ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Ψηφιακές Υπογραφές στην Κρυπτογραφία

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΑΝΑΓΝΩΣΤΟΠΟΥΛΟΥ ΠΕΡΣΕΦΟΝΗΣ

Επιβλέπων: Παπαϊωάννου Αλέξανδρος

Καθηγητής Ε.Μ.Π.

Αθήνα, Νοέμβριος 2011

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ

ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΚΑΤΕΥΘΥΝΣΗ ΜΑΘΗΜΑΤΙΚΟΥ

Ψηφιακές Υπογραφές στην Κρυπτογραφία

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΑΝΑΓΝΩΣΤΟΠΟΥΛΟΥ ΠΕΡΣΕΦΟΝΗΣ

Επιβλέπων: Παπαϊωάννου Αλέξανδρος

Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 25η Νοεμβρίου 2011.

……..	……..	……..
Α. Παπαϊωάννου	Π. Στεφανέας	Χ. Κουκουβίνος

Αθήνα, Νοέμβριος 2011

Περίληψη

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά «κρυπτός» + «γράφω» και είναι ένας επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Κύριος στόχος της είναι να παρέχει μηχανισμούς για δύο ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάσει την πληροφορία εκτός από τα μέλη.

Η ψηφιακή υπογραφή μπορεί να θεωρηθεί ως το ψηφιακό «ταίρι» της χειρόγραφης υπογραφής. Η ψηφιακή υπογραφή ενός μηνύματος είναι ένας αριθμός που εξαρτάται από κάποια κρυφή πληροφορία γνωστή μόνο στον υπογράφοντα και επιπροσθέτως από το περιεχόμενο του μηνύματος που υπογράφεται. Πρέπει να είναι επαληθεύσιμες, δηλαδή αν προκύψει κάποια διαμάχη για το αν μια οντότητα υπέγραψε ένα έγγραφο, μια αμερόληπτη τρίτη οντότητα πρέπει να είναι σε θέση να επιλύσει το θέμα δίκαια.

Οι ψηφιακές υπογραφές έχουν πολλές εφαρμογές στην ασφάλεια πληροφοριών, συμπεριλαμβάνοντας την πιστοποίηση (εξακρίβωση της προέλευσης ενός μηνύματος), την ακεραιότητα των δεδομένων (μη τροποποίηση του μηνύματος κατά τη μετάδοση) και τη μη αποκήρυξη (μια οντότητα δε μπορεί να αρνηθεί την υπογραφή που δημιούργησε).

Η ιδέα και η χρησιμότητα των ψηφιακών υπογραφών αναγνωρίστηκε αρκετά χρόνια πριν οποιαδήποτε πρακτική εφαρμογή ήταν διαθέσιμη. Το σχήμα υπογραφής RSA ήταν η πρώτη μέθοδος που ανακαλύφθηκε και παραμένει μέχρι σήμερα μια από τις πιο πρακτικές και πολύπλευρες διαθέσιμες τεχνικές. Διαδοχική έρευνα είχε ως αποτέλεσμα πολλές εναλλακτικές τεχνικές ψηφιακών υπογραφών. Μερικές προσφέρουν σημαντικά πλεονεκτήματα όσον αφορά τη λειτουργικότητα και την εφαρμογή τους.

Abstract

The word cryptography comes from the Greek words “kryptos” (=hidden) and “grapho” (=write) and it is scientific sector that deals with the study, the development and the use of techniques of coding and decoding in order to hide the content of a message. Its main purpose is to provide tools and mechanisms to two or more members so as to communicate without interruptions from anyone else.

A digital signature can be considered as the digital counterpart of a handwritten signature. A digital signature is a number dependent on some secret information known only to the signer, and, additionally, on the content of the message being signed. They must be verifiable, which means that if a dispute arises as to whether a party signed a document, an unbiased third party should be able to resolve the problem equitably.

Digital signatures have many applications in information security, including authentication (verification of the origin of the message), data integrity (non-modification of the message during transmission) and non-repudiation (an entity in not able to repudiate a signature it did create).

The concept and utility of digital signatures was recognized several years before any practical realization was available. The first method discovered was the RSA signature scheme, which remains today one of the most practical and versatile techniques available. Subsequent research has resulted in many alternative digital signature techniques. Some of them offer significant advantages in terms of functionality and implementation.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Η επιστήμη της κρυπτογραφίας

Κρυπτογραφία είναι ο επιστημονικός κλάδος που πραγματεύεται τη μελέτη και υλοποίηση μεθόδων τροποποίησης των μεταδιδομένων πληροφοριών ώστε να γίνονται κατανοητές μόνο από τον προβλεπόμενο παραλήπτη. Μαζί με τον κλάδο της κρυπτανάλυσης, που ασχολείται με τη μελέτη τρόπων παραβίασης αυτών, συνιστούν την επιστήμη της κρυπτολογίας.

Η ανάγκη της ασφαλούς επικοινωνίας είναι πολύ παλιά. Μια Βαβυλωνιακή επιγραφή του 1500 π.Χ. η οποία περιγράφει μια μέθοδο κατασκευής σμάλτων για αγγειοπλαστική, θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο. Η Σπαρτιατική σκυτάλη ανάγεται στον $5^{ο}$ π.Χ. αιώνα. Πρόκειται για μια ξύλινη ράβδο συγκεκριμένης διαμέτρου γύρω από την οποία ήταν τυλιγμένη μια λωρίδα από περγαμηνή. Ο αποστολέας έγραφε το κείμενο κατά μήκος της σκυτάλης και στη συνέχεια ξετύλιγε τη λωρίδα η οποία έδειχνε να περιέχει μια σειρά από γράμματα χωρίς νόημα. Για να διαβάσει το μήνυμα ο παραλήπτης απλά τύλιγε τη λωρίδα γύρω από μια σκυτάλη ίδιας διαμέτρου. Ο Ιούλιος Καίσαρας έγραφε στους φίλους του αντικαθιστώντας τα γράμματα του κειμένου με γράμματα που βρίσκονται τρεις θέσεις μετά στο Λατινικό αλφάβητο. Έτσι, σήμερα, το σύστημα κρυπτογράφησης που στηρίζεται στην αντικατάσταση των γραμμάτων του αλφαβήτου με άλλα που βρίσκονται σε καθορισμένο αριθμό θέσης πριν ή μετά, λέγεται κρυπτοσύστημα αντικατάστασης του Καίσαρα.

Μπορεί η πρώτη στρατιωτική χρήση της κρυπτογραφίας να αποδίδεται στους Σπαρτιάτες, αλλά η τελευταία δεν έπαψε ποτέ να αποτελεί τεχνική υψίστης στρατιωτικής σημασίας. Κατά τους δύο παγκόσμιους πολέμους, λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρξε για ασφάλεια κατά τη μετάδοση ζωτικών πληροφοριών μεταξύ των στρατευμάτων των χωρών, η κρυπτογραφία αναπτύχθηκε όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα και να αποτελούνται από μηχανικές κατασκευές, τις κρυπτομηχανές. Οι Γερμανοί έκαναν εκτενή χρήση ενός συστήματος γνωστού ως Enigma, για την παραβίαση του οποίου επιστρατεύτηκαν οι καλύτεροι μαθηματικοί. Οι Βρετανοί, με τη βοήθεια των Πολωνών, έσπασαν τον κώδικα και βρέθηκαν μπροστά σε ένα δίλημμα: αν ειδοποιούσαν τους κατοίκους της πόλης Coventry για τον επικείμενο βομβαρδισμό της, τότε οι Γερμανοί θα καταλάβαιναν ότι το σύστημα δεν είναι πλέον ασφαλές. Πράγματι, ο βομβαρδισμός έγινε και χάθηκαν πολλές ανθρώπινες ζωές αλλά όπως λέγεται σώθηκαν πολύ περισσότερες.

Τα μεταπολεμικά χρόνια η κρυπτογραφία γνώρισε νέα ανάπτυξη χάρη κυρίως στην τεχνολογία των υπολογιστών και σήμερα απέχει πολύ από την κρυπτογραφία του δεύτερου παγκοσμίου πολέμου. Ο σκοπός που εξυπηρετεί παραμένει ο ίδιος αλλά χρησιμοποιείται για πλήθος εφαρμογών άγνωστων στον τότε κόσμο. Η κινητή τηλεφωνία, η δορυφορική τηλεόραση, τα ασύρματα δίκτυα, τα συστήματα συναγερμών χρησιμοποιούν κρυπτογραφικά εργαλεία. Ο αριθμός των συστημάτων που περιέχουν βάσεις δεδομένων με προσωπικές πληροφορίες αυξάνεται διαρκώς και κρίνεται αναγκαία η προστασία των δεδομένων από ανεπιθύμητη προσπέλαση.

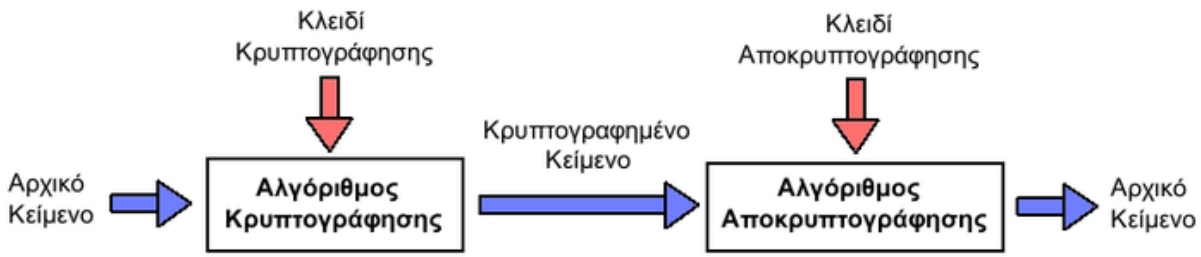
Η κρυπτογραφία έχει επίσης πολλές εφαρμογές σε δραστηριότητες της καθημερινής μας ζωής, όπως η χρήση πιστωτικών καρτών και η ανάληψη χρημάτων από συσκευές ATM, που πρέπει με κάθε τρόπο να παραμένουν ασφαλείς. Στη σύγχρονη εποχή της πληροφόρησης και του συνεχώς αναπτυσσόμενου ηλεκτρονικού εμπορίου καθίσταται επιτακτική η διασφάλιση των ηλεκτρονικών μας συναλλαγών. Η ηλεκτρονική υποβολή της φορολογικής μας δήλωσης για παράδειγμα, σίγουρα μας διευκολύνει, αλλά πόσο σίγουροι είμαστε ότι τα στοιχεία και οι πληροφορίες μας παραμένουν ασφαλή κατά τη συναλλαγή;

Η κρυπτογραφία καλύπτει αυτές ακριβώς τις ανάγκες για αξιοπιστία και εμπιστευτικότητα, παρέχοντας τις βασικές υπηρεσίες της ασφάλειας που είναι η απόρρητη συναλλαγή (privacy), η ακεραιότητα των δεδομένων (data integrity), η πιστοποίηση ταυτότητας (authentication) και η μη απάρνηση.

Η πιστοποίηση της γνησιότητας των πληροφοριών που λαμβάνονται ηλεκτρονικά είναι σημαντική και αναγκαία. Πρέπει να πιστοποιούνται οι ημερομηνίες αποστολής εγγράφων, η ταυτότητα του αποστολέα, η ταυτότητα του ηλεκτρονικού υπολογιστή και πλήθος στοιχείων που μέχρι τώρα βασίζονταν σε παραδοσιακά μέσα επεξεργασίας πληροφοριών. Η τάση αυτή που επικρατεί επιτάσσει και την αντικατάσταση των παραδοσιακών τρόπων πιστοποίησης, δηλαδή της χειρόγραφης υπογραφής και των σφραγίδων των οργανισμών. Η κρυπτογραφία παρέχει τέτοιους μηχανισμούς, τις ψηφιακές υπογραφές (digital signatures) και τις ψηφιακές χρονοσφραγίδες (digital timestamps).

1.2 Το γενικό πλαίσιο των συστημάτων κρυπτογράφησης

Τα σύγχρονα κρυπτοσυστήματα είναι σε γενικές γραμμές μηχανισμοί μετατροπής δεδομένων από μια αρχική μορφή (plaintext) σε μια νέα (ciphertext), από την οποία δεν προκύπτει σαφές νόημα. Η διαδικασία αυτή καλείται κρυπτογράφηση και η αντίστροφή της αποκρυπτογράφηση. Τόσο η κρυπτογράφηση όσο και η κρυπτογράφηση απαιτούν την παρουσία ενός αλγορίθμου και ενός κλειδιού (key). Το τελευταίο δεν είναι τίποτα άλλο από μια ακολουθία χαρακτήρων (string). Η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης φαίνεται στο σχήμα που ακολουθεί:

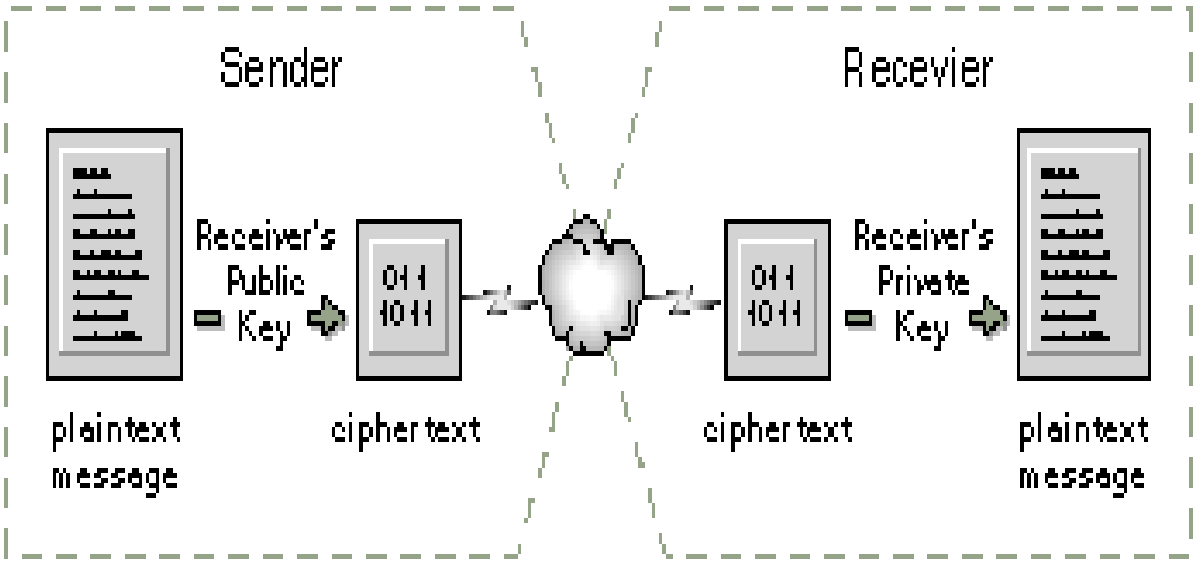


Ανάλογα με το είδος των κλειδιών που χρησιμοποιούνται, η κρυπτογραφία διακρίνεται σε ασύμμετρη (asymmetric or public-key cryptography) και συμμετρική (symmetric or secret-key cryptography).

Ασύμμετρη κρυπτογραφία:

Η ασύμμετρη κρυπτογραφία χρησιμοποιεί δυο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσιο και το άλλο ιδιωτικό. Το πρώτο δημοσιοποιείται ενώ το ιδιωτικό κρατείται μυστικό. Η ανάγκη αποστολέας και παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται, μαζί και πολλά προβλήματα. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η πιστοποίηση των δημόσιων κλειδιών από οργανισμούς ώστε να μην είναι δυνατή η πλαστοπροσωπία. Η ασύμμετρη κρυπτογραφία μπορεί να χρησιμοποιηθεί και για την παραγωγή ψηφιακών υπογραφών.

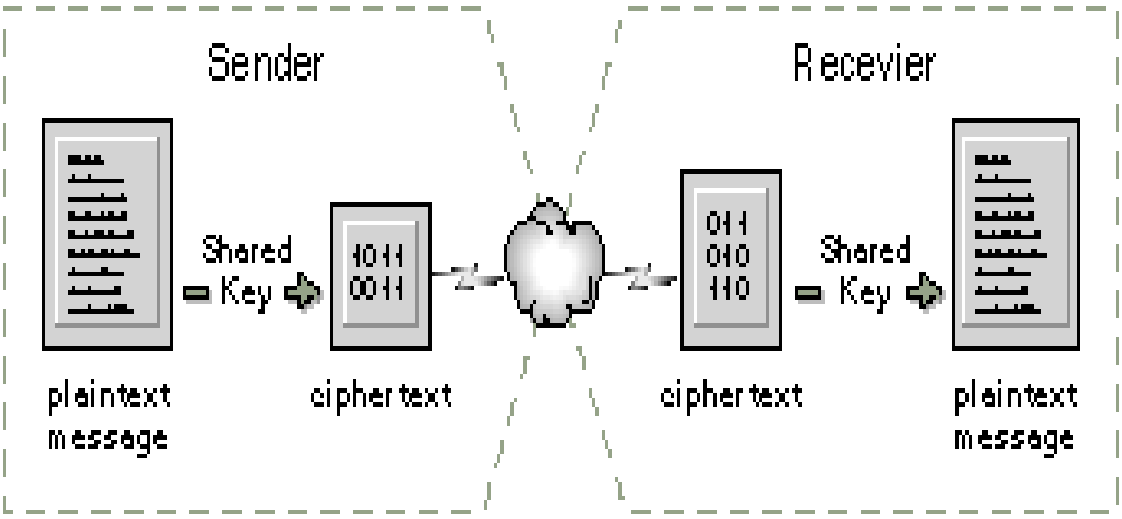
Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στο χρήστη Β, χρησιμοποιεί το δημόσιο κλειδί του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει. Ο Β, αφού λάβει το μήνυμα, το αποκρυπτογραφεί με το ιδιωτικό του κλειδί. Κανένας τρίτος δε μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει το δημόσιο κλειδί του Β μπορεί να του στείλει μήνυμα, αλλά μόνο ο Β μπορεί να το διαβάσει γιατί είναι ο μόνος που γνωρίζει το ιδιωτικό κλειδί. Η διαδικασία φαίνεται καλύτερα στο σχήμα 1.2.1.



