Ψηφιακές Υπογραφές στην Κρυπτογραφία

Διπλωματική εργασία
της
Χατζή Χρυσούλας

Εξεταστική Επιτροπή:

Παπαϊωάννου Αλέξανδρος - Αναπληρωτής καθηγητής ΕΜΠ (Επιβλέπων καθηγητής)

Κουκουβίνος Χρήστος – Καθηγητής ΕΜΠ

Στεφανέας Πέτρος – Λέκτορας ΕΜΠ

ΕΜΠ, Ιούλιος 2013

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

1. ΕΙΣΑΓΩΓΗ

1.1 Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ Η ΙΣΤΟΡΙΑ ΤΗΣ

Κρυπτολογία είναι η επιστημονική περιοχή στην οποία εφαρμόζονται τα αποτελέσματα της θεωρίας πληροφοριών και επειδή κατά γράμμα κρυπτολογία σημαίνει τη μελέτη απόκρυψης, κυρίως ασχολείται με τη διεύρυνση των μεθόδων για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων.

Ανέκαθεν στόχος ήταν τα μηνύματα να μπορούν να μεταφέρονται με τέτοιο τρόπο, ώστε να μη γίνονται απο αυτούς για τους οποίους δεν προορίζονται. Από παλιά δε, χρησιμοποιούνταν μυστικοί κώδικες κυρίως σε στρατιωτικό και διπλωματικό πλάισιο. Επειδή, όμως, η ανάπτυξη της τεχνολογίας έχει σημειώσει μεγάλη πρόοδο τελευταία, καθίσταται επιτακτική και η ανάγκη ανάπτυξης μεθόδων κρυπτογράφησης μηνυμάτων πέραν των στρατιωτικών και διπλωματικών πλαισίων.

Ένας σημαντικός τομέας στον οποίο βρίσκει μεγάλη εφαρμογή η κρυπτολογία, είναι οι ηλεκτρονικές συναλαγές στις τράπεζες. Αυτές είναι αδύνατο να λειτουργήσουν χωρίς την κρυπτολογία, γιατί οι μαγνητικές κάρτες, τα κλειδιά των τραπεζών, κ.ά. που χρησιμοποιούνταν για μεταφορές χρημάτων, χρησιμοποιούν όλα κρυπτογραφικά εργαλεία.

Απαραίτητη είναι επίσης η χρήση της Κρυπτολογίας για την προστασία της ιδιωτικής ζωής. Λόγω του μεγάλου αριθμού συστημάτων που αφορούν δεδομένα με προσωπικές πληροφορίες, όπως ιατρικές βάσεις δεδομένων, δικαστικές βάσεις δεδομένων, τηλεφωνικές υποκλοπές, καλό είναι όλα αυτά τα αποθηκευμένα δεδομένα να προστατεύονται.

Η Κρυπτολογία χωρίζεται σε δύο επιστημονικούς κλάδους, την κρυπτογραφία και την κρυπτανάλυση.

- Η κρυπτογραφία έχει ως αντικείμενο της την ανάπτυξη και μελέτη μεθόδων και μεθοδολογιών κρυπτογράφησης, όπου κάποιος χρησιμοποιεί κυρίως μυστικά κλειδιά. Χωρίς αυτά είναι αδύνατον να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα.

- Η κρυπτανάλυση σκοπό έχει την ανάπτυξη τεχνικών ώστε να αποκρυπτογραφούνται κρυπτογραφημένα μηνύματα. Χωρίς την εκ των προτέρων γνώση κάποιων κλειδιών.

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Αν πάμε πολύ πίσω, θα δούμε ότι οι ρίζες της Κρυπτολογίας βρίσκονται στην Αρχαία Αίγυπτο, τη Βαβυλώνα και τις Ινδίες. Δείγμα αυτού μια βαβυλωνιακή ταμπλέτα του 1500 π.Χ. που περιέχει μια κρυπτογραφημένη συνταγή για να κάνει κάποιος τα κεραμικά γυαλιστερά.

Στην Ελλάδα έχουμε αρκετές περιπτώσεις γραπτών μυστικών μηνυμάτων. Ο Ηρόδοτος μας αναφέρει στην Ιστορία του πως ο Ιστιαίος της Μιλήτου στέλνει μήνυμα στους δικούς του γραμμένο στο κεφάλι έμπιστου σκλάβου. Επίσης, αναφέρει πως ο Δημάρατος που ήταν εξόριστος στη Σούσα της Περσίας, στέλνοντας μήνυμα καλυμμένο με κερί στους Σπαρτιάτες, τους προειδοποιεί για το σχέδιο εισβολής του Ξέρξη, ώστε να μην αιφνιδιαστούν.

Ένας άλλος τρόπος αποστολής μηνυμάτων γύρω στον $5^{ο}$ π.Χ. αιώνα είναι η ***Σπαρτιατική σκυτάλη***, η οποία είναι ένα ξύλινο ραβδί γύρω στο οποίο τυλίγεται μια λωρίδα απο δέρμα ή περγαμηνή. Το μήνυμα γράφεται κατα μήκος της στυτάλης και ύστερα ξετυλίγει τη λωρίδα πάνω στην οποία έχει ήδη αναδιαταχτεί. Για να μπορέσει κάποιος να το διαβάσει θα πρέπει να τυλίξει τη λωρίδα γύρω από μια σκυτάλη ίδιας διαμέτρου με αυτή που χρησιμοποίησε ο αποστολέας.

Τον $2^{ο}$ π.Χ. αιώνα, ο ***Πολύβιος*** έκανε ένα κρυπτοσύστημα όπου τα γράμματα του απλού κειμένου (α.κ.) αντικαθίστανται απο ζεύγη συμβόλων (αριθμών) όπως φαίνεται στον πίνακα:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Το απλό κείμενο “LET NONE ENTER IGNORANT OF GEOMETRY” δίνει το κρυπτοκείμενο:

31 15 44 33 34 33 15 15 33 44 15 42 24 22 33
34 42 11 33 44 34 21 22 15 34 32 15 44 42 54 .

Αργότερα, ο ***Ιούλιος Καίσαρας*** χρησιμοποιούσε συχνά μυστική γραφή. Η αντικατάσταση που έκανε ήταν να μετατοπίζει 3 θέσεις προς τα δεξιά τα γράμματα του λατινικού αλφαβήτου, με τα 3 τελευταία X,Y,Z να γίνονται αντίστοιχα A,B,C. Για παράδειγμα το απλό κείμενο: "BOUDICCA HAS BURNED LONDINIUM"

γίνεται ERXGLFFD KDV EXUQHG ORQGLQLXP .

Κατά τον 4^{ο} μ.Χ. αιώνα ο Βραχμάνος λόγιος ***Βατσιγιάνα*** προτείνει στο Κάμα Σούτρα μια μυστική γραφή. Μία τεχνική, δηλαδή, ζευγαρώματος των γραμμάτων του αλφαβήτου τυχαία, όπου στη συνέχεια κάθε γράμμα αντικαθίσταται απο το ταίρι του. Παραδείγματος χάριν, αν ζευγαρώσουμε τα γράμματα του ελληνικού αλφαβήτου ως ακολούθως:

α δ η ι κ μ ο ρ σ θ υ ζ

ω χ β γ ζ ψ λ ν ε φ π τ

το απλό κείμενο "συνάντηση τα μεσάνυχτα" κωδικοποιείται ως : «επρωρζβεβ ζω ψσεωρπδζω».

Ο ***Αλ Κιντί***, ο σημαντικότερος εκπρόσωπος των Αράβων κρυπρολόγων στην πραγματεία του: «*περί αποκρυπτογράφησης κρυπτογραφημένων μηνυμάτων*» λέει ότι: «Για να μπορέσουμε να διαβάσουμε ενα κ.κ., αν γνωρίζουμε τη γλώσσα του, θα πρέπει να βρούμε ένα διαφορετικό α.κ. στην ίδια γλώσσα που να καλύπτει περίπου ένα φύλλο και μετά να μετρήσουμε τη συχνότητα εμφάνισης κάθε γράμματος. Το συχνότερα εμφανιζόμενο γράμμα ονομάζουμε πρώτο, το αμέσως επόμενο δεύτερο κ.ο.κ.»

Στη συνέχεια, για να αποκρυπτογραφήσουμε το κ.κ., ταξινομούμε με τον ίδιο τρόπο τα συμβολά του. Βρίσκουμε τον συχνότερα εμφανιζόμενο σύμβολο και το αντικαθιστούμε με το πρώτο γράμμα, το δεύτερο σε συχνότητα συμβολο με το δεύτερο γράμμα κ.ο.κ.

Ο Φλωρεντιανός ***Λέον Μπατίστα Αλμπέρτι*** (1404) ήταν ο πρώτος που σκέφτηκε ένα πολυαλφαβητικό σύστημα στην κρυπτανάλυση, δηλαδή ένα σύστημα με περισσότερα από ένα κρυπτοφραφικά αλφάβητα. Στη συνέχεια, επινόησε και την πρώτη (μετά τη σκυτάλη) κρυπτογραφική μηχανή, τους λεγόμενους *δίσκους του Alberti*. Το σύστημα αποτελούνταν από δύο ομοκεντρικούς δίσκους διαφορετικής διαμέτρου που περιστρέφονταν ανεξάρτητα και καθένας τους είχε χαραγμένο ένα αλφάβητο στην περιφέρειά του. Ο έξω δίσκος αντιπροσώπευε το α.κ. και οι αντίστοιχες θέσεις του μέσα δίσκου έδιναν το κ.κ.

Ιδιαίτερα ενδιαφέρον ήταν το πρώτο τυπωμένο βιβλίο κρυπτογραφίας (1518) του ***Τριθεμίου***, η *Πολυγραφία*, που περιείχε τετράγωνα γραμμάτων όπου η πρώτη γραμμή περιείχε τα 26 γράμματα του λατινικού αλφαβήτου και οι υπόλοιπες 26 γραμμές ήταν κυκλικές μεταθέσεις της 1^{ης} γραμμής κατά 0,1,2..,25 θέσεις. Οι στήλες

αντιστοιχούν στο α.κ. και το κ.κ. βρίσκεται στην τομή γραμμής και στηλης. Έτσι, το α.κ. “deus” δίνει το κ.κ. DFWS.

Ο ***Cardano*** χρησιμοποίησε στη συνέχεια τη *μέθοδο της μάσκας*, όπου τοποθετώντας μια διάτρητη κάρτα πάνω σε λευκό χαρτί, το α.κ. γράφεται μέσα στα παράθυρα. Βγάζουμε τη μάσκα και συμπληρώνουμε το χαρτί με τυχαίες λέξεις. Για να διαβάσουμε, πρέπει να τοποθετήσουμε πάλι τη μάσκα και διαβάζουμε το μήνυμα που βρίσκεται μέσα στα παράθυρα. Η μέθοδος αυτή είχε μεγάλη απήχηση στους διπλωματικούς κύκλους του 1800.

Σπουδαίο επίσης ήταν το κρυπτοσύστημα του ***Vigenere*** όπου το α.κ. και το κ.κ. είναι το κλειδί. Ο *πίνακας Vigenere* ήταν μια πολύ ασφαλής κρυπτογραφική μέθοδος για 300 περίπου χρόνια μέχρι που ο F.Kaziski κατάφερε να βρεί μία μέθοδο κρυπτοανάλυσης των πινάκων Vigenere.

Μεγάλη επιτυχία σαν κρυπτολόγος είχε και ο ***Charles Babbage***, ο εφευρέτης της αναλυτικής μηχανής, δηλαδή ο πρόδρομος των σημερινών computers. Αυτός κατάφερε να σπάσει διγραφικά κρυπτοσυστήματα, δηλαδή συστήματα όπου ζεύγη γραμμάτων κρυπτογραφούνται, όπως το σύστημα *Playfair*.

Ο Γερμανός εφευρέτης ***Άρθουρ Σέρμπιους***, ανέπτυξε το 1918 ένα νέο μηχανικό κρυπτογραφικό σύστημα, γνωστό σαν *Αίνιγμα*. Η βασική μορφή του αποτελείται από ένα πληκτρολόγιο για την εισαγωγή του α.κ., μια αναδιατακτική μονάδα που αντιστοιχίζει κάθε γράμμα του α.κ. σ’ ένα γράμμα του κ.κ. και έναν ηλεκτρονικό πίνακα που δείχνει το αντίστοιχο γράμμα του κ.κ. Αυτό, όμως, μια ομάδα κρυπτοαναλυτών κατάφερε να το σπάσει και να αποσπάσει σημαντικές πληροφορίες κατά τη διάρκεια του πολέμου.

Μετά τον πόλεμο η κρυπτογραφία γνώρισε ιδιαίτερη άνθιση, χάρη στην τεχνολογία των υπολογιστών. Τα κλασσικά συστήματα κρυπτογραφίας έπρεπε να λύσουν το πρόβλημα της ανταλλαγής κλειδιών. Να βρεθεί, δηλαδή, ένας τρόπος ασφαλής, ώστε ο αποστολέας και ο παραλήπτης κρυπτομηνυμάτων να μπορούν να ανταλλάξουν το τρέχον κλειδί. Πέρα από την ασφάλεια, το πρόβλημα είναι και στις περιπτώσεις όπου η επικοινωνία πρέπει να γίνεται γρήγορα, φθηνά και τα κλειδιά να αλλάζουν συχνά.

Ο ***Ουίτφιλντ Ντίφι*** και ο ***Μάρτιν Χέλμαν*** το 1976 στη μελέτη τους «*Νέες κατευθύνσεις για την κρυπτογραφία*» πρότειναν κάτι καινοτόμο. Να υπάρχει δημόσια επικοινωνία μεταξύ δύο ατόμων χωρίς να υπάρχει ανάγκη ανταλλαγής κλειδιών μεταξύ τους. Το σκεπτικό ήταν το εξής: Ο αποστολέας Α κλειδώνει το μήνυμα σ’ ένα κουτί και το στέλνει στον παραλήπτη Β με το δημόσιο ταχυδρομείο.

Ο Β προσθέτει το δικό του λουκέτο στο κουτί και το στέλνει πίσω στον Α. Ο Α αφαιρεί το δικό του λουκέτο και το στέλνει εκ νέου στον Β, ο οποίος μπορεί τώρα ν' ανοίξει το κουτί (αφού είναι ασφαλισμένο μόνο με το δικό του λουκέτο) και να διαβάσει το μήνυμα.

Αργότερα, τρεις επιστήμονες, οι ***Ρόναλντ Ριβέστ***, ***Άντι Σάμιρ*** και ***Λέοναρντ Άντλεμαν*** επινόησαν το πρώτο ολοκληρωμένο δημόσιο κρυπτοσύστημα, το RSA. Πρόκειται για ένα κρυπτοσύστημα δημοσίου κλειδιού, του οποίου η ασφάλεια βασίζεται στο ότι δεν υπάρχει ταχύς αλγόριθμος παραγοντοποίησης μεγάλων αριθμών που να είναι γινόμενο δύο μεγάλων πρώτων.

1.2 ΣΧΗΜΑΤΑ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ

Οι *ψηφιακές υπογραφές* είναι ένας από τους σπουδαιότερους κλάδους της εφαρμοσμένης Κρυπτογραφίας και αποτελούν ίσως την πιο σημαντική εξέλιξη στην ιστορία της. Η πλήρης ονομασία τους είναι ***Σχήματα Ψηφιακών Υπογραφών (Digital Signature Schemes)*** ή απλούστερα, ***Σχήματα Υπογραφών*** και η ιδέα και χρησιμότητά τους αναγνωρίστηκαν πολύ πριν οποιαδήποτε πρακτική εφαρμογή ήταν εφικτή. Η πρώτη μέθοδος που ανακαλύφθηκε ήταν το σχήμα υπογραφής RSA, το οποίο μέχρι και σήμερα είναι μία από τις πιο πρακτικές τεχνικές που διαθέτουμε. Μεταγενέστερες έρευνες είχαν ως αποτέλεσμα πολλές εναλλακτικές τεχνικές ψηφιακών υπογραφών με σημαντικά πλεονεκτήματα στη λειτουργικότητα και στην εφαρμογή τους.

Σκοπός μιας ψηφιακής υπογραφής είναι να συνδέσει την ταυτότητα ενός ατόμου με ένα ποσό πληροφορίας. Για να γίνουμε πιο συγκεκριμένοι, θα μελετήσουμε την αντιστοιχία της με μια χειρόγραφη υπογραφή.

Μια χειρόγραφη υπογραφή σε ένα έγγραφο δηλώνει το άτομο που είναι υπεύθυνο γι'αυτό. Η αντιστοιχία μεταξύ ατόμων και υπογραφών είναι μονοσήμαντη, έτσι ώστε αν προκύψει κάποιο νομικό θέμα, να μπορεί να διαπιστωθεί εύκολα (με τη βοήθεια ενός γραφολόγου) αν η υπογραφή ανήκει όντως στο άτομο αυτό. Ο ρόλος της ψηφιακής υπογραφής είναι ανάλογος με αυτόν της χειρόγραφης, αλλά για δεδομένα αποθηκευμένα σε ψηφιακή μορφή. Σημαντικό είναι να αναφέρουμε ότι όλο και περισσότερες χώρες, μετά τις ΗΠΑ, αρχίζουν να αναγνωρίζουν νομικά την ισχύ της ψηφιακής υπογραφής.

Η ανάγκη επινόησης μιας τέτοιας υπογραφής είναι αποτέλεσμα της μεγάλης ποσότητας πληροφορίας που διακινείται πλέον μέσω του διαδικτύου. Οι ηλεκτρονικές συναλλαγές, η επικοινωνία μέσω ηλεκτρονικού ταχυδρομίου, οι ηλεκτρονικές δημοπρασίες και πολλές άλλες δραστηριότητες απαιτούν κάποια επιβεβαίωση της μιας πλευράς στην άλλη. Επίσης, συχνά είναι απαραίτητο να κατοχυρωθεί η ευρεσιτεχνία (copyright) δεδομένων αποθηκευμένων σε ηλεκτρονική μορφή. Τέλος, η ανακάλυψη των ψηφιακών υπογραφών επέφερε σημαντική πρόοδο στον τομέα της ασφάλειας υπολογιστικών συστημάτων.

