο εξής :

$k - k' \prec 6n^{-\frac{3}{2}}(ed-1)$ και επειδή $ed \le n^{\frac{3}{2}}$ ισχύει ότι $0 \prec k - k' \prec 6$. Αν συμβολίσουμε με $\lceil k' \rceil$ τον μικρότερο ακέραιο που είναι μεγαλύτερος ή ίσος του k', τότε μία από τις τιμές $\lceil k' \rceil + i$ με $i = 0,1,2,3,4,5$ θα ισούται με k. Ελέγχουμε ποιά από τις έξι τιμές είναι η σωστή και από τις σχέσεις $n = p \cdot q$ και $p + q = n + 1 + \frac{ed-1}{k}$ προκύπτει η παραγοντοποίηση του n. Ο χρόνος που απαιτείται για όλους τους παραπάνω υπολογισμούς είναι $O(\log^2 n)$ αφού κάναμε μόνο βασικές αριθμητικές πράξεις ακεραίων μεγέθους $O(\log n)$. □

Το παραπάνω αποτέλεσμα γενικεύεται και για πρώτους p, q διαφορετικού μεγέθους, χρησιμοποιώντας μία τεχνική των Durfee και Nguyen και τότε η παραγοντοποίηση του n υπολογίζεται σε χρόνο $O(\log^9 n)$.

3.**Χρήση του ίδιου κλειδιού** d

Αν $m_1, m_2 \in \{0,1,2,...,n-1\}$ είναι μηνύματα που πρόκειται να υπογραφούν και $s_1, s_2 \in \{0,1,2,...,n-1\}$ οι υπογραφές αντίστοιχα των μηνυμάτων m_1, m_2 τότε έχουμε $s_1 = m_1^d \bmod n$ και $s_2 = m_2^d \bmod n$ και επομένως $s_1 s_2 = (m_1 m_2)^d \bmod n$.

Παρατηρούμε δηλαδή πως αν είναι γνωστές οι υπογραφές s_1, s_2 των μηνυμάτων m_1, m_2 τότε εύκολα μπορούμε να υπολογίσουμε και την υπογραφή του μηνύματος $m_1 m_2$.

Εκτός από τις προϋποθέσεις που αναφέραμε για την ασφάλεια της υπογραφής ένας άλλος τρόπος για να αποφύγουμε τις προσβολές είναι ο διπλασιασμός της δυαδικής γραφής του μηνύματος. Δεν υπάρχει καμία γνωστή μέθοδος υπολογισμού s τέτοιου ώστε $s^e = m \bmod n$ και η δυαδική γραφή του m να είναι της μορφής ww. Επιπλέον αν m_1, m_2 είναι δύο μηνύματα της μορφής ww τότε είναι πολύ μικρή η πιθανότητα εύρεσης ακέραιου m με $0 \le m \le n-1$ και $m = (m_1 m_2) \bmod n$ τέτοιου ώστε να είναι και της μορφής ww.

Ένας άλλος τρόπος για να αποφύγουμε τις προσβολές είναι η χρήση μίας συνάρτησης συμπύκνωσης $h: \{0,1\}^* \to \{0,1,...,n-1\}$ μοναδικής κατεύθυνσης και ελεύθερης σύμπτωσης. Τότε η υπογραφή του μηνύματος m είναι η $s = h(m)^d \bmod n$.

Ο παραλήπτης για να επαληθεύσει την υπογραφή υπολογίζει το $s^e \bmod n$ και το $h(m)$ και ελέγχει αν αυτές οι δύο τιμές είναι ίσες. Με την χρήση της συνάρτησης συμπύκνωσης ο υπογράφων αποφεύγει προσβολές διότι αν κάποιος πάρει ένα τυχαίο s και υπολογίσει το s^e τότε θα πρέπει να βρει και κατάλληλο m τέτοιο ώστε $h(m) = s^e \bmod n$ που είναι υπολογιστικά ανέφικτο. Έπειτα αν έχουμε δύο μηνύματα m_1, m_2 με υπογραφές $h(m_1)^d \pmod n, h(m_2)^d \pmod n$ δεν είναι εύκολο να βρεθεί m τέτοιο ώστε $h(m) = h(m_1)h(m_2) \pmod n$. Επομένως δεν μπορεί να βρεθεί μήνυμα του οποίου η υπογραφή να είναι η $(h(m_1)h(m_2))^d \pmod n$.

3.6 Οι υπογραφές RSA στην πράξη

(i) Πρόβλημα ανατμηματοποίησης (Reblocking Problem)

Μια προτεινόμενη χρήση του RSA είναι να υπογράψουμε το μήνυμα και μετά να κρυπτογραφήσουμε την υπογραφή που προκύπτει. Θα πρέπει όμως να μας απασχολούν τα σχετικά μεγέθη των moduli που εμπλέκονται όταν υλοποιούμε τη διεργασία αυτή. Ας υποθέσουμε ότι ο Α επιθυμεί να υπογράψει και στη συνέχεια να κρυπτογραφήσει ένα μήνυμα για τον Β. Έστω ότι τα δημόσια κλειδιά των Α και Β είναι (n_A, e_A) και (n_B, e_B) αντίστοιχα. Αν είναι $n_A \succ n_B$ τότε υπάρχει μια πιθανότητα

να μη μπορεί να ανακτηθεί το μήνυμα από τον Β, όπως φαίνεται στο παρακάτω παράδειγμα.

Παράδειγμα (*πρόβλημα ανατμηματοποίησης*): Έστω $n_A = 8387 \cdot 7499 = 62894113$, $e_A = 5$, $d_A = 37726937$, $n_B = 55465219$, $e_B = 5$ και $d_B = 44360237$. Να σημειωθεί ότι $n_A \succ n_B$. Ας υποθέσουμε ότι το $m = 1368797$ είναι ένα μήνυμα με περίσσεια που πρόκειται να υπογραφεί με το ιδιωτικό κλειδί του Α και μετά να κρυπτογραφηθεί χρησιμοποιώντας το δημόσιο κλειδί του Β. Ο Α υπολογίζει τα παρακάτω:

1. $s = m^{d_A} \bmod n_A \quad 1368797^{37726937} \bmod 62894113 \quad 59847900 \quad =$
2. $c = s^{e_B} \bmod n_B \quad 59847900^5 \bmod 55465219 \quad 38842235 \quad =$

Για να ανακτήσει το μήνυμα και να επαληθεύσει την υπογραφή, ο Β υπολογίζει τα παρακάτω:

1. $s' = c^{d_B} \bmod n_B \quad 38842235^{44360237} \bmod 55465219 \quad 4382681 \quad =$
2. $m' = s'^{e_A} \bmod n_A \quad 4382681^5 \bmod 62894113 \quad 54383568 \quad =$

Παρατηρούμε ότι $m \neq m'$. Ο λόγος γι' αυτό είναι ότι το s είναι μεγαλύτερο από το modulus n_B. Εδώ, η πιθανότητα εμφάνισης αυτού του προβλήματος είναι $\frac{(n_A - n_B)}{n_A} \approx 0.12$.

Υπάρχουν διάφοροι τρόποι για να ξεπεράσουμε το πρόβλημα ανατμηματοποίησης.

1. Αναδιάταξη. Το πρόβλημα της εσφαλμένης αποκρυπτογράφησης δεν θα εμφανιστεί ποτέ αν εκτελεστεί πρώτα η πράξη στην οποία χρησιμοποιείται το μικρότερο modulus. Δηλαδή, αν $n_A \succ n_B$, η οντότητα Α θα πρέπει πρώτα να κρυπτογραφήσει το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Β και μετά να υπογράψει το προκύπτον κρυπτοκείμενο χρησιμοποιώντας το ιδιωτικό κλειδί του Α. Η προτιμητέα σειρά των πράξεων όμως, είναι πάντοτε να υπογράφεται πρώτα το μήνυμα και μετά να κρυπτογραφείται η υπογραφή γιατί αν ο Α πρώτα κρυπτογραφήσει και μετά υπογράψει, ο αντίπαλος θα μπορούσε να αφαιρέσει την υπογραφή και να την αντικαταστήσει με τη δική του υπογραφή. Ακόμα κι αν ο

αντίπαλος δεν γνωρίζει τι είναι υπογεγραμμένο, μπορεί να υπάρχουν καταστάσεις όπου αυτό να αποτελεί πλεονέκτημα για τον αντίπαλο. Άρα η αναδιάταξη δεν είναι η ενδεδειγμένη λύση.

2. Δύο moduli ανά οντότητα. Κάθε οντότητα πρέπει να παράγει ξεχωριστά moduli για κρυπτογράφηση και υπογραφή. Αν το modulus υπογραφής κάθε χρήστη είναι μικρότερο απ' όλα τα πιθανά moduli κρυπτογράφησης, τότε δεν θα εμφανιστεί ποτέ λαθεμένη αποκρυπτογράφηση. Αυτό μπορούμε να το εγγυηθούμε απαιτώντας να είναι τα moduli κρυπτογράφησης αριθμοί των $(t+1)$ bit και τα moduli υπογραφής αριθμοί των t bit.

3. Προκαθορισμός της μορφής του modulus. Στη μέθοδο αυτή επιλέγουμε τους πρώτους p, q έτσι ώστε το modulus n να έχει μια ειδική μορφή: το υψηλότερης τάξης bit είναι 1 και τα επόμενα k bit είναι όλα 0. Ένα modulus n των t bit αυτής της μορφής μπορεί να βρεθεί ως εξής:
Για να έχει το n την απαιτούμενη μορφή πρέπει να ισχύει $2^{t-1} \le n \le 2^{t-1} + 2^{t-k-1}$. Επιλέγουμε έναν τυχαίο πρώτο p των $\left\lceil \frac{t}{2} \right\rceil$ bit και αναζητούμε έναν πρώτο q στο διάστημα μεταξύ των $\left\lceil \frac{2^{t-1}}{p} \right\rceil$ και $\left\lfloor \frac{2^{t-1} + 2^{t-k-1}}{p} \right\rfloor$. Τότε το $n = p \cdot q$ είναι ένα modulus του ζητούμενου τύπου. Αυτή η επιλογή του modulus n δεν αποτρέπει τελείως το πρόβλημα της λαθεμένης αποκρυπτογράφησης, αλλά μπορεί να ελαττώσει την πιθανότητα εμφάνισής του σε έναν πολύ μικρό αριθμό. Ας υποθέσουμε ότι ο n_A είναι ένα τέτοιο modulus και ότι ο $s = m^{d_A} \bmod n_A$ είναι μια υπογραφή στο m. Ας υποθέσουμε επιπλέον ότι ο s έχει ένα 1 σε μια από τις $k+1$ υψηλής τάξης θέσεις bit, άλλη από την υψηλότερη. Τότε ο s, αφού είναι μικρότερος του n_A, πρέπει να έχει ένα 0 στην υψηλότερης τάξης θέση bit και έτσι είναι αναγκαστικά μικρότερος από οποιοδήποτε άλλο modulus παρόμοιας μορφής. Η πιθανότητα ότι ο s δεν έχει κάποιο 1 στις $k+1$ υψηλής τάξης θέσεις bit, άλλη από την υψηλότερη, είναι μικρότερη από $\left(\frac{1}{2}\right)^k$, αριθμός που είναι πολύ μικρός αν επιλέξουμε το k να είναι περίπου 100.

Παράδειγμα (*προκαθορισμός της μορφής του modulus*) : Ας υποθέσουμε ότι θέλουμε να κατασκευάσουμε ένα modulus n των 12 bit τέτοιο ώστε το υψηλής τάξης bit να είναι 1 και τα επόμενα $k = 3$ bit να είναι 0. Στην αρχή επιλέγουμε έναν πρώτο των 6 bit, $p = 37$. Επιλέγουμε έναν πρώτο q στο διάστημα μεταξύ των $\left\lceil \frac{2^{11}}{p} \right\rceil = 56$ και $\left\lceil \frac{2^{11} + 2^8}{p} \right\rceil = 62$. Οι πιθανές τιμές για το q είναι 59 και 61. Αν επιλέξουμε $q = 59$, τότε $n = 37 \cdot 59 = 2183$, που έχει δυαδική αναπαράσταση 100010000111. Αν επιλέξουμε $q = 61$, τότε $n = 37 \cdot 61 = 2257$, που έχει δυαδική αναπαράσταση 100011010001.

(ii) Συναρτήσεις περίσσειας

Για να αποφύγουμε μια επίθεση υπαρξιακής πλαστογράφησης στο σχήμα υπογραφών RSA, απαιτείται μια κατάλληλη συνάρτηση περίσσειας *R*. Η συνετή επιλογή μιας συνάρτησης περίσσειας είναι ένα κρίσιμο ζήτημα για την ασφάλεια του συστήματος.

(iii) Το σχήμα ψηφιακών υπογραφών RSA με παράρτημα

Σε προηγούμενη ενότητα περιγράψαμε πώς μπορεί ένα σχήμα ψηφιακών υπογραφών με ανάκτηση μηνύματος να τροποποιηθεί για να δώσει ένα σχήμα ψηφιακών υπογραφών με παράρτημα. Για παράδειγμα, αν χρησιμοποιήσουμε τον MD5 για να διασπείρουμε μηνύματα οποιουδήποτε δυαδικού μήκους σε δυαδικές συμβολοσειρές μήκους 128, τότε θα μπορούσαμε να χρησιμοποιήσουμε τον αλγόριθμο δημιουργίας και πιστοποίησης της υπογραφής στα σχήματα ψηφιακών υπογραφών με ανάκτηση του μηνύματος που είδαμε στα παραπάνω, για να υπογράφουμε αυτές τις τιμές διασποράς. Αν το n είναι ένα modulus RSA των k bit, τότε απαιτείται μια κατάλληλη συνάρτηση περίσσειας *R* για να αντιστοιχίζουμε ακεραίους των 128 bit σε ακεραίους των k bit.

(iv) Χαρακτηριστικά επιδόσεων της παραγωγής και επαλήθευσης υπογραφών

Έστω $n = p \cdot q$ ένα modulus RSA των $2k$ bit, όπου p, q είναι πρώτοι των k bit ο καθένας. Ο υπολογισμός μιας υπογραφής $s = m^d \bmod n$, για ένα μήνυμα m απαιτεί $O(k^3)$ πράξεις bit. Αφού ο υπογράφων τυπικά γνωρίζει τα p και q, μπορεί να υπολογίσει τα $s_1 = m^d \bmod p$, $s_2 = m^d \bmod q$, και να προσδιορίσει το s χρησιμοποιώντας το Κινέζικο θεώρημα υπολοίπων. Παρόλο που η πολυπλοκότητα της διαδικασίας αυτής παραμένει $O(k^3)$, είναι πολύ πιο αποδοτική σε ορισμένες περιπτώσεις.

Η επαλήθευση των υπογραφών είναι σημαντικά πιο γρήγορη από την υπογραφή αν ο δημόσιος εκθέτης επιλέγεται να είναι ένας μικρός αριθμός. Αν γίνει αυτό, η επαλήθευση απαιτεί $O(k^2)$ πράξεις bit. Προτεινόμενες τιμές για το e στην πράξη, είναι 3 ή $2^{16}+1$. Φυσικά, τα p, q πρέπει να επιλέγονται έτσι, ώστε να είναι $\gcd(e,(p-1)(q-1)) = 1$.

Το σχήμα υπογραφών RSA, ταιριάζει απόλυτα στις περιπτώσεις που η επαλήθευση υπογραφών είναι η δεσπόζουσα πράξη η οποία εκτελείται. Για παράδειγμα, όταν ένα έμπιστο τρίτο μέλος δημιουργεί ένα πιστοποιητικό δημόσιου κλειδιού για μια οντότητα Α, αυτό απαιτεί μόνο μία παραγωγή υπογραφής και η υπογραφή αυτή μπορεί να επαληθευτεί πολλές φορές από διάφορες άλλες οντότητες.

(v) Επιλογή παραμέτρων

Από το 1996, για τα moduli υπογραφών RSA συστήνεται ένα ελάχιστο των 768 bit. Ένα modulus τουλάχιστον των 1024 bit συστήνεται για υπογραφές οι οποίες απαιτούν πολύ μεγαλύτερους χρόνους ζωής ή οι οποίες είναι κρίσιμες για τη συνολική ασφάλεια ενός μεγάλου δικτύου. Είναι ενδεδειγμένο να παραμένουμε ενήμεροι για την πρόοδο που σημειώνεται στην παραγοντοποίηση ακεραίων και να είμαστε προετοιμασμένοι για την προσαρμογή των παραμέτρων ανάλογα.

Δεν έχουν αναφερθεί αδυναμίες του σχήματος υπογραφών RSA όταν επιλέγεται ο δημόσιος εκθέτης e να είναι ένας μικρός αριθμός όπως ο $2^{16}+1$. Δεν συστήνεται να περιορίζουμε το μέγεθος του ιδιωτικού εκθέτη d προκειμένου να βελτιώσουμε την αποδοτικότητα της παραγωγής υπογραφών.

(vi) Αποδοτικότητα εύρους ζώνης (bandwidth efficiency)

Η αποδοτικότητα εύρους ζώνης για ψηφιακές υπογραφές με ανάκτηση μηνύματος αναφέρεται στον λόγο του λογαρίθμου (βάση 2) του μεγέθους του χώρου υπογραφής M_S προς τον λογάριθμο (βάση 2) του μεγέθους του M_R, του χώρου εικόνας της συνάρτησης περίσσειας. Συνεπώς, η αποδοτικότητα εύρους ζώνης προσδιορίζεται από την περίσσεια R. Για το RSA (και για το σχήμα ψηφιακών υπογραφών Rabin) η συνάρτηση περίσσειας που καθορίζεται από το ISO/IEC 9796 δέχεται μηνύματα των k bit και τα κωδικοποιεί σε στοιχεία των $2k$ bit στο M_S από τα οποία σχηματίζεται μια υπογραφή των $2k$ bit. Η αποδοτικότητα εύρους ζώνης στην περίπτωση αυτή είναι $\frac{1}{2}$. Παραδείγματος χάρη, με ένα modulus μεγέθους 1024 bit, το μέγιστο μέγεθος ενός μηνύματος το οποίο μπορεί να υπογραφεί είναι 512 bit.