Σχήμα 1.2.1 Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης στην ασύμμετρη κρυπτογραφία

Συμμετρική κρυπτογραφία:

Εδώ, αποστολέας και παραλήπτης γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί. Το κύριο πρόβλημα είναι η ανταλλαγή του κλειδιού χωρίς κάποιος τρίτος να λάβει γνώση αυτού. Είναι όμως σημαντικά ταχύτερη από την ασύμμετρη κρυπτογραφία. Γι' αυτό το λόγο, τα κρυπτοσυστήματα δημοσίου κλειδιού στην πράξη χρησιμοποιούνται για την ανταλλαγή κλειδιών και στη συνέχεια οι δυο πλευρές μπορούν να επικοινωνήσουν με ασφάλεια με τη χρήση κάποιου συμμετρικού κρυπτοσυστήματος.



Σχήμα 1.2.2 Διαδικασία κρυπτογράφησης και αποκρυπτογράφησης στη συμμετρική κρυπτογραφία

1.3 Σχήμα Ψηφιακής Υπογραφής (Digital Signature Scheme)

Σε πολλές περιπτώσεις στην καθημερινή ζωή χρειάζεται να υπογράψουμε ένα έγγραφο π.χ. ένα συμβόλαιο ή μια υπεύθυνη δήλωση. Τα σχήματα ψηφιακών υπογραφών είναι μέθοδοι υπογραφής ψηφιακών δεδομένων. 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 βρίσκουν εφαρμογή στις ηλεκτρονικές αγορές (e-commerce), στην επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου (e-mail), στις ηλεκτρονικές συναλλαγές με τράπεζες (e-banking) και γενικά σε δραστηριότητες κατά τις οποίες απαιτείται επιβεβαίωση της ταυτότητας της μίας πλευράς στην άλλη. Ο παραλήπτης ενός υπογεγραμμένου ηλεκτρονικού μηνύματος μπορεί να διαπιστώσει τη γνησιότητά του με έναν δημόσιο αλγόριθμο επαλήθευσης και σ' αυτή την περίπτωση είναι βέβαιος για την προέλευση, την ακεραιότητα και τη μη αποκήρυξη του από τον αποστολέα.

Την ιδέα της ψηφιακής υπογραφής εισήγαγαν πρώτοι οι Diffie και Helman και η χρησιμότητά της αναγνωρίστηκε αρκετά χρόνια πριν οποιαδήποτε πρακτική εφαρμογή ήταν εφικτή. Η πρώτη μέθοδος που ανακαλύφθηκε ήταν το σχήμα υπογραφής RSA, το οποίο παραμένει μία από τις πιο πρακτικές και πολύπλευρες τεχνικές. Στη συνέχεια βέβαια επινοήθηκαν πολλές εναλλακτικές τεχνικές, με σημαντικά πλεονεκτήματα ως προς τη λειτουργικότητα και την εφαρμογή τους.

Σκοπός μιας ψηφιακής υπογραφής είναι να δηλώσει το άτομο που είναι υπεύθυνο για το περιεχόμενο ενός μηνύματος, δηλαδή το ίδιο ακριβώς πράγμα που κάνει μια χειρόγραφη υπογραφή όταν βρεθεί πάνω σε ένα έγγραφο. Είναι με λίγα λόγια το ψηφιακό ταίρι της χειρόγραφης υπογραφής. Ας δούμε όμως μερικές διαφορές μεταξύ χειρόγραφων και ψηφιακών υπογραφών.

Όπως ξέρουμε, η χειρόγραφη υπογραφή αποτελεί αναπόσπαστο μέρος ενός εγγράφου και κάθε γνήσιο αντίγραφό του την περιέχει. Αντίθετα μια ψηφιακή υπογραφή δεν επισυνάπτεται στο μήνυμα. Μπορεί να αφαιρεθεί γι αυτό πρέπει με κάποιο τρόπο να δεσμεύεται με το μήνυμα για το οποίο δημιουργήθηκε. Αυτό επιτυγχάνεται με την κρυπτογράφηση του υπογεγραμμένου μηνύματος, όπως θα δούμε στη συνέχεια.

Για την πιστοποίηση μιας χειρόγραφης υπογραφής είναι απαραίτητη η βοήθεια ειδικού γραφολόγου. Η επαλήθευση όμως των ψηφιακών υπογραφών γίνεται με έναν δημοσίως γνωστό αλγόριθμο που μπορεί να χρησιμοποιήσει ο οποιοσδήποτε. Για την αποφυγή πλαστογράφησης το μόνο που χρειάζεται είναι ένα ασφαλές σχήμα ψηφιακής υπογραφής.

Παρατηρώντας δυο χειρόγραφες υπογραφές σε δυο έγγραφα διαπιστώνουμε εύκολα ότι δεν είναι πανομοιότυπες, αλλά αντίθετα διαφέρουν, ίσως και αρκετά. Αυτό δε συμβαίνει με τις ψηφιακές υπογραφές και μπορεί να δημιουργήσει προβλήματα. Για παράδειγμα, αν ο Α εξουσιοδοτήσει τον Β να πάρει από την τράπεζα ένα χρηματικό ποσό, θα πρέπει να ναι σίγουρος ότι ο Β δε θα μπορεί να επαναλάβει τη διαδικασία. Γι αυτό η υπογραφή μπορεί να περιέχει και άλλες πληροφορίες, όπως ώρα και ημερομηνία, προκειμένου να ακυρώνεται μετά τη χρήση της.

Ορισμός:

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

1. M το πεπερασμένο σύνολο όλων των μηνυμάτων.

2. S το πεπερασμένο σύνολο όλων των υπογραφών.

3. K το πεπερασμένο σύνολο όλων των πιθανών κλειδιών που μπορεί να χρησιμοποιηθούν για την υπογραφή.

4. Υπάρχει μετασχηματισμός $\text{sig}_K(m)$: $M \rightarrow S$. Είναι γνωστός μόνο στον υπογράφοντα και ονομάζεται συνάρτηση υπογραφής (Signing Function).

5. Υπάρχει μετασχηματισμός $\text{ver}_K(m, s)$: $M \times S \rightarrow \{$ αληθής, ψευδής$\}$. Είναι δημόσια γνωστός και ονομάζεται συνάρτηση επαλήθευσης (Verification Function). Χρησιμοποιείται για να επαληθεύσει ότι η υπογραφή s έχει πράγματι προκύψει από την εφαρμογή του sig_K στο m. Δηλαδή:

$$\text{ver}_K(m,s) = \begin{cases} \text{αληθής, αν } \text{sig}_K(m) = s, \\ \text{ψευδής, διαφορετικά.} \end{cases}$$

Ένα ζεύγος (m,s) ∈ M×S καλείται υπογεγραμμένο μήνυμα. Ο χρήστης Α ενός σχήματος ψηφιακής υπογραφής επιλέγει ένα κλειδί k, δημοσιοποιεί τη συνάρτηση ver_K και κρατά μυστική την sig_K. Ο παραλήπτης Β ενός υπογεγραμμένου μηνύματος (m, s) το οποίο υποτίθεται ότι προέρχεται από τον Α, υπολογίζει την τιμή ver_K(m, s) και δέχεται το μήνυμα ως γνήσιο μόνο αν ver_K(m,s)= αληθής.

Κάθε σχήμα υπογραφής πρέπει να ικανοποιεί τις ακόλουθες βασικές ιδιότητες:

1. Να ισχύει ver_K(m, s)= αληθής αν και μόνο αν sig_K(m)= s.

2. Να είναι υπολογιστικά εύκολο για κάποιον να υπογράψει ένα μήνυμα και για κάποιον άλλον να επαληθεύσει τη γνησιότητα της υπογραφής.

3. Να είναι υπολογιστικά ανέφικτο για οποιονδήποτε εκτός του υπογράφοντα να βρει s για δοθέν m τέτοιο ώστε ver_K(m, s)= αληθής.

Οι συναρτήσεις ver_K και sig_K χρειάζεται να είναι πολυωνυμικού χρόνου (polynomial-time functions), με τη ver_K δημόσια και την sig_K γνωστή μόνο στον υπογράφοντα. Για ένα τρίτο άτομο Γ θα πρέπει να είναι υπολογιστικά ανέφικτο να πλαστογραφήσει την υπογραφή του Α σε ένα μήνυμα m. Αυτό σημαίνει ότι δοθέντος του m μόνο ο Α μπορεί να υπολογίσει την υπογραφή s ώστε ver_K(m, s)= αληθής. Ένα σχήμα υπογραφής δεν είναι ποτέ απολύτως ασφαλές κι αυτό γιατί ο Γ μπορεί να δοκιμάσει όλες τις πιθανές υπογραφές για ένα μήνυμα m με βάση το δημόσιο αλγόριθμο επαλήθευσης, μέχρι να βρει τη σωστή υπογραφή. Αυτό όμως θα απαιτήσει από τον Γ πάρα πολύ χρόνο. Έτσι, στόχος μας είναι η εύρεση σχημάτων υπογραφής που είναι υπολογιστικά ασφαλή για όσο χρονικό διάστημα απαιτείται.

Ας δούμε τώρα πώς συνδυάζεται η ψηφιακή υπογραφή με τη χρήση ενός κρυπτοσυστήματος δημοσίου κλειδιού. Ο υπογράφων έχει στην κατοχή του δύο κλειδιά , το δημόσιο και το ιδιωτικό, τα οποία σχετίζονται μαθηματικά με τέτοιο τρόπο, ώστε να είναι πρακτικά αδύνατο για κάποιον να υπολογίσει το ένα από το άλλο. Η διαφορά με την κρυπτογράφηση είναι ότι για τη δημιουργία της υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Ας υποθέσουμε λοιπόν ότι ο Α επιθυμεί να στείλει στον Β το μήνυμα m υπογεγραμμένο και κρυπτογραφημένο. Πρώτα υπολογίζει την υπογραφή του s= $sig_κ$(m) και κατόπιν κρυπτογραφεί το υπογεγραμμένο μήνυμα (m ,s) χρησιμοποιώντας το δημόσιο κλειδί του Β. Ο Β λαμβάνει το κρυπτογραφημένο μήνυμα z, το αποκρυπτογραφεί με το ιδιωτικό του κλειδί και παίρνει το ζεύγος (m, s) στο οποίο εφαρμόζει τη συνάρτηση επαλήθευσης. Επαληθεύει ότι ver_K(m, s)= αληθής και είναι βέβαιος ότι ο αποστολέας του m είναι ο Α. Έτσι η διαδικασία ολοκληρώνεται επιτυχώς. Ακόμα κι αν ο Γ υποκλέψει το κρυπτογραφημένο μήνυμα z, δε θα είναι σε θέση να το αποκρυπτογραφήσει άρα δε θα μπορέσει να αποσπάσει το ζεύγος (m,s) και να αλλάξει την υπογραφή.

Θα ήταν το ίδιο ασφαλές αν ο Α κρυπτογραφούσε πρώτα το m και κατόπιν το υπέγραφε; Στην περίπτωση αυτή ο Α στέλνει στον Β το ζεύγος (z, v) όπου z η κρυπτογράφηση του m και v η υπογραφή του z. Ο Β επαληθεύει ότι το μήνυμα εστάλη από τον Α και κατόπιν αποκρυπτογραφώντας το z παίρνει το m. Το πρόβλημα που θα μπορούσε να προκύψει είναι το εξής. Ένας τρίτος, ο Γ, παρεμβαίνει στο δίαυλο επικοινωνίας του Α με τον Β, δεσμεύει το ζεύγος (z, v) και το αντικαθιστά με το (z, w), όπου w η υπογραφή του μηνύματος z με τη συνάρτηση υπογραφής του Γ. Στη συνέχεια ο Γ στέλνει το (z, w) στον Β, ο οποίος χρησιμοποιεί τη συνάρτηση επαλήθευσης του Γ ,και πιστοποιεί ότι το μήνυμα προέρχεται από αυτόν. Έπειτα το αποκρυπτογραφεί και παίρνει το m. Τελικά ο Β πιστεύει ότι αποστολέας του μηνύματος είναι ο Γ και όχι ο Α που πραγματικά το έστειλε. Γι αυτό είναι προτιμότερο να υπογράφεται πρώτα το μήνυμα και μετά να αποστέλλεται.

Τα σχήματα ψηφιακών υπογραφών χωρίζονται σε δύο μεγάλες κατηγορίες.

1. **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 υπογραφής. Το αρχικό μήνυμα είναι δηλαδή απαραίτητο για την επιβεβαίωση της γνησιότητας της υπογραφής. Τέτοια σχήματα είναι τα ElGamal, DSS και Schnorr.

2. **Σχήματα ψηφιακής υπογραφής με ανάκτηση του μηνύματος** (Digital Signature Schemes with message recovery), στα οποία το αρχικό μήνυμα μπορεί να ανακτηθεί από την ίδια την υπογραφή. Παραδείγματα τέτοιων σχημάτων είναι τα RSA, Rabin και Nyberg-Rueppel.

Τόσο τα συμμετρικά και ασύμμετρα κρυπτοσυστήματα, όσο και τα αντίστοιχα σχήματα ψηφιακών υπογραφών, είναι ευάλωτα σε επιθέσεις διάφορων τύπων. Σπάσιμο ενός σχήματος ψηφιακής υπογραφής μπορεί να γίνει με τους ακόλουθους τρόπους:

1. **ολικό σπάσιμο** (total break):ένας αντίπαλος είναι ικανός να υπολογίσει το ιδιωτικό κλειδί του υπογράφοντος ή να βρει έναν αποδοτικό αλγόριθμο υπογραφής λειτουργικά ισοδύναμο με τον έγκυρο.

2. **επιλεκτική πλαστογραφία** (selective forgery):ένας αντίπαλος μπορεί να δημιουργήσει μια έγκυρη υπογραφή για ένα μήνυμα που έχει επιλεγεί εκ των προτέρων. Η δημιουργία της υπογραφής δεν εμπλέκει άμεσα το νόμιμο υπογράφοντα.

3. **υπαρκτή πλαστογραφία** (existential forgery):ένας αντίπαλος μπορεί να πλαστογραφήσει μια υπογραφή για τουλάχιστον ένα μήνυμα. Με άλλα λόγια, καταφέρνει να δημιουργήσει ένα ζεύγος (m, s) με $ver_K(m,s)$= true, χωρίς να γνωρίζει τη συνάρτηση υπογραφής. Ο πλαστογράφος έχει λίγο η καθόλου έλεγχο του μηνύματος του οποίου την υπογραφή αποκτά και έτσι ίσως ο νόμιμος υπογράφων εμπλακεί στην απάτη.

Υπάρχουν δύο βασικές επιθέσεις εναντίον σχημάτων υπογραφής δημοσίου κλειδιού:

1. **επιθέσεις μόνο σε κλειδιά** (key-only attacks):σε αυτήν την περίπτωση ο αντίπαλος έχει στη διάθεσή του μόνο το δημόσιο κλειδί του υπογράφοντα.

2. **επιθέσεις σε μηνύματα** (message attacks):ένας αντίπαλος είναι σε θέση να εξετάσει υπογραφές που αντιστοιχούν είτε σε γνωστά είτε σε επιλεγμένα μηνύματα. Έτσι οι επιθέσεις σε μηνύματα μπορούν να υποδιαιρεθούν περαιτέρω σε:
    - **επίθεση σε γνωστό μήνυμα** (known-message attack):ένας αντίπαλος έχει στη διάθεσή του υπογραφές για ένα σύνολο μηνυμάτων, τα οποία του είναι γνωστά αλλά δεν έχουν επιλεγεί από αυτόν.

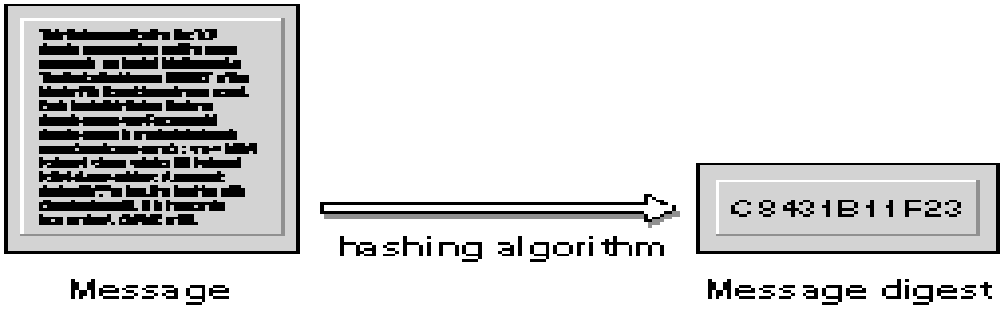
    - **επίθεση σε επιλεγμένο μήνυμα** (chosen-message attack):ένας αντίπαλος αποκτά έγκυρες υπογραφές του νόμιμου υπογράφοντα, για μια λίστα μηνυμάτων που έχουν επιλεγεί εκ των προτέρων. Η επίθεση αυτή καλείται μη προσαρμόσιμη (non-adaptive), γιατί τα μηνύματα επιλέγονται πριν ελεγχθεί οποιαδήποτε υπογραφή.