Στο σημείο αυτό, μπορούμε να δώσουμε τις βασικές διαφορές μεταξύ χειρόγραφων και ψηφιακών υπογραφών:

- Μία χειρόγραφη υπογραφή επισυνάπτεται με φυσικό τρόπο στο έγγραφο (ή μήνυμα), έτσι ώστε κάθε γνήσιο αντίγραφό του να την περιέχει. Αποτελεί, λοιπόν, αναπόσπαστο κομμάτι του. Αντιθέτως, μία ψηφιακή υπογραφή είναι δυνατό να αφαιρεθεί από το αρχικό μήνυμα. Για να ξεπεραστεί το πρόβλημα αυτό, είναι απαραίτητο ο *αλγόριθμος υπογραφής* να συνδέει με κάποιο

τρόπο το μήνυμα με την υπογραφή. Ένας τρόπος να επιτευχθεί αυτό είναι να κρυπτογραφήσουμε το υπογεγραμμένο μήνυμα προτού το στείλουμε σ'αυτόν που επιθυμούμε. Συνεπώς, είναι υψίστης σημασίας η διαδικασία να γίνεται με τη σειρά *Υπογραφή* $\rightarrow$ *Κρυπτογράφηση*. Διαφορετικά, αν κάποιος αντίπαλος καταφέρει να υποκλέψει το υπογεγραμμένο μήνυμα του Α προς τον Β, τότε μπορεί να αφαιρέσει την υπογραφή του Α και προσθέτοντας τη δική του, θα μπορεί να υποδύεται τον Α σε μελλοντικές συναλλαγές του με τον Β.

- Μια χειρόγραφη υπογραφή επαληθεύεται συγκρίνοντάς την με προηγούμενες αυθεντικές υπογραφές του ατόμου σε άλλα έγγραφα. Η μέθοδος αυτή δεν είναι ιδιαίτερα ασφαλής, καθώς είναι σχετικά εύκολη η πλαστογράφηση. Ο μόνος που μπορεί να επιβεβαιώσει την αυθεντικότητα μιας υπογραφής με ανάλογη ασφάλεια είναι ο γραφολόγος. Από την άλλη μεριά, η επαλήθευση μιας ψηφιακής υπογραφής πραγματοποιείται με τη χρήση ενός δημοσίως γνωστού *αλγόριθμου επαλήθευσης*. Είναι φανερό ότι οποιοσδήποτε μπορεί να επαληθεύσει τη γνησιότητα μιας ψηφιακής υπογραφής. Η χρήση ασφαλών σχημάτων υπογραφών μειώνει την πιθανότητα πλαστογράφησης.

Ορισμός 1.1: Ένας ***αλγόριθμος υπογραφής*** είναι μια μέθοδος για να παραχθεί μια ψηφιακή υπογραφή.

Ορισμός 1.2: Ένας ***αλγόριθμος επαλήθευσης*** είναι μία μέθοδος για να επαληθευτεί αν μια ψηφιακή υπογραφή είναι αυθεντική.

Επισημαίνουμε ότι καθώς η ψηφιακή υπογραφή δεν αποτελεί μέρος του μηνύματος στο οποίο επισυνάπτεται, καλό θα ήταν αυτό να περιέχει πληροφορίες, όπως ημερομηνία και ώρα, έτσι ώστε να αποφεύγεται η επαναχρησιμοποίησή του. Φτάνει να αναλογιστούμε τί συνέπειες θα είχε για τον Α το να δώσει στον Β μια ηλεκτρονική επιταγή υπογεγραμμένη ψηφιακά, χωρίς ημερομηνία και ώρα.

Συνοψίζοντας, μια ***ψηφιακή υπογραφή*** είναι μία κρυπτογραφημένη ομάδα δεδομένων, η οποία σχετίζεται με το περιεχόμενο, (προαιρετικά) την ημερομηνία δημιουργίας του μηνύματος και την ταυτότητα του αποστολέα. Η διαδικασία εξασφαλίζει ότι το μήνυμα δεν έχει αλλαχθεί από τη στιγμή που υπογράφηκε από τον Α και ότι αυτός είναι ο "πραγματικός" αποστολέας του μηνύματος.

Οι ψηφιακές υπογραφές έχουν πολλές εφαρμογές στην ασφάλεια πληροφοριών, συμπεριλαμβανομένης της αυθεντικότητας, της ακεραιότητας και της μη απάρνησης των δεδομένων. Μία από τις σημαντικότερες είναι η πιστοποίηση δημοσίων κλειδιών σε μεγάλα δίκτυα. Σ'αυτή την περίπτωση, είναι απαραίτητη η μεσολάβηση μίας *Έμπιστης Αρχής (Trusted Third Party (TTP)),* η οποία συνδέει την ταυτότητα κάθε χρήστη με ένα δημόσιο κλειδί. Αυτό, δίνει τη δυνατότητα σε άλλους χρήστες να μπορούν να πιστοποιήσουν μεταγενέστερα τη γνησιότητα ενός δημοσίου κλειδιού χωρίς τη βοήθεια μιας TTP.

Πιο συγκεκριμένα, μία Έμπιστη Αρχή είναι μία εξουσία πιστοποίησης, η οποία πιστοποιεί την αυθεντικότητα των δημοσίων κλειδιών και λειτουργεί ως εξής:

- Όλοι οι χρήστες στο δίκτυο έχουν ένα αντίγραφο του δημόσιου κλειδιού της TTP.
- Η TTP είναι υπεύθυνη για την έκδοση *ψηφιακών πιστοποιητικών (digital certificates)*. Με άλλα λόγια, υπογράφει ψηφιακά ακολουθίες δεδομένων της μορφής (Α, δημόσιο κλειδί του Α), όπου Α κάποιος χρήστης. Η TTP υπογράφει αυτά τα δεδομένα μόνο εάν πιστεύει ότι πράγματι το δημόσιο κλειδί ανήκει στον Α.
- Όταν ο χρήστης Α στείλει στον Β το δημόσιο κλειδί του, ο Β εμπιστεύεται την προέλευσή του, ότι δηλαδή ανήκει στον Α, αφού θεωρεί αξιόπιστο το έργο της TTP.

Με αυτό τον τρόπο, επιλύονται προβλήματα σχετικά με τη σύνδεση ενός δημόσιου κλειδιού με τον κάτοχό του, η επικύρωση της οποίας είναι απαραίτητη κάποια μελλοντική χρονική στιγμή ή όταν είναι αδύνατη η φυσική παρουσία του κατόχου.

Τα σχήματα ψηφιακών υπογραφών βασίζονται σε αλγόριθμους κρυπτογράφησης δημοσίου κλειδιού και αποτελούνται από δύο συνιστώσες: έναν *αλγόριθμο υπογραφής* και έναν *αλγόριθμο επαλήθευσης.* Για την υπογραφή ενός μηνύματος m, συνήθως ο Α δημιουργεί αρχικά μία σύνοψη αυτού του μηνύματος (message digest) με την εφαρμογή μιας κρυπτογραφικής συνάρτησης κατακερματισμού (για την ώρα θα συμβολίζουμε τη σύνοψη επίσης με m). Στη συνέχεια, η σύνοψη του μηνύματος κρυπτογραφείται χρησιμοποιώντας το ιδιωτικό κλειδί του Α και κατάλληλο μυστικό αλγόριθμο υπογραφής sig_K. Η παραγόμενη ακολουθία χαρακτήρων $sig_K(m)$ αποτελεί την ψηφιακή υπογραφή του Α και μπορεί να επαληθευτεί μελλοντικά με τη χρήση ενός δημόσιου αλγόριθμου επαλήθευσης ver_K.

Ας δώσουμε, όμως, τώρα έναν πιο αυστηρό ορισμό του σχήματος ψηφιακής υπογραφής:

<u>Ορισμός 1.3</u>: ***(Σχήμα ψηφιακής υπογραφής)***

Ένα σχήμα ψηφιακής υπογραφής είναι μια πεντάδα (M, Y, K, S, V), όπου ικανοποιούνται τα ακόλουθα:

- M: ο χώρος όλων των δυνατών μηνυμάτων
- Y: ο χώρος όλων των δυνατών υπογραφών
- K: ο χώρος όλων των πιθανών κλειδιών
- Για κάθε K $\in$ K, υπάρχει ένας αλγόριθμος υπογραφής $sig_K \in S$ και ο αντίστοιχος αλγόριθμος επαλήθευσης $ver_K \in V$. Κάθε $sig_K : M \to Y$ και $ver_K : M \times Y \to$ {αληθής, ψευδής} είναι συναρτήσεις τέτοιες ώστε να ικανοποιείται η ακόλουθη ισότητα για κάθε μήνυμα m ∈ M και για κάθε υπογραφή $s \in Y$:

$$ver_K(m,s) = \begin{cases} \alpha\lambda\eta\theta\acute{\eta}\varsigma, \ \alpha\nu \ s = sig_K(m) \\ \psi\varepsilon\upsilon\delta\acute{\eta}\varsigma, \ \text{αν} \ s \neq sig_K(m) \end{cases}$$

Κάθε σχήμα ψηφιακής υπογραφής θα πρέπει να έχει τις παρακάτω ιδιότητες:

1. Δοθέντος ενός ζεύγους (m,s), ο αλγόριθμος επαλήθευσης επιστρέφει απάντηση "αληθής" ή "ψευδής", ανάλογα με το αν η υπογραφή είναι αυθεντική ή όχι.

2. Θα πρέπει να ισχύει $ver_K(m,s) =$ αληθής $\Leftrightarrow \ sig_K(m) = s, \ \forall \ m \in M, s \in S$.

3. Θα πρέπει να είναι υπολογιστικά εύκολο για κάποιον να παράξει την υπογραφή του και για οποιονδήποτε άλλο να επαληθεύσει τη γνησιότητά της. Αυτό σημαίνει ότι για κάθε K∈K ,οι sig_K και ver_K πρέπει να είναι συναρτήσεις (αλγόριθμοι) πολυωνυμικού χρόνου. Η ver_K είναι δημόσια, ενώ η sig_K μυστική, γνωστή μόνο στον υπογράφοντα.

4. Θα πρέπει να είναι υπολογιστικά αδύνατο για έναν αντίπαλο να πλαστογραφήσει την υπογραφή του Α σε ένα μήνυμα m. Αυτό σημαίνει ότι, δοθέντος μηνύματος m, μόνο ο Α πρέπει να είναι σε θέση να κατασκευάσει υπογραφή s, έτσι ώστε $ver_K(m,s) =$ αληθής.

Σημείωση 1.1: Ένας *αλγόριθμος πολυωνυμικού χρόνου* είναι ένας αλγόριθμος, ο οποίος στη χειρότερη περίπτωση είναι πολυπλοκότητας $O(n^k)$, όπου n το μέγεθος εισόδου και k μία σταθερά.

Τα σχήματα ψηφιακών υπογραφών διακρίνονται σε δύο μεγάλες κατηγορίες:

A. ***Σχήματα ψηφιακών υπογραφών με παράρτημα*** *(digital signature schemes with appendix):* Στα σχήματα αυτής της κατηγορίας, το αρχικό μήνυμα είναι απαραίτητο για την επαλήθευση γνησιότητας της υπογραφής.

B. ***Σχήματα ψηφιακών υπογραφών με δυνατότητα ανάκτησης του μηνύματος*** *(digital signature schemes with message recovery):* Στα σχήματα αυτά, το αρχικό μήνυμα μπορεί να ανακτηθεί από την ίδια την υπογραφή.

Οι κατηγορίες αυτές μπορούν να υποδιαιρεθούν περαιτέρω σε:

- *Ντετερμινιστικά σχήματα υπογραφής,* στα οποία δεν υπάρχει περίπτωση λάθους του αλγόριθμου επαλήθευσης. Ο υπολογισμός που προτείνει ο αλγόριθμος είναι γραμμικός.
- *Τυχαιοποιημένα σχήματα υπογραφής,* στα οποία ο αλγόριθμος επαλήθευσης είναι πιθανοτικός, δηλαδή, υπάρχει πιθανότητα να δώσει λάθος αποτέλεσμα. Παρόλα αυτά, οι αλγόριθμοι αυτοί είναι πιο αποδοτικοί, γι'αυτό τα τυχαιοποιημένα σχήματα συνήθως προτιμώνται.

Σημείωση 1.2: Ένας αλγόριθμος είναι *αποδοτικός* αν έχει πολυωνυμικό χρόνο εκτέλεσης.

1.3 ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ (Cryptographic Hash Functions)

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού παίζουν πρωταρχικό ρόλο στην σύγχρονη κρυπτογραφία. Η λειτουργία τους είναι όμοια με αυτή των συναρτήσεων κατακερματισμού που χρησιμοποιούνται σε άλλα πεδία εφαρμογών σε υπολογιστές, δηλαδή απεικονίζουν στοιχεία ενός συνόλου με πολλά στοιχεία, σε κάποιο άλλο σύνολο με λιγότερα στοιχεία. Στην εργασία αυτή, περιοριζόμαστε στις κρυπτογραφικές συναρτήσεις κατακερματισμού, οι οποίες έχουν εφαρμογές στην ακεραιότητα των δεδομένων και στην πιστοποίηση μηνυμάτων.

Οι συναρτήσεις κατακερματισμού είναι υπολογιστικά εφικτές συναρτήσεις της μορφής h: $X \to Y$, όπου $|X| > |Y|$ και Y πεπερασμένο σύνολο, ενώ δεν αποκλείεται $|X| = \infty$. Δέχονται ως όρισμα ένα οσοδήποτε μεγάλο μήνυμα m και παράγουν ως αποτέλεσμα ένα αλφαριθμητικό σταθερού μήκους, ίσου ή μικρότερου του μεγέθους του ορίσματος. Πιο συγκεκριμένα, μια συνάρτηση κατακερματισμού h αντιστοιχίζει σειρές bit μεταβλητού μεγέθους σε μία ακολουθία συγκεκριμένου μεγέθους. Η ακολουθία αυτή συμβολίζεται με h(x) και ονομάζεται σύνοψη του μηνύματος (message digest), ή αποτύπωμα (fingerprint), ή τιμή κατακερματισμού (hash value), είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Από τη σύνοψη του μηνύματος είναι υπολογιστικά ανέφικτο να εξάγουμε το αρχικό μήνυμα, δηλαδή η αντιστροφή μιας τέτοιας συνάρτησης είναι αδύνατη. Λέμε, λοιπόν, οτι οι κρυπτογραφικές συναρτήσεις κατακερματισμού ειναι συναρτήσεις μονής κατεύθυνσης (one-way functions).

<u>Ορισμός 1.4:</u> Μια συνάρτηση κατακερματισμού $h : X \to Y$ θα λέγεται ***μοναδικής κατεύθυνσης*** αν για κάθε $x \in X$, υπάρχει αλγόριθμος πολυωνυμικού χρόνου που να υπολογίζει την τιμή h(x), ενώ είναι υπολογιστικά αδύνατο να βρούμε $x \in X$ με h(x) = y για κάθε $y \in h(Y)$.

Παράδειγμα 1.1:

Αν p είναι τυχαία επιλεγμένος 1024-bit πρώτος αριθμός και g είναι ένα πρωταρχικό στοιχείο modp, τότε η συνάρτηση f: {0, 2, …, p-2} → {1, 2, …, p-1}, με τύπο $f(x) = g^x \bmod p$, είναι εύκολο να υπολογιστεί με γρήγορη ύψωση σε εκθέτη. Όμως, δεν μπορούμε να υπολογίσουμε την αντίστροφή της σε πολυωνυμικό χρόνο. Έτσι, η f μπορεί να χρησιμοποιηθεί σα συνάρτηση μοναδικής κατεύθυνσης.

■

Ένα επιπλέον σημαντικό χαρακτηριστικό των hash συναρτήσεων είναι η υπερβολικά μεγάλη «ευαισθησία» που έχουν στο περιεχόμενο του μηνύματος εισόδου. Αυτό σημαίνει ότι και η παραμικρή αλλαγή του, συνεπάγεται την παραγωγή μιας εντελώς διαφορετικής σύνοψης. Για να το κατανοήσουμε καλύτερα, μπορούμε να δούμε το εξής παράδειγμα:

Έστω οτι εφαρμόζουμε μια συνάρτηση κατακερματισμού στο αλφαριθμητικό "RAM". Αυτό που θα πάρουμε ως αποτέλεσμα, είναι το αλφαριθμητικό "8d8bea89388715ee7c01183a0667e892". Άν, όμως, εφαρμόσουμε την ίδια συνάρτηση στο αλφαριθμητικό "RAM", θα πάρουμε το "73ac38c363394f66211f67f0a92b480a", το οποίο δεν έχει καμία ομοιότητα με το προηγούμενο.

Όπως βλεπουμε, η πιθανότητα δύο διαφορετικά μηνύματα να έχουν την ίδια σύνοψη, είναι εξαιρετικά μικρή.

Μπορούμε τώρα, με βάση τα παραπάνω, να δώσουμε τον ορισμό της συνάρτησης κατακερματισμού:

Ορισμός 1.5: Μια *(μονόδρομη) συνάρτηση κατακερματισμού h* είναι ένας μετασχηματισμός που έχει τις ακόλουθες ιδιότητες:

- **Συμπίεση** (compression): το όρισμα x έχει ένα αυθαίρετο, πεπερασμένο μήκος, ενώ η h(x) έχει περιορισμένο, σταθερό μήκος
- **Ευκολία στον υπολογισμό** (ease of computation): δοθείσης της συνάρτησης h και ενός ορίσματος x, το h(x) μπορεί να υπολογιστεί εύκολα.
- **Αντίσταση 1ου ορίσματος** (preimage resistance)-**μη αντιστρεψιμότητα:** είναι υπολογιστικά αδύνατο για ένα δεδομένο στοιχείο y του πεδίου τιμών της h, να βρεθεί στοιχείο x του πεδίου ορισμού, τέτοιο ώστε h(x) = y.
- **Αντίσταση 2ου ορίσματος** (2nd - preimage resistance): είναι υπολογιστικά ανέφικτο για δεδομένο στοιχείο x_1 του πεδίου ορισμού της h, να βρεθεί άλλο στοιχείο x_2, έτσι ώστε $h(x_1) = h(x_2)$.