(vii) Παράμετροι καθολικής εφαρμογής (system-wide)

Κάθε οντότητα πρέπει να έχει ένα διαφορετικό modulus RSA γιατί δεν είναι ασφαλές να χρησιμοποιούμε ένα modulus καθολικής εφαρμογής. Ο δημόσιος εκθέτης e μπορεί να είναι μια παράμετρος καθολικής εφαρμογής, και είναι σε πολλές εφαρμογές.

(viii) Σύντομα και μακροσκελή μηνύματα

Ας υποθέσουμε ότι το n είναι ένα modulus RSA των $2k$ bit το οποίο χρησιμοποιείται στον αλγόριθμο δημιουργίας και πιστοποίησης της υπογραφής για το RSA, για την υπογραφή μηνυμάτων των k bit (δηλαδή η αποδοτικότητα εύρους ζώνης είναι $\frac{1}{2}$). Ας υποθέσουμε ότι η οντότητα Α επιθυμεί να υπογράψει ένα μήνυμα

m των k bit. Μια προσέγγιση είναι να διαμερίσουμε το m σε τμήματα των k bit τέτοια ώστε $m_1 \| m_2 \| ... \| m_t$ και να υπογράψουμε κάθε τμήμα μεμονωμένα (κάτι τέτοιο βέβαια δεν προτείνεται). Η απαίτηση εύρους ζώνης γι' αυτό είναι $2kt$ bit. Εναλλακτικά, ο Α θα μπορούσε να διασπείρει το μήνυμα m σε μια συμβολοσειρά μήκους $l \le k$ και να υπογράψει την τιμή διασποράς. Η απαίτηση εύρους ζώνης για την υπογραφή αυτή είναι $kt + 2k$, όπου ο όρος kt προέρχεται από την αποστολή του μηνύματος m. Αφού $kt + 2k \le 2kt$ όταν $t \ge 2$, συνεπάγεται ότι η πλέον αποδοτική μέθοδος εύρους ζώνης είναι να χρησιμοποιήσουμε ψηφιακές υπογραφές RSA με παράρτημα. Για ένα μήνυμα μεγέθους το πολύ k bit είναι προτιμότερο το RSA με ανάκτηση μηνύματος.

3.7 Παραλλαγές του σχήματος RSA

Το 1996 ο M. Bellare και ο P.Rogaway παρουσίασαν κάποιες παραλλαγές του σχήματος RSA που βασίζονται στη χρήση διαφορετικών συναρτήσεων συμπύκνωσης. Τα παρακάτω σχήματα βελτιώνουν την ασφάλεια και την αποδοτικότητα της υπογραφής RSA.

RSA-FDH

Το σχήμα αυτό χρησιμοποιεί συνάρτηση συμπύκνωσης που το πεδίο τιμών της είναι το Z_n^*. Μία τέτοια συνάρτηση θα μπορούσε να κατασκευαστεί από την συνάρτηση MD5. Θεωρούμε λοιπόν συνάρτηση $h:\{0,1\}^* \to Z_n^*$. Η υπογραφή τότε ενός μηνύματος m είναι η : $s = h(m)^d \pmod n$.

Για να επαληθεύσουμε την υπογραφή s ενός μηνύματος m ελέγχουμε αν $h(m) = s^e \pmod n$.

Το 2000 ο J. S. Coron απέδειξε ότι η ασφάλεια της υπογραφής RSA με χρήση της παραπάνω συνάρτησης συμπύκνωσης βελτιώνεται σημαντικά και ότι επιπλέον βελτιώνεται και η αποδοτικότητα του σχήματος αφού μπορούν να χρησιμοποιηθούν μικρότεροι ακέραιοι n και να παρέχουν το ίδιο επίπεδο ασφάλειας με την κλασσική

υπογραφή RSA. Η συνάρτηση αυτή μπορεί να χρησιμοποιηθεί για την βελτίωση και άλλων σχημάτων όπως αυτό του Rabin και των Gennaro - Halevi - Rabin.

RSA-PSS

Έστω ότι k είναι η παράμετρος ασφαλείας του σχήματος RSA. Για παράδειγμα έστω ότι k είναι το μήκος του ακεραίου n και έστω και δύο ακέραιοι k_1, k_2 με $1 \le k_1, k_2 \le k$ που ικανοποιούν την ανίσωση $k_1 + k_2 \le k - 1$. Θεωρούμε τις συναρτήσεις συμπύκνωσης: $G : \{0,1\}^{k_2} \to \{0,1\}^{k-k_2-1}$ και $H : \{0,1\}^{*} \to \{0,1\}^{k_2}$, όπου η μία επεκτείνει και η άλλη συμπιέζει τα δεδομένα.

Έστω και οι συναρτήσεις: $G_1 : \{0,1\}^{k_2} \to \{0,1\}^{k_1}$ η οποία επιστρέφει τα πρώτα k_1−ψηφία του $G(w)$ για $w \in \{0,1\}^{k_2}$ και $G_2 : \{0,1\}^{k_2} \to \{0,1\}^{k-k_1-k_2-1}$ η οποία επιστρέφει τα τελευταία $k - k_1 - k_2 - 1$ ψηφία του $G(w)$ για $w \in \{0,1\}^{k_2}$.

Η παραγωγή κλειδιού είναι ίδια με αυτήν του RSA.

Αλγόριθμος υπογραφής

Επιλέγουμε τυχαίο $r \in \{0,1\}^{k_1}$. Θέτουμε $w = H(m \| r)$, όπου m το μήνυμα που υπογράφουμε σε δυαδική μορφή και $m \| r$ η παράθεση των στοιχείων m και r. Θέτουμε $y = 0 \| w \| (G_1(w) \oplus r) \| G_2(w)$. Η υπογραφή του μηνύματος m είναι η: $s = y^d \pmod n$.

Αλγόριθμος επαλήθευσης

Υπολογίζουμε το $y = s^e \pmod n$ και το χωρίζουμε σε $b \| w \| a \| c$, όπου το b είναι το πρώτο ψηφίο, το w τα επόμενα k_2 ψηφία, το a τα επόμενα k_1 ψηφία και το c τα

τελευταία $k-k_1-k_2-1$ ψηφία του y. Υπολογίζουμε το $r=a\oplus G_1(w)$ και δεχόμαστε την υπογραφή αν και μόνον αν $b=0$, $G_2(w)=c$ και $H(m\|r)=w$.

Το πλεονέκτημα της υπογραφής RSA-PSS έναντι της RSA-FDH είναι ότι απαιτεί τη χρήση συνάρτησης συμπύκνωσης με τυπικό πεδίο τιμών και ότι προσφέρει την αποδοτικότητα και την ασφάλεια της FDH αλλά με καλύτερο όριο.

Κεφάλαιο 4

ΑΛΛΑ ΣΧΗΜΑΤΑ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ

4.1 Σχήμα ψηφιακής υπογραφής Rabin

Μετά την εμφάνιση της υπογραφής RSA, μία νέα υπογραφή παρουσιάζεται το 1979 από τον M. Rabin η οποία βασίζει και αυτή την ασφάλειά της στην δυσκολία παραγοντοποίησης μεγάλων ακεραίων.

α) Αλγόριθμος παραγωγής κλειδιού

Κάθε οντότητα δημιουργεί ένα δημόσιο και ένα αντίστοιχα ιδιωτικό κλειδί. Ο Α κάνει τα παρακάτω:

1. Ο Α παράγει δυο μεγάλους τυχαίους πρώτους αριθμούς p και q.
2. Υπολογίζει $n = p \cdot q$
3. Το δημόσιο κλειδί του Α είναι το n και το μυστικό κλειδί είναι το (p, q).

β) Αλγόριθμος υπογραφής

Ο Α υπογράφει ένα μήνυμα $m \in M$. Κάνει τα παρακάτω:

1. Η υπογραφή ενός μηνύματος m είναι μία από τις τετραγωνικές του ρίζες, δηλαδή $s = m^{\frac{1}{2}} \bmod n$.

γ) Αλγόριθμος επαλήθευσης

Ο Β μπορεί να επαληθεύσει την υπογραφή του Α και να ανακτήσει το μήνυμα m κάνοντας τα παρακάτω:

1.Για να επαληθεύσει την υπογραφή s ενός μηνύματος m, ελέγχει αν ισχύει $m = s^2 \bmod n$.

Παράδειγμα : Για να υπογράψουμε το μήνυμα $m = 23$ επιλέγουμε δύο πρώτους αριθμούς $p = 7$, $q = 11$ και υπολογίζουμε το $n = p \cdot q = 77$. Το ιδιωτικό κλειδί είναι το ζεύγος $(p, q) = (7,11)$ και το δημόσιο κλειδί ο ακέραιος $n = 77$. Υπολογίζουμε τις τετραγωνικές ρίζες του $23 \bmod 77$. Επειδή $7,4 = 3 \bmod 4$ θα έχουμε :

$x = \pm 23^{\frac{7+1}{4}} \bmod 7 \quad \pm 4 \bmod 7$ και $x = \pm 23^{\frac{11+1}{4}} \bmod 11 \quad \pm 1 \bmod 11$.

Χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο υπολογίζουμε u, v τέτοια ώστε $up + vq = 1$ και έχουμε $2 \cdot 11 - 3 \cdot 7 = 1$. Επομένως οι ζητούμενες ρίζες είναι οι 67, 10, 32, 45. Επιλέγουμε $s = 45$ (Οποιαδήποτε από τις τέσσερις ρίζες θα μπορούσε να επιλεγεί σαν υπογραφή του μηνύματος m).

Για να επαληθεύσουμε την υπογραφή s υπολογίζουμε το $s^2 \bmod n = 45^2 \bmod 77 = 23 \bmod 77 = m$ και δεχόμαστε την υπογραφή ως έγκυρη.

Η υπογραφή του Rabin δεν είναι και τόσο εύχρηστη μιας και για να υπογραφεί ένα μήνυμα απαιτείται να είναι τετραγωνικό υπόλοιπο $\bmod ulo\, n$. Το πρόβλημα αυτό αντιμετωπίζεται με κατάλληλες τροποποιήσεις του μηνύματος έτσι ώστε το νέο μήνυμα να έχει τετραγωνική ρίζα.

Ασφάλεια της υπογραφής του Rabin

Όπως είδαμε για να υπογραφεί ένα μήνυμα πρέπει να υπολογιστεί η τετραγωνική του ρίζα $\bmod ulo\, n$. Αν είναι γνωστό το ιδιωτικό κλειδί τότε ο υπολογισμός αυτός είναι σχετικά εύκολος. Αν όμως δεν γνωρίζουμε τους παράγοντες του n, τότε η προσβολή της υπογραφής του Rabin είναι ένα πρόβλημα ισοδύναμο με την παραγοντοποίηση του ακεραίου n.

Πράγματι, αν υποθέσουμε την ύπαρξη ενός αλγόριθμου που για κάθε τετραγωνικό υπόλοιπο $\bmod n$ επιστρέφει μία τετραγωνική του ρίζα, τότε επιλέγοντας τυχαία έναν ακέραιο x με $1 \le x \le n-1$ και υπολογίζοντας το (x, n) έχουμε τις εξής δύο περιπτώσεις $(x, n) = 1$ ή $(x, n) \neq 1$.

Αν $(x,n)\neq 1$, τότε $(x,n)=p$ ή $(x,n)=q$ και η παραγοντοποίηση του n έχει βρεθεί.

Αν $(x,n)=1$, τότε υπολογίζουμε έναν ακέραιο c με $1\le c\le n-1$ και τέτοιο ώστε $c=x^2 \bmod n$. Από τον αλγόριθμο όμως παίρνουμε έναν ακέραιο m με $1\le m\le n-1$, για τον οποίο ισχύει $m=c^{\frac{1}{2}} \bmod n$ δηλαδή $c=m^2 \bmod n$. Άρα έχουμε $x^2=m^2 \bmod n$.

Καθώς $(x,n)=1$ ισχύει και ότι $(x,p)=(x,q)=1$. Ξεχωρίζουμε λοιπόν τώρα τις εξής περιπτώσεις:

1. $m=x \bmod p$ και $m=x \bmod q$. Λόγω των δύο ισοτιμιών θα ισχύει ότι $m=x \bmod n$ και επομένως $m=x$ και άρα $(m-x,n)=(0,n)=n$.
2. $m=-x \bmod p$ και $m=-x \bmod q$. Σ' αυτήν την περίπτωση $m=-x \bmod n$ και επομένως $m=n-x$ και έχουμε $(m-x,n)=(n-2x,n)=1$.
3. $m=x \bmod p$ και $m=-x \bmod q$. Από τις δύο ισοτιμίες προκύπτει ότι το $m-x$ διαιρείται από το p αλλά όχι και από το q. Άρα $(m-x,n)=p$.
4. $m=-x \bmod p$ και $m=x \bmod q$. Σε αντίθεση με την τρίτη περίπτωση, εδώ το $m-x$ διαιρείται από το q αλλά όχι και από το p. Άρα $(m-x,n)=q$.

Στις δύο τελευταίες περιπτώσεις παρατηρούμε ότι βρίσκουμε την παραγοντοποίηση του n. Η επιλογή του x γίνεται με τυχαίο τρόπο και επομένως καθεμία από τις παραπάνω περιπτώσεις έχει την ίδια πιθανότητα εμφάνισης. Άρα αν όντως υπήρχε ένας αλγόριθμος που για κάθε τετραγωνικό υπόλοιπο να μας έδινε μία τετραγωνική του ρίζα $\bmod ulo\, n$, η πιθανότητα παραγοντοποίησης του n θα ήταν ίση με $\frac{1}{2}$ και στην περίπτωση που ο αλγόριθμος θα μας έδινε όλες τις τετραγωνικές ρίζες του ακεραίου θα είχαμε κατευθείαν την παραγοντοποίηση του n.

4.2 Σχήμα ψηφιακής υπογραφής T.Okamoto - A.Shiraishi (ESIGN)

Το 1985 παρουσιάζεται στο NTT της Ιαπωνίας ένα νέο σχήμα από τους Okamoto και Shiraishi γνωστό ως υπογραφή ESIGN . Το νέο αυτό σχήμα είναι εμπνευσμένο από την υπογραφή των Ong, Schnorr και Shamir και βασίζει την ασφάλειά του στην δυσκολία παραγοντοποίησης ακεραίων και στη δυσκολία επίλυσης ανισοτήτων.

α) Αλγόριθμος παραγωγής κλειδιού

1. Επιλέγουμε δύο τυχαίους πρώτους αριθμούς p, q περίπου ίδιου μήκους έτσι ώστε $p \geq q$ και υπολογίζουμε τον ακέραιο $n = p^2 q$.
2. Επιλέγουμε έναν θετικό ακέραιο $k \geq 4$ και μία συνάρτηση συμπύκνωσης μοναδικής κατεύθυνσης $h : \{0,1\}^* \to Z_n$.
3. Το δημόσιο κλειδί είναι το (n, k) και το ιδιωτικό κλειδί είναι το (p, q) .

β) Αλγόριθμος υπογραφής

1. Για να υπογράψουμε ένα μήνυμα m υπολογίζουμε πρώτα το $u = h(m)$ και επιλέγουμε έναν ακέραιο x με $0 \leq x \leq pq$. Υπολογίζουμε $v = u - x^k \pmod n$ με $v \in \{0,1,...,n-1\}$.
2. Υπολογίζουμε $w = \left\lceil \frac{v}{pq} \right\rceil$.
3. Υπολογίζουμε $y = w \cdot (kx^{k-1})^{-1} \pmod p$ με $y \in \{0,1,...,p-1\}$.
4. Η υπογραφή του μηνύματος m είναι η $s = x + ypq \pmod n$.

γ) Αλγόριθμος επαλήθευσης

1. Για να επαληθεύσουμε την υπογραφή s ενός μηνύματος m , υπολογίζουμε πρώτα $z = s^k \pmod n$ με $z \in \{0,1,...,n-1\}$ και έπειτα $u = h(m)$.
2. Δεχόμαστε την υπογραφή αν και μόνον αν $u \leq z \leq u + 2^{2/3 \log n}$.

Απόδειξη αλγόριθμου επαλήθευσης :

Έχουμε $z = s^k = (x + ypq)^k = \sum_{i=0}^{k} \binom{k}{i} x^{k-i} (ypq)^i \equiv x^k + kypqx^{k-1} (\mathrm{mod}\, n)$. Όμως $kx^{k-1} y = w (\mathrm{mod}\, p)$ και έτσι $kx^{k-1} y = w + lp$ για κάποιο $l \in Z$. Άρα $s^k = x^k + pq(w + lp) = x^k + pqw \equiv x^k + pq\left\lfloor \frac{v}{pq} \right\rfloor$. Καθώς $v = pqv_1 + v_2$ έχουμε $z = s^k = x^k + pq(v_1 + e) = x^k + v + pqe \equiv h(m) \; pqe (\mathrm{mod}\, n)$, όπου $e = 0 \; \acute{\eta} \; 1$. Καθώς $pqe \le pq$ προκύπτει ότι $h(m) \le z \le h(m) + pq \le h(m) + 2^{2/3 \log n}$.

Το παραπάνω σχήμα μπορεί να γίνει ταχύτερο αν κάνουμε κάποιους υπολογισμούς πριν τη φάση της υπογραφής. Έτσι μπορούμε να υπολογίσουμε τα $x^k (\mathrm{mod}\, n)$, $(kx^{k-1})^{-1} (\mathrm{mod}\, p)$ που είναι ανεξάρτητα του μηνύματος m και έπειτα το w και το s που εξαρτώνται από το μήνυμα m.