    - **προσαρμόσιμη επίθεση σε επιλεγμένο μήνυμα** (adaptive chosen-message attack): ένας αντίπαλος μπορεί να χρησιμοποιήσει τον υπογράφοντα ζητώντας υπογραφές μηνυμάτων οι οποίες εξαρτώνται είτε από το δημόσιο κλειδί του υπογράφοντα ή από προηγουμένως αποκτηθείσες υπογραφές και μηνύματα. Αυτός ο τρόπος επίθεσης είναι ο πιο δύσκολος στην πρόληψή του. Είναι κατανοητό ότι δοθέντων αρκετών μηνυμάτων και αντίστοιχων υπογραφών, ένας αντίπαλος θα μπορούσε να συμπεράνει έναν τρόπο ώστε στη συνέχεια να πλαστογραφήσει μια υπογραφή της επιλογής του. Ενώ μια προσαρμόσιμη επίθεση σε επιλεγμένο μήνυμα ίσως είναι πρακτικά ανέφικτη, ένα καλώς σχεδιασμένο σχήμα υπογραφής πρέπει να προλαμβάνει και αυτή την πιθανότητα.

Το επίπεδο ασφαλείας που απαιτείται σε ένα σχήμα ψηφιακής υπογραφής μπορεί να ποικίλλει ανάλογα με την εφαρμογή για την οποία προορίζεται. Για παράδειγμα, σε περιπτώσεις όπου ένας αντίπαλος είναι ικανός να εξαπολύσει μόνο μια επίθεση κλειδιού, ίσως να επαρκεί ο σχεδιασμός του σχήματος ώστε να αποκλείεται απόπειρα επιλεκτικής πλαστογραφίας. Σε περιπτώσεις όπου ο αντίπαλος είναι ικανός να επιτεθεί σε μήνυμα είναι μάλλον απαραίτητη η προφύλαξη του σχήματος απέναντι στην πιθανότητα υπαρκτής πλαστογραφίας.

1.4 Συναρτήσεις κατακερματισμού (hash functions)

Σ' αυτή την ενότητα θα ασχοληθούμε με τις συναρτήσεις κατακερματισμού οι οποίες έχουν πολλές εφαρμογές στην κρυπτογραφία, με κυριότερη την ενίσχυση της ασφάλειας των ψηφιακών υπογραφών. Καλούμε συνάρτηση κατακερματισμού κάθε συνάρτηση h: D→R όπου το σύνολο R είναι πεπερασμένο σύνολο και |D|>|R|, ενώ δεν αποκλείεται D= ∞. Μια τέτοια συνάρτηση δέχεται ως είσοδο ένα οσοδήποτε μεγάλο μήνυμα και στην έξοδο δίνει ένα αλφαριθμητικό σταθερού μήκους. Πιο συγκεκριμένα, μια συνάρτηση κατακερματισμού h αντιστοιχίζει σειρές bit μεταβλητού μεγέθους σε ακολουθία συγκεκριμένου μεγέθους (συνήθως 160 bits). Η ακολουθία αυτή συμβολίζεται με h(x) και λέγεται σύνοψη του μηνύματος (message digest). Το ενδιαφέρον με τις συναρτήσεις τύπου hash είναι ότι η παραμικρή αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης. Από αυτές, εμείς θα εξετάσουμε το είδος που μας ενδιαφέρει άμεσα, τις **κρυπτογραφικές συναρτήσεις κατακερματισμού.**



Σχήμα 1.4.1 Σύνοψη μηνύματος με τη χρήση αλγόριθμου κατακερματισμού

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού πρέπει να ικανοποιούν τις παρακάτω ιδιότητες:

1. **συμπίεση:** η είσοδος είναι οποιουδήποτε μήκους ενώ η έξοδος έχει περιορισμένο σταθερό μήκος.

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

3. **αντίσταση πρώτου ορίσματος-μη αντιστρεψιμότητα:** δεδομένης της h και ενός στοιχείου y ∈ R, είναι υπολογιστικά ανέφικτο να βρεθεί x ∈ D τέτοιο ώστε h(x)= y. Να σημειωθεί ότι δε γνωρίζουμε αν υπάρχουν συναρτήσεις μονής κατεύθυνσης. Υπάρχουν όμως συναρτήσεις των οποίων οι τιμές υπολογίζονται εύκολα, αλλά δε γνωρίζουμε αλγόριθμο πολυωνυμικού χρόνου για την αντιστροφή τους.

4. **αντίσταση δεύτερου ορίσματος:** για δοθέν όρισμα x_1 είναι υπολογιστικά ανέφικτο να βρεθεί όρισμα x_2 τέτοιο ώστε $x_1 \neq x_2$ και $h(x_1)= h(x_2)$. Με άλλα λόγια είναι υπολογιστικά ανέφικτη η εύρεση σύγκρουσης (collision) για δοθέν x_1. Σε αυτή την περίπτωση η συνάρτηση κατακερματισμού καλείται ασθενώς ανθεκτική σε συγκρούσεις.

Οι συναρτήσεις κατακερματισμού μονής κατεύθυνσης αποτελούν την κινητήριο δύναμη της σύγχρονης κρυπτογραφίας. Διευκολύνουν τα συμβαλλόμενα μέρη καθώς οι κρυπτογραφικές διαδικασίες εφαρμόζονται στη σύνοψη του μηνύματος, η οποία είναι μικρότερη και πιο εύκολη στη διαχείριση. Επιπλέον, βοηθούν στο να ελεγχθεί η ακεραιότητα των δεδομένων. Αν το μήνυμα που αποστέλλεται έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λαμβάνεται παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοση έχει αλλοιωθεί. Τέλος, ένα message digest μπορεί να δημοσιοποιηθεί ή να υποκλαπεί χωρίς να αποκαλύπτεται το περιεχόμενο του αυθεντικού κειμένου. Έτσι η χρήση τους θεωρείται αναγκαία σχεδόν σε κάθε σχήμα ψηφιακής υπογραφής. Αυτό το γεγονός οδήγησε στην ανάπτυξη μιας σειράς συναρτήσεων κατακερματισμού με σημαντικότερες τις HMAC, MD KAI SHA.

Παρ' όλες τις κρυπτογραφικές τους ιδιότητες, οι συναρτήσεις κατακερματισμού έχουν και κάποια μειονεκτήματα. Καθώς τα message digests είναι καθορισμένου μήκους, δεν είναι τόσο απεριόριστα στο πλήθος όσο όλα τα δυνατά μηνύματα, με αποτέλεσμα άλλες επιθέσεις εναντίον σχημάτων ψηφιακής υπογραφής που χρησιμοποιούν συναρτήσεις τύπου hash. Μερικές συναρτήσεις μάλιστα, παράγουν έξοδο μικρού μήκους, με αποτέλεσμα να μπορεί εύκολα να βρεθεί άλλο μήνυμα με ίδια σύνοψη. Αυτό τις καθιστά ευάλωτες σε επιθέσεις birthday attack.

Birthday attack

Η birthday attack ανήκει στις επιθέσεις ωμής βίας και στηρίζεται στο παράδοξο των γενεθλίων, σύμφωνα με το οποίο σε μια τυχαία επιλογή 23 ανθρώπων, η πιθανότητα δύο από αυτούς να έχουν γενέθλια την ίδια μέρα είναι τουλάχιστον 0,5 (για την ακρίβεια 0,507). Αυτό αποδεικνύεται ως εξής: θα υπολογίσουμε την πιθανότητα και τα 23 άτομα να έχουν γενέθλια διαφορετική μέρα γενεθλίων. Τότε, το πρώτο άτομο δεσμεύει μία μέρα άρα το δεύτερο έχει πιθανότητα (1-1/365) να έχει διαφορετική μέρα γενεθλίων απ' όλους. Για το τρίτο άτομο, είναι δύο οι κατειλημμένες μέρες και (1-2/365) η αντίστοιχη πιθανότητα. Συνεχίζοντας με τον ίδιο τρόπο, η ζητούμενη πιθανότητα ισούται με (1-1/365)×(1-2/365)…..(1-22/365)= 0,493. Άρα η πιθανότητα τουλάχιστον δύο να έχουν γενέθλια την ίδια μέρα είναι 1-0,493= 0,507.

Πιο γενικά, έστω ότι έχουμε n αντικείμενα με n μεγάλο, και r άτομα. Αν το κάθε άτομο επιλέξει ένα αντικείμενο, τότε η πιθανότητα τουλάχιστον δύο άτομα να διαλέξουν το ίδιο είναι κατά προσέγγιση ίση με $1-e^{-r^2/2N}$. Για $r \approx 1.177\sqrt{N}$ η πιθανότητα είναι τουλάχιστον 50%. Ομοίως , αν μια συνάρτηση f παράγει μια τιμή μεταξύ n διαφορετικών ισοπίθανων τιμών, τότε υπολογίζοντας την τιμή της συνάρτησης για περίπου $1{,}177\sqrt{N}$ εισόδους αναμένεται να βρούμε ένα ζεύγος (x_1, x_2) τέτοιο ώστε $f(x_1) = f(x_2)$. Έτσι, το παράδοξο των γενεθλίων εφαρμόζεται στην κρυπτογραφία σαν μέθοδος εύρεσης συγκρούσεων μιας συνάρτησης κατακερματισμού.

Επομένως, ένας ανέντιμος υπογράφοντας που παρέχει την υπογραφή του στο έγγραφο x_1 μπορεί στη συνέχεια να το αρνηθεί ισχυριζόμενος ότι το έγγραφο που υπέγραψε ήταν το x_2 (τα x_1 και x_2 αποτελούν μία σύγκρουση της συνάρτησης κατακερματισμού). Η επίθεση μπορεί να χρησιμοποιηθεί και από έναν ανέντιμο επαληθευτή που πείθει ένα ανυποψίαστο άτομο να υπογράψει το έγγραφο x_1 και μετά ισχυρίζεται ότι η υπογραφή αφορά στο έγγραφο x_2.

Κεφάλαιο 2

Το κρυπτοσύστημα και το σχήμα υπογραφής RSA

Στο κεφάλαιο αυτό περιγράφουμε το RSA, ένα από τα πρώτα συστήματα ασύμμετρης κρυπτογραφίας, που παρέχει τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Είναι σήμερα το πιο διαδεδομένο σύστημα και οφείλει το όνομά του στα αρχικά των μελετητών που το δημοσίευσαν το 1978 Ron Rivest, Adi Shamir και Leonard Adleman.

2.1 Το κρυπτοσύστημα RSA

Υπενθυμίζουμε ότι το κρυπτοσύστημα RSA είναι σύστημα δημοσίου κλειδιού, που σημαίνει ότι ο μετασχηματισμός κρυπτογράφησης αποτελεί δημόσια πληροφορία, ενώ ο μετασχηματισμός αποκρυπτογράφησης παραμένει κρυφός και γνωστός μόνο στον παραλήπτη.

Το σύστημα πραγματοποιεί υπολογισμούς στην ομάδα των ακεραίων modulo **n**, δηλαδή στο σύνολο $\mathbb{Z}_n = \{0, 1, 2,\ldots, n-1\}$, όπου n είναι το γινόμενο δύο μεγάλων τυχαία επιλεγμένων και διακεκριμένων πρώτων αριθμών **p**,**q** (μεγαλύτεροι από 100-ψήφιο/330 bits).

Το κλειδί K του συστήματος είναι η πεντάδα **K= (n, p, q, a, b)**.

Ο αριθμός **b** καλείται **εκθέτης κωδικοποίησης** (encryption exponent) και επιλέγεται έτσι ώστε $1 < b < \varphi(n)$ και ΜΚΔ$(b, \varphi(n))= 1$, όπου φ η συνάρτηση του Euler (βλ. παράρτημα Α).

Ο αριθμός **a** καλείται **εκθέτης αποκωδικοποίησης** (decryption exponent) και υπολογίζεται ώστε $ab \equiv 1 \bmod \varphi(n)$. Είναι δηλαδή ο πολλαπλασιαστικός αντίστροφος του b modulo φ(n).

Το ζεύγος **(n, b)** αποτελεί το δημόσιο κλειδί (public key) ενώ το ζεύγος **(p, q, a)** αποτελεί το ιδιωτικό κλειδί (private key).

Ας δούμε όμως πιο αναλυτικά τη διαδικασία. Έστω ότι ο Α θέλει να στείλει στον Β ένα μυστικό μήνυμα.

Παραγωγή κλειδιού:

Ο Β επιλέγει δύο μεγάλους πρώτους αριθμούς p, q, υπολογίζει το γινόμενό τους $n= pq$ και τη συνάρτηση Euler $\varphi(n)= (p-1)(q-1)$. Διαλέγει εκθέτη κωδικοποίησης b με $1 < b < \varphi(n)$ τέτοιο ώστε ΜΚΔ$(b,\varphi(n))= 1$ και υπολογίζει τον εκθέτη αποκωδικοποίησης a ως εξής:

$$ab \equiv 1 \bmod \varphi(n) \Leftrightarrow a \equiv b^{\varphi(\varphi(n))-1} \bmod \varphi(n)$$

Πράγματι, αν πολλαπλασιάσουμε με b την τελευταία σχέση, έχουμε:

$a \equiv b^{\varphi(\varphi(n))} \bmod \varphi(n) \equiv 1 \bmod \varphi(n)$, όπως προκύπτει από το θεώρημα του Euler (βλ. παράρτημα Α) και το ότι ΜΚΔ$(b, \varphi(n))= 1$. Στην πράξη, ο a υπολογίζεται εύκολα με τον επεκτεταμένο ευκλείδειο αλγόριθμο (βλ. παράρτημα Α). Ο Β τελικά δημοσιοποιεί το ζεύγος (n, b) και κρατά μυστικό το (p, q, a).

Διαδικασία κρυπτογράφησης:

Υποθέτουμε ότι ο Α θέλει να στείλει στον Β το μήνυμα Μ. Πρώτα, το μετατρέπει σε ένα θετικό ακέραιο m στο δεκαδικό ή στο δυαδικό σύστημα. Πρέπει $1 < m < n$ και ΜΚΔ(m, n)= 1 (η πιθανότητα να μην ισχύει κάτι τέτοιο είναι $1/10^{100}$). Στη συνέχεια υψώνει τον m στον εκθέτη κωδικοποίησης b και καταλήγει στο κρυπτοκείμενο $z= E_K(m)= m^b \bmod n$

Διαδικασία αποκρυπτογράφησης:

Ο Β λαμβάνει το κρυπτοκείμενο z, υψώνει το z στον εκθέτη αποκωδικοποίησης a και ανακτά το μήνυμα $m= D_K(z)= z^a \bmod n$.

Απόδειξη:
Αφού $ab \equiv 1 \bmod \varphi(n)$, υπάρχει ακέραιος κ τέτοιος ώστε $ab-1= \kappa\varphi(n)$.
Τότε $D_K(z)= z^a \equiv m^{ab} \equiv m^{\kappa\varphi(n)+1} \equiv m^{\kappa\varphi(n)} m \equiv (m^{\varphi(n)})^{\kappa} m \bmod n \equiv 1^{\kappa} m \bmod n= m \bmod n$, όπως προκύπτει από το θεώρημα του Euler και το ότι ΜΚΔ(m, n)= 1.

Παράδειγμα 2.1.1: Η Pat επιλέγει πρώτους αριθμούς p= 101 και q= 113. Άρα n= pq= 11413 το modulo της κρυπτογράφησης και $\varphi(n)= (p-1)(q-1)= 11200$. Αφού $11200=2^6 5^2 7$ πρέπει να διαλέξει εκθέτη κωδικοποίησης που να μη διαιρείται από τους 2,5 ή 7. Επιλέγει έτσι b= 3533. Τότε:

$$a= 3533^{-1} \bmod 11200= 6597.$$

Η Pat δημοσιοποιεί τους n= 11413 και b= 3533 σε έναν κατάλογο, ενώ ο a= 6597 είναι ο μυστικός της εκθέτης αποκωδικοποίησης. Έστω ότι ο Bob θέλει να κρυπτογραφήσει το μήνυμα 9726 και να το στείλει στην Pat. Υπολογίζει

$$9726^{3533} \bmod 11413= 5671$$

και μεταδίδει το κρυπτοκείμενο 5671. Όταν η Pat το λάβει, χρησιμοποιεί το ιδιωτικό της κλειδί και υπολογίζει

$$5671^{6597} \bmod 11413= 9726,$$

ανακτώντας έτσι το μήνυμα.