Εκτός απο τις βασικές ιδιότητες των συναρτήσεων κατακερματισμού, υπάρχουν και κάποιες επιπλέον που θα ήταν σκόπιμο να αναφερθούν:

- **Μή συσχέτιση** (non-correlation): τα bit εισόδου και εξόδου δεν πρέπει να είναι συσχετισμένα.
- **Αντίσταση κοντινής σύγκρουσης** (near-collision resistance): πρέπει να είναι υπολογιστικά δύσκολο να βρεθούν ορίσματα x_1, x_2, ώστε οι αντίστοιχες τιμές $h(x_1)$, $h(x_2)$ να διαφέρουν ελάχιστα.

- **Αντίσταση μερικού ορίσματος** (partial preimage resistance) - **Τυπική μονοδρομικότητα** (local one-wayness): η υπολογιστική δυσκολία ανάκτησης μιας οποιασδήποτε υπακολουθίας χαρακτήρων πρέπει να είναι αντίστοιχη με μιας ολόκληρης εισόδου.

1.3.1 ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ ΚΑΙ ΣΥΝΑΡΤΗΣΕΙΣ ΣΥΜΠΙΕΣΗΣ

Σε κρυπτογραφικές εφαρμογές υπολογιστών, όπου έχουμε το αλφαβητο Σ = {0,1} , μια συνάρτηση κατακερματισμού ορίζεται μαθηματικά ώς εξής: $h:\Sigma^* \to \Sigma^n$, n $\in N$. Επομένως, οι συναρτήσεις κατακερματισμού απεικονίζουν ακολουθίες αυθαίρετου μήκους σε ακολουθίες σταθερού μήκους. 'Οπως φαίνεται και από τον ορισμό, οι συναρτήσεις αυτές δεν ειναι 1-1.

***Παράδειγμα 1.2*:**

Η απεικόνιση $h:\Sigma^* \to \Sigma^n$, n $\in N$, που στέλνει το $b_1b_2...b_k$ του {0,1}* στο $(b_1 + b_2 +...+b_k)$mod2, αποτελεί μια συνάρτηση κατακερματισμού. Για παράδειγμα, η ακολουθία 01101011 απεικονίζεται στο 1, ενώ η ακολουθία 110011 στο 0. Γενικά, αν το πλήθος των μονάδων μιας ακολουθίας b είναι περιττός αριθμός απεικονίζεται στο 1, διαφορετικά αν είναι άρτιος απεικονίζεται στο 0.

■

Οι συναρτήσεις κατακερματισμού κατασκευάζονται χρησιμοποιώντας συναρτήσεις συμπίεσης (compression functions). Μια *συνάρτηση συμπίεσης*, είναι μια απεικόνιση $h:\Sigma^m \to \Sigma^n$, όπου n, m$\in N$, m > n και απεικονίζει ακολουθίες σταθερού μήκους σε ακολουθίες μικρότερου μήκους.
Μιά συνάρτηση hash μπορεί να κατασκευαστεί εφαρμόζοντας επανειλημμένα μια συνάρτηση συμπίεσης μέχρι να επεξεργαστούμε ολόκληρο το μήνυμα.

***Παράδειγμα 1.3*:**

Η απεικόνιση $h:\Sigma^m \to \Sigma^n$, όπου n, m$\in N$ που στέλνει το $b_1b_2...b_m$ του $\{0,1\}^m$ στο $(b_1 + b_2 +...+b_m)\text{mod}2$, αποτελεί μια συνάρτηση συμπίεσης αν m > 1, αφού n = 1. Για παραδειγμα, το 101010 απεικονίζεται στο 1, ενώ το 001111 στο 0. ■

Παρατηρούμε ότι ο χώρος των δυνατών μηνυμάτων είναι πολύ μεγαλύτερος από το χώρο των message digests και επειδή οι συναρτήσεις κατακερματισμού δεν είναι 1-1, η ύπαρξη μηνυμάτων που έχουν την ίδια συνοψη είναι αναπόφευκτη. Αυτό που μας ενδιαφέρει στην κατασκευή μιας συνάρτησης κατακερματισμού, για να ενισχύσουμε την ασφάλεια της, είναι να είναι πολύ δύσκολο να βρεθούν τέτοια μηνύματα.

Ορισμός 1.6: Όταν υπάρχει ένα ζεύγος τιμών (x_1,x_2), για τις οποίες ισχύει $x_1 \neq x_2$ και $h(x_1) = h(x_2)$, τότε λέμε ότι έχουμε μια ***σύγκρουση (collision)*** για την h.

Παράδειγμα 1.4:

Μία σύγκρουση της συνάρτησης κατακερματισμού του Παραδείγματος 1.2, είναι ένα ζεύγος διακεκριμένων ακολουθιών με περιττό πλήθος μονάδων, όπως οι (111, 001).

■

Ορισμός 1.7: Η συνάρτηση h ονομάζεται ***ασθενώς ανθεκτική σε συγκρούσεις (weak collision resistance)***, αν για δεδομένο $x_1 \in X$, είναι ανέφικτος ο υπολογισμός μιάς σύγκρουσης (x_1, x_2).

Ορισμός 1.8: Η συνάρτηση h ονομάζεται ***(ισχυρώς) ανθεκτική σε συγκρούσεις (strong collision resistance)***, αν είναι ανέφικτος ο υπολογισμός οποιασδήποτε σύγκρουσης (x_1, x_2) της h.

Ορισμός 1.9: Η δυσκολία εύρεσης δύο διαφορετικών τιμών του πεδίου ορισμού της h , x_1, x_2, έτσι ώστε $h(x_1) = h(x_2)$, ονομάζεται ***αντίσταση σε συγκρούσεις***.

Παρατηρήσεις:

1. Ο όρος ασθενής αντίσταση σε συγκρούσεις ταυτίζεται με τον όρο αντίσταση $2^{ου}$ ορισματος, ενώ ο όρος ισχυρή αντίσταση σε συγκρούσεις ταυτίζεται με τον όρο αντίσταση σε συγκρούσεις.

2. Οι συναρτήσεις κατακερματισμού μοναδικής κατεύθυνσης είναι ασθενώς ανθεκτικές σε συγκρούσεις, ενώ μπορεί να δειχθεί ότι οι ισχυρώς ανθεκτικές συναρτήσεις κατακερματισμού είναι μοναδικής κατεύθυνσης. Η ιδέα έχει ως εξής: υποθέτουμε ότι υπάρχει ένας αλγόριθμος αντιστροφής για την h. Επιλέγουμε μιά τυχαία ακολουθία x_1 και υπολογίζουμε την αντίστροφη εικόνα του $y = h(x_1)$, έστω x_2 , χρησιμοποιώντας τον αλγόριθμο. Αν $x_1 \neq x_2$, το ζεύγος (x_1,x_2) είναι μία σύγκρουση της h.

1.3.2 ΣΥΝΑΡΤΗΣΕΙΣ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ ΚΑΙ ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Μία απο τις κυριότερες εφαρμογές των συναρτήσεων κατακερματισμού είναι πάνω στις ψηφιακές υπογραφές. Εφόσον το μήκος μιας ψηφιακής υπογραφής είναι σχεδόν το ίδιο με το μήκος του προς υπογραφή μηνύματος, συχνά είναι προτιμότερο οι κρυπτογραφικές διαδικασίες να εφαρμόζονται στη σύνοψη του μηνύματος. Έτσι, κερδίζουμε σε χώρο και σε χρόνο, αφού η σύνοψη είναι πιο μικρή και πιο εύκολη στη διαχείριση απο το αρχικό μήνυμα. Συνεπώς, ενισχύεται η αποδοτικότητα των αλγόριθμων υπογραφής και επαλήθευσης και διαφυλάσσεται η ακεραιότητα των δεδομένων. Τέλος, οι hash συναρτήσεις αποτελούν μια αξιόπιστη λύση έναντι των πλαστογραφήσεων.

Η εξέλιξη της κρυπτογραφίας και η ανάγκη για ασφαλέστερες ηλεκτρονικές επικοινωνίες, οδήγησαν στην εμφάνιση κάποιων σημαντικών συναρτήσεων κατακερματισμού και σχετικών τεχνολογιών.

Αξίζει να αναφέρουμε τις ακόλουθες:

- **HMAC :** Είναι μια τεχνική με την οποία ελέγχουμε αν κάποιο αρχείο έχει τροποποιηθεί. Εφαρμόζουμε μια συνάρτηση κατακερματισμού στο κείμενο και στέλνουμε την σύνοψη κρυπτογραφημένη μαζί με το αρχικό κείμενο. Ο παραλήπτης την αποκρυπτογραφεί, κατακερματίζει το μήνυμα και αν το αποτέλεσμα συμφωνεί με το αρχικό κείμενο, τότε το μήνυμα έφτασε αφαλές. Η συνάρτηση κατακερματισμού είναι δημόσια γνωστή.

- **<u>Η Σειρά MD</u> (Message Digest):** Η ύπαρξη της οφείλεται στον Ron Rivest και είναι συναρτήσεις κατακερματισμού που δίνουν ως αποτέλεσμα έναν αριθμό των 128 bits. Η διαφορά τους είναι στην ταχύτητα με την οποία μπορούν να υπολογιστούν και στην ισχύ τους.

- **<u>Η σειρά SHA</u> (Secure Hash Algorithm):** Δημοσιεύτηκε το 1993 απο το National Institut of Standards and Technology (NIST), αλλά το 1995 εντοπίστηκε μια αδυναμία στον αλγόριθμο της και έτσι τον τροποποίησαν. Ο νέος αλγόριθμος ονομάστηκε SHA-1 και αποτελεί την πλέον δημοφιλή συνάρτηση κατακερματισμού. Το μήνυμα εισόδου πρέπει να είναι μικρότερο απο 2^{64} bits και η έξοδός του κρυπτογράφημα μήκους 160 bits.

1.3.3 Birthday attack

Μερικές συναρτήσεις κατακερματισμού παράγουν στην έξοδό τους σύνοψη μικρού μήκους. Αυτό αποτελεί μεγάλο μειονέκτημα, καθώς διευκολύνει την εύρεση ενός άλλου μηνύματος με την ίδια σύνοψη, πράγμα που τις καθιστά ευάλωτες σε επιθέσεις birthday attack. Ας εξηγήσουμε, όμως, τι εννοούμε με τον όρο birthday attack.

Η birthday attack ανήκει στις επιθέσεις ωμής βίας, δηλαδή βασίζεται στη δοκιμή κάθε πιθανού κλειδιού για την εύρεση του σωστού. Η λειτουργία της στηρίζεται στο *παράδοξο των γενεθλίων (birthday paradox)*, το οποίο είναι το ακόλουθο:

Παράδοξο γενεθλίων:

«Εάν έχουμε μια τάξη με 23 μαθητές, η πιθανότητα 2 απο αυτούς να έχουν γενέθλια την ίδια μέρα είναι τουλάχιστον 50% (για την ακρίβεια 0.507).»

Άν οι μαθητές ήταν 30, τότε η πιθανότητα ανέρχεται σε 70% περίπου και γενικά, όσο περισσότεροι είναι οι μαθητές, τόσο αυξάνεται η πιθανότητα. Πιο γενικά, υποθέτουμε ότι έχουμε n αντικείμενα, όπου n είναι αρκετά μεγάλο. Επιπλέον, έχουμε r ανθρώπους και καθένας απ'αυτούς διαλέγει ένα αντικείμενο (με επανατοποθέτηση, έτσι ώστε περισσότεροι από ένας άνθρωποι να μπορούν να διαλέγουν το ίδιο αντικείμενο). Τότε, η πιθανότητα τουλάχιστον 2 ανθρωποι να

έχουν διαλέξει το ίδιο αντικείμενο είναι περίπου ίση με $1-e^{-r^2/2n}$. Επιλέγοντας $r^2/2n = \ln 2$, βρίσκουμε ότι $r \approx 1{,}17\sqrt{n}$ και η πιθανότητα είναι περίπου ίση με 50%.

Η εφαρμογή του Παράδοξου των Γενεθλίων στην Κρυπτογραφία απαιτεί μια μικρή τροποποίηση:

« Έστω ότι έχουμε 2 τάξεις, κάθε μία με 30 μαθητές. Ποιά είναι η πιθανότητα ένας μαθητής απο την $1^η$ τάξη να έχει την ίδια μέρα γενέθλια με κάποιο μαθητή απο την $2^η$ τάξη;»

Ας δούμε μια γενικότερη διατύπωση του προβλήματος: Έστω ότι έχουμε n αντικείμενα και 2 ομάδες, με r ατομα η καθεμιά. Κάθε άτομο από κάθε ομάδα διαλέγει ένα αντικείμενο (με επανατοποθέτηση). Άν θέσουμε $\lambda = r^2/n$, τότε η πιθανότητα ένα άτομο από την $1^η$ ομάδα να επιλέξει το ίδιο αντικείμενο με ένα άτομο από την $2^η$ ομάδα, είναι ίση με $1-e^{-\lambda}$. Παρατηρούμε ότι για $r \approx \sqrt{n}$, η πιθανότητα αυτή είναι αρκετά μεγάλη. Όσο αυξάνουμε το r, η πιθανότητα γίνεται και μεγαλύτερη.

Βλέπουμε ότι στην περίπτωση των τάξεων με τους 30 μαθητές που αναφέραμε πριν, είναι: $n = 365$ και $r = 30$, οπότε $\lambda = 30^2/365 = 2.466$ και $1-e^{-\lambda} = 0{,}915$.
Άρα, η πιθανότητα ένας μαθητής από την $1^η$ τάξη να έχει την ίδια μέρα γενέθλια με ένα μαθητή από την $2^η$ τάξη, είναι ίση με 91.5%.

Παρατηρούμε ότι το παράδοξο των γενεθλίων είναι μια μέθοδος εύρεσης των συγκρούσεων μιας συνάρτησης κατακερματισμού, όταν η έξοδος της είναι μια ακολουθία μικρού μήκους. Έστω h μία συνάρτηση κατακερματισμού που παράγει έξοδο μεγέθους m-bits. Τότε υπάρχουν $n = 2^m$ πιθανές έξοδοι. Αν υπολογίσουμε για περίπου $r = \sqrt{n} = 2^{m/2}$ τυχαία επιλεγμένα x τις αντίστοιχες τιμές h(x), τότε υπάρχει μεγάλη πιθανότητα να βρούμε 2 τιμές x_1, x_2 ($x_1 \neq x_2$), έτσι ώστε $h(x_1) = h(x_2)$. Άν υπολογίσουμε την h για περισσότερες τιμές του x, π.χ. $r = 10\times 2^{m/2}$, τότε η πιθανότητα να βρούμε μια σύγκρουση είναι πολύ μεγάλη.

Παράδειγμα 1.5:

Ένα χαρακτηριστικό παράδειγμα birthday attack είναι το ακόλουθο:

Έστω ότι ο Α θέλει να υπογράψει ηλεκτρονικά ένα έγγραφο. Πρώτα, εφαρμόζει σ'αυτό μια συνάρτηση κατακερματισμού, η οποία παράγει μια σύνοψη 50 bits. Στη συνέχεια, υπογράφει τη σύνοψη χρησιμοποιώντας ένα απο τα γνωστά σχήματα ψηφιακής υπογραφής.

Αυτό, κάθιστα πολύ δύσκολο το να τον εξαπατήσει κάποιος Β (κάνοντας τον να υπογράψει ένα πλαστό εγγραφο), αφού η πιθανότητα ένα πλαστό έγγραφο να έχει την ίδια σύνοψη με το αυθεντικό είναι 1 στις 2^{50}, δηλαδή 1 στις 10^{15}. Ο Β, λοιπόν, μπορεί να δοκιμάσει αρκετά πλαστά έγγραφα, αλλά είναι σχεδον απίθανο να βρεί κάποιο με τη σωστή σύνοψη.

Ωστόσο, έχοντας μελετήσει το Πρόβλημα των Γενεθλίων μπορεί να δράσει ως εξής:

Βρίσκει 30 έγγραφα που να μοιάζουν με το αυθεντικό, στα οποία μπορεί να κάνει μια πολύ μικρή τροποποίηση, π.χ. να προσθέσει ένα κενό στο τέλος μίας πρότασης, να κάνει μια μικρή αλλαγή σε μία λέξη κλπ. Σε κάθε τέτοιο έγγραφο έχει 2 επιλογές: να κάνει αυτή την μικρή τροποποίηση ή να το αφήσει όπως είναι. Με αυτόν τον τρόπο μπορεί να παράξει 2^{30} έγγραφα, τα οποία είναι σχεδόν ίδια με το αυθεντικό. Στην συνέχεια, υπολογίζει την σύνοψη αυτών των 2^{30} εγγράφων, χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού με τον Α και τις αποθηκεύει σε ένα αρχείο.

Τώρα, ο Β παίρνει το πλαστό εγγραφο με το οποίο θέλει να εξαπατήσει τον Α και δημιουργεί, με τον ίδιο τρόπο, 2^{30} παραλλαγές αυτού. Υπολογίζει τις συνόψεις τους και τις αποθηκεύει σε ένα άλλο αρχείο. Από το τροποποιημένο παράδοξο των γενεθλίων, παίρνοντας $r = 2^{30}$ και $n = 2^{50}$, έχουμε $\lambda = r^2/n = 2^{10} = 1024$ και η πιθανότητα μια παραλλαγή του αυθεντικού εγγράφου να έχει την ίδια σύνοψη με μία απο τις παραλλαγές του πλαστού, είναι περίπου $1-e^{-1024} \approx 1$.