Παράδειγμα : Επιλέγουμε δύο τυχαίους πρώτους αριθμούς $p = 11$, $q = 13$ και υπολογίζουμε τον ακέραιο $n = p^2 \cdot q = 1573$. Επιλέγουμε ένα θετικό ακέραιο $k = 8$. Έστω και μία δημόσια γνωστή συνάρτηση συμπύκνωσης $h : \{0,1\}^* \to Z_n$. Το δημόσιο κλειδί είναι το ζεύγος $(n, k) = (1573, 8)$ και το ιδιωτικό κλειδί η παραγοντοποίηση του n, δηλαδή το ζεύγος $(p, q) = (11, 13)$. Πριν υπογράψουμε ένα μήνυμα $m \in \{0,1\}^*$ υπολογίζουμε το $u = h(m)$. Έστω ότι η τιμή της συνάρτησης συμπύκνωσης του m είναι 1231.

Για να υπογράψουμε λοιπόν το $u = 1231$ επιλέγουμε ακέραιο $x = 5$ με $0 \le x \le 143$ και υπολογίζουμε το $w = \left\lfloor \frac{(u - x^k)(\mathrm{mod}\, n)}{pq} \right\rfloor \equiv \left\lfloor \frac{(1231 - 5^8)(\mathrm{mod} 1573)}{143} \right\rfloor \equiv 5$ και το $y = w\left(kx^{k-1}\right)^{-1} \equiv 5\left(8 \cdot 5^7\right)^{-1} = 8 \,\mathrm{mod}\, 11$.

Η υπογραφή s του μηνύματος m τελικά είναι η $s = x + ypq \equiv 5 + 8 \cdot 11 \cdot 13 = 1149 \,\mathrm{mod}\, 1573$.

Για να επαληθεύσουμε την υπογραφή s του μηνύματος m υπολογίζουμε το $h(m) = 1231$ και το $z = s^k \equiv 1149^8 \equiv 1236 \,\mathrm{mod}\, 1573$ και ελέγχουμε αν ισχύει

$u \le z \le u + 2^{2/3\log n}$. Πράγματι $1231 \prec 1236 \prec 1239$ ($\lceil 2/3\log 1573 \rceil = 3$) και επομένως η υπογραφή είναι έγκυρη.

Ασφάλεια του σχήματος ESIGN

Όπως αναφέραμε ήδη, η ασφάλεια του σχήματος βασίζεται στη δυσκολία παραγοντοποίησης ακεραίων και επίλυσης ανισοτήτων. Αρχικά για το σχήμα αυτό προτάθηκε το k το οποίο ανήκει στο δημόσιο κλειδί να είναι ίσο με δύο. Αυτή η εκδοχή του σχήματος όμως προσβλήθηκε από τους Brickell και DeLaurentis ένα χρόνο μετά και γι'αυτό τέθηκε το $k = 3$ το οποίο επίσης προσβλήθηκε όπως και άλλες παραλλαγές του σχήματος. Οι Okamoto, Shiraishi λοιπόν προτείνουν για την ασφάλεια του σχήματος το k να είναι ίσο με μία από τις τιμές: 8, 16, 32, 64, 128, 256, 512, 1024. Επίσης τα p, q πρέπει να έχουν μήκος τουλάχιστον 192 ψηφία, γεγονός που κάνει το n να είναι τουλάχιστον 576 ψηφία. Με αυτές τις παραμέτρους η υπογραφή ESIGN γίνεται τόσο ασφαλής όσο και η υπογραφή RSA και η ταχύτητά της είναι καλύτερη από αυτήν του RSA. Οι Fujioka, Okamoto και Miyaguchi το 1991 περιέγραψαν μία υλοποίηση της υπογραφής με $e = 32$ η οποία είναι είκοσι φορές πιο γρήγορη από την υπογραφή RSA και το μήκος του κλειδιού και της υπογραφής είναι συγκρίσιμα με αυτά του RSA.

4.3 Σχήμα ψηφιακής υπογραφής U.Feige - A.Fiat - A.Shamir (FFS)

Το 1987 οι Fiat και Shamir παρουσίασαν μία ψηφιακή υπογραφή την FS. Ένα χρόνο αργότερα οι Feige, Fiat και Shamir πρότειναν ένα σχήμα ελάχιστα βελτιωμένο. Το σχήμα αυτό βασίζει την ασφάλειά του στην δυσκολία υπολογισμού τετραγωνικών ριζών $\bmod n$, ένα πρόβλημα που σχετίζεται άμεσα με την παραγοντοποίηση του n.

α) Αλγόριθμος παραγωγής κλειδιού

1. Έστω $n = pq$, όπου p, q πρώτοι. Επιλέγουμε ένα θετικό ακέραιο k και τυχαίους διακεκριμένους ακέραιους $s_1, s_2, ..., s_k \in \{0,1,...,n-1\}$.

2. Υπολογίζουμε $u_j = s_j^{-2} (\mathrm{mod}\, n)$ με $u_j \in \{0,1,...,n-1\}$ και $1 \le j \le k$.

3. Το δημόσιο κλειδί είναι η k−άδα $(u_1, u_2, ..., u_k)$ και ο ακέραιος n και το ιδιωτικό κλειδί είναι η k−άδα $(s_1, s_2, ..., s_k)$.

β) Αλγόριθμος υπογραφής

Έστω m το μήνυμα που θέλουμε να υπογράψουμε.

1. Επιλέγουμε ένα τυχαίο ακέραιο r με $1 \le r \le n-1$ και υπολογίζουμε $u = r^2 \bmod n$ με $u \in \{0,1,...,n-1\}$.

2. Υπολογίζουμε $e = (e_1, e_2, ..., e_k) = h(m \| u)$ όπου $m \| u$ στο δυαδικό σύστημα, $e_i \in \{0,1\}$ και $h : \{0,1\}^* \to \{0,1\}^k$ μία συνάρτηση συμπύκνωσης μοναδικής κατεύθυνσης.

3. Υπολογίζουμε $s = r \prod_{j=1}^{k} s_j^{e_j} (\mathrm{mod}\, n)$ με $s \in \{0,1,...,n-1\}$.

4. Η υπογραφή του μηνύματος m είναι η (e, s).

γ) Αλγόριθμος επαλήθευσης

1. Υπολογίζουμε $w = s^2 \prod_{j=1}^{k} u_j^{e_j} (\mathrm{mod}\, n)$ με $w \in \{0,1,...,n-1\}$ και $e' = h(m \| w)$.

2. Δεχόμαστε την υπογραφή, αν και μόνον αν $e = e'$.

Απόδειξη αλγορίθμου επαλήθευσης :

Θέλουμε $e = e' \Leftrightarrow h(m \| u) \quad h(m \| w) \Leftrightarrow u = w$.

Πράγματι $w = s^2 \prod_{j=1}^{k} u_j^{e_j} \quad r^2 \prod_{j}^{k} s_j^{2e_j} \quad r^2 \prod_{j}^{k} (s_j^2 u_j)^{e_j} \quad r^2 \quad u \bmod n$.

Παράδειγμα : Επιλέγουμε δύο πρώτους αριθμούς $p = 11$, $q = 17$ και υπολογίζουμε το $n = p \cdot q = 187$. Επιλέγουμε και ένα θετικό ακέραιο $k = 8$ καθώς και τυχαίους

διακριτούς ακέραιους $s_1 = 5, s_2 = 12, s_3 = 43$ και υπολογίζουμε τα $u_1 = s_1^{-2}$ $(5^{-1})^2$ $15 \bmod 187$, $u_2 = s_2^{-2}$ $(12^{-1})^2$ $100 \bmod 187$ και $u_3 = s_3^{-2}$ $(43^{-1})^2$ $89 \bmod 187$.
Το δημόσιο κλειδί είναι η τριάδα $(u_1 = 15, u_2 = 100, u_3 = 89)$ και ο ακέραιος $n = 187$ και το ιδιωτικό κλειδί είναι η τριάδα $(s_1 = 5, s_2 = 12, s_3 = 43)$.
Για να υπογράψουμε ένα μήνυμα m, επιλέγουμε έναν ακέραιο $r = 7$ με $1 \le r \le n-1$ και υπολογίζουμε το $u = r^2 = 7^2 = 49 \bmod 187$. Κατόπιν υπολογίζουμε το $e = h(m \| u)$ όπου $h : \{0,1\}^* \to \{0,1\}^3$ μία δημόσια γνωστή συνάρτηση συμπύκνωσης. Έστω λοιπόν ότι εδώ ισχύει $h(m \| u) = 101$, δηλαδή $e_1 = 1, e_2 = 0, e_3 = 1$. Υπολογίζουμε το $s = r \prod_{j=1}^{k} s_j^{e_j} = 7 \prod_{j=1}^{3} s_j^{e_j} = 9 \bmod 187$. Η υπογραφή του μηνύματος m είναι η $(e, s) = (101, 9)$.
Για να επαληθεύσουμε την υπογραφή του μηνύματος m υπολογίζουμε το $w = s^2 \prod_{j=1}^{k} u_j^{e_j} = 9^2 \prod_{j=1}^{3} u_j^{e_j} = 49 \bmod 187$. Υπολογίζουμε το $e' = h(m \| w)$ 101 e και διαπιστώνουμε ότι η υπογραφή του μηνύματος m είναι έγκυρη.

Αποδοτικότητα και ασφάλεια του σχήματος FFS

Όσον αφορά την αποδοτικότητα, κάνοντας χρήση αυτού του σχήματος χρειαζόμαστε περισσότερο αποθηκευτικό χώρο έναντι του RSA αλλά η διαδικασία υπογραφής είναι πιο γρήγορη σε αντίθεση με τη διαδικασία επαλήθευσης. Έτσι αν αυτό που μας ενδιαφέρει είναι να υπογράψουμε γρήγορα και ο αποθηκευτικός χώρος δεν είναι περιορισμένος τότε είναι προτιμότερο να χρησιμοποιήσουμε την υπογραφή των Feige, Fiat και Shamir έναντι της RSA. Όσον αφορά την ασφάλεια του σχήματος, αν ληφθούν τα απαραίτητα μέτρα ώστε να είναι αδύνατη η παραγοντοποίηση του n, η h να είναι τυχαία συνάρτηση συμπύκνωσης και τα s_i να είναι διακεκριμμένα, το σχήμα αποδεικνύεται ασφαλές έναντι μίας επίθεσης προσαρμόσιμα επιλεγμένου μηνύματος.

4.4 Σχήμα ψηφιακής υπογραφής DSA

Το σχήμα υπογραφών DSA (όπως και τα σχήματα ElGamal, Schnorr και ελλειπτικών καμπυλών, που θα δούμε παρακάτω) στηρίζεται σε κυκλικές ομάδες Z_p^* όπου p είναι ένας μεγάλος πρώτος αριθμός αλλά οι μηχανισμοί τους μπορούν να γενικευθούν και σε οποιαδήποτε πεπερασμένη κυκλική ομάδα (εκτός από τις ελλειπτικές καμπύλες). Ανήκει στην κατηγορία των πιθανοτικών υπογραφών με συνημμένο το μήνυμα αλλά μπορούν να μετασχηματισθούν σε υπογραφές με ανάκτηση του μηνύματος. Μία βασική συνθήκη για την ασφάλεια όλων των σχημάτων των υπογραφών είναι ότι ο υπολογισμός λογαρίθμων στο Z_p^* είναι υπολογιστικά ανέφικτος. Αυτή η συνθήκη βέβαια δεν είναι αρκετή για την ασφάλεια αυτών των σχημάτων.

Θα χρησιμοποιήσουμε μία hash συνάρτηση $h:\{0,1\}^* \to Z_q$ για κάποιο ακέραιο q.

α) Αλγόριθμος δημιουργίας κλειδιού

1. Ο Α επιλέγει έναν πρώτο αριθμό q τέτοιο που $2^{159} \prec q \prec 2^{160}$.
2. Διαλέγει t έτσι ώστε $0 \le t \le 8$ και επιλέγει έναν πρώτο αριθμό p όπου $2^{511+64t} \prec p \prec 2^{512+64t}$ με την ιδιότητα ότι ο q διαιρεί τον $p-1$.
3. Επιλέγει ένα γεννήτορα α της μοναδικής κυκλικής ομάδας τάξης q στο Z_p^*.

i) Επιλέγει ένα στοιχείο $g \in Z_p^*$ και υπολογίζει $a = g^{\frac{p-1}{q}} \bmod p$.

ii) Αν $a = 1$ τότε εκτέλεσε το προηγούμενο βήμα.

4. Επιλέγει έναν τυχαίο ακέραιο d τέτοιο που $1 \le d \le q-1$.
5. Υπολογίζει $y = a^d \bmod p$.
6. Το δημόσιο κλειδί του Α είναι (p, q, a, y) και το μυστικό κλειδί είναι το d.

β) Αλγόριθμος δημιουργίας υπογραφής

1. Ο Α επιλέγει έναν τυχαίο μυστικό ακέραιο k με $0 \prec k \prec q$.

2. Υπολογίζει $r = (a^k \bmod p) \bmod q$.

3. Υπολογίζει $k^{-1} \bmod q$.

4. Υπολογίζει $s = k^{-1}(h(m) + dr) \bmod q$.

5. Η υπογραφή του Α για το μήνυμα m είναι το ζευγάρι (r, s).

γ) Αλγόριθμος πιστοποίησης της υπογραφής

1. Ο Β Εξασφαλίζει το δημόσιο κλειδί του Α το (p, q, a, y).

2. Πιστοποιεί ότι $0 \prec r \prec q$ και $0 \prec s \prec q$ αλλιώς απορρίπτει την υπογραφή.

3. Υπολογίζει $w = s^{-1} \bmod q$ και $h(m)$.

4. Υπολογίζει $u_1 = w \cdot h(m) \bmod q$ και $u_2 = w \cdot r \bmod q$.

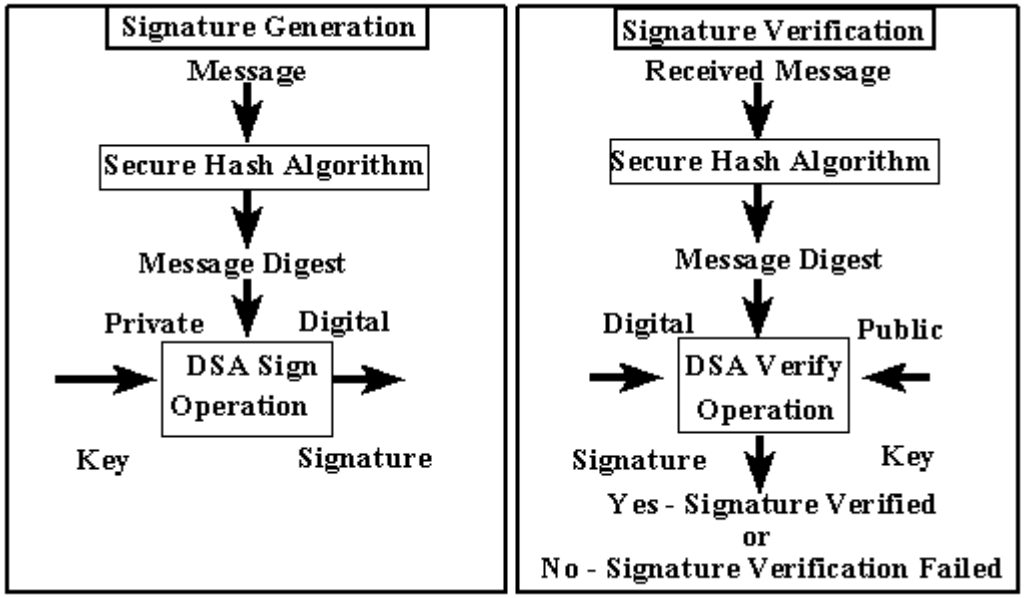
5. Υπολογίζει $v = (a^{u_1} \cdot y^{u_2} \bmod p) \bmod q$.

6. Αποδέχεται την υπογραφή αν και μόνο αν $v = r$.

Απόδειξη του αλγόριθμου πιστοποίησης :

Αν (r, s) είναι η υπογραφή του μηνύματος m τότε θα ισχύει $h(m) = -dr + ks (\bmod q)$. Πολλαπλασιάζοντας και τα δύο μέλη με w θα έχουμε $wh(m) + drw = k (\bmod q)$. Αλλά ξέρουμε ότι $u_1 + du_2 = k (\bmod q)$. Τελικά $(a^{u_1} \cdot y^{u_2} \bmod p) \bmod q = (a^k \bmod p) \bmod q$. Άρα $v = r$.

Η δημιουργία και η επαλήθευση υπογραφής φαίνονται και το παρακάτω σχήμα:



Παράδειγμα : Ο Α επιλέγει πρώτους $p = 124540019$ και $q = 17389$ τέτοιους που ο q διαιρεί τον $(p-1)$. Επιλέγει ένα τυχαίο στοιχείο $g = 110217528 \in Z_p^*$ και υπολογίζει $a = g^{17389} \bmod p = 10083255$. Επειδή $a \neq 1$, ο a είναι ένας γεννήτορας της μοναδικής κυκλικής υποομάδας τάξης q στο Z_p^*. Επιλέγει ένα τυχαίο αριθμό $d = 12496$ τέτοιο που $1 \leq d \leq q-1$ και υπολογίζει $y = a^d \bmod p = 10083255^{12496} \bmod 124540019 = 119946265$. Το δημόσιο κλειδί του Α είναι $(p, q, a, y) = (124540019, 17389, 10083255, 119946265)$ και το μυστικό κλειδί είναι το $d = 12496$.

Ο Α για να υπογράψει το μήνυμα m επιλέγει έναν τυχαίο ακέραιο $k = 9557$ και υπολογίζει $r = (a^k \bmod p) \bmod q$ $(10083255^{9557} \bmod 124540019) \bmod 17389$ $27039923 \bmod 17389 = 34$. Μετά υπολογίζει $k^{-1} \bmod q = 7631$, $h(m) = 5246$ και τελικά $s = 7631 \cdot (5246 + 12496 \cdot 34) \bmod 17389 = 13049$. Η υπογραφή για το m είναι το ζευγάρι $(r, s) = (34, 13049)$.