Όποιος λοιπόν θέλει να λάβει ένα μυστικό μήνυμα, επιλέγει μια πεντάδα K=(n, p, q, a, b) όπως παραπάνω και δημοσιοποιεί το δημόσιο κλειδί του (n, b). Οποιοσδήποτε μπορεί τώρα να του στείλει ένα κρυπτογραφημένο μήνυμα. Μόνο όμως ο κάτοχος του αυθεντικού ιδιωτικού κλειδιού (p, q, a) μπορεί να αποκρυπτογραφήσει και να αναγνώσει το μήνυμα. Η εύρεση του ιδιωτικού κλειδιού a από το δημόσιο κλειδί b είναι εξαιρετικά δύσκολη έως και αδύνατη, καθώς απαιτεί την παραγοντοποίηση του μεγάλου αριθμού n σε πρώτους παράγοντες. Στη δυσκολία αυτού του προβλήματος έγκειται και η ασφάλεια του RSA. Με τα σημερινά δεδομένα η παραγοντοποίηση ακεραίου μεγαλύτερου από 200-ψήφιο παραμένει πρακτικά ανέφικτη. Όμως οι αλγόριθμοι γίνονται συνεχώς αποτελεσματικότεροι και οι υπολογιστές ταχύτεροι.

2.2 Το σχήμα υπογραφής RSA

Από τα πλέον διαδεδομένα σχήματα ψηφιακής υπογραφής είναι το σχήμα υπογραφής RSA, βασισμένο στο κρυπτοσύστημα RSA. Η ευρεία χρήση του οφείλεται στο γεγονός ότι δεν είναι παρά μια εφαρμογή του κρυπτοσυστήματος, με αντιστροφή του ρόλου των κλειδιών.

Ας θεωρήσουμε το σύστημα RSA με δημόσιο κλειδί (n, b) και ιδιωτικό κλειδί (p, q, a). Τότε οι συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης ορίζονται αντίστοιχα από τις σχέσεις: $E_K(m)= m^b$ και $D_K(m)= m^a$, $\forall$ μήνυμα $m \in M$. Παρατηρούμε ότι $D_K(E_K(m))= E_K(D_K(m))= m$. Ο μετασχηματισμός κρυπτογράφησης είναι δηλαδή αμφιμονοσήμαντος. Έτσι, το κρυπτοσύστημα RSA μπορεί να χρησιμοποιηθεί για την κατασκευή ενός σχήματος ψηφιακής υπογραφής. Σ΄ αυτή την περίπτωση ο χώρος των μηνυμάτων και ο χώρος των υπογραφών είναι το σύνολο $\mathbb{Z}_n=\{0,1,2,\ldots,n-1\}$. Συνάρτηση υπογραφής sig_K είναι η D_K ενώ συνάρτηση επαλήθευσης ver_K είναι η E_K.

Ας δούμε τώρα συνοπτικά τις διαδικασίες παραγωγής κλειδιού, υπογραφής και επαλήθευσης, υποθέτοντας ότι ο Α θέλει να στείλει στον Β μήνυμα υπογεγραμμένο με τη μέθοδο RSA:

Παραγωγή κλειδιού:

Η διαδικασία παραγωγής κλειδιού για το σχήμα υπογραφής RSA είναι ίδια με αυτή του κρυπτοσυστήματος. Ο Α επιλέγει κλειδί K= (n, p, q, a, b), δημοσιοποιεί το ζεύγος (n, b) και κρατά μυστικό το (p, q, a).

Δημιουργία υπογραφής:

Ο Α μετατρέπει το μήνυμα σε ένα θετικό ακέραιο m στο δεκαδικό ή στο δυαδικό σύστημα, με $m \in [0, n-1]$ (βλ. παράρτημα Α). Στη συνέχεια υπολογίζει το $s= sig_K(m)= D_K(m)= m^a \bmod n$. Το s είναι η ψηφιακή υπογραφή του. Το ζεύγος (m, s) μεταδίδεται μέσω του καναλιού στον Β.

Επαλήθευση υπογραφής:

Ο Β αποσπά από το ζεύγος (m,s) την ψηφιακή υπογραφή s την οποία αποκρυπτογραφεί με το δημόσιο κλειδί του Α, καταλήγοντας στο $z= E_K(s)= s^b \bmod n$. Αν z= m τότε δέχεται την υπογραφή ως γνήσια. Διαφορετικά, την απορρίπτει.

Παράδειγμα 2.2.1: υποθέτουμε ότι ο Α επιθυμεί να στείλει ένα υπογεγραμμένο μήνυμα στον Β. Θεωρεί τους πρώτους p= 79, q= 101 και υπολογίζει n=pq=7979. Καθώς φ(n)= 7800, επιλέγει τον ακέραιο b= 7 ο οποίος είναι πρώτος προς τον φ(n). Κατόπιν υπολογίζει τον αντίστροφο του b (modφ(n)) ο οποίος είναι ο a= 3343. Κρατά τον a μυστικό και δημοσιοποιεί το ζεύγος (7979, 7) το οποίο ορίζει τη συνάρτηση επαλήθευσης. Στη συνέχεια υπογράφει το μήνυμα m= 123, κάνοντας τον υπολογισμό: $123^{3343} \equiv 5660 \pmod{7979}$, και στέλνει στον Β το ζεύγος (123,5660). Ο Β επαληθεύει την υπογραφή υπολογίζοντας: $5660^7 \equiv 123 \pmod{7979}$.

Ας δούμε στη συνέχεια μερικές προσβολές του σχήματος ψηφιακής υπογραφής RSA. Ας υποθέσουμε ότι η συνάρτηση επαλήθευσης του Α ορίζεται από το δημόσιο κλειδί (n,b). Τότε ο Γ επιλέγει μια τυχαία υπογραφή $s \in S$ και υπολογίζει το αντίστοιχο μήνυμα $m= s^b \bmod n$. Στη συνέχεια στέλνει στον Β το ζεύγος (m ,s) προφασιζόμενος ότι είναι ο Α. Το m είναι βέβαια μια τυχαία ακολουθία. Εντούτοις, αν έχει κάποια σημασία για τον Β, αυτός εφαρμόζει τη συνάρτηση επαλήθευσης και αφού είναι αληθής βεβαιώνεται ότι το μήνυμα προήλθε από

τον Α. Ο Γ κατάφερε τελικά να τον εξαπατήσει πραγματοποιώντας υπαρκτή πλαστογράφηση με επίθεση μόνο στο δημόσιο κλειδί του Α.

Ευάλωτο σε επιθέσεις καθιστά το RSA και η πολλαπλασιαστική του ιδιότητα, σύμφωνα με την οποία αν $s_1= m_1^a \bmod n$ και $s_2= m_2^a \bmod n$ οι υπογραφές των μηνυμάτων m_1 και m_2 αντίστοιχα, τότε $s_1s_2= (m_1m_2)^a \bmod n$. Δηλαδή, αν είναι γνωστές οι υπογραφές s_1 και s_2 των μηνυμάτων m_1 και m_2 αντίστοιχα, τότε υπολογίζουμε εύκολα την υπογραφή s_1s_2 του m_1m_2.

Υποθέτουμε ότι ο Γ κατάφερε να υποκλέψει τα ζεύγη (m_1, s_1) και (m_2, s_2) που έστειλε ο Α στον Β. Υπολογίζοντας $s=s_1s_2 \bmod n$ αποκτά μια έγκυρη υπογραφή για το μήνυμα $m= m_1m_2 \bmod n$, μεταδίδει στον Β το ζεύγος (m, s) κι αυτός επαληθεύει το μήνυμα και πείθεται ότι προήλθε από τον Α. Ο Γ κατάφερε και πάλι να εξαπατήσει τον Β, πραγματοποιώντας υπαρκτή πλαστογραφία με επίθεση στο γνωστό μήνυμα $m= m_1m_2$.

Η πολλαπλασιαστική ιδιότητα μπορεί να χρησιμοποιηθεί και ως εξής: έστω ότι ο Γ θέλει να αποκτήσει μια έγκυρη υπογραφή του Α για το μήνυμα m που έχει επιλεγεί εκ των προτέρων. Τότε βρίσκει μηνύματα $m_1, m_2 \in Z_n$ τέτοια ώστε $m= m_1m_2 \bmod n$. Ζητά από τον Α τις υπογραφές s_1 και s_2 των μηνυμάτων m_1 και m_2 και υπολογίζει την υπογραφή $s= s_1s_2 \bmod n$. Στέλνει το ζεύγος (m, s) στον Β, ο οποίος και το δέχεται. Καταφέρνει έτσι να υποδυθεί τον Α και να ξεγελάσει τον Β. Αυτού του τύπου η επίθεση χαρακτηρίζεται ως επιλεκτική πλαστογραφία με επίθεση στο επιλεγμένο μήνυμα m.

Ένα μέσο προστασίας από τις παραπάνω επιθέσεις είναι η χρήση μιας συνάρτησης κατακερματισμού h. Σ' αυτή την περίπτωση, η υπογραφή s του μηνύματος m είναι

$$s= h(m)^a \bmod n.$$

Ο Α στέλνει στον Β το ζεύγος (m, s). Ο Β αποσπά την υπογραφή και την αποκρυπτογραφεί, καταλήγοντας έτσι στη σύνοψη h(m) του μηνύματος, ήτοι:

$$h(m)= s^b \bmod n.$$

Έπειτα εφαρμόζει τη δημόσια γνωστή συνάρτηση κατακερματισμού στο μήνυμα που έλαβε και δημιουργεί τη σύνοψη $h(m)^*$. Συγκρίνει τις δύο συνόψεις και αν βρεθούν ίδιες, τότε δέχεται το μήνυμα.

Αυτή η διαδικασία καθιστά τις προαναφερθείσες προσβολές σχεδόν αδύνατες. Πράγματι, αν ο ανέντιμος Γ πάρει ένα s και υπολογίσει την τιμή s^b, θα πρέπει να βρει m τέτοιο ώστε

$$h(m)= s^b \bmod n,$$

πράγμα που είναι υπολογιστικά ανέφικτο (όπως προκύπτει από τις ιδιότητες των συναρτήσεων hash). Επίσης, αν ο Γ έχει στα χέρια του τις $s_1= h(m_1)^a \bmod n$ και $s_2= h(m_2)^a \bmod n$, τότε η $s= s_1s_2\equiv h(m_1)^a\, h(m_2)^a \bmod n$ είναι μεν η υπογραφή του message digest $h(m_1)\, h(m_2) \bmod n$, εξαιρετικά δύσκολο όμως να βρεθεί το αρχικό μήνυμα $m= m_1m_2 \bmod n$ (όπως πάλι προκύπτει από τις ιδιότητες των hash συναρτήσεων).

Ένας εναλλακτικός τρόπος προστασίας είναι η **συνάρτηση πλεονάζουσας πληροφορίας** (redundancy function). Πρόκειται για μια δημόσια γνωστή αντιστρέψιμη προβολή από το χώρο Μ των απλών κειμένων σε έναν υπόχωρό του με συγκεκριμένες ιδιότητες. Ένα παράδειγμα τέτοιας συνάρτησης είναι η μετατροπή ενός δυαδικού κειμένου σε τέτοια μορφή ώστε ανάμεσα σε κάθε 8 bit να υπάρχει η λέξη 10101. Μια τυχαία επιλεγμένη συμβολοακολουθία από το χώρο των υπογραφών είναι πρακτικά απίθανο να δώσει ένα μήνυμα που να έχει τις ιδιότητες που προσδιορίζει η συνάρτηση πλεονάζουσας πληροφορίας σε τυχαίο μήνυμα.

Κεφάλαιο 3
Το κρυπτοσύστημα και το σχήμα υπογραφής ElGamal

3.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο είδαμε ότι η ασφάλεια του κρυπτοσυστήματος RSA και κατ' επέκταση του σχήματος ψηφιακής υπογραφής RSA, έγκειται στην δυσκολία της παραγοντοποίησης ενός μεγάλου ακεραίου σε γινόμενο πρώτων. Με την εξέλιξη της κρυπτογραφίας επινοήθηκαν κρυπτοσυστήματα που επίσης στήριξαν την ασφάλειά τους σε δισεπίλυτα προβλήματα της θεωρίας αριθμών, όπως το **Πρόβλημα Διακριτού Λογαρίθμου** (DLP) και το **Πρόβλημα των Diffie-Hellman** (DHP). Στο κεφάλαιο αυτό παρουσιάζουμε το σχήμα υπογραφής ElGamal και το Πρότυπο Ψηφιακής Υπογραφής. Αυτά παρουσιάζονται στο $\mathbb{Z}^*_p$ για μεγάλο πρώτο p, αλλά οι μηχανισμοί τους μπορούν να γενικευθούν σε οποιαδήποτε πεπερασμένη κυκλική ομάδα.

3.2 Το Πρόβλημα Διακριτού Λογαρίθμου (Discrete Logarithm Problem-DLP)

Προτού ορίσουμε το πρόβλημα υπενθυμίζουμε ότι είναι εύκολο για κάποιον να υπολογίσει το b^x για μεγάλο x σε σχετικά μικρό χρόνο. Αν όμως μας δοθεί αριθμός y ο οποίος είναι της μορφής b^x με b γνωστό, είναι εξίσου εύκολο να υπολογίσουμε το μοναδικό x τέτοιο ώστε $y=b^x$; Με άλλα λόγια, υπάρχει αποδοτικός αλγόριθμος που να το υπολογίζει; Η επίλυση της παραπάνω εξίσωσης στο $\mathbb{Z}^*_p$, για p πρώτο, είναι το Πρόβλημα του Διακριτού Λογαρίθμου και η απάντηση στο τελευταίο ερώτημα είναι αρνητική αν επιλέξουμε κατάλληλα το σώμα στο οποίο εργαζόμαστε, δηλαδή αν το p έχει τουλάχιστον 150 ψηφία και το p-1 τουλάχιστον έναν μεγάλο πρώτο παράγοντα.

Ορισμός 3.2.1: έστω G μια πεπερασμένη κυκλική ομάδα τάξεως n, g ένας γεννήτορας της G και $\beta \in G$. Ο **Διακριτός Λογάριθμος** του β με βάση g, συμβολίζεται με $\log_g\beta$ και είναι ο μοναδικός ακέραιος x, με $0 \leq x \leq n-1$ τέτοιος ώστε $\beta = g^x$.

Παράδειγμα 3.2.1: έστω ο πρώτος p= 97. Τότε το σύνολο $\mathbb{Z}^*_{97}$ είναι κυκλική ομάδα τάξεως n= 96. Ένας γεννήτορας της $\mathbb{Z}^*_{97}$ είναι ο g=5. Αφού $5^{32}= 35$, έχουμε ότι $\log_5 35 =32$ στο $\mathbb{Z}^*_{97}$.

Ορισμός 3.2.2 (πρόβλημα διακριτού λογαρίθμου): δοθέντος ενός πρώτου p, ενός γεννήτορα g του $\mathbb{Z}^*_p$ και ενός στοιχείου $\beta \in \mathbb{Z}^*_p$, να βρεθεί ακέραιος x με $0 \leq x \leq p-2$, τέτοιος ώστε $g^x \equiv \beta \bmod p$.

Πρόταση 3.2.1: Η δυσκολία του DLP είναι ανεξάρτητη από την επιλογή του γεννήτορα g του $\mathbb{Z}^*_p$.

Απόδειξη: έστω g και g΄ δύο γεννήτορες του $\mathbb{Z}^*_p$ και β ∈ $\mathbb{Z}^*_p$. Έστω x= $\log_g\beta$, y= $\log_{g'}\beta$ και z= $\log_g g'$. Τότε $g^x = \beta = g'^y = (g^z)^y$ δηλαδή x= zy mod p.

Αλλά τότε y= x z^{-1}mod p ή $\log_{g'}\beta = (\log_g\beta)(\log_g g')^{-1}$modp.

Δείξαμε λοιπόν, ότι αν μπορούμε να υπολογίσουμε το διακριτό λογάριθμο σε μια βάση g τότε μπορούμε να τον υπολογίσουμε σε οποιαδήποτε βάση g΄ όπου g, g΄ γεννήτορες του $\mathbb{Z}^*_p$.

3.3 Το πρόβλημα των Diffie-Hellman (Diffie-Hellman Problem-DHP)

Το πρόβλημα διατυπώθηκε το 1976 από τους Whitfield Diffie και Martin Hellman σε μια δημοσίευση με τίτλο “New Directions in Cryptography” που αποτέλεσε σταθμό στην ιστορία της σύγχρονης κρυπτογραφίας.

Ορισμός 3.3.1: το πρόβλημα των Diffie-Hellman (DHP) είναι το εξής: Δοθέντος ενός πρώτου αριθμού p, ενός γεννήτορα g του $\mathbb{Z}^*_p$ και των στοιχείων g^β mod p και g^γ mod p ∈ $\mathbb{Z}^*_p$, να βρεθεί το $g^{\beta\gamma}$ mod p.

Παρατήρηση: αν θέσω x= g^γ mod p και y =g^β mod p, τότε γ= $\log_g x$ και y= $\log_g y$. Επομένως αν μπορούμε να λύσουμε το DLP, μπορούμε να υπολογίσουμε τα β, γ άρα και το $g^{\beta\gamma}$ mod p.

Πόρισμα 3.3.1: το DHP ανάγεται με πολυωνυμικό αλγόριθμο στο DLP.

3.4 Το κρυπτοσύστημα ElGamal

Το κρυπτοσύστημα ElGamal είναι ένα από τα πιο γνωστά κρυπτοσυστήματα δημοσίου κλειδιού και στηρίζεται στο DHP. Ας δούμε συνοπτικά τις διαδικασίες παραγωγής κλειδιού, κρυπτογράφησης και αποκρυπτογράφησης:
Υποθέτουμε ότι ο Α θέλει να στείλει ένα κρυπτογραφημένο μήνυμα στον Β.