Έχοντας βρει, λοιπόν, 2 τέτοια έγγραφα με την ίδια σύνοψη, ζητάει από τον Α να υπογράψει αυτήν του αυθεντικού εγγράφου. Ο Α είναι απίθανο να αντιληφθεί τη διαφορά, οπότε υπογράφει. Ο Β, τώρα μπορεί να προσαρτήσει την υπογραφή στο πλαστό εγγραφο, η οποία είναι έγκυρη και γι'αυτό, αφού τα 2 έγγραφα έχουν την ίδια σύνοψη. Έτσι, μπορεί να ισχυριστεί ότι ο Α υπέγραψε το πλαστό έγγραφο αντί το αυθεντικό.

Ας υποθέσουμε, όμως, ότι ο Α θεωρεί ότι ένα κόμμα είναι λάθος και το αφαιρεί από το έγγραφο. Στη συνέχεια, υπογράφει το έγγραφο, το οποίο έχει τελείως διαφορετική σύνοψη από αυτό που του ζήτησε ο Β να υπογράψει. Άρα, ο Β απέτυχε στο να τον εξαπατήσει, καθώς το να βρεί ένα πλαστό έγγραφο με την ίδια «νέα» σύνοψη είναι σχεδόν απίθανο.

■

***Σημείωση 1.3**:* Για να πετύχουμε μεγαλύτερη ασφάλεια απέναντι στις birthday attacks, καλό θα ήταν να χρησιμοποιούμε συνάρτηση κατακερματισμού με έξοδο διπλάσιου μεγέθους από αυτό που θεωρούμε απαραίτητο. Ένας καλύτερος τρόπος προστασίας απο τις birthday attacks, είναι να κάνουμε πάντα μία μικρή αλλαγή πρίν υπογράψουμε ένα ηλεκτρονικό έγγραφο.

1.4 ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ ΣΕ ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΩΝ

Ο απώτερος σκοπός ενός αντιπάλου είναι η πλαστογράφηση της υπογραφής, δηλαδή να παράξει μία υπογραφή, η οποία να γίνει δεκτή ως έγκυρη.

Οι πιο συνηθισμένοι τύποι επιθέσεων σε σχήματα ψηφιακών υπογραφών είναι οι εξής:

1. **Επίθεση μόνο σε κλειδί (key–only attack) :** Ο αντίπαλος γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντα, δηλαδή τη συνάρτηση επαλήθευσης ver_K.
2. **Επίθεση σε μήνυμα (message attack) :** Ο αντίπαλος δύναται να εξετάσει τις αντίστοιχες υπογραφές είτε γνωστών, είτε επιλεγμένων μηνυμάτων. Διακρίνουμε 3 κατηγορίες επίθεσης σε μήνυμα:
   i. ***Επίθεση σε γνωστό μήνυμα (known message attack):*** Ο αντίπαλος έχει μια λίστα με υπογεγραμμένα μηνύματα, έστω (x_1,y_1), (x_2,y_2),... , όπου τα x_i είναι τα μηνύματα και τα y_i οι αντίστοιχες υπογραφές τους (έτσι ώστε $y_i = sig_K(x_i)$, i = 1,2…).
   ii. ***Επίθεση σε επιλεγμένο μήνυμα (chosen-message attack) :*** Ο αντίπαλος αποκτά έγκυρες υπογραφές από μία επιλεγμένη λίστα μηνυμάτων πριν επιχειρήσει να σπάσει το σχήμα υπογραφής. Τα μηνύματα επιλέγονται προτού ελεγχθεί οποιαδήποτε υπογραφή, γι'αυτό και η επίθεση αυτή χαρακτηρίζεται ως *μη-προσαρμόσιμη (non-adaptive)*. Η επίθεση σε επιλεγμένο μήνυμα εναντίων των σχημάτων υπογραφών είναι ανάλογη με αυτή σε επιλεγμένο κρυπτοκείμενο ενάντια σε σχήματα κρυπτογράφησης δημοσίου κλειδιού.
   iii. ***Προσαρμόσιμη Επίθεση σε επιλεγμένο μηνυμα (adaptive chosen-message attack):*** Ο αντίπαλος ζητά υπογραφές μηνυμάτων, οι οποίες εξαρτώνται από το δημόσιο κλειδί του υπογράφοντα και ίσως να ζητά υπογραφές μηνυμάτων, οι οποίες εξαρτώνται από προηγουμένως αποκτηθείσες υπογραφές ή μηνύματα.

Ο αντίπαλος, χρησιμοποιώντας τις παραπάνω επιθέσεις, μπορεί να «σπάσει» το σχήμα υπογραφής. Υπάρχει μια ομάδα κριτηρίων που περιγράφουν αυτό που ονομάζουμε «σπάσιμο» ενός σχήματος υπογραφής:

1. **Ολικό σπάσιμο (total break):** Ο αντίπαλος έχει τη δυνατότητα να υπολογίσει το ιδιωτικό κλειδί του υπογράφοντα, δηλαδή τη συνάρτηση υπογραφής sig_K. Έτσι, μπορεί να παράξει έγκυρες υπογραφές σε οποιοδήποτε μήνυμα.

2. **<u>Επιλεκτική πλαστογράφηση</u> (selective forgery):** Ο αντίπαλος είναι δυνατόν να δημιουργήσει μία έγκυρη υπογραφή για ένα μήνυμα επιλεγμένο εκ των προτέρων. Με άλλα λόγια, δεδομένου ενός μηνύματος m, μπορεί να προσδιορίσει υπογραφή s έτσι ώστε $ver_K(m,s)$ = true. Δημιουργώντας την υπογραφή s, δεν εμπλέκει άμεσα το νόμιμο υπογράφοντα.
3. **<u>Υπαρκτή πλαστογράφηση</u> (existential forgery):** Ο αντίπαλος είναι ικανός να δημιουργήσει μια έγκυρη υπογραφή για ένα τουλάχιστον μήνυμα. Με άλλα λόγια, μπορεί να παράξει ένα ζεύγος (m,s), έτσι ώστε $ver_K(m,s)$ = true, όπου m μήνυμα. Έχει ελάχιστο ή καθόλου έλεγχο του μηνύματος, του οποίου την υπογραφή αποκτά κι έτσι ο νόμιμος υπογράφων μπορεί να εμπλακεί στην απάτη.

<u>Παρατηρήσεις</u>:

1. Ένα σχήμα ψηφιακής υπογραφής δεν μπορεί να είναι απόλυτα ασφαλές, από τη στιγμή που ένας αντίπαλος μπορεί για δεδομένο μήνυμα m να δοκιμάσει όλες τις πιθανές υπογραφές, χρησιμοποιώντας τη συνάρτηση επαλήθευσης ver_K , έως ότου βρει μία έγκυρη. Έτσι, έχοντας στη διάθεσή του αρκετό χρόνο, μπορεί να πλαστογραφήσει την υπογραφή οποιουδήποτε μηνύματος. Στόχος μας είναι να κατασκευάσουμε σχήματα υπογραφής υπολογιστικά ασφαλή.

2. Οι προσαρμόσιμες επιθέσεις σε επιλεγμένο μήνυμα εμποδίζονται πιο δύσκολα από κάθε άλλο είδος επιθέσεων. Δεδομένων, λοιπόν, υπαρκτών μηνυμάτων και των αντίστοιχων υπογραφών, ο αντίπαλος θα μπορούσε εύκολα να πλαστογραφήσει την υπογραφή της επιλογής του. Όμως, μια τέτοια επίθεση είναι σχεδόν πάντα πρακτικά ανέφικτη, οπότε ένα ορθά σχεδιασμένο σχήμα υπογραφής πρέπει να προλαμβάνει κάθε τέτοια πιθανότητα.

1.5 ΜΑΘΗΜΑΤΙΚΗ ΕΙΣΑΓΩΓΗ

1.5.1 MODULAR ΑΡΙΘΜΗΤΙΚΗ ΚΑΙ ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΑΛΓΕΒΡΑΣ

Ορισμός 1.10: Μία ***ομάδα*** είναι ένα σύνολο G εφοδιασμένο με μία διμελή πράξη $*$, τέτοια ώστε να ικανοποιούνται τα ακόλουθα αξιώματα:

a) Η $*$ είναι προσεταιριστική, δηλαδή ισχύει $a*b=b*a$, για όλα τα $a,b\in G$.
b) Υπάρχει ένα στοιχείο $e\in G$, τέτοιο ώστε $e*a=a*e=a$, για κάθε $a\in G$. Το e καλείται *ταυτοτικό στοιχείο*.
c) Για κάθε $a\in G$ υπάρχει ένα στοιχείο $a'\in G$, με την ιδιότητα $a'*a=a*a'=e$. Το a' καλείται *αντίστροφο* του a.

Ορισμός 1.11: Αν G είναι μια πεπερασμένη ομάδα, τότε η ***τάξη*** της είναι το πλήθος των στοιχείων της και συμβολίζεται με $|G|$.

Το σύνολο των ακεραίων $\mathbf{Z}$ με πράξη την πρόσθεση σχηματίζει μια ομάδα με ταυτοτικό στοιχείο το 0 και αντίστροφο στοιχείο ενός ακεραίου a το $-a$.

Το σύνολο $\mathbf{Z}_n$ με πράξη την πρόσθεση modulo n σχηματίζει μια ομάδα τάξης n.

Η *πολλαπλασιαστική ομάδα του* $\mathbf{Z}_n$ είναι η $\mathbf{Z}_n^*=\{a\in\mathbf{Z}_n:\text{ΜΚΔ}(a,n)=1\}$, δηλαδή το σύνολο των υπολοίπων modulo n που είναι σχετικά πρώτα προς το n. Αν n πρώτος, τότε $\mathbf{Z}_n^*=\{a:1\le a\le n-1\}$. Η τάξη της $\mathbf{Z}_n^*$ είναι η $|\mathbf{Z}_n^*|=\varphi(n)$. Αν $a,b\in\mathbf{Z}_n^*$, τότε $ab\in\mathbf{Z}_n^*$, δηλαδή η $\mathbf{Z}_n^*$ είναι κλειστή ως προς τον πολλαπλασιασμό. Κάθε στοιχείο του $\mathbf{Z}_n^*$ θα έχει πολλαπλασιαστικό αντίστροφο που ανήκει στο $\mathbf{Z}_n^*$.

Ορισμός 1.12: Αν ένα υποσύνολο H μιας ομάδας G είναι κλειστό ως προς τη διμελή πράξη της G και επιπλέον το H είναι ομάδα, τότε το H λέγεται ***υποομάδα*** της G.

1.5.2 ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΑΡΙΘΜΩΝ

Θεώρημα 1.1: Έστω οι ακέραιοι $n \geq 2$ και $a \in \mathbf{Z}_n$. Τότε, ο a έχει πολλαπλασιαστικό αντίστροφο αν και μόνο αν ΜΚΔ(a,n) = 1. Ο αντίστροφος, αν υπάρχει, θα είναι μοναδικός.

Θα βρίσκουμε τον πολλαπλασιαστικό αντίστροφο του a με τον ***Επεκτεταμένο Ευκλείδιο Αλγόριθμο***:

Εφόσον ΜΚΔ(a,n) = 1, υπάρχουν ακέραιοι $x, y \in \mathbf{Z}$ με $ax + ny = 1$. Ο x δεν είναι πολλαπλάσιο του n, διότι τότε η παραπάνω σχέση μας δίνει ότι το 1 είναι πολλαπλάσιο του n που είναι άτοπο, αφού $n \geq 2$. Άρα, ο x, αν διαιρεθεί με τον n θα έχει μη μηδενικό υπόλοιπο. Από τον Αλγόριθμο του Ευκλείδη, θα υπάρχουν ακέραιοι q, r, ώστε $x = qn + r$ με $1 \leq r \leq n-1$. Αντικαθιστώντας αυτή την τιμή του x στην προηγούμενη ισότητα, έχουμε

$$a(qn + r) + ny = 1 \Rightarrow$$

$$ar = 1 - (aq + y)n \Rightarrow$$

$$ar - 1 = -(aq + y)n \Rightarrow$$

$$ar = 1 \bmod n$$

Επομένως, ο r είναι πολλαπλασιαστικός αντίστροφος του a.

Παράδειγμα 1.6:

Ψάχνουμε να βρούμε τον πολλαπλασιαστικό αντίστροφο του στοιχείου 11 $\in \mathbf{Z}_{30}$. Σε πρώτη φάση, εκτελούμε τον Αλγόριθμο του Ευκλείδη:

30	11	30 = 2×11 + 8
8	11	11 = 1×8 + 3
8	3	8 = 2×3 + 2
2	3	3 = 2×1 + 1
2	1	2 = 2×1 + 0
0	1	άρα, ΜΚΔ(11, 30) = 1.

Αφού ΜΚΔ(11, 30) = 1, συμπεραίνουμε ότι υπάρχει ο πολλαπλασιαστικός αντίστροφος του $11 \in \mathbf{Z}_{30}$. Για να τον βρούμε, θα χρησιμοποιήσουμε τις σχέσεις της μορφής $x = qn + r$ σε κάθε βήμα του Αλγόριθμου του Ευκλείδη για να καταλήξουμε σε μια σχέση της μορφής $ax + ny = 1$.

Από την προτελευταία σχέση έχουμε: $1 = 3 - 2 \times 1$

και αντικαθιστώντας το 2 από την αμέσως προηγούμενη σχέση: $1 = 3 - 1(8 - 2 \times 3) = 3 \times 3 - 1 \times 8$

Η αμέσως προηγούμενη δίνει: $1 = 3(11 - 1 \times 8) - 1 \times 8 = 3 \times 11 - 4 \times 8$

Και η πρώτη σχέση δίνει:

$$1 = 3 \times 11 - 4(30 - 2 \times 11) = 3 \times 11 - 4 \times 30 + 8 \times 11 = 11 \times 11 - 4 \times 30$$

δηλαδή, $1 = 11 \times 11 - 4 \times 30 = ax + ny$.

Άρα, $x = 11$ και $y = -4 \Rightarrow 11^{-1} = 11$, δηλαδή ο πολλαπλασιαστικός αντίστροφος του $11 \in \mathbf{Z}_{30}$ είναι το 11.

Πράγματι, $11 \times 11 = 121 = 1 \bmod 30$. ■

<u>Θεώρημα 1.2</u>: **(Θεμελιώδες Θεώρημα της Αριθμητικής (ΘΘΑ))**

Για κάθε ακέραιο $n > 1$ υπάρχουν πρώτοι $p_1 \le p_2 \le \ldots \le p_k$, τέτοιοι ώστε $n = p_1 p_2 \cdots p_k$ και η παραγοντοποίηση αυτή είναι μοναδική.

Το ΘΘΑ είναι συνήθως γνωστό με την εξής πιο συνοπτική μορφή:

Κάθε ακέραιος n μπορεί να αναλυθεί σε πρώτους παράγοντες, δηλαδή γράφεται ως $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, όπου $p_i \neq p_j$, $1 \le i \le j \le k$, πρώτοι και α_i ακέραιοι, ώστε $\alpha_i \ge 0$, $1 \le i \le k$.

<u>Ορισμός 1.13:</u> Η συνάρτηση $\varphi(n) = \mathrm{n}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right)$, όπου $p_1, p_2, \ldots, p_k$ οι πρώτοι παράγοντες του $n \in \mathbf{Z}$, ονομάζεται ***συνάρτηση Euler*** και ορίζεται ως το

πλήθος των ακεραίων στο διάστημα $1 \le r \le n$ που είναι πρώτοι προς τον n (δηλαδή ΜΚΔ $(r, n) = 1$).

Πόρισμα 1.1: Αν ο n είναι πρώτος τότε $\varphi(\mathrm{n}) = \mathrm{n} - 1$.

Σύμφωνα με το Θεώρημα 1, μπορούμε να καταλήξουμε στο εξής:

Πόρισμα 1.2: Τα πλήθος των στοιχείων του $\mathbf{Z}_n$ που έχουν πολλαπλασιαστικό αντίστροφο ισούται με $\varphi(n)$.

Θεώρημα 1.3: **(Euler)**

Αν ΜΚΔ $(y, n) = 1$, τότε $y^{\varphi(n)} = 1 \bmod n$, $y, n \in \mathbf{Z}$.

Ορισμός 1.14: Αν b είναι ο μικρότερος θετικός ακέραιος, τέτοιος ώστε $a^b = 1 \bmod n$, τότε λέμε ότι ο a ***ανήκει στον εκθέτη*** b modulo 1.

Ορισμός 1.15: Αν ο ακέραιος g ανήκει στον εκθέτη $\varphi(n) \bmod n$, τότε ο g ονομάζεται ***πρωταρχικό στοιχείο ή πρωταρχική ρίζα*** $\bmod n$.

Ορισμός 1.16: Αν $a \in \mathbf{Z}$, $n \ge 2$ και ΜΚΔ $(a, n) = 1$, λέμε ότι ο a είναι ***τετραγωνικό υπόλοιπο*** *(quadratic residue (QR))* $\bmod n$, αν $a = x^2 \bmod n$ για $x \in \mathbf{Z}$. Αν ΜΚΔ $(a, n) = 1$ και $a \notin QR$, ο a λέγεται ***μη τετραγωνικό υπόλοιπο (QNR)*** $\bmod n$.

Πόρισμα 1.3: Αν ο n είναι πρώτος, τότε $|QR| = |QNR|$.

Παράδειγμα 1.7:

Βρίσκουμε τα QR για $n = 13$:

$1^2 = 1 = 12^2$

$2^2 = 4 = 11^2$

$3^2 = 9 = 10^2$

$4^2 = 3 = 9^2$

$5^2 = 12 = 8^2$

$6^2 = 10 = 7^2$

‘Αρα, QR = { 1, 3, 4, 9, 10, 12 } και QNR = { 2, 5, 6, 7, 8, 11 }. Παρατηρούμε ότι $|QR| = |QNR|$.

Ορισμός 1.16: Αν $x^2 = a \bmod n$, όπου $a \in QR_n$, τότε το x λέγεται ***τετραγωνική ρίζα*** $\bmod n$.

Ορισμός 1.17: Έστω $1 \le a \le n$. Ο a ονομάζεται ***τετραγωνική ρίζα της μονάδας*** $\bmod n$ αν $a^2 \bmod n = 1$.

Πόρισμα 1.4: Αν p πρώτος και $1 \le a < p$ με $a^2 \bmod p = 1$, τότε $a = 1$ ή $a = p - 1$.

2. ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ RSA

Το σχήμα υπογραφής RSA είναι μια εφαρμογή του πρώτου κρυπτοσυστήματος δημοσίου κλειδιού στην ιστορία της Κρυπτογραφίας. Η ασφάλειά του έγκειται σε μεγάλο βαθμό στη δυσκολία του να βρούμε πρώτους παράγοντες μεγάλων ακεραίων, όπως υποδηλώνεται και στο Θεώρημα Πρώτων Αριθμών (Prime Number Theorem (P.N.T.)).

2.1 ΤΟ ΘΕΩΡΗΜΑ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ (The Prime Number Theorem)

Το Θεώρημα Πρώτων Αριθμών (P.N.T.) ένα από τα πλέον δημοφιλή θεωρήματα της Θεωρίας Αριθμών, το οποίο βασίζεται στη συνάρτηση $\pi(x)$.

Η συνάρτηση $\pi(x)$ εκφράζει το πλήθος των πρώτων αριθμών που δεν υπερβαίνουν τον πραγματικό αριθμό x. Δεν υπάρχει κάποιος γνωστός τύπος που να προσδιορίζει τη συνάρτηση αυτή. Αυτό συμβαίνει, διότι δεν μπορούμε να γνωρίζουμε πλήρως τον τρόπο με τον οποίο είναι κατανεμημένοι οι πρώτοι αριθμοί μέσα στους ακεραίους, καθώς έχει αποδειχτεί ότι τα κενά μεταξύ διαδοχικών πρώτων αριθμών μπορεί να είναι οσοδήποτε μεγάλα.

Σύμφωνα με το ***P.N.T.***, η συνάρτηση $\pi(x)$ είναι ασυμπτωτικά ίση με τη συνάρτηση $x/\log x$, δηλαδή

$$\pi(x) \sim \frac{x}{\log x} \quad (x \to \infty)$$

Γνωρίζουμε ότι $\frac{x}{\log x} \sim 10\%$, δηλαδή περίπου σε κάθε 10 αριθμούς ο ένας θα είναι πρώτος.

2.2 ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RSA

Τα αρχικά του κρυπτοσυστήματος RSA προέρχονται από τα ονόματα των μελετητών που το δημοσίευσαν το 1978, Rivest, Shamir και Adleman. Το RSA αποτελεί κρυπτοσύστημα δημοσίου κλειδιού. Ας γίνουμε, όμως, λίγο πιο ξεκάθαροι πάνω στο τι εννοούμε με τον όρο *κρυπτογράφηση με δημόσιο κλειδί.*

Ένα βασικό πρόβλημα της κρυπτογραφίας ήταν ανέκαθεν η ασφαλής μεταφορά του κλειδιού από τον αποστολέα στον παραλήπτη, χωρίς να πέσει σε "εχθρικά χέρια ". Το πρόβλημα αυτό εξαλείφεται αν δεν υπάρχει κλειδί, το οποίο πρέπει να μείνει μυστικό, πράγμα το οποίο συνιστάται στο σύστημα κρυπτογράφησης με δημόσιο κλειδί. Το σύστημα αυτό έχει κρυπτογραφικό κλειδί που όχι μόνο είναι γνωστό, αλλά και δημοσιευμένο σε κάποιον κατάλογο. Η ιδέα πρωτοεμφανίστηκε το 1976 από τους Diffie και Helman και η πρώτη υλοποίηση της πρότασής τους είναι το κρυπτοσύστημα RSA.

Στην κρυπτογράφηση με δημόσιο κλειδί, χρησιμοποιούνται δύο διαφορετικά κλειδιά: ένα για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση του μηνύματος. Τα ένα κλειδί παραμένει ιδιωτικό (κρυφό), ενώ το άλλο γνωστοποιείται σε οποιονδήποτε ενδιαφερόμενο. Τα δύο κλειδιά ανήκουν σε μία φυσική οντότητα και το όλο σύστημα είναι σχεδιασμένο, έτσι ώστε η γνώση του δημοσίου κλειδιού να μην επιτρέπει σε κανέναν να μπορεί να υπολογίσει το ιδιωτικό.

Έστω, λοιπόν, ότι ο Α έχει δημιουργήσει ένα ζεύγος κλειδιών, διατηρεί μυστικό το ιδιωτικό και γνωστοποιεί το δημόσιο. Οποιοσδήποτε Β μπορεί να κρυπτογραφήσει ένα μήνυμα, χρησιμοποιώντας το δημόσιο κλειδί του Α, αλλά αυτό το μήνυμα μπορεί να διαβαστεί μόνο από τον Α, γιατί μόνο αυτός έχει το κατάλληλο αποκωδικοποιητικό κλειδί. Παράλληλα, οποιοσδήποτε Β μπορεί, χρησιμοποιώντας το δημόσιο κλειδί του Α, να αποκωδικοποιήσει ένα μήνυμα, το οποίο μόνο ο Α θα μπορούσε να έχει κωδικοποιήσει.

Πρακτικά, το δημόσιο κλειδί μπορεί να παρομοιαστεί με το κλειδί μιας καταπακτής, δια μέσου της οποίας τα μηνύματα εξαφανίζονται. Με τον όρο καταπακτή θέλουμε να τονίσουμε ότι εύκολα μπαίνει κανείς, αλλά βγαίνει μόνο αν έχει τα κατάλληλα μέσα. Η συμπεριφορά αυτή της καταπακτής πραγματοποιείται στα ψηφιακά μηνύματα που έχουν τη μορφή μιας μεγάλης αλυσίδας από 0 και 1, καθώς είναι εύκολο να πολλαπλασιάσει κανείς δύο μεγάλους αριθμούς, αλλά αδύνατο να παραγοντοποιήσει κάποιο μεγάλο αριθμό σε λογικό χρόνο, όπως "αποδεικνύει" το P.N.T.

Μπορούμε τώρα να προχωρήσουμε στην περιγραφή του RSA. Το κρυπτοσύστημα αυτό βασίζεται στη γνώση της συνάρτησης Euler φ(n) του modulo n

για την αποκρυπτογράφηση του μηνύματος. Οι υπολογισμοί γίνονται στο σύνολο $\mathbf{Z}_n$ = {0, 1, 2, …, n-1}, όπου n είναι το γινόμενο δύο μεγάλων, τυχαία επιλεγμένων, διακεκριμένων, πρώτων αριθμών p, q και φ(n) = (p-1)(q-1).

ΜΕΘΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ RSA

Παραγωγή κλειδιού

- Ο Α επιλέγει δύο μεγάλους, τυχαίους πρώτους αριθμούς p, q περίπου ίδιου μεγέθους (στην πράξη με 100 περίπου ψηφία).
- Υπολογίζει τα n = pq (περί τα 200 ψηφία) και φ(n) = $n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$=(p-1)(q-1).
- Επιλέγει ένα τυχαίο ακέραιο e, έτσι ώστε 1 < e < φ(n) και ΜΚΔ(e, φ(n)) = 1.
- Υπολογίζει το μοναδικό ακέραιο d, τέτοιο ώστε 1 < d < φ(n) και ed = 1modφ(n), διαδικασία που γίνεται μία μόνο φορά για κάθε e με τον Επεκτεταμένο Ευκλείδιο Αλγόριθμο (Ε.Ε.Α.).

Το δημόσιο κλειδί του Α είναι το (n, e) και το ιδιωτικό του το (d, p, q).

Σημείωση 2. 1*:* Ο e ονομάζεται **εκθέτης κρυπτογράφησης**, ενώ ο d **εκθέτης αποκρυπτογράφησης**.

Σημείωση 2.2: Ο υπολογισμός του d προκύπτει από τον Ε.Ε.Α. ως εξής:
$d = e^{\phi(\phi(n))-1} \bmod \phi(n)$. Πράγματι, πολλαπλασιάζοντας με e λαμβάνουμε
$ed = e^{\phi(\phi(n))} \bmod \phi(n) = 1 \bmod \phi(n)$, όπως προκύπτει από το θεώρημα του Euler και το ότι ΜΚΔ (e, φ(n)) = 1.

Κρυπτογράφηση με δημόσιο κλειδί RSA

Ο Β κρυπτογραφεί ένα μήνυμα m και το στέλνει στον Α να το αποκρυπτογραφήσει.

1. *Κρυπτογράφηση:* Ο Β κάνει τα ακόλουθα:
   - Αναπαριστά το μήνυμα ως έναν ακέραιο m, $0 < m < n-1$.
   - Βρίσκει το δημόσιο κλειδί του Α, (n, e).
   - Υπολογίζει το $c = m^e \bmod n$ και το στέλνει στον Α.

2. *Αποκρυπτογράφηση:* Ο Α, για να ανακτήσει το αρχικό μήνυμα m από το c, υπολογίζει το $m = c^d \bmod n$, χρησιμοποιώντας το ιδιωτικό του κλειδί d.

Παράδειγμα 2.1:

Έστω $e = 7$ και $n = pq = 187$, ενώ το αρχικό μήνυμα είναι 3 με ΜΚΔ(3,187) = 1. Το κρυπτογραφημένο μήνυμα του Β θα είναι $c = m^7 = 3^7 = 2187 = 130 \bmod 187$.

Ο Α, για να αποκρυπτογραφήσει το μήνυμα c, πρέπει να γνωρίζει τον εκθέτη αποκωδικοποίησης d που λαμβάνεται από τους παράγοντες του $n = 187 = 11 \times 17$ που μόνο αυτός γνωρίζει.

Εφόσον λοιπόν $n = 11 \times 17 \Rightarrow \phi(n) = (p-1)(q-1) = 10 \times 16 = 160$ και $\phi(\phi(n)) = 64$, επομένως,

$d = e^{\phi(\phi(n))-1} = 7^{63} = (7^9)^7 = (40 \times 353 \times 607)^7 = 7^7 = 823 \times 543 = 23 \bmod 160$.

Αφού βρέθηκε ότι $d = 23$, θα είναι $c^d = 130^{23} = 3 \bmod 187$.

Άρα, $m = 3$.

■

Παρατηρήσεις:

1) Τονίζουμε ότι ο εκθέτης αποκωδικοποίησης d υπολογίζεται μόνο από το $\phi(n)$ και τους παράγοντες του n (δηλαδή τα p, q) και όχι από το e και το n που είναι δημόσια πληροφορία.

2) *(Ασφάλεια του RSA)*

Αν κάποιος γνωρίζει τους p, q μπορεί εύκολα να υπολογίσει το φ(n) και άρα και το d. Επομένως, είναι πολύ σημαντικό οι p, q να κρατούνται μυστικοί.Το πρόβλημα παραγοντοποίησης του n και το πρόβλημα υπολογισμού του εκθέτη αποκρυπτογράφησης d στο RSA από το δημόσιο κλειδί (n, e) είναι υπολογιστικά ισοδύναμα. Επιλέγουμε, λοιπόν, αρκετά μεγάλους τους πρώτους p, q, ούτως ώστε να είναι ανέφικτη η παραγοντοποίηση του n σε λογικό χρόνο.

2.3 ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ RSA

Το σχήμα υπογραφής RSA είναι ένα ντετερμινιστικό σχήμα ψηφιακής υπογραφής με δυνατότητα ανάκτησης του μηνύματος. Είναι μία εφαρμογή του κρυπτοσυστήματος RSA στην οποία αντιστρέφονται οι ρόλοι των κλειδιών (δημόσιο-ιδιωτικό). Πιο συγκεκριμένα, θεωρούμε ένα κρυπτοσύστημα RSA με δημόσιο κλειδί (n, e) και ιδιωτικό d. Τότε η συνάρτηση κρυπτογράφησης ορίζεται ως $E_e(m) = m^e \text{mod} n$ και η συνάρτηση αποκρυπτογράφησης ως $D_d(m) = m^d \text{mod} n$, για κάθε $m \in \mathbf{Z}_n$.

Είναι προφανές ότι ισχύει $D_K(E_K(m)) = m$, για ένα απλό κείμενο m και ένα κλειδί K. Επίσης αποδεικνύεται ότι $E_K(D_K(m)) = m$, αφού για το σχήμα υπογραφής θεωρούμε ότι ο χώρος των κρυπτοκειμένων ταυτίζεται με το χώρο των απλών κειμένων, δηλαδή το $\mathbf{Z}_n$, όπου n = pq.Ο χώρος υπογραφών είναι επίσης το $\mathbf{Z}_n$.

Απόδειξη:

Αφού $ed = 1 \text{mod} \phi(n)$, υπάρχει ένας ακέραιος k, τέτοιος ώστε
$ed = 1 + k\phi(n)$. Έχουμε ότι $D(E(m)) = m^{ed} \text{mod} n$. Συνεπώς,
$D(E(m)) = m^{1+k\phi(n)} \text{mod} n = mm^{k\phi(n)} \text{mod} n = m(m^{\phi(n)})^k \text{mod} n = m \text{mod} n$, όπως προκύπτει από το θεώρημα Euler. Επομένως, η κρυπτογράφηση και η αποκρυπτογράφηση είναι αντίστροφες πράξεις.
Η διαδικασία παραγωγής κλειδιού για το σχήμα υπογραφής RSA είναι ίδια με αυτή του κρυπτοσυστήματος, όπως την περιγράψαμε παραπάνω.

■

Το σχήμα υπογραφής RSA

Υποθέτουμε ότι ο A στέλνει στον B το μήνυμα m υπογεγραμμένο ψηφιακά με το RSA.

1. *Δημιουργία υπογραφής:*

- Ο A υπολογίζει το $s = sig_K(m) = D_K(m) = m^d \text{mod} n$, το οποίο είναι η υπογραφή του A για το μήνυμα m.
- Ο A στέλνει στον B το ζεύγος (m, s).

2. *Επαλήθευση υπογραφής:*

- Ο Β χρησιμοποιεί το δημόσιο κλειδί του Α για να υπολογίσει το $z = s^e \bmod n$.
- Αν $z = m$, τότε $ver_K(m, s)$ = αληθής και ο Β αποδέχεται την υπογραφή ως έγκυρη, διαφορετικά την απορρίπτει.

Παράδειγμα 2.2:

Έστω ότι ο Α θέλει να δημιουργήσει ένα σχήμα υπογραφής RSA. Επιλέγει τους πρώτους $p = 79$ και $q = 101$ και υπολογίζει το $n = pq = 7979$. Αφού είναι $\phi(n) = 7800$, ο Α επιλέγει τον ακέραιο $e = 7$ που είναι πρώτος προς τον $\phi(n)$ και κατόπιν υπολογίζει τον αντίστροφο του e $(\bmod \phi(n))$, που είναι ο $d = 3343$. Έπειτα, υπογράφει το μήνυμα $m = 123$, υπολογίζοντας το $m^d = 123^{3343} = 5660 \pmod{7979}$ και στέλνει το ζεύγος (123, 5660) στον Β.

Ο Β μπορεί, αν και όχι μόνο δε γνωρίζει αλλά ούτε είναι σε θέση να υπολογίσει τον $d = 3343$ (αφού μόνο ο Α θα μπορούσε να πάρει από το $m = 123$ το $d = 5660$), να επαληθεύσει την υπογραφή του Α εάν υπολογίσει το $5660^7 = 123 \bmod 7979$. ■

Παρατηρήσεις:

1) Η *συνάρτηση υπογραφής* sig_K αποτελεί ιδιωτική πληροφορία, ενώ η *συνάρτηση επαλήθευσης* ver_K δημόσια. Ως εκ τούτου, ο Α είναι ο μόνος που μπορεί να δημιουργήσει μια υπογραφή s για το μήνυμα m, έτσι ώστε $ver_K(m, s)$ = αληθής, ενώ οποιοσδήποτε μπορεί να επαληθεύσει την υπογραφή.

2) Εφόσον το RSA ανήκει στα σχήματα υπογραφής με ικανότητα ανάκτησης του μηνύματος, ο Α, αντί για το ζεύγος (m, s), μπορεί να στείλει στον Β μόνο το s.

3) Το ζεύγος (m, s) καλείται ***υπογεγραμμένο μήνυμα***.

2.3.1 ΠΡΟΣΒΟΛΕΣ ΤΟΥ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ RSA

Αν κάποιος Γ μπορεί να υπολογίσει ένα ζεύγος (m, s) τέτοιο ώστε ver_K (m, s) = αληθής και το μήνυμα m δεν έχει προηγουμένως υπογραφεί από τον Α, τότε η υπογραφή s καλείται ***πλαστογράφηση***.

Ας δούμε στη συνέχεια μερικές πλαστογραφήσεις του σχήματος ψηφιακής υπογραφής RSA:

I. **Παραγοντοποίηση ακεραίων (Integer factorization)**

Αν ο Γ καταφέρει να παραγοντοποιήσει το n, τότε μπορεί να υπολογίσει το φ(n) και κατόπιν το ιδιωτικό κλειδί d του Α, λύνοντας την ισοδυναμία $ed = 1 \bmod \phi(n)$. Αυτό αποτελεί ολική κατάρρευση του συστήματος, πράγμα σχεδόν απίθανο, καθώς έχει υπολογιστεί ότι η πιθανότητα τυχαίας εύρεσης των p και q είναι $1/10^{100}$.

II. **Επιλογή υπογραφής πριν το κείμενο(Choosing signature and then computing message)**

Έστω ότι ο Γ επιλέγει μια τυχαία υπογραφή $s \in \{0, \ldots, n-1\}$ και υπολογίζει $m \in \{0, \ldots, n-1\}$, τέτοιο ώστε $m = s^e \bmod n$. Η s είναι μία έγκυρη (αλλά πλαστογραφημένη) υπογραφή για το μήνυμα m. Ο Γ στέλνει στον Β το ζεύγος (m, s) προφασιζόμενος ότι είναι ο Α. Αν το μήνυμα m έχει κάποια σημασία για τον Β, ο Γ κατάφερε να εξαπατήσει τον Α, πραγματοποιώντας μία υπαρκτή πλαστογράφηση χρησιμοποιώντας επίθεση μόνο σε κλειδί. Παρόλα αυτά, είναι σχεδόν απίθανο ότι το μήνυμα m θα βγάζει νόημα.