Ο Β υπολογίζει $w = s^{-1} \bmod q = 1799$, $u_1 = w \cdot h(m) \bmod q$ $5246 \cdot 1799 \bmod 17389 = 12716$, $u_2 = w \cdot r \bmod q$ $1799 \cdot 34 \bmod 17389 = 8999$ και τέλος υπολογίζει

$v = (a^{u_1} \cdot y^{u_2} \bmod p) \bmod q \quad (10083255^{12716} \cdot 11994626^{8999} \bmod 124540019) \bmod 17389 = 27039929 \bmod 17389 = 34$. Επειδή $v = r$ ο Β αποδέχεται την υπογραφή.

Ασφάλεια του σχήματος DSA

Η ασφάλεια του DSA στηρίζεται σε δύο διαφορετικά αλλά συσχετιζόμενα προβλήματα των διακριτών λογαρίθμων.

Στον αλγόριθμο πιστοποίησης υπολογίζουμε $s^{-1} \bmod q$. Αν $s = 0$ τότε το s^{-1} δεν υπάρχει. Για να αποφύγουμε αυτή την περίπτωση ο Α πρέπει να ελέγξει αν $s = 0$ και αν ισχύει ότι το s είναι ένα τυχαίο στοιχείο του Z_q τότε η πιθανότητα να συμβεί αυτό ($s = 0$) είναι $\left(\frac{1}{2}\right)^{160}$ (μηδαμινή πιθανότητα να συμβεί). Επίσης πρέπει να ελέγξει αν $r = 0$. Αν ισχύει ότι $s = 0$ ή $r = 0$ τότε πρέπει να επιλέξει μία καινούργια τιμή για το k.

Δεν είναι απαραίτητο κάθε μέλος να επιλέξει δικούς του πρώτους p, q .Στο σχήμα DSA επιτρέπεται οι p, q, a να είναι κοινοί για όλους. Αυτό βέβαια είναι ένα σημαντικό πλεονέκτημα για τον αντίπαλο.

4.5 Σχήμα ψηφιακής υπογραφής ElGamal

Το σχήμα υπογραφής ElGamal είναι ένας τυχαιοποιημένος, μη ντετερμινιστικός μηχανισμός υπογραφής, δηλαδή για κάθε μήνυμα απλού κειμένου υπάρχουν πολλές έγκυρες υπογραφές και ο αλγόριθμος επαλήθευσης οφείλει να αποδέχεται κάθε μια από αυτές ως αυθεντική. Το σχήμα υπογραφής ElGamal παίζει ουσιαστικό ρόλο στο χώρο των ψηφιακών υπογραφών.

Δημιουργεί υπογραφές με συνημμένο το μήνυμα, με μηνύματα σε δυαδική μορφή αυθαίρετου μήκους και χρησιμοποιεί μία hash συνάρτηση $h : \{0,1\}^* \to Z_q$, όπου p είναι ένας μεγάλος πρώτος αριθμός.

α) Αλγόριθμος δημιουργίας κλειδιού

1. Ο Α επιλέγει ένα μεγάλο πρώτο αριθμό p και ένα γεννήτορα a της πολλαπλασιαστικής ομάδας Z_p^*.

2. Επιλέγει ένα τυχαίο ακέραιο d με $1 \le d \le p-2$.

3. Υπολογίζει $y = a^d \bmod p$.

4. Το δημόσιο κλειδί του Α είναι (p, a, y) και το μυστικό κλειδί είναι το d.

β) Αλγόριθμος δημιουργίας υπογραφής

1. Ο Α επιλέγει ένα τυχαίο μυστικό ακέραιο k με $1 \le k \le p-2$ με $\gcd(k, p-1) = 1$.

2. Υπολογίζει $r = a^k \pmod p$.

3. Υπολογίζει $k^{-1} \pmod p$.

4. Υπολογίζει $s = k^{-1}(h(m) - d \cdot r) \bmod (p-1)$.

5. Η υπογραφή του Α για το μήνυμα m είναι το ζευγάρι (r, s).

γ) Αλγόριθμος πιστοποίησης της υπογραφής

1. Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το (p, a, y).

2. Πιστοποιεί ότι $1 \le r \le p-1$, αλλιώς απορρίπτει την υπογραφή.

3. Υπολογίζει $v_1 = y^r \cdot r^s \bmod p$.

4. Υπολογίζει $h(m)$ και $v_2 = a^{h(m)} \bmod p$.

5. Αποδέχεται την υπογραφή αν και μόνο αν $v_1 = v_2$.

Απόδειξη του αλγόριθμου πιστοποίησης :

Αν η υπογραφή δημιουργήθηκε από τον Α τότε $s = k^{-1}(h(m) - d \cdot r) \bmod (p-1)$. Πολλαπλασιάζοντας και τα δύο μέλη με k θα έχουμε $k \cdot s \quad (h(m) \equiv d \cdot r) \bmod (p-1)$ $\Leftrightarrow h(m) \quad (d \equiv r + k \cdot s) \bmod (p-1)$. Τελικά θα έχουμε $a^{h(m)} = a^{dr+ks} = (a^d)^r r^s \pmod p$. Άρα $v_1 = v_2$.

Παράδειγμα : Ο Α επιλέγει πρώτο αριθμό $p = 2357$ και ένα γεννήτορα $a = 2$ της Z_{2357}^* . Ο Α επιλέγει ένα μυστικό κλειδί $d = 1751$ και υπολογίζει $y = a^d \bmod p = 2^{1751} \bmod 2357 = 1185$. Το δημόσιο κλειδί του Α είναι $(p, a, y) = (2357, 2, 1185)$. Για απλότητα θεωρούμε ότι τα μηνύματα είναι ακέραιοι από το Z_p^* και $h(m) = m$. Για να υπογράψει ο Α ένα μήνυμα $m = 1463$, επιλέγει ένα τυχαίο ακέραιο $k = 1529$, υπολογίζει $r = a^k (\bmod p)$ $2^{1529} \bmod 2357$ 1490 και $k^{-1} (\bmod p) = 245$. Τελικά ο Α υπολογίζει $s = k^{-1}(h(m) - d \cdot r) \bmod (p-1)$ $245(1463 - 1751 \cdot 1490) \bmod 2356 = 1777$. Η υπογραφή του Α για το μήνυμα $m = 1463$ είναι το ζευγάρι $(r, s) = (1490, 1777)$.

Ο Β υπολογίζει $v_1 = y^r \cdot r^s \bmod p$ $1185^{1490} \cdot 1490^{1777} \bmod 2357 = 1072$, $h(m) = 1463$ και $v_2 = a^{h(m)} \bmod p$ $2^{1463} \bmod 2357$ 1072. Ο Β αποδέχεται την υπογραφή επειδή $v_1 = v_2$.

Ασφάλεια του σχήματος ElGamal

Ένας αντίπαλος μπορεί να προσπαθήσει να πλαστογραφήσει την υπογραφή του Α για το μήνυμα m επιλέγοντας ένα τυχαίο ακέραιο k υπολογίζοντας $r = a^k (\bmod p)$. Ο αντίπαλος πρέπει να καθορίσει το $s = k^{-1}(h(m) - d \cdot r) \bmod (p-1)$. Αν το πρόβλημα του διακριτού λογαρίθμου είναι υπολογιστικά ανέφικτο τότε το μόνο που μπορεί να κάνει είναι να το επιλέξει τυχαία, οπότε η πιθανότητα επιτυχίας είναι μόνο $\frac{1}{p}$ που είναι μηδαμινή για μεγάλο p.

Για κάθε μήνυμα που υπογράφεται πρέπει να επιλέγεται διαφορετικό k , αλλιώς ο αντίπαλος θα μπορέσει να βρει το μυστικό κλειδί με μεγάλη πιθανότητα. Έστω $s_1 = k^{-1}(h(m_1) - d \cdot r) \bmod (p-1)$ και $s_2 = k^{-1}(h(m_2) - d \cdot r) \bmod (p-1)$. Τότε $(s_1 - s_2) \cdot k$ $(h(m_1) - h(m_2)) (\bmod (p-1))$. Αν $(s_1 - s_2) \neq 0 (\bmod (p-1))$ τότε $k = (s_1 - s_2)^{-1} (h(m_1) - h(m_2)) (\bmod (p-1))$. Οπότε αν το είναι γνωστό το d μπορεί εύκολα να βρεθεί.

Αν δεν χρησιμοποιήσουμε hash συνάρτηση τότε $s = k^{-1}(m - d \cdot r) \bmod (p-1)$. Η επίθεση από τον αντίπαλο με υπαρξιακή πλαστογράφηση μπορεί εύκολα να πραγματοποιηθεί. Ο αντίπαλος επιλέγει ένα ζευγάρι ακεραίων (u, v) με

$\gcd(v, p-1)=1$. Υπολογίζει $r = a^u \cdot y^v \bmod p = a^{u+dv} \bmod p$ και $s = -r \cdot v^{-1} \bmod(p-1)$. Το ζευγάρι (r,s) είναι μία νόμιμη υπογραφή για το μήνυμα $m = s \cdot u \bmod(p-1)$ επειδή $(a^m a^{-dr})^{s^{-1}} = a^u y^v = r$.

Στον αλγόριθμο πιστοποίησης ο Β θα πρέπει να ελέγξει αν $0 \le r \le p$. Αν δε γίνει αυτός ο έλεγχος, τότε ο αντίπαλος μπορεί να υπογράψει μηνύματα της επιλογής του με νόμιμη υπογραφή. Έστω ότι (r,s) είναι η υπογραφή για το μήνυμα m που δημιούργησε ο Α. Ο αντίπαλος επιλέγει ένα μήνυμα m' της επιλογής του και υπολογίζει $h(m')$ και $u = h(m') \cdot [h(m)]^{-1} \bmod(p-1)$ (υποθέτοντας ότι $[h(m)]^{-1} \bmod(p-1)$ υπάρχει). Μετά υπολογίζει $s' = s \cdot u(\bmod(p-1))$ και r' τέτοιο που $r' = r \cdot u(\bmod(p-1))$ και $r' = r(\bmod p)$ (υπάρχει πάντα τέτοιο r' σύμφωνα με το Κινέζικο θεώρημα). Το ζευγάρι (r', s') είναι μια υπογραφή για το μήνυμα m' που θα γίνει αποδεκτή από τον Β αν δεν ελέγξει ότι $0 \prec r' \prec p$.

Το σχήμα υπογραφής που είδαμε βασίζεται στην πολλαπλασιαστική ομάδα Z_p^*. Μπορεί να γενικευθεί σε οποιαδήποτε πεπερασμένη αβελιανή ομάδα G. Θα δούμε το **γενικευμένο** σχήμα υπογραφής ElGamal όπου απαιτείται μία hash συνάρτηση $h: \{0,1\}^* \to Z_n$ όπου n είναι ο αριθμός των στοιχείων της G. Θεωρούμε ότι κάθε στοιχείο $r \in G$ μπορεί να αναπαρασταθεί σε δυαδική μορφή, οπότε η $h(r)$ ορίζεται.

α) Αλγόριθμος δημιουργίας κλειδιού

1. Ο Α επιλέγει μία κατάλληλη κυκλική ομάδα G με n στοιχεία και ένα γεννήτορα a.
2. Επιλέγει ένα τυχαίο μυστικό ακέραιο d με $1 \le d \le n-1$. Υπολογίζει το στοιχείο της ομάδας $y = a^d$.
3. Το δημόσιο κλειδί του Α είναι (a, y) με τον ορισμό της πράξης της ομάδας και το μυστικό κλειδί είναι το d.

β) Αλγόριθμος δημιουργίας υπογραφής

1. Ο Α επιλέγει ένα τυχαίο μυστικό ακέραιο k με $1 \le k \le n-1$ και $\gcd(k,n)=1$.

2. Υπολογίζει το στοιχείο της ομάδας $r = a^k$

3. Υπολογίζει $k^{-1} (\mathrm{mod}\, n)$.

4. Υπολογίζει $h(m)$ και $h(r)$.

5. Υπολογίζει $s = k^{-1}(h(m) - h(r)) \bmod n$.

6. Η υπογραφή του Α για το μήνυμα m είναι το ζευγάρι (r,s).

γ) Αλγόριθμος πιστοποίησης της υπογραφής

1. Ο Β Εξασφαλίζει το δημόσιο κλειδί του Α το (a,y).

2. Υπολογίζει $h(m)$ και $h(r)$.

3. Υπολογίζει $v_1 = y^{h(r)} \cdot r^s$.

4. Υπολογίζει $v_2 = a^{h(m)}$.

5. Αποδέχεται την υπογραφή αν και μόνο αν $v_1 = v_2$.

Παράδειγμα : Έστω το πεπερασμένο σώμα F_{2^5}, που κατασκευάζεται από το ανάγωγο πολυώνυμο $f(x) = x^5 + x^2 + 1$ πάνω στο F_2. Τα στοιχεία του σώματος είναι 31 δυαδικές πεντάδες με το 00000 όπως φαίνονται στον παρακάτω πίνακα .

i	a^i	i	a^i	i	a^i	i	a^i
0	00001	8	01101	16	11011	24	11110
1	00010	9	11010	17	10011	25	11001
2	00100	10	10001	18	00011	26	10111
3	01000	11	00111	19	00110	27	01011
4	10000	12	01110	20	01100	28	10110
5	00101	13	11100	21	11000	29	01001
6	01010	14	11101	22	10101	30	10010
7	10100	15	11111	23	01111		

Το στοιχείο $a = (00010)$ είναι ένας γεννήτορας για την $G = F_{2^5}^*$, η πολλαπλασιαστική κυκλική ομάδα του σώματος. Η τάξη της ομάδας είναι $n = 31$. Έστω ότι $h: \{0,1\}^* \to Z_{31}$ είναι η hash συνάρτηση. Ο Α επιλέγει ένα μυστικό κλειδί $d = 19$ και υπολογίζει $y = a^d$ $(00010)^{19}$ (00110). Το δημόσιο κλειδί του Α είναι $(a, y) = (00010, 00110)$. Για να υπογράψει το μήνυμα $m = 10110101$ ο Α επιλέγει ένα τυχαίο ακέραιο $k = 24$ και υπολογίζει $r = a^{24} = (11110)$ και $k^{-1} \bmod 31 = 22$. Ο Α υπολογίζει $h(m) = 16$, $h(r) = 7$ και $s = k^{-1}(h(m) - h(r)) \bmod n = 22(16 - 19 \cdot 7) \bmod 31 = 30$. Η υπογραφή του Α για το μήνυμα m είναι $(r, s) = (11110, 30)$.

Ο Β υπολογίζει $h(m) = 16$, $h(r) = 7$, $v_1 = y^{h(r)} \cdot r^s$ $(00110)^7 \cdot (11110)^{30} = (11011)$ και $v_2 = a^{h(m)} = a^{16} = (11011)$. Ο Β αποδέχεται την υπογραφή επειδή $v_1 = v_2$.

Μία από τις πιο σημαντικές εφαρμογές του γενικευμένου σχήματος υπογραφής ElGamal είναι η περίπτωση όπου η πεπερασμένη αβελιανή ομάδα G είναι κατασκευασμένη από το σύνολο των στοιχείων μιας ελλειπτικής καμπύλης πάνω σε ένα πεπερασμένο σώμα F_q .

4.6 Σχήμα ψηφιακής υπογραφής Schnorr

Ένα άλλο σχήμα υπογραφής, γνωστή παραλλαγή του σχήματος ElGamal, είναι το σχήμα υπογραφής Schnorr, που είναι επίσης τυχαιοποιημένο με παράρτημα.. Όπως και το DSA στηρίζεται σε μία υποομάδα τάξης q στο Z_p^*, όπου p είναι ένας μεγάλος πρώτος αριθμός. Το σχήμα αυτό χρησιμοποιεί μία hash συνάρτηση $h: \{0,1\}^* \to Z_q$.

α) Αλγόριθμος δημιουργίας κλειδιού

Είναι ο ίδιος με αυτόν του σχήματος DSA χωρίς τους περιορισμούς για τα μεγέθη p, q.

β) Αλγόριθμος δημιουργίας υπογραφής

1. Ο Α επιλέγει ένα τυχαίο μυστικό ακέραιο k τέτοιο που $1 \le k \le q-1$..
2. Υπολογίζει $r = a^k \bmod p$, $e = h(m \| r)$ και $s = de + k \bmod q$.
3. Η υπογραφή του Α για το μήνυμα m είναι το ζευγάρι (s, e).

γ) Αλγόριθμος πιστοποίησης της υπογραφής

1. Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το (p, q, a, y).
2. Υπολογίζει $v = a^s y^{-e} \bmod p$ και $e' = h(m \| v)$.
3. Αποδέχεται την υπογραφή αν και μόνο αν $e = e'$.

Απόδειξη του αλγόριθμου πιστοποίησης:

Αν η υπογραφή δημιουργήθηκε από τον Α τότε $v = a^s y^{-e} \quad a^s a^{de} = a^k \quad r (\bmod p)$. Έτσι $h(m \| v) = h(m \| r)$ και $e = e'$.