Παραγωγή κλειδιού:

- Ο Β επιλέγει έναν μεγάλο πρώτο p και έναν γεννήτορα g του $\mathbb{Z}^*_p$ (βλ. παράρτημα).
- Επιλέγει έναν τυχαίο ακέραιο α, με 1 ≤ α ≤ p-2 και υπολογίζει το g^α mod p.

Το δημόσιο κλειδί του Β είναι το (p, g, g^α) και το ιδιωτικό κλειδί είναι το α.

Κρυπτογράφηση:

- Ο Α βρίσκει το δημόσιο κλειδί του Β.
- Μετατρέπει το μήνυμα σε ένα θετικό ακέραιο m στο δεκαδικό ή το δυαδικό σύστημα με $0 \leq m \leq p-1$.
- Επιλέγει έναν τυχαίο ακέραιο κ με $1 \leq \kappa \leq p-2$.
- Υπολογίζει τα $\gamma = g^{\kappa} \bmod p$ και $\delta = m\,(g^{\alpha})^{\kappa} \bmod p$.
- Στέλνει στον Β το κρυπτογραφημένο κείμενο (γ, δ).

Αποκρυπτογράφηση:

- Ο Β χρησιμοποιεί το ιδιωτικό του κλειδί και υπολογίζει το $\gamma^{-\alpha} = g^{-\alpha\kappa}$.
- Ανακτά το m υπολογίζοντας το: $\gamma^{-\alpha}\,\delta \bmod p = g^{-\alpha\kappa}\, m\, g^{\alpha\kappa} \bmod p = m \bmod p$. Για τον υπολογισμό του $\gamma^{-\alpha}$ αρκεί να υπολογίσει κανείς το $\gamma^{p-1-\alpha}$.

Παράδειγμα 3.4.1: Ο Β επιλέγει πρώτο p= 2579 και γεννήτορα g= 2 του $\mathbb{Z}^*_{2579}$. Στη συνέχεια επιλέγει το ιδιωτικό του κλειδί α= 765 και υπολογίζει το $g^{\alpha} \bmod p = 2^{765} \bmod 2579 = 949$. Το δημόσιο κλειδί του είναι το (2579, 2, 949).

Έστω ότι ο Α θέλει να στείλει στον Β το μήνυμα m= 1299. Επιλέγει τυχαίο κ= 853 και υπολογίζει τα:

$$\gamma = 2^{853} \bmod 2579 = 435 \text{ και } \delta = 1299 \cdot 949^{853} \bmod 2579 = 2396.$$

Έπειτα στέλνει στον Β το μήνυμα (435, 2396)

Ο Β λαμβάνει το μήνυμα και υπολογίζει το:

$$\gamma^{p-1-\alpha} = 435^{1813} \bmod 2579 = 1980$$

τέλος, υπολογίζει το $1980 \cdot 396 \bmod 2579 = 1299$ και ανακτά το m.

Η ασφάλεια του κρυπτοσυστήματος ElGamal βασίζεται όπως είπαμε, στη δυσκολία του DHP. Από το 1996 προτείνεται ένα ελάχιστο 768 bits για τα modulo p της κρυπτογράφησης. Η ασφάλεια του ενισχύεται επίσης από το γεγονός ότι η συνάρτηση κρυπτογράφησης εξαρτάται από τον τυχαία επιλεγμένο κ. Έτσι, στο ίδιο μήνυμα αντιστοιχούν πολλά διαφορετικά κρυπτογραφήματα. Είναι ωστόσο σημαντικό να επιλέγονται τυχαίοι κ για κάθε μήνυμα που στέλνεται, διαφορετικά, ένας αντίπαλος είναι σε θέση να ανακτήσει επόμενα μηνύματα.

Απόδειξη: ας υποθέσουμε ότι ο Α μεταδίδει κρυπτογραφημένα μηνύματα στον Β με τη μέθοδο ElGamal, αφού πρώτα έχει αποκτήσει το δημόσιο κλειδί του (p, g ,g^{α}). Αν για τα μηνύματα m_1, m_2 που θέλει να αποστείλει, επιλέξει τον ίδιο ακέραιο $\kappa \in \mathbb{Z}_{p-1}$, θα έχουμε:

$$\gamma_1 = g^{\kappa} \bmod p \ , \ \delta_1 = m_1 (g^{\alpha})^{\kappa} \bmod p$$

$$\gamma_2 = g^{\kappa} \bmod p \ , \ \delta_2 = m_2 (g^{\alpha})^{\kappa} \bmod p$$

Τότε όμως $\delta_2 \delta_1^{-1} = m_2 m_1^{-1} \bmod p \Rightarrow m_2 = \delta_2 \delta_1^{-1} m_1 \bmod p$. Έτσι, αν ένας αντίπαλος έχει υποκλέψει το (γ_1, δ_1) και γνωρίζει το m_1, τότε μπορεί να ανακτήσει ένα άλλο μήνυμα m_2.

3.5 Το σχήμα υπογραφής ElGamal

Το σχήμα υπογραφής ElGamal προτάθηκε το 1985 από τον Taher ElGamal. Η διαφορά του από το RSA είναι ότι για κάθε μήνυμα υπάρχουν πολλές υπογραφές και ο αλγόριθμος επαλήθευσης οφείλει να αποδέχεται κάθε μία από αυτές ως αυθεντική. Οι διαδικασίες παραγωγής κλειδιού, υπογραφής και επαλήθευσης έχουν ως εξής:

Παραγωγή κλειδιού:

- Η διαδικασία παραγωγής κλειδιού είναι ίδια με αυτή του κρυπτοσυστήματος. Το αποτέλεσμα είναι η παραγωγή κλειδιού K= (p, g, α, β), όπου p πρώτος τέτοιος ώστε το DLP να είναι υπολογιστικά απρόσιτο στο $\mathbb{Z}^*_p$, $g \in \mathbb{Z}^*_p$, $0 \le g \le p-2$ και $\beta \equiv g^{\alpha} \bmod p$. Το δημόσιο κλειδί είναι το (p, g, β), ενώ το α είναι το ιδιωτικό. Υποθέτουμε ότι ο Α θέλει να στείλει ένα υπογεγραμμένο μήνυμα m στον Β χρησιμοποιώντας το κλειδί K= (p, g, α, β).

Δημιουργία υπογραφής:

- Ο Α επιλέγει ένα τυχαίο ακέραιο $\kappa \in \mathbb{Z}^*_{p-1}$.

- Υπολογίζει τα

  $$\gamma = g^{\kappa} \bmod p \qquad (1)$$

  και

  $$\delta = (m - \alpha\gamma)\, \kappa^{-1} (\mathrm{mod}(p-1)) \qquad (2)$$

- Η ψηφιακή υπογραφή για το μήνυμα m είναι το ζεύγος (γ, δ).

- Ο Α στέλνει στον Β την τριάδα (m, γ, δ), δηλαδή το αρχικό κείμενο με τη ψηφιακή του υπογραφή.

Επαλήθευση υπογραφής:

- Ο Β υπολογίζει την τιμή της συνάρτησης:

$$\mathrm{ver}_k(m, \gamma, \delta)=\begin{cases}\text{αληθής, αν } \beta^{\gamma}\gamma^{\delta} \equiv g^{m} \bmod p, \\ \text{ψευδής διαφορετικά.}\end{cases} \qquad (3)$$

Λήμμα 3.5.1: Αν p πρώτος και g πρωταρχικό στοιχείο του $\mathbb{Z}^*_p$, τότε για κάθε x, y∈ Z ισχύει

$$g^x \equiv g^y \bmod p \Leftrightarrow x \equiv y \bmod (p-1).$$

Θα αποδείξουμε ότι η σχέση (3) ορίζει πράγματι μια συνάρτηση επαλήθευσης. Αν $sig_k(m)=(\gamma, \delta)$, τότε από τις (1) και (2) έχουμε:

$$\beta^{\gamma}\gamma^{\delta} \equiv g^{\alpha\gamma} g^{\kappa\delta} \equiv g^{\alpha\gamma+\kappa\delta} \bmod p$$

και

$$m \equiv \alpha\gamma+\kappa\delta \ (\mathrm{mod}(p-1))$$

άρα $\beta^{\gamma}\gamma^{\delta} \equiv g^{m} \bmod p$, όπως προκύπτει από το λήμμα 3.5.1.

Αντιστρόφως, έστω ότι ισχύει η παραπάνω ισοτιμία. Τότε υπάρχουν α, κ τέτοια ώστε:

$$\beta \equiv g^{\alpha} \bmod p \quad \text{και} \quad \gamma \equiv g^{\kappa} \bmod p.$$

Άρα

$$g^{m} \equiv g^{\alpha\gamma+\kappa\delta} \bmod p$$

και επομένως,

$$m \equiv \alpha\gamma+\kappa\delta \ (\mathrm{mod}(p-1)).$$

Παράδειγμα 3.5.1: Έστω ότι ο Α επιθυμεί να υπογράψει το μήνυμα m= 100. Επιλέγει p= 467, g= 2, α= 127. Τότε $\beta= g^{\alpha} \bmod p=2^{127} \bmod 467= 132$. Στη συνέχεια επιλέγει κ= 213 με $213^{-1} \bmod 466=431$ και υπολογίζει τα $\gamma=2^{213} \bmod 467=29$ και δ=(100-127*29)431mod466=51. Έπειτα στέλνει στον Β την τριάδα (100, 29, 51). Ο Β λαμβάνει το μήνυμα και επαληθεύει ότι $132^{29}\, 29^{51}=189 \bmod 467=2^{100}$. Συνεπώς δέχεται την υπογραφή ως γνήσια.

Λόγω της ευρείας χρήσης του σχήματος υπογραφής ElGamal είναι σκόπιμο να σταθούμε λίγο σε θέματα που αφορούν την ασφάλειά του. Το τυχαία επιλεγμένο κ πρέπει να κρατείται κρυφό καθώς η γνώση του δίνει τη δυνατότητα σε οποιονδήποτε να υπολογίσει το ιδιωτικό κλειδί α από τη σχέση:

$$\alpha = (m-\kappa\delta)\,\gamma^{-1}(\mathrm{mod}(p-1)),$$

και να υπογράψει έπειτα μηνύματα παριστάνοντας κάποιον άλλον.

Έστω ότι τα μηνύματα m_1, m_2 έχουν υπογραφεί με τη χρήση του κλειδιού (g, α, β) και έχουν προκύψει τα υπογεγραμμένα μηνύματα (m_1, γ, δ_1) και (m_2, γ, δ_2).

Τότε έχουμε:

$$\beta^{\gamma}\gamma^{\delta_1} = g^{m_1} \mod p \text{ και } \beta^{\gamma}\gamma^{\delta_2} = g^{m_2} \mod p$$

Άρα

$$g^{m_1-m_2} = \gamma^{\delta_1-\delta_2} \mod p = g^{\kappa(\delta_1-\delta_2)} \mod p$$

απ' όπου προκύπτει ότι:

$$m_1 - m_2 = \kappa(\delta_1 - \delta_2) \ (\mathrm{mod}(p-1)) .$$

Έτσι, αν κάποιος έχει στην κατοχή του τα δύο υπογεγραμμένα μηνύματα, είναι εύκολο να υπολογίσει τον κ και να επιτύχει ολικό σπάσιμο με επίθεση σε γνωστά μηνύματα. Γι αυτό κάθε φορά που υπογράφεται ένα μήνυμα, θα πρέπει να χρησιμοποιείται διαφορετικό κ. Άλλωστε, η αλλαγή του κ δεν επηρεάζει τη συνάρτηση επαλήθευσης, η οποία εξαρτάται από τα g και β.

Ας υποθέσουμε τώρα ότι ένας αντίπαλος σκοπεύει να πλαστογραφήσει μια υπογραφή χωρίς να γνωρίζει το ιδιωτικό κλειδί του υπογράφοντος. Αν επιλέξει μια τιμή για το γ και προσπαθήσει να βρει δ τέτοιο ώστε να ικανοποιεί τη συνάρτηση επαλήθευσης, τότε πρέπει να υπολογίσει το διακριτό λογάριθμο $\log_{\gamma} g^{m} \beta^{-\gamma}$. Στην περίπτωση που επιλέξει δ και επιχειρήσει να υπολογίσει αντίστοιχο γ, τότε θα πρέπει να βρει το m στην ισοδυναμία $\beta^{\gamma}\gamma^{\delta} = g^{m} \mod p$, η επίλυση της οποίας ούτε έχει κάποια γνωστή εφικτή λύση ούτε μπορεί να αναχθεί σε κάποιο γνωστό πρόβλημα της κρυπτολογίας. Αν τέλος επιλέξει γ και δ και προσπαθήσει να υπολογίσει το m, βρίσκεται και πάλι αντιμέτωπος με το DLP. Υπάρχει παρ' όλα αυτά τρόπος με τον οποίο μπορεί να επιτευχθεί πλαστογράφηση υπογραφής, με επιλογή των γ, δ και m ταυτόχρονα.

Έστω ότι ο Γ θέλει να πλαστογραφήσει την υπογραφή του Α. αρχικά επιλέγει ακεραίους i και j με $0 \leq i, j \leq p-2$ και ΜΚΔ $(j, p-1)= 1$. Στη συνέχεια υπολογίζει:

$$\gamma= g^i \beta^j \bmod p,$$
$$\delta= -\gamma j^{-1} \bmod (p-1),$$
$$m= -\gamma i j^{-1} \bmod (p-1).$$

Το j^{-1} υπολογίζεται modulo(p-1), γι' αυτό και αρχικά απαιτούμε $(j, p-1)=1$. Έχουμε με αυτό τον τρόπο μια έγκυρη υπογραφή για το ElGamal.

Πράγματι,

$$\begin{aligned}
\beta^{\gamma} \gamma^{\delta} &\equiv \beta^{g^i\beta^j} (g^i \beta^j)^{-g^i\beta^j j^{-1}} (\text{mod } p) \\
&\equiv \beta^{g^i\beta^j} g^{-ij^{-1}g^i\beta^j} \beta^{-g^i\beta^j} (\text{mod } p) \\
&\equiv g^{-ij^{-1}g^i\beta^j} (\text{mod } p) \\
&\equiv g^{-\gamma ij^{-1}} (\text{mod } p) \\
&\equiv g^m (\text{mod } p).
\end{aligned}$$

3.6 Το πρότυπο ψηφιακής υπογραφής (Digital Signature Standard-DSS)

Το πρότυπο ψηφιακής υπογραφής (DSS) προτάθηκε το 1991 από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Ηνωμένων Πολιτειών (National Institute of Standards and Technology-NIST). Είναι βασισμένο στον αλγόριθμο ψηφιακής υπογραφής (Digital Signature Algorithm-DSA) και αποτελεί μια παραλλαγή του ElGamal με στόχο τη μείωση του μεγέθους της παραγόμενης υπογραφής.

Λήμμα 3.6.1: Αν p πρώτος τέτοιος ώστε $q \mid (p-1)$ και g_0 πρωταρχικό στοιχείο-γεννήτορας του $\mathbb{Z}^*_p$, τότε το

$$g= g_0^{(p-1)/q}$$

είναι q-οστή ρίζα της μονάδας modulo p,δηλαδή

$$g^q \equiv 1 \bmod p.$$

Απόδειξη: Πράγματι, αφού $q \mid (p-1)$ θα υπάρχει $\lambda \in \mathbb{Z}$ τέτοιος ώστε

$$p-1= \lambda q.$$

Όμως τότε

$$g^q \equiv (g_0^{(p-1)/q})^q \equiv g_0^{p-1} \equiv 1 \pmod p,$$

αφού το g_0 είναι πρωταρχικό στοιχείο του $\mathbb{Z}^*_p$.

Κατασκευή κλειδιού για το DSS:

1. Ο Α επιλέγει πρώτο q μεγέθους 160-bit και έναν πρώτο p μεγέθους n-bit με

   $n \equiv 0 \bmod 64$ και $512 \leq n \leq 1024$, τέτοιους ώστε $q \mid p-1$.

2. Υπολογίζει g που να είναι q-οστή ρίζα της μονάδας (βλ.λήμμα 3.6.1).
3. Επιλέγει ακέραιο α με $1 < \alpha < q-1$.
4. Υπολογίζει $\beta= g^{\alpha} \bmod p$.

Το δημόσιο κλειδί του Α είναι το (p, q, α, β).

Υποθέτουμε ότι ο Α θέλει να στείλει στον Β το μήνυμα m υπογεγραμμένο ψηφιακά με το DSS χρησιμοποιώντας το παραπάνω κλειδί.

Δημιουργία υπογραφής:

1. Ο Α επιλέγει έναν τυχαίο ακέραιο κ, $1 \leq \kappa \leq q-1$.
2. Υπολογίζει τα

$$\gamma = (g^{\kappa} \bmod p) \bmod q \qquad (4)$$

και

$$\delta = (m+\alpha\gamma)\, \kappa^{-1} \bmod q \qquad (5)$$

3. Η ψηφιακή υπογραφή του Α για το μήνυμα m είναι το ζεύγος (γ, δ)
4. Ο Α στέλνει στον Β την τριάδα (m, γ, δ).