III. **Πολλαπλασιαστική ιδιότητα του RSA (Multiplicative property of RSA)**

Έστω $s_1, s_2 \in \{0, \ldots, n-1\}$ οι υπογραφές των μηνυμάτων $m_1, m_2 \in \{0, \ldots, n-1\}$, αντίστοιχα, με $s_1 = m_1^d \bmod n$ και $s_2 = m_2^d \bmod n$. Τότε, $s = s_1 s_2 = (m_1 m_2)^d \bmod n$. Επομένως, αν είναι γνωστές οι υπογραφές s_1, s_2 των μηνυμάτων m_1, m_2, τότε υπολογίζουμε εύκολα την υπογραφή s του $m_1 m_2$. Αυτό είναι ένα παράδειγμα υπαρκτής πλαστογράφησης χρησιμοποιώντας επίθεση σε γνωστό μήνυμα.

2.3.2 ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΠΙΘΑΝΕΣ ΕΠΙΘΕΣΕΙΣ

Α. Ένα μέσο προστασίας από τις προσβολές που περιγράψαμε παραπάνω είναι η χρήση μιας *συνάρτησης κατακερματισμού (hash function)* $h: \{0, 1\}^* \rightarrow \{0, \dots, n-1\}$, η οποία είναι μοναδικής κατεύθυνσης και δημοσίως γνωστή. Τότε, η υπογραφή s του μηνύματος m ορίζεται ως $s = h(m)^d \bmod n$, $s \in [0, \dots, n-1]$ και ο Α στέλνει στον Β το υπογεγραμμένο μήνυμα (m, s). Ο Β με τη σειρά του υπολογίζει το $x = s^e \bmod n$, $x \in [0, \dots, n-1]$ και στη συνέχεια την τιμή h(m). Αν h(m) = x, τότε ο Β δέχεται το μήνυμα m, διαφορετικά το απορρίπτει.

Η διαδικασία αυτή καθιστά την υπαρκτή πλαστογράφηση σχεδόν αδύνατη. Πράγματι, αν ο Γ πάρει ένα τυχαίο s και υπολογίσει το s^e θα πρέπει να βρει m τέτοιο ώστε $h(m) = s^e \bmod n$, το οποίο για όλες σχεδόν τις τιμές της h είναι υπολογιστικά ανέφικτο.

Επίσης, αν είναι γνωστά δύο υπογεγραμμένα μηνύματα (m_1, s_1) και (m_2, s_2), με $s_1 = h(m_1)^d \bmod n$ και $s_2 = h(m_2)^d \bmod n$, είναι σχεδόν αδύνατο να βρεθεί m του οποίου η υπογραφή να είναι $s = (h(m_1)h(m_2))^d \bmod n$. Αυτό συμβαίνει διότι αν έχουμε $h(m_1) = x_1$ και $h(m_2) = x_2$, είναι πάλι υπολογιστικά ανέφικτο, σχεδόν για όλες τις περιπτώσεις, να βρεθεί m τέτοιο ώστε $h(m) = x_1x_2 \bmod n$. Αν επιπλέον η h είναι ισχυρώς ανθεκτική σε συγκρούσεις, τότε δεν είναι δυνατό να αντικατασταθεί ένα υπογεγραμμένο μήνυμα $(m_1, h(m_1)^d)$ από ένα άλλο $(m_2, h(m_2)^d)$ με $h(m_1) = h(m_2)$.

Β. Ένας δεύτερος τρόπος προστασίας είναι η χρήση μιας *συνάρτησης πλεονάζουσας πληροφορίας (redundancy function)*.

Ορισμός: Η *συνάρτηση πλεονάζουσας πληροφορίας* είναι μια δημόσια γνωστή αντιστρέψιμη προβολή από το χώρο $\mathbb{M}$ των απλών κειμένων σε έναν υπόχωρό του με συγκεκριμένες ιδιότητες.

Ένα τέτοιο παράδειγμα είναι η μετατροπή ενός δυαδικού κειμένου σε τέτοια μορφή ώστε ανάμεσα σε κάθε 8 bit να υπάρχει η λέξη 10101. Αυτό καθιστά σχεδόν αδύνατη την πλαστογράφηση, εφόσον είναι πρακτικά απίθανο μια τυχαία επιλεγμένη υπογραφή s, να δώσει ένα μήνυμα που να έχει τις ιδιότητες που προσδιορίζει σε τυχαίο μήνυμα m η συνάρτηση πλεονάζουσας πληροφορίας του Α.

Ένα άλλο παράδειγμα είναι ο διπλασιασμός της δυαδικής γραφής του μηνύματος. Δηλαδή, αν το μήνυμα m έχει δυαδική γραφή w, τότε ο Α θεωρεί το μήνυμα m′ που αντιστοιχεί στη δυαδική γραφή ww. Στέλνει στον Β το ζεύγος (m′, s), ο οποίος εκτελεί τη συνηθισμένη διαδικασία επαλήθευσης. Καθώς δεν υπάρχει

γνωστή μέθοδος επιλογής s τέτοιου ώστε, $s^e = m \bmod n$ και η δυαδική γραφή του m να είναι της μορφής ww, χωρίς τη χρήση του μυστικού κλειδιού d, η υπαρκτή πλαστογράφηση δεν αποτελεί πλέον απειλή για την επικοινωνία του A με τον B. Επίσης, αν οι θετικοί ακέραιοι m_1 και m_2 έχουν δυαδική γραφή της μορφής ww, είναι πολύ μικρή η πιθανότητα ο ακέραιος $m = m_1 m_2 \bmod n$, $m \in [0, \ldots, n-1]$, να έχει δυαδική γραφή της ίδιας μορφής.

ΚΕΦΑΛΑΙΟ 3

3. ΤΑ ΣΧΗΜΑΤΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΑΥΤΟΤΗΤΑΣ

Τα σχήματα πιστοποίησης ταυτότητας χρησιμοποιούνται στα συστήματα όπου είναι απαραίτητο να αποδειχθεί η ταυτότητα κάποιου. Στην πράξη, όμως, δεν είναι πάντοτε ασφαλή. Ένας αντίπαλος δύναται να υποκλέψει όλες τις απαραίτητες πληροφορίες που χρειάζεται για να λειτουργήσει ως νόμιμος χρήστης. Είναι, λοιπόν, φανερό ότι τα σχήματα αυτά πρέπει να εξασφαλίζουν ότι δεν μπορεί οποιοσδήποτε παρακολουθεί ένα σύστημα να λειτουργεί ως νόμιμος χρήστης. Επιπροσθέτως, κάθε χρήστης που πιστοποιεί την ταυτότητά του στο σύστημα, δεν πρέπει να αποκαλύπτει την πληροφορία αναγνώρισής του. Διαφορετικά, οποιοσδήποτε άλλος χρήστης του συστήματος θα μπορούσε εύκολα να "προσποιείται" ότι είναι κάποιος άλλος χρήστης.

Ένα αντιπροσωπευτικό παράδειγμα είναι το σύστημα ***πρόκληση και ανταπόκριση*** *(challenge and response),* το οποίο είναι ένα απλό σχήμα αναγνώρισης βασισμένο σε οποιοδήποτε κρυπτοσύστημα ιδιωτικού κλειδιού. Πιο συγκεκριμένα, έστω ότι ο Α και ο Β θέλουν να επικοινωνήσουν, χρησιμοποιούν ένα μυστικό κλειδί Κ, γνωστό και στους δύο:

- Ο Β διαλέγει μια *πρόκληση* x, η οποία είναι μια τυχαία ακολουθία μήκους 64-bits και τη στέλνει στον Α.
- Ο Α υπολογίζει το $y = e_k(x)$.
- Ο Β υπολογίζει το $y' = e_k(x)$ και πιστοποιεί ότι $y' = y$.

Οποιοδήποτε σχήμα πιστοποίησης ταυτότητας, το οποίο περιλαμβάνει πρωτόκολλο *μάρτυρα-πρόκλησης-ανταπόκρισης (witness-challenge-response protocol)* μπορεί να μετατραπεί σε ένα σχήμα υπογραφής. Για να το επιτύχουμε αυτό, αντικαθιστούμε την τυχαία πρόκληση x του επαληθευτή με μία συνάρτηση κατακερματισμού μονής κατεύθυνσης $x = h(e \square m)$, όπου e είναι ο *μάρτυρας (witness)* και m το μήνυμα προς υπογραφή.

3.1 ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ Feige-Fiat-Shamir

Το σχήμα υπογραφής Feige-Fiat-Shamir ανήκει στα σχήματα υπογραφής με παράρτημα και αποτελεί τυχαιοποιημένο μηχανισμό. Απαιτεί τη χρήση μιας συνάρτησης κατακερματισμού μονής κατεύθυνσης $h:\{0,1\}^* \to \{0,1\}^k$, για κάποιους σταθερούς θετικούς ακεραίους k. Το $\{0,1\}^k$ αντιστοιχεί στο σύνολο των ακολουθιών από 0 και 1 μήκους k-bit, ενώ το $\{0,1\}^*$ στο σύνολο όλων των ακολουθιών από 0 και 1 (αυθαίρετου μήκους).

Παραγωγή κλειδιού:

- Ο Α επιλέγει 2 τυχαίους, διακεκριμένους, μυστικούς, πρώτους αριθμούς p, q και υπολογίζει το γινόμενο $n = pq$.
- Επιλέγει ένα θετικό ακέραιο k και διακεκριμένους, τυχαίους ακεραίους $s_1, s_2, ..., s_k \in \mathbf{Z}_n^*$.
- Υπολογίζει το $\upsilon_j = \mathrm{s}_j^{-2} \mod n$, $1 \le \mathrm{j} \le \mathrm{k}$.

Το δημόσιο κλειδί του Α είναι το $((\upsilon_1, \upsilon_2, ..., \upsilon_n), n)$ και το ιδιωτικό του το $(s_1, s_2, ..., s_k)$.

Το σχήμα υπογραφής Feige-Fiat-Shamir

1. *Δημιουργία υπογραφής:*
    - Ο Α επιλέγει έναν τυχαίο ακέραιο $r,\ 1 \le r \le n-1$.
    - Υπολογίζει το $u = r^2 \bmod n$.
    - Υπολογίζει το $e = e_1, e_2, ..., e_k = h(m \square u)$, όπου $e_i \in \{0,1\}$, για κάθε $i = 1, 2, ..., k$.
    - Υπολογίζει το $s = r\prod_{j=1}^{k} s_j^{e_j} \bmod n$.
    - Η υπογραφή του Α για το μήνυμα m είναι το ζεύγος (e, s) .

2. *Επαλήθευση υπογραφής:*

- Ο Β ανακτά το δημόσιο κλειδί του Α $((\upsilon_1, \upsilon_2, ..., \upsilon_n), n)$.
- Υπολογίζει το $w = \mathrm{s}^2 \prod_{j=1}^{k} \upsilon_j^{e_j} \bmod n$.
- Υπολογίζει το $\mathrm{e}' = h(m \| w)$.
- Άν $e = e'$, ο Β αποδέχεται την υπογραφή ως έγκυρη, αλλιώς την απορρίπτει.

<u>Απόδειξη ορθότητας της διαδικασίας επαλήθευσης</u>:

$$w = \mathrm{s}^2 \prod_{j=1}^{k} \upsilon_j^{e_j} = r^2 \prod_{j=1}^{k} s_j^{2e_j} \prod_{j=1}^{k} \upsilon_j^{e_j} = r^2 \prod_{j=1}^{k} \left(s_j^2 \upsilon_j\right)^{e_j} = r^2 = \mathrm{u} \bmod n$$

Αφού $w = u$, προκύπτει ότι $e = h(m \| u) = h(m \| w) = e'$.

■

Παράδειγμα 3.1:

Έστω ότι ο Α επιλέγει $p = 3571$ και $q = 4523$ και υπολογίζει το $n = 16151633$. Τα s_j, υ_j, καθώς και οι ενδιάμεσες εκτιμήσεις των s_j^{-1} φαίνονται στον παρακάτω πίνακα.

j	1	2	3	4	5
s_j	42	73	85	101	150
$s_j^{-1} \bmod n$	4999315	885021	6270634	13113207	11090788
$\upsilon_j = \mathrm{s}_j^{-2} \bmod n$	503594	4879734	7104483	1409171	6965302

Θεωρούμε τη συνάρτησης κατακερματισμού $h : \{0,1\}^* \to \{0,1\}^5$. Ο Α επιλέγει $r =$ 23181 και υπολογίζει $u = r^2 \bmod n$ = 4354872. Για να υπογράψει το μήνυμα m, ο Α υπολογίζει το $e = h(m \| u)$ = 10110 (η τιμή κατακερματισμού έχει επινοηθεί σε αυτό

το παράδειγμα) και σχηματίζει το $s = rs_1 s_3 s_4 \bmod n$ = (23181)(42)(85)(101) $\bmod n$ = 7978909. Η υπογραφή του Α για το μήνυμα m είναι το (e, s) = (10110, 7978909).

Για να επαληθεύση την υπογραφή, ο Β υπολογίζει $s^2 \bmod n$ = 2926875 και αναπτύσει $w = s^2 \upsilon_1 \upsilon_3 \upsilon_4 \bmod n$ = (2926875)(503594)(7104483)(1409171) $\bmod n$ = 4354872. Διαπιστώνει ότι $w = u$, άρα $e = h(m \square u) = h(m \square w) = e'$ κι έτσι αποδέχεται την υπογραφή. ■

Παρατηρήσεις:

1. Παρατηρούμε ότι αν το n έχει μέγεθος t-bits, τότε το ιδιωτικό κλειδί που παράγεται είναι μεγέθους kt-bits και το δημόσιο μεγέθους (k+1)t-bits. Μπορούμε να μειώσουμε αυτά τα μεγέθη αν επιλέξουμε τιμές s_j, 1 ≤ j ≤ k μήκους t'-bits, όπου t' < t . Για παράδειγμα, αν t = 768 και k = 128 , τότε το ιδιωτικό κλειδί απατεί αποθηκευτικό χώρο 98304-bits και το δημόσιο 99072-bits.

2. Αν επιλέξουμε το n να είναι μεγέθους t = 768-bits και k = 128-bits, τότε, η παραγωγή υπογραφής του σχήματος Feige-Fiat-Shamir απαιτεί κατά μέσο όρο k/2 = 64 modular πολλαπλασιασμούς με χρήση απλών τεχνικών εκθετοποίησης. Αντίστοιχα, το RSA απαιτεί κατά μέσο όρο 1152 modular πολλαπλασιασμούς (768 υψώσεις στο τετράγωνο και 384 πολλαπλασιασμούς). Αντίθετα, η επαλήθευση υπογραφής απαιτεί μόνο έναν modular πολλαπλασιασμό για το RSA αν ο δημόσιος εκθέτης είναι e = 3 και 64 modular πολλαπλασιασμούς για το Feige-Fiat-Shamir. Παρατηρούμε, λοιπόν, ότι για εφαρμογές όπου η παραγωγή υπογραφής πρέπει να εκτελείται άμεσα και ο χώρος αποθήκευσης κλειδιών δεν είναι περιορισμένος, το σχήμα υπογραφής Feige-Fiat-Shamir είναι προτιμότερο σε σχέση με το RSA.

3.1.1 ΑΣΦΑΛΕΙΑ ΤΟΥ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ Feige-Fiat-Shamir

Η ασφάλεια του σχήματος υπογραφής Feige-Fiat-Shamir βασίζεται στη δυσκολία υπολογισμού των τετραγωνικών ριζών modulo n. Επίσης, είναι αποδεδειγμένα ασφαλές απέναντι σε μια προσαρμόσιμη επίθεση σε επιλεγμένο μήνυμα (adaptive message chosen attack), υπό την προϋπόθεση ότι η παραγοντοποίηση είναι απρόσιτη, η h είναι μια τυχαία συνάρτηση και τα s_i είναι διακεκριμένα.

3.1.2 ΥΠΟΓΡΑΦΕΣ Feige-Fiat-Shamir ΣΕ ΣΥΣΤΗΜΑΤΑ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΑΥΤΟΤΗΤΑΣ

Το σχήμα υπογραφής Feige-Fiat-Shamir μπορεί να τροποποιηθεί, ώστε να εφαρμόζεται σε συστήματα πιστοποίησης ταυτότητας. Στην προκειμένη περίπτωση, πρωταρχικό ρόλο παίζει μία Έμπιστη Αρχή (TTP), η οποία επιλέγει τους πρώτους p, q και υπολογίζει το n, καθώς επίσης, τα ιδιωτικά και δημόσια κλειδιά κάθε χρήστη στο σύστημα. Το modulo n είναι κοινό για όλους τους χρήστες.

Θεωρούμε μία ακολουθία bit $\mathrm{I_A}$, η οποία περιέχει πληροφορία που ταυτοποιεί τον A. Η TTP υπολογίζει $\upsilon_j = f(I_A \| j)$, 1 ≤ j ≤ k, όπου $f : \{0,1\}^* \to Q_n$ είναι μία συνάρτηση μονής κατεύθυνσης και το j αναπαρίσταται δυαδικά. Επιπλέον, υπολογίζει μια τετραγωνική ρίζα s_j από το $\upsilon_j^{-1} \bmod n$. Το δημόσιο κλειδί του A είναι η πληροφορία πιστοποίησης ταυτότητας $\mathrm{I_A}$, ενώ το ιδιωτικό του κλειδί είναι το $(\mathrm{s}_1, s_2, ..., s_k)$. Ασφαλώς, το ιδιωτικό κλειδί μεταφέρεται μυστικά από την TTP στον A και οι συναρτήσεις h, f και modulo n είναι *γενικές (system-wide) ποσότητες.*

Το πλεονέκτημα αυτής της διαδικασίας είναι ότι το δημόσιο κλειδί μπορεί να έχει παραχθεί από μία μικρότερη ποσότητα $\mathrm{I_A}$ κι έτσι μειώνεται το κόστος αποθήκευσης και μεταφοράς. Όμως, το ότι τα ιδιωτικά κλειδιά των χρηστών είναι γενικά γνωστά στην TTP και το γεγονός ότι τα modulo n είναι γενικά (system-wide), αποτελούν μεγάλα μειονεκτήματα, εφόσον την κάνουν πιο ευάλωτη σε πιθανές επιθέσεις.