Παράδειγμα : Ο Α επιλέγει πρώτους αριθμούς $p = 129841$ και $q = 541$ τέτοιους που ο q διαιρεί τον $(p-1)$. Επιλέγει ένα τυχαίο στοιχείο $g = 26346 \in Z_p^*$ και υπολογίζει $a = 26346^{240} \bmod 129841 = 26$. Επειδή $a \neq 1$, ο a είναι ένας γεννήτορας της μοναδικής κυκλικής υποομάδας τάξης q στο Z_p^*. Επιλέγει ένα μυστικό ακέραιο αριθμό $d = 423$ και υπολογίζει $y = a^d \bmod p \quad 26^{423} \bmod 129841 \quad 115917$. Το δημόσιο κλειδί του Α είναι $(p, q, a, y) = (129841, 541, 26, 115917)$.
Ο Α για να υπογράψει το μήνυμα $m = 11101101$ επιλέγει έναν τυχαίο ακέραιο αριθμό $k = 327$ τέτοιο που $1 \le k \le 540$ και υπολογίζει $r = a^k \bmod p \quad 26^{327} \bmod 129841$

49375 και $e = h(m \| r) = 155$. Τελικά ο Α υπολογίζει $s = 423 \cdot 155 + 327 \bmod 541 = 431$. Η υπογραφή για το m είναι το ζευγάρι $(s, e) = (431,155)$.

Ο Β υπολογίζει $v = a^s y^{-e} \bmod p$ $26^{431} \cdot 11^{917^{-155}} \bmod 129841 = 49375$ και $e' = h(m \| v) = 155$. Ο Β αποδέχεται την υπογραφή επειδή $e = e'$.

Οι υπογραφές Schnorr χρησιμοποιούνται ευρέως σε μηχανισμούς πρόκλησης – ανταπόκρισης στις «έξυπνες» κάρτες γιατί το απαντητικό μέρος του μηχανισμού απαιτεί την τιμή s που είναι εύκολο να υπολογιστεί (μια πρόσθεση και ένας πολλαπλασιασμός modulo κάποιου πρώτου αριθμού σε οποιαδήποτε κυκλική ομάδα κι αν γίνονται οι υπολογισμοί).

4.7 Σχήμα ψηφιακής υπογραφής ελλειπτικών καμπυλών

Τα κρυπτοσυστήματα των ελλειπτικών καμπυλών παρουσιάστηκαν το 1985 από τους V. Miller και N. Koblitz ανεξάρτητα. Τα δύο σημαντικά πλεονεκτήματα που είδαν ήταν:

1. Η πολύ μεγάλη ευκαμψία στην επιλογή της ομάδας (δηλαδή για κάθε δύναμη του πρώτου αριθμού q υπάρχει μόνο μία πολλαπλασιαστική ομάδα F_q^*, αλλά υπάρχουν πολλές ελλειπτικές καμπύλες E/F_q).
2. Η έλλειψη κατάλληλων αλγορίθμων (subexponential time) για να σπάσουν ένα τέτοιο κρυπτοσύστημα αν η E είναι κατάλληλα επιλεγμένη.

Θα περιγράψουμε το σχήμα υπογραφής των ελλειπτικών καμπυλών (ECDSA) που είναι ανάλογο του σχήματος υπογραφής DSA. Για απλότητα θα χρησιμοποιήσουμε ελλειπτικές καμπύλες στο σώμα F_p όπου p είναι πρώτος αριθμός, αν και η κατασκευή μπορεί να προσαρμοσθεί και σε άλλα πεπερασμένα σώματα. Έστω E είναι μία ελλειπτική καμπύλη στο F_p και έστω P είναι ένα σημείο τάξης q στο $E(F_p)$.

α) Αλγόριθμος δημιουργίας κλειδιού

1. Ο Α επιλέγει ένα τυχαίο ακέραιο x με $1 \le x \le q-1$.

2. Υπολογίζει $Q = x \cdot P$.

3. Το δημόσιο κλειδί του Α είναι το Q και το μυστικό το x.

β) Αλγόριθμος δημιουργίας υπογραφής

1. Ο Α επιλέγει ένα τυχαίο ακέραιο k με $1 \le k \le q-1$.

2. Υπολογίζει $k \cdot P = (x_1, y_1)$ και $r = x_1 \bmod q$ (Ο x_1 είναι ένας ακέραιος μεταξύ των 0 και $p-1$, ο r είναι το ελάχιστο μη αρνητικό υπόλοιπο). Αν $r = 0$ τότε επέστρεψε στο βήμα 1 αφού αν $r = 0$ η εξίσωση της υπογραφής $s = k^{-1}(h(m) + x \cdot r) \bmod q$ δε διασφαλίζει τη μυστικότητα του x και άρα το 0 δεν είναι αποδεκτή τιμή για το r.

3. Υπολογίζει $k^{-1} \bmod q$.

4. Υπολογίζει $s = k^{-1}(h(m) + x \cdot r) \bmod q$ (Η $h(m)$ είναι η hash τιμή για το μήνυμα m). Αν $s = 0$ τότε επέστρεψε στο βήμα 1. (Αν $s = 0$ τότε η τιμή $s^{-1} \bmod q$ που απαιτείται στον αλγόριθμο πιστοποίησης δεν υπάρχει).

5. Η υπογραφή του Α για το μήνυμα m είναι το ζευγάρι (r, s).

γ) Αλγόριθμος πιστοποίησης της υπογραφής

1. Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το Q.

2. Ελέγχει ότι οι r, s είναι ακέραιοι στο διάστημα $[1, q-1]$.

3. Υπολογίζει $w = s^{-1} \bmod q$ και $h(m)$.

4. Υπολογίζει $u_1 = w \cdot h(m) \bmod q$ και $u_2 = w \cdot r \bmod q$.

5. Υπολογίζει $u_1 \cdot P + u_2 \cdot Q = (x_0, y_0)$ και $v = x_0 \bmod q$.

6. Αποδέχεται την υπογραφή αν και μόνο αν $v = r$.

Απόδειξη του αλγόριθμου πιστοποίησης :

Έχουμε $u_1 \cdot P + u_2 \cdot Q = (u_1 + u_2 \cdot x) \cdot P = s^{-1}(h(m) + x \cdot r) \cdot P = k \cdot P$.

Παρατήρηση: κανένας δε γνωρίζει κάποια μέθοδο για να βρει τους (r, s) χωρίς να γνωρίζει τους k και x.

Η βασική διαφορά αυτού του σχήματος από το DSA είναι το διάστημα στο οποίο επιλέγεται ο τυχαίος αριθμός r.

Κεφάλαιο 5

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΜΙΑΣ ΧΡΗΣΗΣ

Τα σχήματα ψηφιακών υπογραφών μιας χρήσης είναι μηχανισμοί ψηφιακών υπογραφών οι οποίοι μπορούν να χρησιμοποιηθούν για την υπογραφή ενός, το πολύ, μηνύματος γιατί διαφορετικά οι υπογραφές μπορούν να πλαστογραφηθούν. Απαιτείται ένα νέο δημόσιο κλειδί για κάθε μήνυμα που υπογράφεται. Οι δημόσιες πληροφορίες που είναι αναγκαίες για την επαλήθευση υπογραφών μιας χρήσης αναφέρονται συχνά ως παράμετροι επικύρωσης. Όταν συνδυάζονται υπογραφές μιας χρήσης με τεχνικές πιστοποίησης αυθεντικότητας των παραμέτρων επικύρωσης, τότε καθίστανται δυνατές πολλαπλές υπογραφές.

Τα περισσότερα σχήματα ψηφιακών υπογραφών μιας χρήσης έχουν το πλεονέκτημα ότι η παραγωγή και η επαλήθευση υπογραφών είναι πολύ αποδοτικές. Τα σχήματα ψηφιακών υπογραφών μιας χρήσης είναι χρήσιμα σε εφαρμογές όπως είναι οι έξυπνες κάρτες, όπου απαιτείται χαμηλή υπολογιστική πολυπλοκότητα.

5.1 Το σχήμα υπογραφών μιας χρήσης Rabin

Το σχήμα υπογραφών μιας χρήσης του Rabin ήταν ένα από τα πρώτα που προτάθηκαν για ψηφιακή υπογραφή οποιουδήποτε είδους. Επιτρέπει την υπογραφή ενός μεμονωμένου μηνύματος. Η επαλήθευση μιας υπογραφής απαιτεί την αλληλεπίδραση μεταξύ του υπογράφοντα και αυτού που επαληθεύει. Αντίθετα με άλλα σχήματα ψηφιακών υπογραφών, η επαλήθευση μπορεί να γίνει μόνο μία φορά. Το σχήμα υπογραφών μιας χρήσης του Rabin δεν είναι πρακτικό.

ΣΥΜΒΟΛΙΣΜΟΙ:

- $M_0 : 0^l$ η συμβολοσειρά μήκους l που αποτελείται από μηδενικά.
- $M_0(i) : 0^{l-e} \| b_{e-1}...b_1 b_0$, όπου $b_{e-1}...b_1 b_0$ είναι η δυαδική αναπαράσταση του i.
- K : ένα σύνολο συμβολοσειρών των l bit.

- E : ένα σύνολο μετασχηματισμών κρυπτογράφησης δεικτοδοτημένο από ένα σύνολο κλειδιών K .
- E_t : ένας μετασχηματισμός κρυπτογράφησης που ανήκει στο E με $t \in K$. Κάθε E_t απεικονίζει συμβολοσειρές των l bit σε συμβολοσειρές των l bit.
- h : μια δημόσια γνωστή μονόδρομη hash συνάρτηση με $h: \{0,1\}^* \to \{0,1\}^l$.
- n : ένας θετικός ακέραιος ο οποίος χρησιμεύει ως παράμετρος ασφάλειας.

α) Αλγόριθμος παραγωγής κλειδιών

Ο Α επιλέγει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού E, παράγει $2n$ τυχαίες συμβολοσειρές και δημιουργεί ένα σύνολο παραμέτρων επικύρωσης. Ο Α θα πρέπει να κάνει τα παρακάτω:

1. Να επιλέξει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού E (π.χ., το DES).
2. Να παραγάγει $2n$ τυχαίες μυστικές συμβολοσειρές $k_1, k_2, ..., k_{2n} \in K$, δυαδικού μήκους l η κάθε μία.
3. Να υπολογίσει τα $y_i = E_{k_i}(M_0(i)), 1 \le i \le 2n$.
4. Το δημόσιο κλειδί του Α είναι $(y_1, y_2, ..., y_{2n})$ και το ιδιωτικό κλειδί του Α είναι $(k_1, k_2, ..., k_{2n})$.

β) Αλγόριθμος παραγωγής της υπογραφής

Ο Α υπογράφει ένα δυαδικό μήνυμα m οποιουδήποτε μήκους. Η επαλήθευση υπογραφών είναι αλληλεπιδραστική με τον Α. Ο Α θα κάνει τα παρακάτω:

1. Να υπολογίσει το $h(m)$.
2. Να υπολογίσει τα $s_i = E_{k_i}(h(m)), 1 \le i \le 2n$.
3. Η υπογραφή του Α για το m είναι $(s_1, s_2, ..., s_{2n})$.

γ) Αλγόριθμος επαλήθευσης της υπογραφής

Για να επαληθεύσει την υπογραφή $(s_1, s_2, ..., s_{2n})$ του Α στο *m*, ο *B* θα πρέπει:

1. Να προμηθευτεί το αυθεντικό κλειδί $(y_1, y_2, ..., y_{2n})$ του Α.
2. Να υπολογίσει το *h*(*m*).
3. Να επιλέξει *n* διαφορετικούς τυχαίους αριθμούς $r_j, 1 \le r_j \le 2n$, για $1 \le j \le n$.
4. Να ζητήσει από τον Α τα κλειδιά k_{r_j}, $1 \le j \le n$.
5. Να επαληθεύσει την αυθεντικότητα των κλειδιών που παρέλαβε, υπολογίζοντας το $z_j = E_{k_{r_j}}(M_0(r_j))$ και ελέγχοντας ότι $z_j = y_{r_j}$ για κάθε $1 \le j \le n$.
6. Να επαληθεύσει ότι $s_{r_j} = E_{k_{r_j}}(h(m))$ για $1 \le j \le n$.

Επίλυση αντιδικιών : Για την επίλυση ενδεχόμενων αντιδικιών μεταξύ του Α που υπογράφει και του Β που επαληθεύει με τη χρήση του παραπάνω αλγορίθμου, θα πρέπει να ακολουθηθεί η εξής διαδικασία:

1. Ο Β παρέχει σε ένα τρίτο έμπιστο μέλος (TTP) το μήνυμα *m* και την υπογραφή $(s_1, s_2, ..., s_{2n})$.
2. Το TTP παραλαμβάνει τα $k_1, k_2, ..., k_{2n}$ από τον Α.
3. Το TTP επαληθεύει την αυθεντικότητα του ιδιωτικού κλειδιού υπολογίζοντας το $z_i = E_{k_i}(M_0(i))$ και ελέγχοντας αν είναι $y_i = z_i$, $1 \le i \le 2n$. Αν ο έλεγχος αυτός αποτυγχάνει, το TTP αποφαίνεται υπέρ του Β (δηλαδή η υπογραφή θεωρείται έγκυρη).
4. Το TTP υπολογίζει το $u_i = E_{k_i}(h(m))$, $1 \le i \le 2n$. Αν $u_i = s_i$ για το πολύ *n* τιμές του i με $1 \le i \le 2n$ η υπογραφή δηλώνεται ότι είναι πλαστογραφημένη και το TTP αποφαίνεται υπέρ του Α (ο οποίος αρνείται ότι έχει δημιουργήσει την υπογραφή). Αν $n+1$ ή περισσότερες τιμές του i δίνουν $u_i = s_i$, η υπογραφή θεωρείται έγκυρη και το TTP αποφαίνεται υπέρ του Β.

Πρωτόκολλο επίλυσης αντιδικιών : Το σκεπτικό για την επιδίκαση αντιδικιών στο σχήμα υπογραφών μιας χρήσης του Rabin, έχει ως εξής. Αν ο Β έχει προσπαθήσει να

πλαστογραφήσει την υπογραφή του Α σε ένα νέο μήνυμα m', ο Β είτε χρειάζεται να προσδιορίσει τουλάχιστο ένα παραπάνω κλειδί k' έτσι ώστε τουλάχιστον $n+1$ τιμές του i να δώσουν $u_i = s_i$, είτε να προσδιορίσει το m' τέτοιο ώστε $h(m) = h(m')$. Αυτό δε θα μπορεί να γίνει αν ο αλγόριθμος συμμετρικού κλειδιού και η hash συνάρτηση επιλεγούν κατάλληλα. Αν ο Α προσπαθήσει να δημιουργήσει μια υπογραφή την οποία μπορεί αργότερα να απαρνηθεί, ο Α πρέπει να εξασφαλίσει ότι $u_i = s_i$ για n ακριβώς τιμές του i και να ελπίζει ότι ο Β επιλέγει αυτές τις n τιμές. Η διαδικασία αυτή έχει πιθανότητα μόνο $\frac{1}{\binom{2n}{n}}$.

Παρατήρηση: Ο Α μπορεί να υπογράψει το πολύ ένα μήνυμα με ένα δεδομένο ιδιωτικό κλειδί στο σχήμα μιας χρήσης του Rabin γιατί αλλιώς ο Α θα αποκαλύψει (με μεγάλη πιθανότητα) $n+1$ ή περισσότερες τιμές του ιδιωτικού κλειδιού και ο Β θα είναι σε θέση να πλαστογραφήσει υπογραφές σε νέα μηνύματα. Μια υπογραφή μπορεί μόνο να επαληθευτεί μία φορά χωρίς την αποκάλυψη (με μεγάλη πιθανότητα) περισσότερων από n εκ των $2n$ ιδιωτικών τιμών.

5.2 Το σχήμα υπογραφών μιας χρήσης Merkle

Το σχήμα ψηφιακών υπογραφών μιας χρήσης του Merkle διαφέρει κατά πολύ από εκείνο του Rabin ως προς το ότι η επαλήθευση υπογραφών δεν είναι αλληλεπιδραστική με τον υπογράφοντα. Ένα TTP ή κάποιο άλλο έμπιστο μέσο απαιτείται προκειμένου να πιστοποιεί την αυθεντικότητα των παραμέτρων επικύρωσης που κατασκευάζονται από τον παρακάτω αλγόριθμο.

α) <u>Αλγόριθμος παραγωγής κλειδιών</u>

Για να υπογράψει μηνύματα των n bit, ο Α παράγει $t = n + \lfloor 1gn \rfloor + 1$ παραμέτρους επικύρωσης. Ο Α θα πρέπει να κάνει τα παρακάτω:

1. Να επιλέξει $t = n + \lfloor 1gn \rfloor + 1$ τυχαίες μυστικές συμβολοσειρές $k_1, k_2, ..., k_t$ δυαδικού

μήκους *l* η κάθε μία.

2. Να υπολογίσει $u_t = h(k_t)$, $1 \le i \le t$. Εδώ η *h* είναι μια hash συνάρτηση με $h: \{0,1\}^* \to \{0,1\}^l$.

3. Το δημόσιο κλειδί του Α είναι $(u_1, u_2, ..., u_t)$ και το ιδιωτικό κλειδί του Α είναι $(k_1, k_2, ..., k_t)$.

β) Αλγόριθμος παραγωγής υπογραφής

Ο Α υπογράφει ένα μήνυμα *m* δυαδικού μήκους *n*. Ο Β μπορεί να επαληθεύσει την υπογραφή αυτή χρησιμοποιώντας το δημόσιο κλειδί του Α. Ο Α θα πρέπει να κάνει τα παρακάτω:

1. Να υπολογίσει το *c*, τη δυαδική αναπαράσταση για τον αριθμό των 0 στο *m*.

2. Να σχηματίσει το $w = m \| c = (a_1 a_2 ... a_t)$.

3. Να προσδιορίσει τις θέσεις συντεταγμένων $i_1 \prec i_2 \prec ... \prec i_u$ στο *w* τέτοιες ώστε $a_{i_j} = 1$ με $1 \le j \le u$.

4. Έστω $s_j = k_{i_j}$ με $1 \le j \le u$.

5. Η υπογραφή του Α για το *m* είναι $(s_1, s_2, ..., s_u)$.

γ) Αλγόριθμος επαλήθευσης υπογραφής

Για να επαληθεύσει την υπογραφή $(s_1, s_2, ..., s_u)$ του Α στο *m*, Ο Β θα πρέπει:

1. Να προμηθευτεί το αυθεντικό κλειδί $(u_1, u_2, ..., u_t)$ του Α.