Επαλήθευση υπογραφής:

1. Ο Β υπολογίζει τις τιμές:

$$e_1 = m\delta^{-1} \bmod q \qquad (6)$$

και

$$e_2 = \gamma\delta^{-1} \bmod q \qquad (7)$$

2. Στη συνέχεια υπολογίζει την τιμή της συνάρτησης:

$$\mathrm{ver}_k(m, \gamma, \delta) = \begin{cases} \text{αληθής αν } (g^{e_1}\ \beta^{e_2} \bmod p) \bmod q = \gamma, \\ \text{ψευδής διαφορετικά} \end{cases}$$

και αν $\mathrm{ver}_k(m, \gamma, \delta)$= true, πιστοποιεί ότι το μήνυμα προέρχεται από τον Α.

Πράγματι, από τη σχέση (5) έχουμε:

$m = (-\alpha\gamma+\kappa\delta) \bmod q$

τότε

$\delta^{-1} m = (-\alpha\gamma\delta^{-1}+\kappa) \bmod q$

και

$\kappa = (\delta^{-1} m+\alpha\gamma\delta^{-1}) \bmod q = (e_1+\alpha e_2) \pmod q$

άρα $g^{\kappa} = \gamma = g^{e1+\alpha\, e2} = g^{e1}\,(g^{\alpha})^{e2} = (g^{e1}\,\beta^{e2} \bmod p) \bmod q$.

Παράδειγμα 3.6.1: Έστω ότι ο Α θέλει να στείλει στον Β το μήνυμα m= 3152, υπογεγραμμένο με το σχήμα υπογραφής DSS.

- Επιλέγει q= 107 και p= 86·107= 9203. Το g_0= 2 είναι πρωταρχικό στοιχείο του $\mathbb{Z}^*_{9203}$,

  άρα σύμφωνα με το λήμμα 3.6.1 μπορώ να πάρω

  $g= g_0^{(p-1)/q} \bmod p= 2^{9202/107} \bmod 9203= 2^{86} \bmod 9203=645.$

- Επιλέγει α=111 και υπολογίζει:

  $\beta= g^{\alpha} \bmod p= 645^{111} \bmod 9203= 1336.$

  Το δημόσιο κλειδί του είναι το (p, q, α, β)= (9203, 107, 645, 1336) και το ιδιωτικό του είναι το α=111.

- Για τυχαίο κ=456 υπολογίζει:

  $\gamma= (g^{\kappa} \bmod p) \bmod q=(645^{456} \bmod 9203) \bmod 107= 96,$

  $\kappa^{-1} \bmod q=456^{-1} \bmod 107= 65,$

  $\delta= (m+\alpha\gamma)\, \kappa^{-1} \bmod q= (3152+111\cdot 96)\cdot 65 \bmod 107= 4$

  Έπειτα στέλνει στον Β το (m, γ, δ)=(3152, 96, 4),δηλαδή το μήνυμα m μαζί με την υπογραφή του.

- Ο Β λαμβάνει το μήνυμα και υπολογίζει:

  $\delta^{-1} \bmod q =4^{-1} \bmod 107= 27,$

  $e_1= m\delta^{-1} \bmod q=3152\cdot 27 \pmod{107}=39,$

  $e_2= \gamma\delta^{-1} \bmod q=96\cdot 27 \pmod{107}=24$

  και

  $(g^{e1}\, \beta^{e2} \bmod p) \bmod q=(645^{39}\cdot 1336^{24} \bmod 9203) \bmod 107=96=\gamma.$

  Άρα καταλήγει στο συμπέρασμα ότι η υπογραφή είναι πράγματι του Α.

Παρατηρώντας το DSS βλέπουμε ότι οι υπολογισμοί γίνονται στην υποομάδα Z_q μεγέθους 2^{160}. Η ασφάλεια του σχήματος στηρίζεται στην εικασία ότι η επίλυση του DLP είναι σχεδόν ανέφικτη σε μια τέτοια υποομάδα. Η χρήση μια συνάρτησης κατακερματισμού καθιστά την υπαρκτή πλαστογράφηση πρακτικά αδύνατη, άρα το ολικό σπάσιμο παραμένει η μόνη γνωστή επίθεση ενάντια στο DSS. Βέβαια, όπως και στην περίπτωση του σχήματος ElGamal, είναι αναγκαίο ο τυχαίος κ να είναι διαφορετικός για κάθε καινούρια υπογραφή και σε κάθε περίπτωση να παραμένει κρυφός. Σημαντικό είναι επίσης να αποφευχθεί το ενδεχόμενο $\delta \equiv 0 (\mathrm{mod}\ q)$, γιατί σ' αυτή την περίπτωση δεν υπάρχει το δ^{-1}. Αν συμβεί κάτι τέτοιο, τότε θα πρέπει να επιλεγεί καινούριο κ (η πιθανότητα να συμβεί αυτό είναι $½^{160}$).

Το μέγεθος του q καθορίζεται από τη διαδικασία παραγωγής κλειδιού στα 160 bits ενώ το μέγεθος του p μπορεί να είναι οποιοδήποτε πολλαπλάσιο του 64 μεταξύ των 512 και 1024 bits. Τον Οκτώβριο του 2001 το NIST πρότεινε μήκος 1024 bits για μεγαλύτερη ασφάλεια.

Το γεγονός ότι οι υπολογισμοί γίνονται modulo q κάνει το μέγεθος της υπογραφής πολύ μικρότερο από την αντίστοιχη υπογραφή ElGamal. Αν για παράδειγμα ο p είναι μεγέθους 1024-bit, τότε το ElGamal παράγει υπογραφή μήκους 2048 bits ενώ το DSS υπογραφή μεγέθους 320 bits.

Κεφάλαιο 4

Υπογραφές μίας χρήσης (One-time Signatures)

Με τον όρο υπογραφές μιας χρήσης εννοούμε σχήματα ψηφιακών υπογραφών στα οποία κάθε κλειδί μπορεί να χρησιμοποιηθεί για να υπογράψει ένα μήνυμα μόνο, διαφορετικά η υπογραφή μπορεί να πλαστογραφηθεί. Το πλεονέκτημά τους είναι ότι τόσο η παραγωγή όσο και η επαλήθευση της υπογραφής υλοποιούνται με πολύ αποδοτικούς αλγόριθμους, γι' αυτό χρησιμοποιούνται σε εφαρμογές χαμηλής υπολογιστικής ισχύος. Βασικό τους εργαλείο είναι η χρήση μια συνάρτησης μονής κατεύθυνσης. Ένα τέτοιο σχήμα είναι το σχήμα υπογραφής Lamport.

4.1 Σχήμα υπογραφής Lamport

Έστω ότι ο Α θέλει να υπογράψει ένα μήνυμα m που είναι μια δυαδική ακολουθία μήκους k-bit, με $k \in \mathbb{N}$. Έστω επίσης ότι S=Y και f: Y→Z είναι μια συνάρτηση μονής κατεύθυνσης δημοσίως γνωστή. Μια τέτοια συνάρτηση είναι για παράδειγμα η $f(x)= g^x \bmod p$, όπου p πρώτος και g γεννήτορας της κυκλικής ομάδας $\mathbb{Z}^*_p$.

Παραγωγή κλειδιού:

- Ο Α επιλέγει 2k τιμές από το σύνολο Y, τα $y_{i,j}$, όπου 1≤ i≤ k και j= 0,1. Ο k×2 πίνακας που προκύπτει είναι το ιδιωτικό του κλειδί.

- Υπολογίζει τα $z_{i,j} \in Z$ τέτοια ώστε $z_{i,j}= f(y_{i,j})$ και κατασκευάζει έτσι το δημόσιο κλειδί του.

Υποθέτουμε ότι ο Α θέλει να στείλει στον Β, υπογεγραμμένο, το μήνυμα
$m= (x_1, x_2,\ldots, x_k)$, όπου $x_i \in \{0,1\}$ και i= 1, 2,…,k.

Δημιουργία υπογραφής:

- Η ψηφιακή υπογραφή του Α για το μήνυμα m είναι η $\mathrm{sig}_K(x_1, x_2,..., x_k) = (y_{1,x_1}, y_{2,x_2},...,y_{k,x_k}) = \vec{s}.$

  Ο Α στέλνει στον Β το ζεύγος (m, s).

Επαλήθευση υπογραφής:

- Ο Β υπολογίζει την τιμή της συνάρτησης:

$$\mathrm{ver}_K((x_1,\ x_2,...,x_k)(s_1,\ s_2,...,s_k)) = \begin{cases} \text{αληθής αν } f(s_i) = z_{i,x_i} \\ \text{ψευδής διαφορετικά} \end{cases},$$

και πιστοποιεί ότι το μήνυμα προέρχεται πράγματι από τον Α αν και μόνο αν $\mathrm{ver}_K(m, s)$= true.

Παράδειγμα 4.1.1: έστω η $f(x)= 3^x \bmod 7879$. Ο Α επιλέγει τυχαίους αριθμούς και κατασκευάζει τον πίνακα:

$$(y_{i,j}) = \begin{bmatrix} y_{1,0} = 5831 & y_{1,1} = 735 \\ y_{2,0} = 803 & y_{2,1} = 2467 \\ y_{3,0} = 4285 & y_{3,1} = 6449 \end{bmatrix}$$

Στη συνέχεια υπολογίζει τις εικόνες των $y_{i,j}$ από την f και κατασκευάζει τον πίνακα:

$$(z_{i,j}) = \begin{bmatrix} z_{1,0} = 2009 & z_{1,1} = 3810 \\ z_{2,0} = 4672 & z_{2,1} = 4721 \\ z_{3,0} = 268 & z_{3,1} = 5731 \end{bmatrix}$$

τον οποίο και δημοσιεύει.

Έστω τώρα ότι ο Α θέλει να στείλει στον Β το μήνυμα m= (1,1,0) υπογεγραμμένο.

Η υπογραφή του θα είναι:

$\mathrm{sig}_K(1,1,0)= (y_{1,1}, y_{2,1}, y_{3,0})= (735, 2467, 4285)$.

Ο Β λαμβάνει την υπογραφή και υπολογίζει:

$f(s_1)= f(y_{1,1})= 3^{375} \bmod 7879$

$= 3810= z_{1,1}$

$f(s_2)= f(y_{2,1})= 3^{2467} \bmod 7879$

$= 4721= z_{2,1}$

$f(s_3)= f(y_{3,0})= 3^{4285} \bmod 7879$

$= 268= z_{3,0}$

Άρα καταλήγει στο συμπέρασμα ότι η υπογραφή είναι γνήσια. Παρατηρούμε ότι από τους δείκτες των $z_{1,1}$, $z_{2,1}$, $z_{3,0}$ μπορεί κάποιος να ανακτήσει το αρχικό μήνυμα m= (1,1,0).

Με λίγα λόγια, αν το i-οστό bit του μηνύματος έχει τιμή $j \in \{0, 1\}$,τότε το i-οστό στοιχείο της υπογραφής είναι η τιμή $y_{i,j}$, που αποτελεί όρισμα του δημόσιου κλειδιού $z_{i,j}$. Το $z_{i,j}$ είναι η εικόνα του $y_{i,j}$ μέσω της συνάρτησης f. Η διαδικασία επαλήθευσης απλώς ελέγχει ότι κάθε στοιχείο της υπογραφής είναι όρισμα του αντίστοιχου στοιχείου του δημόσιου κλειδιού.

Η ασφάλεια του σχήματος Lamport οφείλεται στην αδυναμία ενός «εισβολέα» να αντιστρέψει τη συνάρτηση f. Ωστόσο, το ιδιωτικό κλειδί πρέπει να χρησιμοποιείται για την υπογραφή ενός μηνύματος μόνο, διαφορετικά είναι εύκολο για κάποιον να κατασκευάσει την υπογραφή του νόμιμου υπογράφοντα και σε άλλα μηνύματα. Αυτό γίνεται κατανοητό στο παράδειγμα που ακολουθεί.

Παράδειγμα 4.1.2: έστω ότι ο Α χρησιμοποιεί τον ίδιο πίνακα ($y_{i,j}$) για να υπογράψει τα μηνύματα m_1= (0, 1, 1) και m_2= (1 ,0, 1), με υπογραφές $s_1= (y_{1,0}, y_{2,1}, y_{3,1})$ και $s_2= (y_{1,1}, y_{2,0}, y_{3,1})$ αντίστοιχα. Αν τώρα κάποιος 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) αντίστοιχα. Πρόκειται δηλαδή για υπαρκτή πλαστογραφία με επίθεση σε γνωστά μηνύματα.

Κεφάλαιο 5

Σχήματα υπογραφών με επιπρόσθετη λειτουργικότητα (Signature schemes with additional functionality)

Τα σχήματα υπογραφών που περιγράφονται σε αυτήν την ενότητα παρουσιάζουν συγκεκριμένες ιδιότητες, ώστε να εξυπηρετούν κάποιες πρόσθετες ανάγκες των ατόμων που τις χρησιμοποιούν.

5.1 Σχήματα τυφλής υπογραφής (Blind signature schemes)

Οι ψηφιακές υπογραφές βοηθούν πάρα πολύ στην επικοινωνία μας με τους άλλους, προκειμένου να μη μπορεί κάποιος τρίτος να παραστήσει εμάς. Δεν είναι όμως ο καταλληλότερος τρόπος για να εξασφαλίσει κανείς ανωνυμία. Για το λόγο αυτό, ο Chaum ήταν ο πρώτος το 1983 που πρότεινε τα σχήματα τυφλής ψηφιακής υπογραφής.

Η ανάγκη για τη δημιουργία ενός τέτοιου σχήματος προήλθε από τον αυτοματοποιημένο τρόπο με τον οποίο πληρώνουμε για διάφορα υλικά αγαθά, ο οποίος μπορεί να αποκαλύψει πολλά πράγματα για τις προσωπικές μας συνήθειες. Έτσι χάνεται η έννοια των προσωπικών δεδομένων και του απορρήτου. Ο τρόπος με τον οποίο μπορεί κανείς να διατηρήσει την ανωνυμία του είναι πληρώνοντας με μετρητά, τα οποία ανιχνεύονται εξαιρετικά δύσκολα. Το μειονέκτημα όμως είναι ότι οι παράνομες συναλλαγές παραμένουν καλά κρυμμένες. Πάνω σε αυτή την άποψη στηρίχτηκε και ο Chaum και εφηύρε τα σχήματα των τυφλών υπογραφών, με τη βοήθεια των οποίων μπορείς να κρατήσεις την ανωνυμία σου αλλά και να την άρεις σε εξαιρετικά ειδικές περιπτώσεις.

Το κρυπτογραφικό σύστημα που ανέπτυξε ο Chaum έχει τις παρακάτω πολύ βασικές ιδιότητες:

1. Αδυναμία ενός τρίτου προσώπου να μάθει το χρόνο, το ποσό και τον αποδέκτη μιας πληρωμής που έκανε κάποιος.
2. Ικανότητα απόδειξης πληρωμής (η οποία μπορεί μελλοντικά να χρησιμοποιηθεί για την αποκάλυψη μιας απάτης).
3. Γνώση της ταυτότητας του αποδέκτη της πληρωμής, μόνο όμως κάτω από ειδικές περιστάσεις.
4. Ικανότητα να ακυρώνονται τα μέσα πληρωμής που έχουν αναφερθεί κλεμμένα.

Τα σχήματα τυφλής υπογραφής εξυπηρετούν γενικά ανάγκες ηλεκτρονικής επικοινωνίας που η μια πλευρά επιθυμεί ανωνυμία απέναντι στην άλλη. Πρόκειται ουσιαστικά για ένα πρωτόκολλο επικοινωνίας μεταξύ τους με χαρακτηριστική ιδιότητα το γεγονός ότι ο υπογράφων δε γνωρίζει το περιεχόμενο του μηνύματος που υπογράφει. Έτσι δεν είναι σε θέση αργότερα να συσχετίσει το υπογεγραμμένο μήνυμα με τον αποστολέα (unlinkability). Χρειάζεται όμως να μπορεί να ελέγξει αν η υπογραφή του είναι έγκυρη.

Για να γίνουμε πιο σαφείς, έστω ότι απαιτείται να υπογραφεί ένα έγγραφο χωρίς ο υπογράφων να γνωρίζει το περιεχόμενό του. Το έγγραφο μπαίνει σε φάκελο μαζί με ένα φύλλο καρμπόν και σφραγίζεται. Στη συνέχεια, ο υπογράφων βάζει την υπογραφή του επάνω στο φάκελο και λόγω της παρεμβολής του καρμπόν η υπογραφή μεταφέρεται στο κλειστό έγγραφο. Τελικά, ο παραλήπτης του εγγράφου ανοίγει το φάκελο και έχει στα χέρια του το υπογεγραμμένο έγγραφο.

Οι τυφλές υπογραφές παρουσιάζουν πρακτικό ενδιαφέρον σε πολλές εφαρμογές, όπως το ηλεκτρονικό χρήμα και οι ηλεκτρονικές εκλογές. Όταν πραγματοποιούμε μια αγορά με κανονικά χρήματα ή επιταγή, ένας πωλητής μπορεί να ελέγξει την εγκυρότητά τους. Σε μια κοινωνία όμως που έχει τη δυνατότητα απαλλαγής από την ανάγκη για απτό χρήμα χρειάζεται να αναπτυχθούν νέες μέθοδοι για τη διασφάλιση των ηλεκτρονικών συναλλαγών.