Μπορούμε να βελτιώσουμε τη μέθοδο που μόλις περιγράψαμε, έτσι ώστε να μειώσουμε το μέγεθος του δημοσίου κλειδιού και να αυξήσουμε την

αποδοτικότητα επαλήθευσης της υπογραφής. Αυτό επιτυγχάνεται αν κάθε χρήστης Α παράγει τα δικά του modulo n_A και k μικρούς πρώτους $\upsilon_1, \upsilon_2, ..., \upsilon_k \in Q_n$, καθένας από τους οποίους απαιτεί περίπου 2 bytes για να αναπαρασταθεί. Επιπλέον, επιλέγει μία από τις τετραγωνικές ρίζες s_j από τα $\upsilon_j^{-1} \bmod n$, για κάθε j, $1 \leq j \leq k$. Αυτά αποτελούν το ιδιωτικό του κλειδί, ενώ το δημόσιο κλειδί του είναι το n_A και οι τιμές $\upsilon_1, \upsilon_2, ..., \upsilon_k$.

Σχόλιο: Με τον όρο *modular πολλαπλασιασμός* εννοούμε την παρακάτω διαδικασία: Επιλέγουμε n μήκους k-bit και x, y $\in \mathbf{Z}_n$, 0 $\leq$ x, y $\leq$ n-1. Τότε, το xymodn μπορεί να υπολογιστεί σε δύο βήματα σε χρόνο τάξης $O(k^2)$. Πρώτα, υπολογίζουμε το γινόμενο xy, το οποίο είναι 2k-bits και μετά παίρνουμε το αποτέλεσμα modulo n.

3.2 ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ GQ

Το σχήμα υπογραφής GQ προέρχεται από το πρωτόκολλο πιστοποίησης ταυτότητας Guillou-Quisquater (GQ), στο οποίο η πρόκληση αντικαθίσταται από μία συνάρτηση κατακερματισμού μονής κατεύθυνσης h: {0, 1}$^{*} \rightarrow \mathbf{Z}n$, όπου n ένας θετικός αριθμός. Τυπικές τιμές για ασφαλείς συναρτήσεις κατακερματισμού αποτελούν τα 128 ή 160-bits.

Παραγωγή κλειδιού

- Ο Α επιλέγει τυχαίους, διακεκριμένους πρώτους p, q και υπολογίζει το γινόμενο $n = pq$. Το n πρέπει να έχει μέγεθος τουλάχιστον 768-bits.
- Επιλέγει έναν τυχαίο ακέραιο $e \in \{1, 2, ..., \mathrm{n}-1\}$ μεγέθους τουλάχιστον 128-bits, τέτοιον ώστε ΜΚΔ $(e, (p-1)(q-1)) = 1$.
- Επιλέγει έναν ακέραιο J_A, 1 < J_A < n , έτσι ώστε ΜΚΔ(J_A , n)= 1.
- Τέλος, ορίζει έναν ακέραιο $\alpha \in \mathbf{Z}_n$, έτσι ώστε $J_A \alpha^e = 1 \bmod n$ ακολουθώντας τα εξής βήματα:
  - Υπολογίζει $J_A^{-1} \bmod n$.
  - Υπολογίζει $d_1 = e^{-1} \bmod (p-1)$ και $d_2 = e^{-1} \bmod (\mathrm{q}-1)$.
  - Υπολογίζει $\alpha_1 = (J_A^{-1})^{d_1} \bmod p$ και $\alpha_2 = (J_A^{-1})^{d_2} \bmod \mathrm{q}$.
  - Τέλος, βρίσκει μία λύση α για το σύστημα ισοδυναμιών $\alpha = \alpha_1 \bmod p$ και $\alpha = \alpha_2 \bmod \mathrm{q}$.

Το δημόσιο κλειδί του Α είναι το (n, e, J_A) και το ιδιωτικό του το α .

Το σχήμα υπογραφής GQ

Υποθέτουμε ότι ο Α υπογράφει ένα δυαδικό μήνυμα m αυθαίρετου μήκους και το στέλνει στον Β, ο οποίος θα επαληθεύσει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Α.

1. *Δημιουργία υπογραφής:*

   - Ο Α επιλέγει τυχαίο ακέραιο k και υπολογίζει το $r = k^e \bmod n$.
   - Υπολογίζει το $l = h(m \| r)$.
   - Υπολογίζει το $s = k\alpha^l \bmod n$.
   - Στέλνει στον Β την τριάδα $(m,(s,l))$, όπου το ζεύγος (s,l) αποτελεί την υπογραφή του Α για το μήνυμα m.

2. *Επαλήθευση υπογραφής:*

   - Ο Β αποκτά το αυθεντικό κλειδί του Α (n,e,J_A).
   - Υπολογίζει το $u = s^e J_A^l \bmod n$.
   - Υπολογίζει το $l' = h(m \| u)$ και αποδέχεται την υπογραφή αν και μόνο αν $l = l'$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί

Πράγματι, $u = s^e J_A^l = (k\alpha^l)^e J_A^l = k^e (\alpha^e J_A)^l = k^e = r \bmod n$.
Αφού $u = r$, έχουμε ότι $l = h(m \| r) = h(m \| u) = l'$.

■

Παράδειγμα 3.2:

Παραγωγή κλειδιού: Ο Α επιλέγει τους πρώτους p = 20849, q = 27457 και υπολογίζει το $n = pq$ = 572450993. Στη συνέχεια, επιλέγει έναν ακέραιο e = 47,

έναν J_A= 1091522, λύνει την ταυτότητα $J_A\alpha^e = 1 \bmod n$ και βρίσκει ότι α = 214611724.

Το δημόσιο κλειδί του Α είναι το (n, e, J_A) = (572450993, 47, 1091522) και το ιδιωτικό του το α = 214611724.

Παραγωγή υπογραφής: Ο Α επιλέγει έναν τυχαίο ακέραιο k = 42134 για να υπογράψει το μήνυμα m = 1101110001 και υπολογίζει το $r = k^e \bmod n$ = 297543350. Έπειτα, υπολογίζει το $l = h(m \| r)$ = 2713833 (η τιμή κατακερματισμού επινοήθηκε για το παράδειγμά μας) και $s = k\alpha^l \bmod n$ =(42134) $214611724^{2713833} \bmod n$ = 252000854.

Η υπογραφή του Α για το μήνυμα m είναι το ζεύγος (s, l) = (252000854, 2713833).

Επαλήθευση υπογραφής: Ο Β υπολογίζει $s^e \bmod n$ = 398641962, $J_A^l \bmod n$ = $1091522^{2713833} \bmod n$ = 110523867 και $u = s^e J_A^l \bmod n$ = 297543350. Εφόσον $u = r$, σημαίνει ότι $l' = h(m \| u) = h(m \| r) = l$ και άρα ο Β αποδέχεται την υπογραφή.

■

Παρατηρήσεις:

1. Η δυαδική αναπαράσταση του J_A θα μπορούσε να χρησιμοποιηθεί για να μεταφέρει πληροφορίες σχετικά με τον Α, όπως το όνομα, τη διεύθυνση, τον αριθμό ταυτότητας κλπ. Γι΄αυτό το λόγο, χρησιμεύει ως αναγνωριστικό για τον Α.

2. Με τα μεγέθη που έχουμε ορίσει παραπάνω για το e και το n, το δημόσιο κλειδί για το σχήμα GQ είναι μεγέθους 896+u bits, όπου u είναι ο αριθμός των bits που απαιτούνται για να απεικονίσουν το J_A. Το ιδιωτικό κλειδί a είναι μεγέθους 768-bits.

3. Παρατηρούμε ότι η παραγωγή υπογραφής για το σχήμα GQ απαιτεί 2 modular εκθετοποιήσεις και 1 modular πολλαπλασιασμό. Επιλέγοντας n μεγέθους 768-bits, e 128-bits και μία τιμή κατακερματισμού για το l 128-bits, η παραγωγή υπογραφής απαιτεί κατά μέσο όρο 384 modular πολλαπλασιασμούς (128 υψώσεις στο τετράγωνο και 64 πολλαπλασιασμούς για καθένα από τα e και l). Συγκρίνοντάς το με το σχήμα υπογραφής Feige-Fiat-Shamir, το οποίο απαιτεί 64 modular πολλαπλασιασμούς για παραγωγή υπογραφής, παρατηρούμε ότι το GQ είναι υπολογιστικά πιο εντατικό, αλλά απαιτεί σημαντικά μικρότερο χώρο αποθήκευσης κλειδιών.

3.2.1 ΑΣΦΑΛΕΙΑ ΤΟΥ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ GQ

Η ασφάλεια του σχήματος υπογραφής GQ βασίζεται στην επιλογή του e , το οποίο πρέπει να είναι αρκετά μεγάλο. Όπως είπαμε και προηγουμένως, το e πρέπει να έχει μέγεθος τουλάχιστον 128-bits, διαφορετικά είναι ευάλωτο σε πιθανές πλαστογραφήσεις που βασίζονται στο παράδοξο των γενεθλίων (birthday paradox).

Μία ενδεχόμενη πλαστογράφηση είναι αυτή που θα περιγράψουμε παρακάτω:

Υποθέτουμε ότι ένας αντίπαλος Γ επιλέγει ένα μήνυμα m και υπολογίζει το $l = h(m \| J_A^d)$ για αρκετές τιμές του t, έως ότου $l = t \bmod e$. Αυτό αναμένεται να επιτευχθεί σε O($\sqrt{e}$) δοκιμές. Στη συνέχεια, ορίζει έναν ακέραιο x, τέτοιον ώστε $t = xe + l$ και υπολογίζει το $s = J_A^l \bmod n$. Πράγματι, παρατηρούμε ότι

$$s^e J_A^l = (J_A^x)^e s^e J_A^l = (J_A^x)^e J_A^l = J_A^{xe+l} = J_A^t \bmod n .$$

Επομένως, $h(m \| J_A^t) = l$ και άρα η (s, l) είναι μία έγκυρη αλλά πλαστή υπογραφή για το μήνυμα m.

3.2.2 ΠΑΡΑΛΛΑΓΗ ΤΟΥ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ GQ

Το σχήμα υπογραφής GQ μπορεί να τροποποιηθεί ώστε να παρέχει ανάκτηση του μηνύματος. Έστω χώρος υπογραφής M_s = $\mathbb{Z}_n$ και $m \in M_s$.

Η παραγωγή υπογραφής γίνεται ως εξής:

- Ο Α επιλέγει έναν τυχαίο ακέραιο k, τέτοιον ώστε ΜΚΔ (k, n) = 1.
- Υπολογίζει $r = k^e \bmod n$ και $l = mr \bmod n$.
- Η υπογραφή του Α για το m είναι το $s = k\alpha^l \bmod n$.

Η επαλήθευση της υπογραφής δίνει $u = s^e \alpha^{el} J_A^l = k^e = r \bmod n$ και το μήνυμα m ανακτάται από το $lr^{-1} \bmod n$.

<u>Σημείωση 3.1:</u> Όπως σε όλα τα σχήματα ψηφιακών υπογραφών με ανάκτησης του μηνύματος, απαιτείται μια κατάλληλη συνάρτηση πλεονάζουσας πληροφορίας, για να το διαφυλάσσει από πιθανή υπαρξιακή πλαστογράφηση.

4. ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ElGamal

Στο τρέχον κεφάλαιο θα αναπτύξουμε τη λειτουργία του κρυπτοσυστήματος και σχήματος υπογραφής El Gamal. Προηγουμένως, όμως, οφείλουμε να αναφερθούμε σε δύο προβλήματα της Θεωρίας Αριθμών, το Πρόβλημα Διακριτού Λογαρίθμου (DLP) και το Πρόβλημα των Diffie-Hellman(DHP), στα οποία βασίζεται η ασφάλεια του κρυπτοσυστήματος αυτού.

4.1 ΤΟ ΠΡΟΒΛΗΜΑ ΔΙΑΚΡΙΤΟΥ ΛΟΓΑΡΙΘΜΟΥ (Discrete Logarithm Problem (DLP))

Το ερώτημα που τίθεται είναι αν, δεδομένου ενός αριθμού y της μορφής b^x (όπου το b γνωστό), μπορούμε να υπολογίσουμε το μοναδικό x έτσι ώστε να ισχύει $y = b^x$ σε λογικό χρόνο. Ψάχνουμε, δηλαδή, την ύπαρξη αποδοτικού αλγόριθμου που να υπολογίζει το $x = \log_b y$.Το Πρόβλημα Διακριτού Λογαρίθμου ουσιαστικά είναι η επίλυση της παραπάνω εξίσωσης στο $\mathbf{Z}_p$, όπου p πρώτος.

Ορισμός DLP: Έστω G μια πεπερασμένη κυκλική ομάδα τάξης n,α ένας γεννήτορας της G και κάποιο στοιχείο $b \in G$. Ο *Διακριτός Λογάριθμος* του β στη βάση α συμβολίζεται με $\log_a b$ και είναι ο μοναδικός ακέραιος x , $0 \le x \le n-1$,τέτοιος ώστε $b=a^x$.

Παράδειγμα 4.1:

Έστω p=97, τότε η Z_{97}^* είναι κυκλική ομάδα τάξης 96, αφού 0 97 είναι πρώτος. Ο α=5 είναι γεννήτορας της Z_{97}^* και υπολογίζεται ότι $5^{32}=35 \bmod 97$. Άρα $\log_5 35=32$ στο Z_{97}^*. ■

Ορισμός 4.1: Το Πρόβλημα Διακριτού Λογαρίθμου (DLP) ορίζεται ως εξής:

Δεδομένα:

- Ένας πρώτος αριθμός p.
- Ένας γεννήτορας α του Z_p^*.
- Ένα στοιχείο b του Z_p^*.

Ζητούμενο:

Ένας ακέραιος x, $0 \le x \le p-2$, έτσι ώστε να ισχύει $\alpha^x = b \bmod p$.

Σημείωση 4.1: Αποδεικνύεται παρακάτω ότι η δυσκολία του DLP είναι ανεξάρτητη από το γεννήτορα α. Αν α και α΄ δύο γεννήτορες του $\mathbf{Z}_p^*$, $b \in \mathbf{Z}_p^*$ και $x = \log_\alpha b$, $y = \log_{\alpha'} b$ και $z = \log_\alpha \alpha'$, τότε $\alpha^x = b = \alpha'^y = (\alpha^z)^y$. Δηλαδή, $x = zy \bmod p$, όμως τότε $y = xz^{-1} \bmod p$, άρα $\log_{\alpha'} b = (\log_\alpha b)(\log_\alpha \alpha') \bmod p$.

Γίνεται, λοιπόν, κατανοητό, ότι αν ο διακριτός λογάριθμος υπολογίζεται σε μια βάση α, τότε μπορεί να υπολογιστεί σε οποιαδήποτε άλλη βάση α΄, με την προϋπόθεση ότι α, α΄ είναι γεννήτορες του $\mathbf{Z}_p^*$.

4.2 ΤΟ ΠΡΟΒΛΗΜΑ ΤΩΝ DIFFIE-HELLMAN (DHP)

Το πρόβλημα των Diffie-Hellman (DHP) διατυπώθηκε από Whitfield Diffie και Martin E. Hellman το 1976 σε μία δημοσίευση με τίτλο "New Directions in Cryptography", η οποία αποτέλεσε σταθμό για τη σύγχρονη κρυπτογραφία. Το DHP αποτελεί ένα από τα πιο σημαντικά προβλήματα της θεωρίας αριθμών, καθώς έχει άμεσες εφαρμογές στην Κρυπτογραφία.

Ορισμός DHP: Το πρόβλημα Diffie-Hellman (DHP) ορίζεται ως εξής:

Δεδομένα:

- Ένας πρώτος αριθμός p.
- Ένας γεννήτορας α του Z_p^*.
- Τα στοιχεία $\alpha^c \bmod p$ και $\alpha^b \bmod p \in Z_p^*$.

Ζητούμενο:

Το $\alpha^{bc} \bmod p$.

Σημείωση 4.2: Μπορούμε εύκολα να διαπιστώσουμε ότι το DLP είναι τουλάχιστον το ίδιο δύσκολο με το DHP. Αν θέσουμε $x = \alpha^c \bmod p$ και $y = \alpha^b \bmod p$, βρίσκουμε ότι $c = \log_\alpha x$ και $b = \log_\alpha y$. Είναι, λοιπόν, εμφανές ότι αν το DLP λύνεται σε λογικό χρόνο, τότε μπορούμε να υπολογίσουμε τα b και c κι επομένως το $\alpha^{bc} \bmod p$.

Πόρισμα 4.1: Από την παραπάνω σημείωση προκύπτει ότι DHP $\leq_P$ DLP, δηλαδή ότι το DHP ανάγεται στο DLP με πολυωνυμικό αλγόριθμο.

Επισημαίνουμε ότι δεν είμαστε σε θέση να γνωρίζουμε αν ισχύει και το αντίστροφο του πορίσματος, δηλαδή DHP $\leq_P$ DLP, πράγμα που σημαίνει ότι τα δύο προβλήματα είναι ισοδύναμα κατά Karp (DHP $=_P$ DLP).

4.3 ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ ElGamal

Ένα ευρέως διαδεδομένο κρυπτοσύστημα δημοσίου κλειδιού το οποίο βασίζεται στη δυσκολία επίλυσης του προβλήματος των Diffie-Hellman (DHP) είναι το σύστημα El Gamal, το οποίο θα αναπτύξουμε παρακάτω.

ΜΕΘΟΔΟΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ ElGamal

Υποθέτουμε ότι ο Α θέλει να ανταλλάξει κρυπτογραφημένα μηνύματα με τον Β και χρησιμοποιεί το κρυπτοσύστημα El Gamal. Απαραίτητη προϋπόθεση είναι η δημιουργία ενός δημόσιου κλειδιού και του αντίστοιχου ιδιωτικού. Τα κρυπτογραφημένα μηνύματα που προκύπτουν με χρήση του El Gamal, όπως θα διαπιστώσουμε στη συνέχεια, δεν είναι παρά το απλό κείμενο που φοράει μια "μάσκα" (την οποία εδώ θα συμβολίζουμε με δ) και ένα στοιχείο που χρησιμεύει για την αφαίρεσή της (εδώ θα το συμβολίζουμε με γ).