2. Να υπολογίσει το *c*, τη δυαδική αναπαράσταση για τον αριθμό των 0 στο *m*.

3. Να σχηματίσει το $w = m \| c = (a_1 a_2 ... a_t)$.

4. Να προσδιορίσει τις θέσεις συντεταγμένων $i_1 \prec i_2 \prec ... \prec i_u$ στο *w* τέτοιες ώστε $a_{i_j} = 1$ με $1 \le j \le u$.

5. Να αποδεχτεί την υπογραφή μόνο αν $u_{i_j} = h(s_j)$ για κάθε $1 \le j \le u$.

Ασφάλεια του σχήματος υπογραφών μιας χρήσης του Merkle

Έστω ότι m είναι ένα μήνυμα και $w = m \| c$ η δυαδική συμβολοσειρά που σχηματίζεται στον παραπάνω αλγόριθμο και $(s_1, s_2, ..., s_u)$ μια υπογραφή για το m. Αν h είναι μια ανθιστάμενη-προεικόνας hash συνάρτηση, το παρακάτω μας δείχνει ότι δεν μπορεί να πλαστογραφηθεί μια υπογραφή για ένα μήνυμα $m' \neq m$. Έστω $w' = m' \| c' w'$, όπου c' είναι η συμβολοσειρά των $\lfloor 1gn \rfloor + 1$ bit η οποία είναι η δυαδική αναπαράσταση για τον αριθμό των μηδενικών στο m'. Αφού ένας αντίπαλος έχει πρόσβαση μόνο σε εκείνο το τμήμα του ιδιωτικού κλειδιού του υπογράφοντα το οποίο αποτελείται από τα $(s_1, s_2, ..., s_u)$, το σύνολο των συντεταγμένων θέσεων στο m' που έχουν ένα 1 πρέπει να είναι υποσύνολο των συντεταγμένων θέσεων στο m που έχουν ένα 1 (γιατί αλλιώς το m' θα έχει ένα 1 σε κάποια θέση όπου το m έχει ένα 0 και ο αντίπαλος θα χρειαστεί ένα στοιχείο του ιδιωτικού κλειδιού που δεν έχει αποκαλυφθεί από τον υπογράφοντα). Αλλά αυτό σημαίνει ότι το m' έχει περισσότερα μηδενικά από το m και ότι $c' \succ c$ (όταν θεωρηθούν ως ακέραιοι). Σε αυτήν την περίπτωση το c' θα έχει ένα 1 σε κάποια θέση όπου το c έχει ένα 0. Ο αντίπαλος θα χρειαζόταν ένα στοιχείο του ιδιωτικού κλειδιού, που αντιστοιχεί στη θέση αυτή, το οποίο δε έχει αποκαλυφθεί από τον υπογράφοντα.

Βελτίωση της αποδοτικότητας του σχήματος μιας χρήσης του Merkle

Ο αλγόριθμος παραγωγής και επαλήθευσης υπογραφών μιας χρήσης Merkle απαιτεί $l \cdot (n + \lfloor 1gn \rfloor + 1)$ bit για καθένα από τα κλειδιά, ιδιωτικό και δημόσιο. Το δημόσιο κλειδί πρέπει αναγκαστικά να είναι τόσο μεγάλο επειδή ο αλγόριθμος υπογραφής θεωρεί μεμονωμένα bit του μηνύματος. Το σχήμα μπορεί να γίνει πιο αποδοτικό αν ο αλγόριθμος υπογραφής θεωρεί περισσότερα από ένα bit τη φορά. Ας υποθέσουμε ότι ο Α επιθυμεί να υπογράψει ένα μήνυμα των kt bit. Γράφουμε $m = m_1 \| m_2 \| ... \| m_t$, όπου κάθε m_i έχει δυαδικό μήκος k και το καθένα αναπαριστά έναν ακέραιο μεταξύ των 0 και $2^k - 1$ συμπεριλαμβανομένων. Ορίζουμε $U = \sum_{i=1}^{t} (2^k - m_i) \leq t2^k$. Το U

μπορεί να αναπαρασταθεί με $1gU \le \lfloor 1gt \rfloor + 1 + k$ bit. Αν $r = \frac{\lfloor 1gt \rfloor + 1 + k}{k}$, τότε το U μπορεί να γραφεί σε δυαδική μορφή ως $U = u_1 \| u_2 \| ... \| u_r$, όπου κάθε u_i έχει δυαδικό μήκος k. Σχηματίζουμε τη δυαδική συμβολοσειρά $w = m_1 \| m_2 \| ... \| m_t \| u_1 \| u_2 \| ... \| u_r$. Παράγουμε $t + r$ τυχαίες δυαδικές συμβολοσειρές $k_1, k_2, ..., k_{t+r}$ και υπολογίζουμε τα $v_i = h^{2^k - 1}(k_i)$ με $1 \le i \le t + r$. Το ιδιωτικό κλειδί του τροποποιημένου σχήματος είναι $(k_1, k_2, ..., k_{t+r})$ και το δημόσιο κλειδί είναι $(v_1, v_2, ..., v_{t+r})$. Η υπογραφή για το m είναι $(s_1, s_2, ..., s_{t+r})$, όπου $s_i = h^{m_i}(k_i)$ με $1 \le i \le t$ και $s_i = h^{u_i}(k_{t+i})$ με $1 \le i \le r$. Εδώ το h^c συμβολίζει την c-πλή σύνθεση της h με τον εαυτό της. Σε σχέση με το αρχικό σχήμα, τα προσαρτημένα bit στο μήνυμα λειτουργούν σαν ένα άθροισμα ελέγχου (checksum) ως εξής:

Δοθέντος ενός στοιχείου $s_i = h^a(k_j)$, ένας αντίπαλος μπορεί εύκολα να υπολογίσει την τιμή $h^{a+\delta}(k_j)$ για $0 \le \delta \le 2^k - a$, αλλά δεν είναι σε θέση να υπολογίσει την τιμή $h^{a-\delta}$ για οποιοδήποτε $\delta \succ 0$, αν η h είναι μια μονόδρομη hash συνάρτηση. Για να πλαστογραφήσει μια υπογραφή σε ένα νέο μήνυμα, ο αντίπαλος μπορεί μόνο να ελαττώσει την τιμή του αθροίσματος ελέγχου, το οποίο θα καταστήσει αδύνατο για αυτόν τον υπολογισμό των απαιτούμενων τιμών διασποράς στα προσαρτημένα kr bit.

Παράδειγμα (υπογραφή περισσοτέρων του ενός bit τη φορά) : Στο παράδειγμα αυτό εξηγούμε την τροποποίηση του σχήματος Merkle που περιγράφουμε ακριβώς παραπάνω. Έστω $m = m_1 \| m_2 \| m_3 \| m_4$, όπου $m_1 = 1011, m_2 = 0111, m_3 = 1010$ και $m_4 = 1101$. Τα m_1, m_2, m_3, m_4 είναι οι δυαδικές αναπαραστάσεις των 11, 7, 10, 13 αντίστοιχα. Είναι $U = (16 - m_1) + (16 - m_2) + (16 - m_3) + (16 - m_4)$ $5 + 9 + 6 + 3 = 23$. Στο δυαδικό σύστημα $U = 10111$. Σχηματίζουμε το $w = m||00010111$. Η υπογραφή είναι $(s_1, s_2, s_3, s_4, s_5, s_6)$, όπου $s_1 = h^{11}(k_1)$, $s_2 = h^7(k_2)$, $s_3 = h^{10}(k_3)$, $s_4 = h^{13}(k_4)$, $s_5 = h^1(k_5), s_6 = h^7(k_6)$. Αν ο αντίπαλος προσπαθήσει να μεταβάλλει το μήνυμα, μπορεί να εφαρμόσει τη συνάρτηση h σε μερικά s_i. Αυτό έχει ως αποτέλεσμα να αυξηθεί το άθροισμα των χρησιμοποιούμενων εκθετών (δηλαδή το $\sum m_i$) και

επομένως να μειωθεί η διαφορά $t2^d - \sum m_i$. Ο αντίπαλος δεν θα είναι σε θέση να τροποποιήσει τα δύο τελευταία τμήματα διότι απαιτείται να ελαττώσει η h^{-1} το άθροισμα. Αλλά, αφού η h είναι ανθιστάμενη-προεικόνας, δεν είναι δυνατό να υπολογιστεί η h^{-1} από τον αντίπαλο.

5.3 Το σχήμα υπογραφών μιας χρήσης GMR

Το σχήμα των Godwasser, Micali και Rivest (GMR) είναι ένα σχήμα υπογραφών μιας χρήσης που απαιτεί ένα claw-free ζεύγος μεταθέσεων. Το σχήμα GMR είναι αξιοσημείωτο καθώς ήταν ο πρώτος μηχανισμός ψηφιακών υπογραφών που αποδείχθηκε ότι ήταν ασφαλής εναντίον μιας προσαρμόσιμης επίθεσης επιλεγμένου μηνύματος. Αν και το σχήμα GMR δεν είναι πρακτικό, έχουν προταθεί κάποιες παραλλαγές του οι οποίες υποδεικνύουν ότι η έννοια δεν είναι αμιγώς θεωρητικής σπουδαιότητας.

Ορισμός: Έστω $g_i : X \to X, i = 0,1,$ δύο μεταθέσεις ορισμένες σε ένα πεπερασμένο σύνολο *X*. Οι g_0, g_1 λέγονται ότι είναι ένα claw-free ζεύγος μεταθέσεων αν είναι υπολογιστικά ανέφικτο να βρούμε $x, y \in X$ τέτοια ώστε $g_0(x) = g_1(y)$. Μια τριάδα (x, y, z) στοιχείων που ανήκουν στο X με $g_0(x) = g_1(y) = z$ λέγεται claw. Αν και οι δύο $g_i, i = 0,1$ έχουν την ιδιότητα ότι δοσμένης επιπρόσθετης πληροφορίας, είναι υπολογιστικά εφικτό να υπολογίσουμε τις g_0^{-1}, g_1^{-1} αντίστοιχα, οι μεταθέσεις λέγονται claw-free ζεύγος μεταθέσεων κερκόπορτας.

Για να αποτελούν οι g_0, g_1 ένα claw-free ζεύγος, ο υπολογισμός των g_0^{-1}, g_1^{-1} πρέπει να είναι υπολογιστικά ανέφικτος για όλα τα $x \in X$. Διότι, αν ο υπολογισμός της g_1^{-1} (όμοια και της g_0^{-1}) ήταν εφικτός, θα μπορούσε κάποιος να επιλέξει ένα $x \in X$ και να υπολογίσει τις τιμές $g_0(x) = z$ και $g_1^{-1}(z) = y$, για να λάβει μια (x, y, z).

Παράδειγμα 1 (claw-free ζεύγος μεταθέσεων για τεχνητά μικρές παραμέτρους) :

Έστω $p = 11$, $q = 7$ και $n = pq = 77$. Έχουμε $D_{77} = \left\{ x : \left(\frac{x}{n} \right) \quad 1 \,\mu\varepsilon\, 0 \leq x \prec 38 \right\}$

$\{1, 4, 6, 9, 10, 13, 15, 16, 17, 19, 23, 24, 25, 36, 37\}$. Ο επόμενος πίνακας περιγράφει τις g_0, g_1 (μεταθέσεις στο D_{77}).

x	1	4	6	9	10	13	15	16	17	19	23	24	25	36	37
$g_0(x)$	1	16	36	4	23	15	6	25	19	24	10	37	9	13	17
$g_1(x)$	4	13	10	16	15	17	24	23	1	19	37	6	36	25	9

α) <u>Αλγόριθμος παραγωγής κλειδιών</u>

Κάθε οντότητα επιλέγει ένα claw-free ζεύγος μεταθέσεων κερκόπορτας και μια παράμετρο επικύρωσης. Ο Α θα πρέπει να κάνει τα παρακάτω:

1. Να επιλέξει ένα claw-free ζεύγος μεταθέσεων κερκόπορτας σε κάποιο σύνολο *X*. (Είναι «κερκόπορτας» ως προς το ότι ο Α μπορεί από μόνος του να υπολογίσει τις g_0^{-1}, g_1^{-1})
2. Να επιλέξει ένα τυχαίο στοιχείο $r \in X$. (Το *r* λέγεται παράμετρος επικύρωσης.)
3. Το δημόσιο κλειδί του Α είναι (g_0, g_1, r) και το ιδιωτικό κλειδί του Α είναι (g_0^{-1}, g_1^{-1}).

Ο χώρος υπογραφής M_S στα παρακάτω θα αποτελείται από δυαδικές συμβολοσειρές οι οποίες είναι ελεύθερες-προθέματος.

β) Αλγόριθμος παραγωγής υπογραφής

Ο Α υπογράφει μια δυαδική συμβολοσειρά $m = m_1 m_2 ... m_t$. Ο Β επαληθεύει χρησιμοποιώντας το δημόσιο κλειδί του Α. Ο Α θα πρέπει να κάνει τα εξής:

1 Να υπολογίσει την τιμή $S_r(m) = \prod_{i=0}^{t-1} g_{m_{t-i}}^{-1}(r)$.

2. Η υπογραφή του Α για το *m* είναι η $S_r(m)$

γ) Αλγόριθμος επαλήθευσης υπογραφής

Για να επαληθεύσει την υπογραφή $S_r(m)$ του Α στο *m*, ο Β θα πρέπει να κάνει τα παρακάτω:

1. Να λάβει το αυθεντικό δημόσιο κλειδί (g_0, g_1, r) του Α.

2. Να υπολογίσει την τιμή $r' = \prod_{i=1}^{t} g_{m_i}(S_r(m))$.

3. Να αποδεχτεί την υπογραφή, αν και μόνο αν $r' = r$.

Κωδικοποίηση μηνύματος και ασφάλεια

Το σύνολο των μηνυμάτων τα οποία μπορούν να υπογραφούν χρησιμοποιώντας τον παραπάνω αλγόριθμο πρέπει να προέρχεται από ένα σύνολο δυαδικών συμβολοσειρών οι οποίες είναι ελεύθερες-προθέματος. (Π.χ. οι 101 και 10111 δεν μπορούν να είναι στον ίδιο χώρο διότι η 101 είναι πρόθεμα της 10111.) Μια μέθοδος για να πραγματοποιήσουμε κάτι τέτοιο είναι να κωδικοποιήσουμε μια δυαδική συμβολοσειρά $b_1 b_2 ... b_l$ ως $b_1 b_1 b_2 b_2 ... b_l b_l 01$. Για να δούμε γιατί η απαίτηση «ελεύθερη-προθέματος» είναι αναγκαία, ας υποθέσουμε ότι $m = m_1 m_2 ... m_t$ είναι ένα μήνυμα του οποίου η υπογραφή είναι η $S_r(m) = \prod_{i=0}^{t-1} g_{m_{t-i}}^{-1}(r)$. Αν $m' = m_1 m_2 ... m_u$ με $u \prec t$, τότε ένας αντίπαλος μπορεί να βρει εύκολα μια έγκυρη υπογραφή για το m' από την $S_r(m)$ υπολογίζοντας την $S_r(m') = \prod_{j=u+1}^{t} g_{m_j}(S_r(m)) = \prod_{i=0}^{u-1} g_{m_{u-1}}^{-1}(r)$.

Παράδειγμα 2 (το GMR με τεχνητά μικρές παραμέτρους) :

Παραγωγή κλειδιών: Έστω ότι n, p, q, g_0, g_1 είναι εκείνα που δίνονται στο Παράδειγμα 1 παραπάνω. Ο Α επιλέγει την παράμετρο επικύρωσης $r = 15 \in D_{77}$.

Παραγωγή υπογραφής : Έστω m = 1011000011 το προς υπογραφή μήνυμα. Τότε $S_r(m) = g_1^{-1} \circ g_1^{-1} \circ g_0^{-1} \circ g_0^{-1} \circ g_0^{-1} \circ g_0^{-1} \circ g_1^{-1} \circ g_1^{-1} \circ g_0^{-1} \circ g_1^{-1}(15) = 23$. Η υπογραφή του Α για το μήνυμα m είναι 23.

Επαλήθευση υπογραφής: Για να επαληθεύσει την υπογραφή, ο Β υπολογίζει $r' = g_1 \circ g_0 \circ g_1 \circ g_1 \circ g_0 \circ g_0 \circ g_0 \circ g_0 \circ g_1 \circ g_1(23) = 15$. Αφού $r = r'$, ο Β αποδέχεται την υπογραφή.

5.4 Το σχήμα υπογραφών μιας χρήσης Lamport

Το σχήμα υπογραφών μιας χρήσης Lamport απαιτεί την επιλογή μιας τυχαίας one-way συνάρτησης $f : Z_{p-1} \to Z_p^*$ η οποία αποτελεί δημόσια πληροφορία. Για παράδειγμα μια τέτοιου είδους συνάρτηση είναι η $f(x) = g^x \bmod p$ όπου p πρώτος και g γεννήτορας της Z_p^*. Ο χώρος M των μηνυμάτων αλλά και ο υπογραφόμενος χώρος M_S είναι το σύνολο $\{0,1\}^k$ με $k \in N$, ενώ ο χώρος των υπογραφών S είναι το σύνολο Z_{p-1}. Κάθε μήνυμα $m \in M$ είναι μια δυαδική ακολουθία μήκους k bits όπου καθένα από αυτά τα bits υπογράφεται ανεξάρτητα και ξεχωριστά από τα υπόλοιπα. Αν δηλαδή το i-οστό bit του m με $1 \le i \le k$ έχει τιμή $j \in \{0,1\}$, τότε το i-οστό στοιχείο της υπογραφής είναι η τιμή που αποτελεί όρισμα του δημοσίου κλειδιού $z_{i,j}$. Κάθε $z_{i,j} \in Z_p^*$ είναι η εικόνα του $y_{i,j} \in Z_{p-1}$ μέσω της συνάρτησης $f(x) = g^x \bmod p$. Η διαδικασία της επαλήθευσης απλώς ελέγχει ότι κάθε στοιχείο της υπογραφής είναι όρισμα του κατάλληλου στοιχείου του δημοσίου κλειδιού.