Παράδειγμα 5.1.1: Υποθέτουμε ότι ένας πελάτης (αποστολέας) επιθυμεί η τράπεζά του (υπογράφων) να μη μπορεί να συσχετίσει εκ των υστέρων ένα μήνυμα και μια υπογραφή. Ένα μήνυμα πιθανόν να παριστάνει ένα χρηματικό ποσό από το λογαριασμό του πελάτη το οποίο ξοδεύεται σε μια αγορά. Όταν το μήνυμα και η υπογραφή προσκομίζονται στην τράπεζα για εξόφληση, τότε δεν είναι δυνατό να βρεθεί σε ποιον πελάτη δόθηκε αρχικά η υπογεγραμμένη τιμή. Έτσι αυτό λειτουργεί σαν ηλεκτρονικό χρήμα (electronic cash) και διατηρείται η ανωνυμία.

Παράδειγμα 5.1.2: Η ακεραιότητα ενός συστήματος ηλεκτρονικής ψηφοφορίας (electronic voting) στηρίζεται συνήθως στην επικύρωση των ψήφων από μια ελεγκτική Αρχή, προτού αυτές γίνουν αποδεκτές για καταμέτρηση. Έτσι επιτρέπεται στην Αρχή να ελέγξει τα στοιχεία του κάθε ψηφοφόρου και να επιβεβαιώσει ότι δικαιούται να ψηφίσει και ότι δεν έχει υποβάλλει περισσότερες από μία ψήφους. Παράλληλα όμως είναι σημαντικό να μη γίνει γνωστή η επιλογή κανενός από τους ψηφοφόρους. Η χρήση τυφλής υπογραφής παρέχει αυτήν ακριβώς την εγγύηση. Η ψήφος επικυρώνεται-υπογράφεται χωρίς να αποκαλύπτεται το περιεχόμενό της, παρά μόνον όταν παραληφθεί για καταμέτρηση.

Ας υποθέσουμε τώρα ότι ο Α χρειάζεται την υπογραφή του Β σε ένα μήνυμα m της επιλογής του, χωρίς όμως να θέλει να του αποκαλύψει οτιδήποτε για το μήνυμα. Ένα πρωτόκολλο τυφλής υπογραφής για τη μεταξύ τους επικοινωνία απαιτεί τα εξής:

- Ένα σχήμα ψηφιακής υπογραφής (από τα γνωστά) για τον υπογράφοντα Β. Με $sig_B(m)$ θα συμβολίζουμε την υπογραφή του Β σε ένα μήνυμα m.

- Τις συναρτήσεις f και g τέτοιες ώστε $g(sig_B(f(m))= sig_B(m)$, γνωστές μόνο στον Α. Την f την ονομάζουμε συνάρτηση τύφλωσης (blinding function) και την g συνάρτηση αποτύφλωσης (unblinding function). Τέλος, χρησιμοποιούμε τον όρο τυφλωμένο μήνυμα (blinded message) για το f(m).

Στη συνέχεια θα παρουσιάσουμε το πρωτόκολλο τυφλής υπογραφής του Chaum, που είναι βασισμένο στο σχήμα υπογραφής RSA.

Το σχήμα υπογραφής του Chaum

Έστω ότι ο Α θέλει από τον Β την τυφλή υπογραφή του μηνύματος m. Το δημόσιο κλειδί του Β για το RSA είναι το (n, b) και το ιδιωτικό είναι το (p, q, a). Η διαδικασία είναι η εξής:

1. Ο Α επιλέγει τυχαίο ακέραιο k τέτοιον ώστε $0 \leq k \leq n-1$ και ΜΚΔ(n, k)=1 (παράγοντας τύφλωσης).
2. **Τύφλωση:** Ο Α υπολογίζει το τυφλωμένο μήνυμα $m^* = f(m) = mk^b \bmod n$ και το στέλνει στον Β.
3. **Υπογραφή:** Ο Β υπολογίζει $s^* = sig_B(f(m)) = sig_B(m^*) = (m^*)^a \bmod n$ και το στέλνει στον Β.
4. **Αποτύφλωση:** Ο Α υπολογίζει το $s = g(sig_B(f(m)) = g(s^*) = k^{-1}s^* \bmod n$, που είναι η υπογραφή του Β για το m.

   Πράγματι, $k^{-1}s^* = k^{-1}(m^*)^a = k^{-1}(mk^b)^a = m^a k^{ab-1} = m^a \bmod n$

Παράδειγμα 5.1.3: Ο Β επιλέγει πρώτους p= 29, q= 17 και υπολογίζει n= 29×17= 493. Διαλέγει δημόσιο εκθέτη b=191 με 1 <b < φ(n)= 28×16= 448 και ΜΚΔ(b,448)= 1. Στη συνέχεια υπολογίζει τον ιδιωτικό του εκθέτη a=319 από τη σχέση ab= 1 mod φ(n).
Υποθέτουμε ότι ο Α θέλει την υπογραφή του Β στο μήνυμα m= 351. Τότε, επιλέγει κρυφό ακέραιο k= 31 και υπολογίζει το τυφλωμένο μήνυμα $m^* = 351 \times 31^{191} \bmod 493 = 291$, το οποίο και μεταδίδει στον Β.
Ο Β υπολογίζει $s^* = 291^{319} \bmod 493 = 349$, δηλαδή την υπογραφή του για το τυφλωμένο μήνυμα m^*, και τη στέλνει στον Α.
Ο Α υπολογίζει $31^{-1} \bmod 493 = 334$ και $s = 334 \times 349 \bmod 493 = 218$ και έχει στα χέρια του την υπογραφή του Β για το μήνυμα m.

5.2 Αδιαμφισβήτητα σχήματα υπογραφής (Undeniable signature schemes)

Τα αδιαμφισβήτητα σχήματα υπογραφής προτάθηκαν το 1989 από τους Chaum-van Antwerpen. Βασικό χαρακτηριστικό τους είναι ότι η επαλήθευση της υπογραφής δε μπορεί να γίνει χωρίς τη συνεργασία του υπογράφοντα. Μπορεί επομένως ο υπογράφων να αποφύγει την επαναχρησιμοποίηση του εγγράφου του αν δεν το επιθυμεί. Ας δούμε όμως δυο σενάρια χρήσης ενός τέτοιου σχήματος υπογραφής.

Υποθέτουμε ότι ο Α είναι ένας πελάτης της τράπεζας Β και θέλει να αποκτήσει πρόσβαση σε μια υψηλής ασφάλειας περιοχή της τράπεζας. Η τράπεζα ζητάει από τον Α να υπογράψει ένα κείμενο με ημερομηνία και ώρα πριν του δοθεί η άδεια πρόσβασης. Αν ο Α χρησιμοποιήσει αδιαμφισβήτητη υπογραφή, τότε δεν είναι δυνατόν σε κάποια μεταγενέστερη ημερομηνία να αποδειχθεί ότι η υπογραφή ανήκει σε αυτόν, παρά μόνο με την έγκρισή του.

Υποθέτουμε τώρα ότι μια μεγάλη εταιρεία λογισμικού Α δημιουργεί ένα νέο πακέτο λογισμικού. Η Α υπογράφει το πακέτο και το στέλνει στην εταιρεία Β. Η Β αντιγράφει το πακέτο και το μεταπωλεί στον πελάτη Γ. Ο Γ δε μπορεί να επαληθεύσει τη γνησιότητα του πακέτου χωρίς τη συνεργασία της Α. Αυτό βέβαια δεν εμποδίζει την Β να επαναϋπογράψει το πακέτο με τη δική της υπογραφή, αλλά τότε αφενός χάνεται το αγοραστικό πλεονέκτημα της προέλευσης από τη γνωστή εταιρεία Α, αφετέρου θα ήταν εύκολο να αποδειχθεί μια τέτοια απάτη.

Λήμμα 5.2.1: Έστω οι πρώτοι p, q τέτοιοι ώστε p= 2q+1. Τότε το σύνολο G που δημιουργείται από τα τετραγωνικά υπόλοιπα modulo p των στοιχείων του $\mathbb{Z}^*_p$ αποτελεί πολλαπλασιαστική υποομάδα του $\mathbb{Z}^*_p$ τάξης q.

Παρατήρηση: Από το παραπάνω λήμμα μπορούμε επίσης να υπολογίσουμε μια τέτοια υποομάδα του $\mathbb{Z}^*_p$ που θα αποτελείται από τις μέχρι q δυνάμεις του $g= g_0^{(p-1)/q}$, όπου g_0 πρωταρχικό στοιχείο του $\mathbb{Z}^*_p$.

Ας δούμε τώρα τις διαδικασίες παραγωγής κλειδιού, υπογραφής και επαλήθευσης για το αδιαμφισβήτητο σχήμα υπογραφής Chaum-van Antwerpen. Έστω ότι ο Α θέλει να στείλει στον Β το μήνυμα m υπογεγραμμένο ψηφιακά με το εν λόγω σχήμα.

Παραγωγή κλειδιού:

- Ο Α επιλέγει p, q πρώτους τέτοιους ώστε p=2q+1.
- Κατασκευάζει την τάξης q πολλαπλασιαστική υποομάδα G του $\mathbb{Z}^*_p$ και υπολογίζει ένα πρωταρχικό στοιχείο της g.
- Επιλέγει α τέτοιο που $1 \leq \alpha \leq q-1$ και υπολογίζει $\beta= g^{\alpha} \bmod p$.

Το δημόσιο κλειδί του Α είναι το (p ,g, β) ενώ το ιδιωτικό του το α.

Δημιουργία υπογραφής:

- Ο Α υπολογίζει $s= m^{\alpha} \bmod p$, που είναι η υπογραφή του για το μήνυμα m.
- Στέλνει στον Β το (m, s).

Επαλήθευση υπογραφής:

- Ο Β επιλέγει τυχαίους $e_1, e_2 \in \mathbb{Z}^*_q$ και υπολογίζει το $c=s^{e_1} \beta^{e_2} \bmod p$, το οποίο στέλνει στον Α.
- Ο Α υπολογίζει το $d=c^{\alpha^{-1} \bmod q} \bmod p$ και το στέλνει στον Β.
- Ο Β υπολογίζει την τιμή της συνάρτησης:

$$\mathrm{ver}_K(m, d)=\begin{cases} \text{αληθής αν } d \equiv m^{e_1} g^{e_2} \pmod p, \\ \text{ψευδής διαφορετικά} \end{cases}$$

και πιστοποιεί ότι το μήνυμα m προέρχεται από τον Α αν και μόνο αν $\mathrm{ver}_K(m, d)=$ αληθής.

Πράγματι, $d \equiv c^{\alpha^{-1}} \equiv (s^{e_1} \beta^{e_2})^{\alpha^{-1}} \equiv (m^{\alpha e_1} g^{\alpha e_2})^{\alpha^{-1}} \equiv m^{e_1} g^{e_2} \pmod p.$

Παράδειγμα 5.2.1: Ο Α επιλέγει p= 467= 2×233+1, όπου ο q= 233 είναι επίσης πρώτος. Στη συνέχεια επιλέγει στοιχείο $g_0=2 \in \mathbb{Z}^*_{467}$ και υπολογίζει το $g= 2^2 \bmod 467=4$. Το g=4 είναι γεννήτορας της κυκλικής υποομάδας G του $\mathbb{Z}^*_{467}$. Κατόπιν επιλέγει α=101 και υπολογίζει β= $4^{101} \bmod 467= 449$. Το δημόσιο κλειδί του Α είναι το (p=467, q=233, β=449) και το ιδιωτικό το α=101.
Έστω ότι ο Α θέλει να υπογράψει το μήνυμα m= 119. Η υπογραφή του είναι
$s= 119^{101} \bmod 467= 129.$
Ο Β λαμβάνει (m=119, s=129), επιλέγει κρυφούς ακεραίους $e_1= 38$, $e_2= 397$ από το $\mathbb{Z}^*_{233}$ και υπολογίζει $c=129^{38} 449^{397} \bmod 467= 13$ το οποίο και στέλνει στον Α.
Ο Α υπολογίζει $\alpha^{-1} \bmod q = 101^{-1} \bmod 233=30$ και $d= 13^{30} \bmod 467=9$ και στέλνει το d στον Β.
Τέλος, ο Β κάνει τον υπολογισμό $119^{38} 4^{397} \bmod 467= 9= d$, οπότε δέχεται την υπογραφή ως αυθεντική.

Θεώρημα 5.2.1: Αν $y \neq m^{\alpha} \bmod p$, δηλαδή το y είναι μια πλαστογραφία της υπογραφής του Α, τότε η πιθανότητα ο Β να δεχθεί το y ως έγκυρη υπογραφή για το μήνυμα m είναι 1/q.

Είδαμε λοιπόν, ότι για την επαλήθευση της υπογραφής είναι απαραίτητη η συγκατάθεση του υπογράφοντα. Τότε όμως τι τον εμποδίζει να αποκηρύξει μια έγκυρη υπογραφή του; Αυτό μπορεί να γίνει με έναν από τους ακόλουθους τρεις τρόπους:

1. Να αρνηθεί να συμμετάσχει στη διαδικασία επαλήθευσης.
2. Να εκτελέσει τη διαδικασία επαλήθευσης λανθασμένα.
3. Να ισχυριστεί ότι η υπογραφή είναι πλαστή παρόλο που η συνάρτηση επαλήθευσης επιστρέφει αληθής.

Στην πρώτη περίπτωση η κίνηση αυτή θα θεωρηθεί άμεσα ύποπτη και η υπογραφή δε θα ληφθεί υπ' όψιν. Για να αντιμετωπιστούν οι άλλες δύο, το σχήμα συνοδεύεται από ένα πρωτόκολλο αποκήρυξης (disavowal protocol) με το οποίο ο υπογράφων μπορεί να αποδείξει ότι μια υπογραφή που του αποδίδεται είναι πράγματι πλαστογραφημένη.

Πρωτόκολλο αποκήρυξης:

Έστω ότι ο Α ισχυρίζεται πως η υπογραφή s του μηνύματος m είναι πλαστή. Η διαδικασία αποτελείται από τα παρακάτω βήματα:

1. Ο Β επιλέγει τυχαία $e_1, e_2 \in \mathbb{Z}^*_p$. Στη συνέχεια υπολογίζει το $c=s^{e_1}\beta^{e_2} \bmod p$ και το στέλνει στον Α.
2. Ο Α υπολογίζει το $d=c^{\alpha^{-1} \bmod q} \bmod p$ και το στέλνει στον Β.
3. Ο Β επαληθεύει ότι $d \neq m^{e_1} g^{e_2} (\bmod p)$. Έπειτα επιλέγει τυχαία $f_1, f_2 \in \mathbb{Z}^*_p$ και υπολογίζει το $c'=s^{f_1}\beta^{f_2} \bmod p$, το οποίο στέλνει στον Α.
4. Ο Α υπολογίζει το $d'=(c')^{\alpha^{-1} \bmod q} \bmod p$ και το στέλνει στον Β.
5. Ο Β επαληθεύει ότι $d' \neq m^{f_1} g^{f_2} (\bmod p)$ και συμπεραίνει ότι το s είναι προϊόν πλαστογραφίας αν και μόνο αν

$$(dg^{-e_2})^{f_1} \equiv (d'g^{-f_2})^{e_1} (\bmod p).$$

Απόδειξη:

Έχουμε:

$$(dg^{-e_2})^{f_1} \equiv (c^{\alpha^{-1}} g^{-e_2})^{f_1} \equiv s^{e_1 f_1 \alpha^{-1}} \beta^{e_2 f_1 \alpha^{-1}} g^{-e_2 f_1} \equiv s^{e_1 f_1 \alpha^{-1}} g^{e_2 f_1} g^{-e_2 f_1} \equiv s^{e_1 f_1 \alpha^{-1}}$$

Ομοίως:

$$(d' g^{-e_2})^{f_1} \equiv ((s^{f_1} \beta^{f_2})^{\alpha^{-1}} g^{-f_2})^{e_1} \equiv s^{e_1 f_1 \alpha^{-1}} g^{e_1 f_2} g^{-e_1 f_2} \equiv s^{e_1 f_1 \alpha^{-1}} = (dg^{-e_2})^{f_1}$$

Το πρωτόκολλο αποκήρυξης ουσιαστικά εφαρμόζει δυο φορές τη διαδικασία επαλήθευσης και στη συνέχεια εκτελεί έναν έλεγχο για την επαλήθευση της σωστής εκτέλεσής του από τον υπογράφοντα. Με τη χρήση αυτού του πρωτοκόλλου είναι πολύ δύσκολο για κάποιον να αρνηθεί μια υπογραφή που είναι πράγματι δική του. Η πιθανότητα να κατασκευάσει ο υπογράφων δεδομένα τέτοια που να οδηγούν στο συμπέρασμα ότι πρόκειται για πλαστογραφία είναι 1/q, δηλαδή πολύ μικρή. Έτσι άλλωστε δικαιολογείται ο τίτλος αδιαμφισβήτητη υπογραφή. Συνεπώς, η άρνηση συμμετοχής στο πρωτόκολλο αποκήρυξης λαμβάνεται ως ένδειξη ότι υπογραφή είναι γνήσια.

Παράδειγμα 5.2.2: Όπως και στο προηγούμενο παράδειγμα, ας υποθέσουμε ότι το δημόσιο κλειδί του Α είναι η τετράδα (p= 467, q= 233, g= 4, β= 449) και το ιδιωτικό του κλειδί το α= 101. Έστω ότι το μήνυμα m= 286 υπογράφεται με την πλαστή υπογραφή s= 83 και ο Α θέλει να πείσει τον Β ότι πράγματι η υπογραφή δεν είναι γνήσια.