α) Αλγόριθμος παραγωγής κλειδιών

Ο Α θα πρέπει να κάνει τα παρακάτω:

1. Επιλέγει έναν μεγάλο τυχαίο πρώτο p και ένα γεννήτορα g της Z_p^*.

2. Επιλέγει $2k$ τυχαίους ακεραίους $y_{i,j} \in Z_{p-1}$, όπου το μήκος σε bits του m που πρόκειται να υπογραφεί με $1 \le i \le k$ και $j \in \{0,1\}$.

3. Με την one-way συνάρτηση $f : Z_{p-1} \to Z_p^*$ με $f(x) = g^x \bmod p$ υπολογίζει τα $z_{i,j} = f(y_{i,j})$ για κάθε $1 \le i \le k$ και $j \in \{0,1\}$.

4. Το δημόσιο κλειδί του Α είναι ο $k \times 2$ πίνακας $\left[z_{i,j} \right]$ και το ιδιωτικό του κλειδί είναι ο $k \times 2$ πίνακας $\left[y_{i,j} \right]$.

β) Αλγόριθμος παραγωγής υπογραφής

Ο Α για να υπογράψει ένα δυαδικό μήνυμα m μήκους k bit και να το στείλει θα πρέπει να κάνει τα παρακάτω:

1. Έστω $m = (m_1, m_2, ..., m_k)$.

2. Η υπογραφή του Α για το $m \in \{0,1\}^k$ είναι η $(s_1, s_2, ..., s_k) \in Z_{p-1}$ τέτοια ώστε $S_k(m_1, m_2, ..., m_k) = (s_1, s_2, ..., s_k)$ $(y_{1,m_1}, y_{2,m_2}, ..., y_{k,m_k})$ s.

3. Ο Α στέλνει στον Β την υπογραφή s.

γ) Αλγόριθμος επαλήθευσης υπογραφής

Για να επαληθεύσει την υπογραφή s του Α, ο Β θα κάνει τα παρακάτω:

1. Να λάβει το αυθεντικό δημόσιο κλειδί $(z_{1,j}, z_{2,j}, ..., z_{k,j})$ του Α.

2. Να υπολογίσει τα $f(s_i)$ για κάθε $1 \le i \le k$.

3. Να αποδεχτεί την υπογραφή αν και μόνο αν $f(s_i) = z_{i,0}$ ή $z_{i,1}$ για κάθε $1 \le i \le k$.

Παράδειγμα 1 : Ο Α επιλέγει $p = 7879$ και $g = 3$ της Z_{7879}^* και έστω η one-way συνάρτηση $f : Z_{7878} \to Z_{7879}^*$ με $f(x) = 3^x \bmod 7879$. Ο Α θέλει να υπογράψει ένα δυαδικό μήνυμα m μήκους $k = 3$ bits και να το στείλει στον Β.

Παραγωγή κλειδιών: Επιλέγει $2k = 6$ τυχαίους ακεραίους $y_{i,j} \in Z_{7878}$ με $1 \le i \le 3$, $j \in \{0,1\}$ και κατασκευάζει το ιδιωτικό του κλειδί : $y_{i,j} = \begin{bmatrix} y_{1,0} = 5831 & y_{1,1} = 735 \\ y_{2,0} = 803 & y_{2,1} = 2467 \\ y_{3,0} = 4285 & y_{3,1} = 6449 \end{bmatrix}$.

Μετά ο Α υπολογίζει τα $z_{i,j} = f(y_{i,j}) 3^{y_{i,j}} \bmod 7879$ με $1 \le i \le 3$, $j \in \{0,1\}$ και κατασκευάζει το δημόσιο του κλειδί : $z_{i,j} = \begin{bmatrix} z_{1,0} = 2009 & z_{1,1} = 3810 \\ z_{2,0} = 4672 & z_{2,1} = 4721 \\ z_{3,0} = 268 & z_{3,1} = 5731 \end{bmatrix}$.

Παραγωγή υπογραφής : Ο Α θέλει να υπογράψει για τον Β το $m = 110$. Η υπογραφή του Α για το $m = (m_1, m_2, m_3) = (1,1,0)$ είναι η $s = (s_1, s_2, s_3)$ $S_K(m_1, m_2, m_3)$ $S_K(1,1,0) = (y_{1,1}, y_{2,1}, y_{3,0}) = (735, 2467, 4285)$.

Επαλήθευση υπογραφής: Ο Β παίρνει την υπογραφή, αποκτά το δημόσιο κλειδί του Α και υπολογίζει :

$f(s_1) = 3^{735} \bmod 7879 = 3810 \quad z_{1,1}$, $f(s_2) = 3^{2467} \bmod 7879 = 4721 \quad z_{2,1}$ και $f(s_3) = 3^{4285} \bmod 7879 = 268 \quad z_{3,0}$. Αφού ισχύει $f(s_i) = z_{i,0}$ ή $z_{i,1}$ για κάθε $1 \le i \le 3$, ο Β δέχεται την υπογραφή και από τους δείκτες των $z_{1,1}, z_{2,1}, z_{3,0}$ ανακτά το μήνυμα $m = (m_1, m_2, m_3) = (1,1,0)$.

Δυνατές επιθέσεις και ασφάλεια

Ένας αντίπαλος δε μπορεί να πλαστογραφήσει μια υπογραφή ενός μηνύματος m που έχει παραχθεί με το σχήμα υπογραφής μιας χρήσης Lamport διότι είναι υπολογιστικά ανέφικτη η αντιστροφή της one-way συνάρτησης f. Έτσι ο αντίπαλος δε μπορεί να ανακτήσει το ιδιωτικό κλειδί του υπογράφοντα χρησιμοποιώντας το δημόσιο.

Παρ' όλα αυτά το ιδιωτικό κλειδί πρέπει να χρησιμοποιηθεί για την υπογραφή ενός μόνο μηνύματος γιατί αλλιώς είναι εύκολο για κάποιον να πλαστογραφήσει την υπογραφή του νόμιμου υπογράφοντα σε μηνύματα της επιλογής του.

Παράδειγμα 2 (Υπαρκτή πλαστογραφία με επίθεση σε γνωστά μηνύματα) :

Έστω ότι ο Α επιλέγει για ιδιωτικό κλειδί το $(y_{1,j}, y_{2,j}, y_{3,j})$ με $j \in \{0,1\}$ και υπογράφει για τον Β τα μηνύματα $m_1 = (0,1,1)$ και $m_2 = (1,0,1)$ με αντίστοιχες υπογραφές $s_1 = (y_{1,0}, y_{2,1}, y_{3,1})$ και $s_2 = (y_{1,1}, y_{2,0}, y_{3,1})$. Αν ένας αντίπαλος Γ καταφέρει να υποκλέψει τις υπογραφές αυτές τότε μπορεί να κατασκευάσει τις υπογραφές $s_3 = (y_{1,1}, y_{2,1}, y_{3,1})$ και $s_4 = (y_{1,0}, y_{2,0}, y_{3,1})$ που είναι έγκυρες για τα μηνύματα $m_3 = (1,1,1)$ και $m_4 = (0,0,1)$. Για το λόγο αυτό, κάθε μήνυμα που υπογράφεται απαιτεί την παραγωγή νέου ιδιωτικού και δημοσίου κλειδιού.

Παρατήρηση: Ένα σύστημα ψηφιακής υπογραφής Lamport έχει και ένα πολύ σοβαρό πρακτικό μειονέκτημα. Αν υπολογίσουμε τον αριθμό των συνολικών bits που απαιτούνται προκειμένου να υπογραφεί ένα bit, θα διαπιστώσουμε ότι το υπολογιστικό κόστος καθώς και το κόστος αποθήκευσης είναι μεγάλα. (Π.χ. αν υποθέσουμε ότι ο κρυπταλγόριθμος είναι ο DES για την υπογραφή ενός bit, το ισοδύναμο δημόσιο κλειδί θα έχει μέγεθος ίσο με 256 bits ενώ η υπογραφή δηλαδή το ισοδύναμο ιδιωτικό κλειδί θα έχει μήκος ίσο με 52 bits).

Κεφάλαιο 6

ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΩΝ ΜΕ ΕΠΠΡΟΣΘΕΤΗ ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

6.1 Τυφλά σχήματα υπογραφών (Blind Signature Schemes)

Είναι ένας μηχανισμός μεταξύ του αποστολέα Α και του υπογράφοντα Β. Ο Α στέλνει ένα τμήμα πληροφορίας στον Β, το οποίο το υπογράφει ο Β και το επιστρέφει στον Α. Από αυτή την υπογραφή ο Α μπορεί να υπολογίσει την υπογραφή του Β για ένα μήνυμα m της επιλογής του Α. Ο Β δεν γνωρίζει ούτε το μήνυμα m ούτε την υπογραφή που σχετίζεται με αυτό το μήνυμα.
Στόχος αυτού του σχήματος είναι να εμποδίσει τον Β από το να παρατηρήσει το μήνυμα που υπογράφει και την υπογραφή του, ώστε αργότερα να είναι αδύνατο για αυτόν να συσχετίσει το υπογεγραμμένο μήνυμα με τον αποστολέα Α.
Τα τυφλά σχήματα υπογραφής έχουν εφαρμογές όπου ο αποστολέας Α (πελάτης) δε θέλει ο υπογράφων Β (τράπεζα) να είναι ικανός να συσχετίσει ένα μήνυμα m και μία υπογραφή $S_B(m)$ για το m με τον Α. Αυτό είναι χρήσιμο για εφαρμογές ηλεκτρονικών πληρωμών όπου ένα μήνυμα m μπορεί να αντιπροσωπεύει ένα ποσό που ο Α μπορεί να χρησιμοποιήσει. Όταν τα m και $S_B(m)$ παρουσιάζονται στον Β για πληρωμή, ο Β δεν μπορεί να συμπεράνει πιο τμήμα είναι το μήνυμα δοθέντος της υπογραφής. Αυτό επιτρέπει στον Α να είναι ανώνυμος .

Ένα σχήμα τυφλής υπογραφής πρέπει να έχει τα ακόλουθα χαρακτηριστικά:

1. Ένα μηχανισμό υπογραφής για τον υπογράφοντα Β. Το $S_B(x)$ ορίζει την υπογραφή του Β στο x.
2. Συναρτήσεις f, g (γνωστές μόνο στον αποστολέα) τέτοιες που $g(S_B(f(m))) = S_B(m)$. Η f λέγεται συνάρτηση τύφλωσης (blinding function) , η g

συνάρτηση επαναφοράς (unblinding function) και το $f(m)$ τυφλό μήνυμα (blinded message).

Παράδειγμα 1 : Θα δούμε ένα παράδειγμα όπου η συνάρτηση τύφλωσης f βασίζεται στο RSA. Έστω $n = p \cdot q$ είναι το γινόμενο δύο μεγάλων πρώτων αριθμών. Ο αλγόριθμος δημιουργίας της υπογραφής για τον Β (S_B) είναι ο αλγόριθμος που είδαμε στο RSA με δημόσιο κλειδί (n,e) και ιδιωτικό κλειδί το d. Έστω k είναι κάποιος ακέραιος με $\gcd(n,k)=1$. Η συνάρτηση τύφλωσης $f: Z_n \to Z_n$ ορίζεται από τον τύπο $f(m) = m \cdot k^e \bmod n$ και η συνάρτηση επαναφοράς $g: Z_n \to Z_n$ ορίζεται από τον τύπο $g(m) = k^{-1} \cdot m \bmod n$. Για αυτή την επιλογή των f, g και S_B έχουμε ότι $g(S_B(f(m))) = g(S_B(m \cdot k^e \bmod n)) = g(m^d \cdot k \bmod n) = m^d \bmod n = S_B(m)$.

<u>Πρωτόκολλο τυφλής υπογραφής του Chaum</u>.

α) Ο αποστολέας Α λαμβάνει μία υπογραφή του Β για ένα τυφλό μήνυμα. Από αυτό ο Α υπολογίζει την υπογραφή του Β για ένα μήνυμα m τέτοιο που $0 \le m \le n-1$. Ο Β δεν ξέρει τίποτα για το μήνυμα m ούτε για την υπογραφή που σχετίζεται με αυτό.

β) Ο Β χρησιμοποιεί το RSA, το δημόσιο κλειδί είναι (n,e) και το μυστικό το d. Ο k είναι ένας τυχαίος μυστικός ακέραιος που επιλέγεται από τον Α με $0 \le k \le n-1$ και $\gcd(n,k)=1$.

γ) 1. Ο Α υπολογίζει $m^* = m \cdot k^e \bmod n$ και το στέλνει στον Β. (τύφλωση)

2. Ο Β υπολογίζει $s^* = (m^*)^d \bmod n$ και το στέλνει στον Α. (υπογραφή)

3. Ο Α υπολογίζει $s = k^{-1} \cdot s^* \bmod n$ όπου είναι η υπογραφή του Β για το μήνυμα m. (αποτύφλωση)

Παράδειγμα 2 (σχήμα τυφλής υπογραφής Chaum) : Ο Β επιλέγει τους πρώτους $p=29$, $q=17$ και υπολογίζει $n = p \cdot q = 29 \cdot 17 = 493$. Διαλέγει δημόσιο εκθέτη $e=191$ ($\varphi(n) = 28 \cdot 16 = 448$, $1 \prec e \prec 448$ και $\gcd(e, \varphi(n)) = 1$) και υπολογίζει το μυστικό εκθέτη του $d = 319$ αφού ισχύει $191 \cdot d = 1 \bmod 448$.

Υποθέτουμε ότι ο Α θέλει την υπογραφή του Β στο μήνυμα $m = 351$. Επιλέγει κρυφό ακέραιο $k = 31$ και υπολογίζει το τυφλωμένο μήνυμα $m^* = 351 \cdot 31^{191} \bmod 493 = 291$ και το μεταδίδει στον Β.

Ο Β υπολογίζει $s^* = 291^{319} \bmod 493 = 349$ και το στέλνει στον Α. Η τιμή s^* είναι η υπογραφή του Β για το τυφλωμένο μήνυμα $m^* = 291$. Στη συνέχεια βρίσκει $31^{-1} \bmod 493 = 334$ και $s = 334 \cdot 349 \bmod 493 = 218$ που αποτελεί την υπογραφή του Β για το $m = 351$.

6.2 Αδιαμφισβήτητα σχήματα υπογραφών (Undeniable Signature Schemes)

Σε αυτό το σχήμα της υπογραφής, για την πιστοποίηση της υπογραφής απαιτείται η συνεργασία του λήπτη με τον υπογράφοντα.

Οι εφαρμογές αυτών των σχημάτων είναι πολλές:

1. Έστω ότι ο Α (πελάτης) θέλει να έχει πρόσβαση σε ένα ασφαλές περιβάλλον που ελέγχεται από τον Β (τράπεζα). Το ασφαλές περιβάλλον μπορεί να είναι ο λογαριασμός του πελάτη στην τράπεζα. Ο Β απαιτεί από τον Α να υπογράψει την ώρα και την ημερομηνία πριν έχει πρόσβαση στο ασφαλές περιβάλλον. Αν ο Α χρησιμοποιήσει ένα γνήσιο σχήμα υπογραφής τότε ο Β δε θα μπορεί να αποδείξει (σε κάποια μεταγενέστερη χρονική στιγμή) ότι ο Α είχε πρόσβαση χωρίς τη συμμετοχή του Α στη διαδικασία της πιστοποίησης της υπογραφής.

2. Έστω ότι σε μία μεγάλη συνεργασία ο Α δημιουργεί ένα πακέτο λογισμικού. Ο Α υπογράφει το πακέτο αυτό και το στέλνει στον Β, ο οποίος αποφασίζει να δημιουργήσει αντίτυπα και να τα μεταπωλήσει σε ένα τρίτο άτομο τον Γ. Ο Γ δεν μπορεί να πιστοποιήσει την αυθεντικότητα του λογισμικού χωρίς τη συνεργασία του Α. Βέβαια ο Β δεν εμποδίζεται από το να δημιουργήσει μία δικιά του υπογραφή για το λογισμικό αλλά θα χαθεί το όνομα του Α από αυτό και θα μπει του Β. Αν γίνει αυτό ο Α θα μπορεί εύκολα να ανακαλύψει την απάτη του Β.

Θα δούμε ένα σχήμα γνήσιας υπογραφής.

α) Αλγόριθμος δημιουργίας κλειδιού

1. Ο Α επιλέγει ένα τυχαίο πρώτο $p = 2q + 1$ όπου και ο q είναι πρώτος.

2. Επιλέγει ένα τυχαίο ακέραιο a της υποομάδας, τάξης q στο Z_p^*.

3. Αν $a = 1$, τότε πήγαινε στο βήμα 2 αλλιώς για να βρει το a επιλέγει τυχαίο στοιχείο $b \in Z_p^*$ και υπολογίζει $a = b^{\frac{p-1}{q}} \bmod p$.

4. Επιλέγει ένα τυχαίο ακέραιο $k \in \{1, 2, ..., q-1\}$ και υπολογίζει $y = a^k \bmod p$.

5. Το δημόσιο κλειδί του Α είναι το (p, a, y) και το μυστικό κλειδί το k.

β) Αλγόριθμος δημιουργίας υπογραφής (Chaum-van Antwerpen)

Το μήνυμα m είναι ένα στοιχείο της υποομάδας τάξης q στο Z_p^*.

1. Ο Α υπολογίζει $s = m^k \bmod p$.

2. Η υπογραφή του Α για το μήνυμα m είναι το s.

γ. Αλγόριθμος πιστοποίησης της υπογραφής (Chaum-van Antwerpen)

1. Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το (p, a, y).

2. Επιλέγει τυχαία μυστικούς ακεραίους $x_1, x_2 \in \{1, 2, ..., q-1\}$.

3. Υπολογίζει $z = s^{x_1} \cdot y^{x_2} \bmod p$ και στέλνει το z στον Α.

4. Ο Α υπολογίζει $w = z^{k^{-1}} \bmod p$ (ισχύει $k \cdot k^{-1} = 1 \bmod q$) και στέλνει στον Β.

5. Ο Β υπολογίζει $w' = m^{x_1} \cdot a^{x_2} \bmod p$ και δέχεται την υπογραφή αν και μόνο αν $w = w'$.

Απόδειξη του αλγόριθμου πιστοποίησης:

$w = z^{k^{-1}} = (s^{x_1} \cdot y^{x_2})^{k^{-1}} = (m^{kx_1} \cdot a^{kx_2})^{k^{-1}} = m^{x_1} \cdot a^{x_2} = w' \bmod p$.

Παράδειγμα 1 (αδιαμφισβήτητο σχήμα υπογραφής Chaum- van Antwerpen):

Ο Α επιλέγει τους πρώτους $p = 2q+1 = 2 \cdot 233+1 = 467$ με $q = 233$. Μετά επιλέγει τυχαίο στοιχείο $g_0 = 2 \in Z_{467}^*$ και υπολογίζει το $g = g_0^{\frac{p-1}{q}} \bmod p = 2^2 \bmod 467 = 4$ που είναι γεννήτορας της κυκλικής υποομάδας G του Z_{467}^*. Στη συνέχει επιλέγει $k = 101$ και υπολογίζει $y = 4^{101} \bmod 467 = 449$. Το δημόσιο κλειδί του Α είναι το $(p, a, y) = (467, 4, 449)$ και το ιδιωτικό του κλειδί $k = 101$.

Ο Α θέλει να υπογράψει το μήνυμα $m = 119$. Υπολογίζει την υπογραφή $s = 119^{101} \bmod 467 = 129$.

Ο Β λαμβάνει $(m, s) = (119,129)$ και αποκτά το δημόσιο κλειδί του Α. Επιλέγει κρυφούς ακεραίους $x_1 = 38,\ x_2 = 397$ και υπολογίζει τη τιμή $z = 129^{38} \cdot 449^{397} \bmod 467 = 13$ την οποία και μεταδίδει στον Α.

Ο Α υπολογίζει $k^{-1} \bmod q = 101^{-1} \bmod 233 = 30$, $w = z^{k^{-1}} \bmod p$ 13^30 mod 467 9 και στέλνει το w στον Β.

Τέλος ο Β υπολογίζει $m^{x_1} \cdot a^{x_2} \bmod p$ $119^{38} \cdot 4^{397} \bmod 467$ 9 $z \bmod 467$ οπότε αποδέχεται την υπογραφή ως αυθεντική.

Ο υπογράφων Α μπορεί να αρνηθεί μία υπογραφή που κατασκευάσθηκε με τον παραπάνω αλγόριθμο με τρεις τρόπους:

1. Να αρνηθεί να πάρει μέρος στη διαδικασία πιστοποίησης της υπογραφής.
2. Να εκτελέσει την πιστοποίηση λανθασμένα.
3. Να ισχυρισθεί ότι η υπογραφή είναι πλαστογραφημένη αν και έχει πετύχει η διαδικασία πιστοποίησης.

6.3 Σχήματα υπογραφής εύρεσης πλαστογράφησης (Fail-stop Signature Schemes)

Σε αυτό το σχήμα της υπογραφής ο Α μπορεί να αποδείξει ότι μία υπογραφή είναι πλαστή. Αυτό γίνεται δείχνοντας ότι ο βασικός μηχανισμός που δημιουργεί την υπογραφή είναι δεσμευτικός. Η ικανότητα να αποδείξουμε ότι η υπογραφή είναι πλαστή δε στηρίζεται σε κάποια κρυπτογραφική υπόθεση αλλά ότι μπορεί να

αποτύχει με μικρή πιθανότητα. Η πιθανότητα αποτυχίας είναι ανεξάρτητη από την υπολογιστική δύναμη του πλαστογράφου. Το βασικό πλεονέκτημα αυτού του σχήματος είναι ότι ακόμα και ένας δυνατός υπολογιστικά πλαστογράφος μπορέσει να πλαστογραφήσει μία απλή υπογραφή, η πλαστογράφηση μπορεί να ανακαλυφθεί και ο συγκεκριμένος μηχανισμός δημιουργίας της υπογραφής δε θα χρησιμοποιηθεί στο μέλλον.
Είναι ένα σχήμα υπογραφής μιας χρήσης αλλά μπορεί να γενικευθεί ώστε να επιτρέπονται περισσότερες υπογραφές χρησιμοποιώντας δέντρα αυθεντικότητας.

Ένα σχήμα υπογραφής εύρεσης πλαστογράφησης πρέπει να έχει τις ακόλουθες ιδιότητες:

1. Αν ο υπογράφων υπογράψει ένα μήνυμα με το δεσμευτικό μηχανισμό τότε αυτός που θα πιστοποιήσει την υπογραφή πρέπει να τη δεχτεί ως έγκυρη.
2. Ο πλαστογράφος δε μπορεί να κατασκευάσει υπογραφές που να περάσουν από τον αλγόριθμο πιστοποίησης χωρίς να χρειασθεί εκθετικό χρόνο εργασίας.
3. Αν ο πλαστογράφος καταφέρει να κατασκευάσει μία υπογραφή που περάσει από τον αλγόριθμο πιστοποίησης τότε με μεγάλη πιθανότητα ο αληθινός υπογράφων μπορεί να αποδείξει την πλαστογράφηση.
4. Ο υπογράφων δε μπορεί να κατασκευάσει υπογραφές που μετά από την πάροδο κάποιου χρονικού διαστήματος να ισχυρισθεί ότι είναι πλαστές.

Θα δούμε τους αλγόριθμους για ένα τέτοιο σχήμα, όπου απαιτείται η ύπαρξη και ενός τρίτου έμπιστου ατόμου (TTP), στην πράξη, μιας τράπεζας.

α) Αλγόριθμος δημιουργίας κλειδιού

1. Ο TTP κάνει τα εξής:
i) Επιλέγει πρώτους p, q τέτοιους που ο q διαιρεί τον $p-1$.
ii) Επιλέγει ένα τυχαίο ακέραιο α της υποομάδας, τάξης q στο Z_p^*.
iii) Αν $a=1$ τότε πήγαινε στο βήμα ii.
iv) Επιλέγει ένα τυχαίο ακέραιο t με $1 \le t \le q-1$ και υπολογίζει $b = a^t \bmod p$. Ο ακέραιος t κρατιέται μυστικός από τον TTP.

v) Στέλνει στον Α το (p,q,a,b) .

2. Ο Α κάνει τα εξής:

i) Επιλέγει τυχαία ακέραιους $x_1, x_2, y_1, y_2 \in [0, q-1]$.

ii) Υπολογίζει $b_1 = a^{x_1} b^{x_2} \bmod p$ και $b_2 = a^{y_1} b^{y_2} \bmod p$.

iii) Το δημόσιο κλειδί του Α είναι (b_1, b_2, p, q, a, b) και το μυστικό κλειδί $\bar{x} = (x_1, x_2, y_1, y_2)$.

β) Αλγόριθμος δημιουργίας υπογραφής (van Heijst-Pedersen)

Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου στην υποομάδα τάξης q στο Z_p^*.

Το μήνυμα $m \in [0, q-1]$.

1. Ο Α υπολογίζει $s_{1,m} = x_1 + m y_1 \bmod p$ και $s_{2,m} = x_2 + m y_2 \bmod p$.

2. Η υπογραφή του Α για το μήνυμα m είναι $(s_{1,m}, s_{2,m})$.

γ) Αλγόριθμος πιστοποίησης της υπογραφής (van Heijst-Pedersen)

1. Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το (b_1, b_2, p, q, a, b).

2. Υπολογίζει $v_1 = b_1 \cdot b_2^m \bmod p$ και $v_2 = a^{s_{1,m}} \cdot b^{s_{2,m}} \bmod p$.

3. Ο Β δέχεται την υπογραφή αν και μόνο αν $v_1 = v_2$.

Απόδειξη του αλγόριθμου πιστοποίησης:

$v_1 = b_1 \cdot b_2^m = (a^{x_1} b^{x_2}) \cdot (a^{y_1} b^{y_2})^m = a^{x_1 + m y_1} \cdot b^{x_2 + m y_2} = a^{s_{1,m}} \cdot b^{s_{2,m}} = v_2 \bmod p$.

Ιδιότητα του σχήματος υπογραφής

Έστω ότι το δημόσιο κλειδί είναι (b_1, b_2, p, q, a, b) και το μυστικό κλειδί είναι $\bar{x} = (x_1, x_2, y_1, y_2)$.

(α) Υπάρχουν ακριβώς q^2 τετράδες $\overline{x'} = (x_1', x_2', y_1', y_2')$ με $x_1', x_2', y_1', y_2' \in Z_q$ όπου έχουν το ίδιο αποτέλεσμα με το (b_1, b_2) του τμήματος του δημοσίου κλειδιού.

(β) Έστω T το σύνολο αυτών των τετράδων για το (b_1, b_2). Για κάθε $m \in Z_q$ υπάρχουν ακριβώς q τετράδες στο T όπου δίνουν την ίδια υπογραφή $(s_{1,m}, s_{2,m})$ για το m. Έτσι οι q^2 τετράδες του T δίνουν ακριβώς q διαφορετικές υπογραφές για το m.

(γ). Έστω $m' \in Z_q$ είναι ένα μήνυμα διαφορετικό από το m. Τότε οι q τετράδες του T που δίνουν τις υπογραφές $(s_{1,m}, s_{2,m})$ του Α για το m, δίνουν διαφορετικές υπογραφές για το m'.

Παράδειγμα : Έστω $p = 29$, $q = 7$ και $a = 16$ είναι ένας γεννήτορας της υποομάδας τάξης q στο Z_p^*. Παίρνουμε $b = a^5 \bmod 29 = 23$. Υποθέτουμε ότι το ιδιωτικό κλειδί του Α είναι $\overline{x} = (x_1, x_2, y_1, y_2) = (2,3,5,2)$ και το δημόσιο κλειδί είναι $b_1 = a^2 b^3 \bmod 29 = 7$, $b_2 = a^5 b^2 \bmod 29 = 16$. Στον παρακάτω πίνακα βλέπουμε τις $q^2 = 49$ τετράδες που δίνουν το ίδιο δημόσιο κλειδί

1603	2303	3003	4403	5103	6503	0203
1610	2310	3010	4410	5110	6510	0210
1624	2324	3024	4424	5124	6524	0224
1631	2331	3031	4431	5131	6531	0231
1645	2345	3045	4445	5145	6545	0245
1652	2352	3052	4452	5152	6552	0252
1666	2366	3066	4466	5166	6566	0266

Αν οι 49 τετράδες του παραπάνω πίνακα χρησιμοποιηθούν για την υπογραφή του μηνύματος $m = 1$, τότε υπάρχουν ακριβώς $q = 7$ υπογραφές $(s_{1,m}, s_{2,m})$. Στον επόμενο πίνακα βλέπουμε τις πιθανές και εκείνες τις τετράδες που δημιουργούν κάθε υπογραφή.

Υπογραφές	(2,6)	(3,3)	(4,0)	(5,4)	(6,1)	(0,5)	(1,2)
Τετράδες	1610	1624	1631	1645	1652	1666	1603
	2303	2310	2324	2331	2345	2352	2366
	3066	3003	3010	3024	3031	3045	3052
	4452	4466	4403	4410	4424	4431	4445
	5145	5152	5166	5103	5110	5124	5131
	6531	6545	6552	6566	6503	6510	6524
	0224	0231	0245	0252	0266	0203	0210

Στον τελευταίο πίνακα βλέπουμε για κάθε μήνυμα $m' \in Z_7$, όλες τις υπογραφές για τις 7 τετράδες όπου η υπογραφή του Α είναι $(0,5)$ για το μήνυμα $m = 1$.

Τετράδα	m'						
	0	1	2	3	4	5	6
1666	16	05	64	53	42	31	20
2352	23	05	50	32	14	66	41
3045	30	05	43	11	56	24	62
4431	44	05	36	60	21	52	13
5124	51	05	22	46	63	10	34
6510	65	05	15	25	35	45	55
0203	02	05	01	04	00	03	06

Έστω ότι ο πλαστογράφος θέλει να βρει την υπογραφή του Α για κάποιο μήνυμα m'. Υπάρχουν δύο περιπτώσεις που θα εξετάσουμε:

1. Ο πλαστογράφος έχει πρόσβαση μόνο στο δημόσιο κλειδί του Α. Από την ιδιότητα του σχήματος αυτού, η πιθανότητα ότι η υπογραφή που θα κατασκευάσει να είναι ίδια με την υπογραφή του Α για το μήνυμα m' είναι ίση με $\frac{q}{q^2} = \frac{1}{q}$. Αυτή η πιθανότητα είναι ανεξάρτητη από την υπολογιστική δύναμη του πλαστογράφου.
2. Αν ο πλαστογράφος έχει πρόσβαση σε ένα μήνυμα m και στην αυθεντική υπογραφή του, τότε η πιθανότητα να κατασκευάσει μία πλαστογραφημένη υπογραφή

για ένα μήνυμα m' είναι πάλι $\frac{1}{q}$ όπου ξανά αυτή η πιθανότητα είναι ανεξάρτητη από την υπολογιστική δύναμη του πλαστογράφου.

Θα δούμε τώρα με ποιό τρόπο ο Α θα μπορέσει να αποδείξει με μεγάλη πιθανότητα ότι μία υπογραφή είναι πλαστή. Υποθέτουμε ότι ο πλαστογράφος έχει πλαστογραφήσει μία υπογραφή του Α για ένα μήνυμα και έχει περάσει με επιτυχία τον αλγόριθμο πιστοποίησης. Ο παρακάτω αλγόριθμος απόδειξης της πλαστογραφίας μας δείχνει πως ο Α θα χρησιμοποιήσει την πλαστή υπογραφή για να βρει το μυστικό ακέραιο t που είχαμε υποθέσει παραπάνω ότι τον γνωρίζει μόνο ο TTP.

Αλγόριθμος **απόδειξης** της πλαστογραφίας

Για να αποδείξουμε ότι η υπογραφή $s' = (s'_{1,m}, s'_{2,m})$ είναι πλαστή για ένα μήνυμα m, ο Α θα βρει το $t = \log_a b$ και μετά θα κάνει τα παρακάτω:

1. Υπολογίζει μία υπογραφή $s = (s_{1,m}, s_{2,m})$ για το μήνυμα m χρησιμοποιώντας το δικό του μυστικό κλειδί $\bar{x} = (x_1, x_2, y_1, y_2)$.
2. Αν $s' = s$ τότε τέλος.
3. Υπολογίζει $t = \left(s_{1,m} - s'_{1,m}\right) \cdot \left(s_{2,m} - s'_{2,m}\right)^{-1} \bmod q$.

Απόδειξη του αλγόριθμου απόδειξης της πλαστογραφίας:

Η πιθανότητα να ισχύει $s' = s$ είναι $\frac{1}{q}$. Από τον αλγόριθμο πιστοποίησης έχουμε ότι:

$a^{s_{1,m}} \cdot b^{s_{2,m}} \equiv a^{s'_{1,m}} \cdot b^{s'_{2,m}} \pmod p \Leftrightarrow a^{s_{1,m} - s'_{1,m}} \equiv a^{t(s'_{2,m} - s_{2,m})} \pmod p \Leftrightarrow$

$\Leftrightarrow s_{1,m} - s'_{1,m} \equiv t(s'_{2,m} - s_{2,m}) \pmod q$.

Τελικά έχουμε ότι: $t = (s_{1,m} - s'_{1,m}) \cdot (s'_{2,m} - s_{2,m})^{-1} \pmod q$.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Α. Παπαϊωάννου, Χ. Κουκουβίνος. Εισαγωγή στην Κρυπτογραφία. Εκδόσεις Ε.Μ.Π., 2007.

2. Αλέξανδρος Χ. Παπαϊωάννου. Διακριτά Μαθηματικά. Εκδόσεις Ε.Μ.Π., 2003.

3. Ε. Ζάχος. Σημειώσεις στη Θεωρία Αριθμών και την Κρυπτογραφία. Εκδόσεις Ε.Μ.Π., 2004.

4. Ε. Ζάχος. Αλγόριθμοι και Πολυπλοκότητα. Εκδόσεις Ε.Μ.Π., 2003.

5. Δημήτριος Μ. Πουλάκης. Κρυπτογραφία: Η Επιστήμη της Ασφαλούς Επικοινωνίας. Εκδόσεις Ζήτη, 2006.

6. A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

7. John B. Fraleigh. Εισαγωγή στην Άλγεβρα. Πανεπιστημιακές Εκδόσεις Κρήτης, 2011.

8. R.L. Rivest, A. Shamir, L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978.

9. R.C. Merkle. Secure communications over insecure channels. Communications of the ACM, 1978.

10. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions of Information Theory, 1985.

11. S. Goldwasser, S. Micali R.L. Rivest “A digital signature scheme against adaptive chosen-message attacks” SIAM Journal on computing, 1988.

12. Buchmann A. Johannes. Introduction to Cryptography. Springer, 2000.

13. U. Feige, A. Fiat, A. Shamir. Zero-knowledge proofs of identity. Journal of Cryptology, 1988.

14. M.O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. MIT/LCS/TR 212, 1979.

Σελίδες στο Διαδίκτυο :

www.itl.nist.gov
www.ierf.org
www.rsa.com
www.rsasecurity.com
www.cryptogram.gr
www.wikipedia.org
www.securitymanager.gr