Ο Β επιλέγει ακεραίους e_1= 45, e_2= 237 ∈ $\mathbb{Z}^*_{233}$ και υπολογίζει το $c = 83^{45} \times 449^{237} \bmod 467 = 305$, το οποίο μεταδίδει στον Α.

Ο Α υπολογίζει το $d = 305^{30} \bmod 467 = 109$ και το στέλνει στον Β.

Ο Β επαληθεύει ότι $m^{e_1} g^{e_2} \bmod p = 286^{45} \times 4^{237} \bmod 467 = 149 \neq 109$. Στη συνέχεια επιλέγει ξανά ακεραίους f_1= 125, f_2= 9 ∈ $\mathbb{Z}^*_{233}$ και υπολογίζει $c' = 83^{125} \times 449^{9} \bmod 467 = 270$ το οποίο στέλνει στον Α.

Ο Α υπολογίζει $d' = 270^{30} \bmod 467 = 68$ και στο στέλνει στον Β.

Ο Β επαληθεύει ότι $m^{f_1} g^{f_2} \bmod p = 286^{125} \times 4^{49} \bmod 467 = 25 \neq 68$, εκτελεί τον τελικό έλεγχο:

$$(dg^{-e_2})^{f_1} \bmod p = (109 \times 4^{-237})^{125} \bmod 467 = 188$$

και

$$(d' g^{-f_2})^{e_1} \bmod p = (68 \times 4^{-9})^{45} \bmod 467 = 188,$$

και καταλήγει στο συμπέρασμα ότι η s είναι πράγματι πλαστή.

5.3 Το σχήμα υπογραφής fail-stop

Το σχήμα υπογραφής fail-stop παρέχει επιπλέον ασφάλεια στην περίπτωση που κάποιος πολύ ισχυρός αντίπαλος είναι σε θέση να πλαστογραφήσει μια υπογραφή. Τότε όμως και ο υπογράφων μπορεί με πολύ μεγάλη πιθανότητα να αποδείξει το γεγονός. Ένα τέτοιο σχήμα προτάθηκε το 1992 από τους van Heyst και Pedersen. Πρόκειται για ένα σχήμα μίας χρήσης, όπως το σχήμα Lamport που μελετήθηκε στο προηγούμενο κεφάλαιο. Η βασική διαφορά του από τα σχήματα που περιγράψαμε μέχρι τώρα είναι η ύπαρξη μιας Έμπιστης Αρχής (Trusted Third Party-TTP). Το σχήμα υπογραφής των van Heyst και Pedersen αποτελείται από τους αλγόριθμους υπογραφής και επαλήθευσης καθώς και από έναν αλγόριθμο απόδειξης της πλαστογράφησης.

Σχήμα υπογραφής fail-stop των van Heyst και Pedersen

Έστω p= 2q+1 πρώτος, τέτοιος ώστε ο q να είναι επίσης πρώτος και το DLP να είναι απρόσιτο στο $\mathbb{Z}^*_p$. Έστω ακόμα g πρωταρχικό στοιχείο του $\mathbb{Z}^*_p$ και α ∈ $\mathbb{Z}_q$. Ορίζουμε β= g^{α} mod p. Οι τιμές p, q, g, α, β έχουν επιλεγεί από μια TTP. Τα p, q, g, β είναι δημοσίως γνωστά ενώ το α κρατείται κρυφό. Υποθέτουμε ότι ο Α θέλει να στείλει στον Β το μήνυμα m υπογεγραμμένο με το εν λόγω σχήμα υπογραφής.

Δημιουργία κλειδιού:

- Ο Α επιλέγει τυχαίους κρυφούς ακεραίους $a_1, a_2, b_1, b_2 \in \mathbb{Z}_q$.
- Ο Α υπολογίζει τα:

$$\gamma_1 = g^{a_1}\beta^{a_2} \bmod p$$
και
$$\gamma_2 = g^{b_1}\beta^{b_2} \bmod p.$$

Το δημόσιο κλειδί του Α είναι το K= (γ_1, γ_2) και το ιδιωτικό του η τετράδα (a_1 , a_2, b_1, b_2).

Δημιουργία υπογραφής:

- Ο Α υπολογίζει τα

$$s_1=a_1+mb_1 \bmod q$$

και

$$s_2=a_2+mb_2 \bmod q.$$

Η υπογραφή του Α για το μήνυμα m είναι: s= $sig_K(m)$= (s_1, s_2). Ο Α στέλνει στον Β το (m, s).

Επαλήθευση υπογραφής:

- Ο Β υπολογίζει την τιμή της συνάρτησης:

$$\text{ver}_K(m,s)=\begin{cases}\text{αληθής αν } \gamma_1\gamma_2{}^m = g^{s_1}\beta^{s_2} \bmod p,\\ \text{ψευδής διαφορετικά}\end{cases}$$

και πιστοποιεί ότι το μήνυμα προέρχεται από τον Α αν και μόνο αν $\text{ver}_K(m ,s)$= true.

Πράγματι, αν το ζεύγος (s_1, s_2) είναι μια γνήσια υπογραφή για το μήνυμα m, τότε $\gamma_1\gamma_2{}^m = g^{a_1}\beta^{a_2}g^{b_1m}\beta^{b_2m} = g^{a_1+b_1m}\ \beta^{a_2+b_2m} = g^{s_1}\ \beta^{s_2} \bmod p$.

Υπάρχουν q^2 διακεκριμένες τετράδες (a_1, a_2, b_1, b_2) οι οποίες δίνουν το ίδιο δημόσιο κλειδί (γ_1, γ_2). Από αυτές, ακριβώς q τετράδες δίνουν την ίδια υπογραφή (s_1, s_2). Άρα οι q^2 τετράδες δίνουν q διαφορετικές υπογραφές για ένα μήνυμα m $\in \mathbb{Z}_q$ (για απόδειξη βλ.Cryptography:Theory and Practice του Douglas R.Stinson). Οι q τετράδες που δίνουν την ίδια υπογραφή για το m, δίνουν q διαφορετικές υπογραφές για κάθε άλλο μήνυμα διαφορετικό του m.

Πιθανότητα επιτυχούς πλαστογραφίας:

Έστω ότι ο Γ επιθυμεί να εξάγει την υπογραφή του Β σε κάποιο μήνυμα m'. Τότε έχουμε τα ακόλουθα ενδεχόμενα:

1. Ο Γ έχει πρόσβαση μόνο στο δημόσιο κλειδί του υπογράφοντος (δεν έχει δηλαδή στην κατοχή του ένα μήνυμα και μια έγκυρη υπογραφή για αυτό). Άρα, η πιθανότητα η πλαστή υπογραφή του Γ να είναι ίδια με τη γνήσια υπογραφή του Α για το μήνυμα m' είναι $q/q^2 = 1/q$

2. Ο Γ έχει πρόσβαση σε ένα μήνυμα m και την υπογραφή (s_1, s_2) που δημιούργησε ο Α για αυτό. Τότε, η πιθανότητα η πλαστή υπογραφή να είναι ίδια με τη γνήσια υπογραφή του Α για το m' είναι $1/q$.

Απόδειξη της πλαστογράφησης:

Ας υποθέσουμε τώρα ότι ο Γ έχει πλαστογραφήσει την υπογραφή του Α σε ένα μήνυμα m' και η υπογραφή $s'=(s_1', s_2')$ πέρασε το στάδιο της επαλήθευσης. Η σημασία των υπογραφών fail stop έγκειται ακριβώς στο ότι ο Α μπορεί να αποδείξει ότι η υπογραφή είναι πλαστή. Η διαδικασία που περιγράφεται παρακάτω δείχνει πώς μπορεί ο Α με υψηλή πιθανότητα (συγκεκριμένα $1-1/q$), να χρησιμοποιήσει την πλαστή υπογραφή για να εξάγει τον κρυφό ακέραιο α.

- Ο Α χρησιμοποιεί το ιδιωτικό του κλειδί και υπολογίζει τη γνήσια υπογραφή $s=(s_1, s_2)$ για το m'.
- Αν $s=s'$ επιστρέφει στο πρώτο βήμα.
- Υπολογίζει $\alpha=(s_1-s_1')(s_2-s_2')^{-1} \bmod q$. Όμως ο α υποτίθεται γνωστός μόνο στην TTP. Η εύρεσή του από τον Α αποδεικνύει ότι η υπογραφή είναι πλαστή.

Απόδειξη ορθότητας:

Η πιθανότητα να ισχύει $(s_1,s_2)=(s_1',s_2')$ στο 2ο βήμα της διαδικασίας είναι $q/q^2 = 1/q$, οπότε η ζητούμενη πιθανότητα $(s_1,s_2)\neq(s_1',s_2')$ θα είναι $1-1/q$.

Από τη διαδικασία επαλήθευσης υπογραφής κι αφού η πλαστή υπογραφή έγινε δεκτή, θα είναι:

$$\gamma_1\gamma_2^{m'} \equiv g^{s_1'}\beta^{s_2'} \bmod p .$$

Ομοίως, για τη γνήσια υπογραφή θα έχουμε:

$$\gamma_1\gamma_2^{m'} \equiv g^{s_1}\beta^{s_2} \bmod p .$$

Άρα :

$$g^{s_1}\beta^{s_2} \equiv g^{s_1'}\beta^{s_2'} \bmod p \Rightarrow g^{s_1-s_1'} \equiv g^{\alpha(s_2-s_2')} \bmod p \Rightarrow (s_1-s_1') \equiv \alpha(s_2-s_2') \bmod q.$$

Και αν $s_2 \neq s_2'$, τότε $\alpha=(s_1-s_1')(s_2-s_2')^{-1}$.

Παράδειγμα 5.3.1: Η TTP επιλέγει πρώτους p= 3467 και q= 1733 και βρίσκει στοιχείο g= 4, πρωταρχικό στοιχείο του $\mathbb{Z}^*_{3467}$ τάξης 1733. Έπειτα επιλέγει α= 1567 άρα β= 4^{1567} mod 3467= 514. Η TTP γνωστοποιεί τα (p= 3467, q= 1733, g= 4, β= 514).

Ο Α επιλέγει κρυφούς ακεραίους a_1= 888, a_2= 1024, b_1= 786, b_2= 999 ∈ $\mathbb{Z}_{1733}$ και υπολογίζει

$\gamma_1 = 4^{888}\,514^{1024} \bmod 3467 = 3405$ και
$\gamma_2 = 4^{786}\,514^{1024} \bmod 3467 = 2281$.

Το δημόσιο κλειδί του Α είναι το (3405, 2281) και το ιδιωτικό το (888, 1024, 786, 999).

Υποθέτουμε τώρα ότι ο Α βρίσκεται αντιμέτωπος με την υπογραφή (s_1'=822, s_2'=55) που πλαστογράφησε ο Γ για το μήνυμα m'=3383. Η υπογραφή αυτή ικανοποιεί τη συνθήκη επαλήθευσης και γίνεται δεκτή από τον Β. Πράγματι,

$$\gamma_1 \gamma_2^{m'} \bmod p = 3405 \times 2281^{3383} \bmod 3467 = 2282$$

$$g^{s_1'} \beta^{s_2'} \bmod p = 4^{822} \times 514^{55} \bmod 3467 = 2282$$

Για να αποδείξει την πλαστογράφηση, ο Α χρησιμοποιεί το ιδιωτικό του κλειδί και υπολογίζει την υπογραφή του (s_1, s_2) για το m':

$s_1 = a_1 + m' b_1 \bmod q = 888 + 3383 \times 786 \bmod 1733 = 1504$ και

$s_2 = a_2 + m' b_2 \bmod q = 1024 + 3383 \times 999 \bmod 1733 = 1291$.

Αφού $(s_1, s_2) \neq (s_1', s_2')$ ο Α υπολογίζει α= $682 \times 1236^{-1} \bmod 1733 = 1537$.

Όμως ο α υποτίθεται ότι είναι γνωστός μόνο στην TTP, επομένως η εύρεσή του αποτελεί απόδειξη της πλαστογραφίας.

Παράρτημα

Μετατροπή μηνύματος σε θετικό ακέραιο:

Για να μετατρέψουμε ένα μήνυμα κειμένου M σε ένα θετικό ακέραιο m στο δεκαδικό σύστημα κωδικοποιούμε το αλφάβητο-εδώ το αγγλικό-ως εξής:
διάστημα:00, A:01, B:02, C:03, D:04, E:05, F:06, G:07, H:08, I:09, J:10, K:11, L:12, M:13, N:14, O:15, P:16, Q:17, R:18, S:19, T:20, U:21, V:22, W:23, X:24, Y:25, Z:26.
Για παράδειγμα, το μήνυμα COME NOW θα γίνει: 0315 1305 0014 1523.

Για τη μετατροπή του κειμένου m σε θετικό ακέραιο m στο δυαδικό σύστημα, η κωδικοποίηση του αλφαβήτου γίνεται ως εξής:
διάστημα:00, A:01, B:10, C:11, D:001, E:010, F:011, G:100, H:101, I:110, J:111, K:0001, L:0010, M:0011, N:0100, O:0101, P:0110, Q:0111, R:1000, S:1001, T:1010, U:1011, V:1100, W:1101, X:1110, Y:1111, Z:00001.

Συνάρτηση Euler:

Ορισμός: η συνάρτηση φ(n) ορίζεται ως το πλήθος των θετικών ακεραίων των μικρότερων (ή μικρότερων και ίσων του n) που είναι πρώτοι προς τον n.
Π.χ: φ(30)=8 και οι αριθμοί αυτοί είναι οι 1, 7, 11, 13, 17, 19, 23, 29.

Ιδιότητες της συνάρτησης Euler:

1. Αν p πρώτος, τότε φ(p)=p-1.
2. Αν (m, n)=1, τότε φ(mn)=φ(m)φ(n).

Θεώρημα:

$$\text{Αν } n>1 \text{ και } n=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r} \text{ όπου } p_1, p_{2,k_2} p_r \text{ πρώτοι και } k_{1,}k_{2,}\ldots,k_r \text{ ακέραιοι, τότε}$$
$$\varphi(n)=n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_r).$$

$$\text{Για } n=p_1p_2,\ \varphi(n)=p_1p_2(1-1/p_1)(1-1/p_2)=(p_1-1)(p_2-2).$$

Θεώρημα Euler: $\alpha\nu\ \alpha\in\mathbb{Z}_m$ και $\text{ΜΚΔ}(\alpha,m)=1$, τότε $\alpha^{\varphi(m)}\equiv 1 \bmod \varphi(m)$.

Θεώρημα: για p πρώτο, η ομάδα $\mathbb{Z}_p^*$ είναι πεπερασμένη κυκλική ομάδα τάξεως φ(p)=p-1.

Ορισμός: ένα στοιχείο $\alpha\in\mathbb{Z}_p^*$ καλείται **πρωταρχικό στοιχείο modulo p** αν έχει τάξη φ(p)=p-1.

Επεκτεταμένος Ευκλείδιος Αλγόριθμος

1. $b_0 = b$
2. $n_0 = n$
3. $t_0 = 0$
4. $t = 1$
5. $q = n_0 / b_0$ (rounded off)
6. $r = n_0 - q * b_0$
7. **while** $r > 0$ **do**
8. $temp = t_0 - q * t$
9. **if** $temp >= 0$ **then** $temp = temp$ mod n
10. **if** $temp < 0$ **then** $temp = n - ((-temp)$ mod $n)$
11. $t_0 = t$
12. $t = temp$
13. $n_0 = b_0$
14. $b_0 = r$
15. $q = n_0 / b_0$
16. $r = n_0 - q * b_0$
17. **if** b_0 != 1 **then**

    b has no inverse modulo n

    else

    $b^{-1} = t$ mod n

Βιβλιογραφία

Χ. Κουκουβίνος, Α. Παπαϊωάννου. Εισαγωγή στην Κρυπτογραφία. Εκδόσεις Ε.Μ.Π., 2004.

Ε. Ζάχος. Σημειώσεις στη Θεωρία Αριθμών και στην Κρυπτογραφία. Εκδόσεις Ε.Μ.Π., 2004

Ν. Μπουγέσης. Διπλωματική Εργασία: Ψηφιακές Υπογραφές-Τυφλές Υπογραφές.

Ε. Μπάκα. Διπλωματική Εργασία: Σχήματα ψηφιακής Υπογραφής.

Δ. Τσακτσήρας. Διπλωματική Εργασία: Κρυπτογραφία και Ελλειπτικές Καμπύλες.

Δημήτριος Μ. Πουλάκης. Κρυπτογραφία: Η Επιστήμη της Ασφαλούς Επικοινωνίας. Εκδόσεις Ζήτη, 2004.

Κ. Χαλάτσης. Η παρούσα Κατάσταση σε Θέματα Κρυπτογραφίας. Τμήμα Πληροφορικής και Τηλεπικοινωνιών ΕΚΠΑ, Μάιος 2003.

Κέντρο ΠΛΗ.ΝΕ.Τ.Ν Φλώρινας. Κρυπτογραφία και Ψηφιακή Υπογραφή, 2005.

Douglas R. Stinson. Cryptography: Theory and Practice, Second Edition. Chapman & Hall/ CRC, 2002.

Alfred J. Menedes, Paul C. Van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.

Wade Trappe, Lawrence C. Washington: Introduction to Cryptography with Coding Theory. Pearson Prentice Hall, 2006.

Wikipedia: the free encyclopedia. Public Key Cryptography, Symmetric Key Algorithm, Cryptographic Hash Function, RSA Factoring Challenge, ElGamal Signatures, Blind Signatures.