Παραγωγή κλειδιού:

- Ο Α επιλέγει έναν μεγάλο, τυχαίο, πρώτο αριθμό p κι έναν γεννήτορα α του $\mathbf{Z}_p^*$.
- Επιλέγει έναν τυχαίο ακέραιο b, $1 \le b \le p-2$.
- Υπολογίζει το $\alpha^b \bmod p$.
- Το (p, α, α^b) αποτελεί το δημόσιο κλειδί του Α, ενώ το b το ιδιωτικό.

Σημείωση 4.2: Όλοι οι υπολογισμοί γινονται στο $\mathbf{Z}_p$, όπου ο p πρέπει να επιλεγεί έτσι ώστε να έχει τουλάχιστον έναν μεγάλο παράγοντα και μέγεθος μεγαλύτερο από 768-bits.

Κρυπτογράφηση με δημόσιο κλειδί El Gamal

Έστω ότι ο Β θέλει να κρυπτογραφήσει ένα μήνυμα και να το στείλει στον Α.

1. *Κρυπτογράφηση:* Ο Β κάνει τα ακόλουθα:
   - Αποκτά το αυθεντικό κλειδί του Α, (p, α, α^b).
   - Αναπαριστά το μήνυμα ως έναν ακέραιο m, $0 \le m \le p-1$.
   - Επιλέγει έναν τυχαίο ακέραιο k, $1 \le k \le p-2$.
   - Υπολογίζει τα $\gamma = \alpha^k \bmod p$ και $\delta = m(\alpha^b)^k \bmod p$.
   - Στέλνει στον Α το κρυπτοκείμενο $c = (\gamma,\delta)$.

2. *Αποκρυπτογράφηση:* Ο Α για να ανακτήσει το αρχικό κείμενο από m από το c λειτουργεί ως ακολούθως:
   - Υπολογίζει το $\gamma^{-b} \bmod p$ ($= \alpha^{-bk}$), χρησιμοποιώντας το ιδιωτικό κλειδί b.
   - Ανακτά το μήνυμα m υπολογίζοντας το $\gamma^{-b}\delta \bmod p = \alpha^{-bk} m \alpha^{bk} \bmod p = m \bmod p$.

Παρατηρήσεις:

1. Ο υπολογισμός του γ^{-b} για την αποκρυπτογράφηση του μηνύματος ισοδυναμεί με τον υπολογισμό του γ^{p-1-b}, που συνήθως προτιμάται.

2. Η συνάρτηση κρυπτογράφησης El Gamal είναι Τυχαιοποιημένη (randomized), καθώς ο ακέραιος k επιλέγεται τυχαία. Με αυτό τον τρόπο ενισχύεται η ασφάλεια του κρυπτοσυστήματος, αφού απ'το αρχικό κείμενο m προκύπτουν περισσότερα από ένα διαφορετικά κρυπτοκείμενα.

Παράδειγμα 4.2:

Έστω ότι ο Α επιλέγει πρώτο p=2357 και έναν γεννήτορα α=2 της $\mathbf{Z}^*_{2357}$. Επιλέγει το ιδιωτικό του κλειδί b=1751 και υπολογίζει το $\alpha^b \bmod p = 2^{1751} \bmod 2357 = 1185$. Το δημόσιο κλειδί του Α είναι(2357, 2, 1185).

Κρυπτογράφηση: Για να κρυπτογραφήσει ο Β το μήνυμα m=2035, επιλέγει τυχαίο ακέραιο k=1520 και υπολογίζει τα

$$\gamma = 2^{1520} \bmod 2357 = 1430$$

και

$$\delta = 2035 \times 1185^{1520} \bmod 2357 = 697.$$

Στη συνέχεια στέλνει στον Α το ζεύγος (γ, δ).

Αποκρυπτογράφηση: Για να αποκρυπτογραφήσει, ο Α υπολογίζει το

$$\gamma^{p-1-b} = 1430^{605} \bmod 2357 = 872$$

και ανακτά το μήνυμα m υπολογίζοντας το

$$m = 872 \times 697 \bmod 2357 = 2035.$$ ■

4.4 ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ ElGamal

Το σχήμα ψηφιακής υπογραφής El Gamal παρουσιάστηκε για πρώτη φορά από τον T. El Gamal το 1985. Σε αντίθεση με το RSA, είναι ένα μη ντετερμινιστικό σχήμα υπογραφής, που σημαίνει ότι για ένα δεδομένο μήνυμα υπάρχουν περισσότερες από μία διαφορετικές έγκυρες υπογραφές. Αυτό συμβαίνει, διότι η συνάρτηση υπογραφής sig_K εξαρτάται από ένα επιπλέον όρισμα, κάποιον τυχαίο ακέραιο k. Παρά ταύτα, η συνάρτηση επαλήθευσης ver_K δέχεται ως έγκυρη οποιαδήποτε υπογραφή έχει προκύψει από το σχήμα αυτό.

Υποθέτουμε ότι ο Α θέλει να υπογράψει ψηφιακά ένα μήνυμα m με το El Gamal και να το στείλει στον Β. Αρχικά παράγει το αυθεντικό κλειδί K = (p, α, b, β) με την ίδια διαδικασία που περιγράψαμε παραπάνω για το κρυπτοσύστημα, όπου τα p, α, b έχουν ήδη οριστεί σ'αυτήν και $\beta = \alpha^b \bmod p$. Ο p πρέπει να είναι τέτοιος, ώστε το DLP να είναι υπολογιστικά απρόσιτο στο $\mathbf{Z}_p^*$. Από το 1996 προτείνεται το modulo p να είναι μεγέθους τουλάχιστον 768-bits.

Το σχήμα υπογραφής ElGamal

1. *Δημιουργία υπογραφής:*
   - Ο Α επιλέγει έναν τυχαίο ακέραιο k, τέτοιον ώστε $1 \le k \le p-2$ και ΜΚΔ(k, p-1) = 1.
   - Υπολογίζει τα $\gamma = \alpha^k \bmod p$ και $\delta = (m - b\gamma)k^{-1} \bmod (p-1)$.
   - Τέλος, στέλνει στον Β την τριάδα (m, γ, δ), όπου m το αρχικό μήνυμα και (γ, δ) η ψηφιακή υπογραφή του Α.

2. *Επαλήθευση υπογραφής:*
   - Ο Β ανακτά το δημόσιο κλειδί του Α (p, α, β).
   - Ελέγχει αν $\beta^\gamma \gamma^\delta = \alpha^m \bmod p$. Αν ναι, τότε $ver_K(m, \gamma, \delta)$ = αληθής και αποδέχεται ότι το μήνυμα προέρχεται από τον Α, αλλιώς το απορρίπτει.

Παρατηρήσεις:

1) Η συνάρτηση υπογραφής για ένα μήνυμα m και τυχαίο k είναι η $sig_K(m,k) = (\gamma,\delta)$ και αποτελεί ιδιωτική πληροφορία. Αντίθετα, η διαδικασία επαλήθευσης επιτυγχάνεται χρησιμοποιώντας μόνο δημόσια πληροφορία.

2) Η τριάδα (m,γ,δ) καλείται *υπογεγραμμένο μήνυμα*.

3) Το ElGamal ανήκει στα σχήματα υπογραφής με παράρτημα.Το μήνυμα m δεν μπορεί να ανακτηθεί εύκολα από την υπογραφή (γ,δ) ενώ είναι απαραίτητο να συμπεριληφθεί στη συνάρτηση επαλήθευσης.

Απόδειξη ορθότητας της διαδικασίας επαλήθευσης:

Από τον ορισμό των γ,δ έχουμε ότι:

$$\beta^{\gamma}\gamma^{\delta} = \alpha^{b\gamma}\alpha^{k\delta} \bmod p = \alpha^{b\gamma+k\delta} \bmod p = \alpha^{m} \bmod p ,$$

αφού $b\gamma+k\delta = m \bmod(p-1)$,από τη γνωστή *Πρόταση*:

$\alpha^x = \alpha^y \bmod p \Leftrightarrow x = y \bmod(p-1)$, για κάθε $x, y \in \mathbf{Z}$, p πρώτο αριθμό και α πρωταρχικό στοιχείο του $\mathbf{Z}_p^*$.

■

Παράδειγμα 4.3:

Έστω $p = 467$, $\alpha = 2$ και $b = 127$ τότε

$$\beta = \alpha^b \bmod p = 2^{127} \bmod 467 = 132$$

Υποθέτουμε ότι ο Α θέλει να υπογράψει το μήνυμα $m = 100$ κι επιλέγει $k = 213$.Έτσι, $ΜΚΔ(213,466) = 1$ και $k^{-1} \bmod(p-1) = 213^{-1} \bmod 466 = 431$. Τότε

$$\gamma = 2^{213} \bmod 467 = 29 \quad \text{και} \quad \delta = (100-127\times29)431 \bmod 466 = 51$$

οπότε και στέλνει στον Β το (100, 29, 51).

Ο Β υπολογίζει

$$132^{29}29^{51} = 189 \ (\bmod 467)$$

και $$2^{100} = 189 \ (\bmod 467)$$

Άρα η υπογραφή είναι έγκυρη.

■

4.4.1 ΑΣΦΑΛΕΙΑ ΤΟΥ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ ElGamal

Η ασφάλεια του σχήματος ψηφιακής υπογραφής ElGamal βασίζεται κυρίως στη δυσκολία επίλυσης του Προβλήματος Διακριτού Λογαρίθμου(DLP). Έστω ότι κάποιος Γ προσπαθεί να πλαστογραφήσει την υπογραφή του Α χωρίς να γνωρίζει το ιδιωτικό του κλειδί b. Διακρίνουμε τρεις περιπτώσεις:

I. Ο Γ επιλέγει τυχαία μια τιμή για το γ και προσπαθεί να βρει το αντίστοιχο δ, έτσι ώστε να ικανοποιείται η εξίσωση $\beta^{\gamma}\gamma^{\delta} = \alpha^{m}$ modp. Στην περίπτωση αυτή, ο Γ θα πρέπει να λύσει το Πρόβλημα Διακριτού Λογαρίθμου $\log_{\gamma}\alpha^{m}\beta^{-\gamma}$.

II. Αντίθετα με την περίπτωση (I), ο Γ τώρα επιλέγει πρώτα ένα τυχαίο δ και κατόπιν, προσπαθεί να υπολογίσει το αντίστοιχο γ απο την εξίσωση $\beta^{\gamma}\gamma^{\delta} = \alpha^{m}$ modp. Ωστόσο, αυτό αποτελεί ένα πρόβλημα, το οποίο δε μπορεί να αναχθεί σε κάποιο από τα γνωστά μέχρι τώρα προβλήματα της Κρυπτολογίας και συνεπώς δεν έχει βρεθεί εφικτή λύση.

III. Ο Γ επιλέγει ταυτόχρονα τυχαία γ και δ και προσπαθεί να υπολογίσει το m. Λύνοντας την εξίσωση επαλήθευσης ως προς m, έρχεται πάλι αντιμέτωπος με ένα στιγμιότυπο του DLP, καθώς $m = \log_{\alpha}\beta^{\gamma}\gamma^{\delta}$.

4.4.2 ΕΣΦΑΛΜΕΝΗ ΧΡΗΣΗ ΤΟΥ ElGamal

Παρόλο που, όπως είδαμε προηγουμένως, είναι σχεδόν αδύνατο να πλαστογραφηθεί η υπογραφή του Α, εν τούτοις, υπάρχουν τρόποι να “σπάσει” το σχήμα υπογραφής ElGamal αν χρησιμοποιηθεί απρόσεκτα. Γι’ αυτό είναι πολύ σημαντικό:

- Ο τυχαία επιλεγμένος ακέραιος k να κρατείται οπωσδήποτε μυστικός. Ο λόγος είναι ότι, καθώς οι ποσότητες α,β είναι δημόσια γνωστές, πιθανή γνωστοποίηση του k μπορεί να δώσει τη δυνατότητα σε οποιονδήποτε κάτοχο ενός υπογεγραμμένου μηνύματος (m,(γ,δ)) να μπορεί να υπολογίσει

το ιδιωτικό κλειδί b, από τη σχέση $b = (m-k\delta)\gamma^{-1} \bmod(p-1)$ και συνεπώς να προσδιορίσει τη συνάρτηση υπογραφής sig_K.

- Να επιλέγονται διαφορετικά k για την υπογραφή διαφορετικών μηνυμάτων, αφού η επανάληψη του ίδιου k δίνει σε κάποιον Γ τη δυνατότητα να υπολογίσει το ιδιωτικό κλειδί b. Πράγματι, αν ο Α χρησιμοποιήσει το ίδιο k για να υπογράψει δύο διαφορετικά μηνύματα m_1 και m_2, τότε (γ, δ_1) είναι η υπογραφή για το m_1 και (γ, δ_2) είναι η υπογραφή για το m_2. Έχουμε ότι:

$$\beta^{\gamma}\gamma^{\delta 1} = \alpha^{m1} \bmod p \quad \text{και} \quad \beta^{\gamma}\gamma^{\delta 2} = \alpha^{m2} \bmod p$$

Αφαιρώντας τις δύο σχέσεις κατά μέλη προκύπτει ότι:

$$\alpha^{m1-m2} = \gamma^{\delta 1-\delta 2} \bmod p \Rightarrow \alpha^{m1-m2} = \alpha^{k(\delta 1-\delta 2)} \bmod p ,$$

όπου αντικαταστήσαμε $\gamma = \alpha^k$.

Αυτό ισοδυναμεί με:

$$m_1-m_2 = k(\delta_1-\delta_2) \bmod(\rho-1) \qquad (1)$$

'Εστω τώρα ότι ο d είναι ο ΜΚΔ$(\delta_1-\delta_2, \rho-1)$, τότε ο d διαιρεί το m_1-m_2. Ορίζουμε:

$$m' = (m_1- m_2)/d$$
$$\delta'= (\delta_1- \delta_2)/d$$
$$\rho'= (\rho-1)/d$$

Διαιρώντας την (1) με d και αντικαθιστώντας τα m',δ' και ρ' προκύπτει:

$$m'= k\delta' \bmod\rho' \Rightarrow k = m'(\delta')^{-1} \bmod\rho' \Rightarrow k = m'l \bmod\rho' ,$$

αφού ΜΚΔ$(\delta',\rho') = 1$ και $l = (\delta')^{-1} \bmod\rho'$.

Υπάρχουν, λοιπόν, d πιθανές λύσεις για το k της μορφής:

$$k = m'l + i\rho' \bmod(\rho-1), \text{ για } 0 \le i \le d-1$$

Ο Γ υπολογίζει το α^k για καθε πιθανό k (από τις d παραπάνω υποψήφιες τιμές) μέχρις ότου βρεί αυτό που ικανοποιεί την ισότητα $\gamma = \alpha^k \bmod p$. Τώρα ξέρει το k και μπορεί ν'ανακτήσει την υπογραφή του Α.

Παράδειγμα 4.3:

Ο Α θέλει να υπογράψει ένα μήνυμα $m_1 = 151405$ (το οποίο αντιστοιχεί στη λέξη «one» αν ορίσουμε a = 01, b = 02, …..). Επιλέγει p = 225119 και τον μυστικό αριθμό b. Το α = 11 είναι αρχική ρίζα.

Υπολογίζει $\beta = \alpha^b \bmod p = 18191 \pmod p$.Για να υπογράψει το μήνυμα επιλέγει ένα τυχαίο αριθμό k, τον οποίο κρατάει κρυφό. Υπολογίζει

$$\gamma = \alpha^k \bmod p = 164130 \pmod p$$

και $\delta_1 = k^{-1}(m_1-b\gamma) \bmod(p-1) = 130777 \pmod{(p-1)}$

Το υπογεγραμμένο μήνυμα είναι η τριάδα (151405, 164130, 130777).

Υποθέτουμε τώρα ότι ο Α υπογράφει με τον ίδιο τρόπο κι ένα άλλο μήνυμα m_2 = 202315 (το οποίο αντιστοιχεί στη λέξη «two»).Το υπογεγραμμένο μήνυμα που προκύπτει είναι το (202315, 164130, 164899).

Ο Γ αναγνωρίζει αμέσως ότι ο Α χρησιμοποίησε το ίδιο k, αφού η τιμή του γ είναι η ίδια και στις δύο υπογραφές.Έτσι, υπολογίζει

$$-34122k = (\delta_1-\delta_2)k = m_1-m_2 = -50910 \pmod{p-1}$$

Αφού ΜΚΔ(-34122, p-1) = 2, υπάρχουν 2 πιθανές λύσεις για το k. Διαιρώντας την παραπάνω εξίσωση με το 2 έχουμε:

$$-17061k = -25455 \pmod{(p-1)/2},$$

η οποία έχει λύση $k = 239 \pmod{(p-1)/2}$ και οι δύο τιμές για το k είναι $k_1 = 239$ και $k_2 = 239 + (p-1)/2 = 112789$. Υπολογίζοντας

$$\alpha^{239} = 164130 \pmod{p} \quad \text{και} \quad \alpha^{112789} = 59924 \pmod{p}$$

βρίσκει ότι η πρώτη αντιστοιχεί στη σωστή τιμή του γ. Άρα k = 239.

Τώρα ξαναγράφοντας $\delta_1 k = m_1 - b\gamma \pmod{p-1}$ βρίσκει

$$164130b = \gamma b = m_1 - \delta_1 k = 187104 \pmod{p-1}$$

Αφού ΜΚΔ(164130, p-1) = 2, υπάρχουν 2 πιθανές λύσεις για το b, οι $b_1 = 28862$ και $b_2 = 141421$. Υπολογίζοντας

$$\alpha^{28862} = 206928 \pmod{p} \quad \text{και} \quad \alpha^{141421} = 18191 \pmod{p}$$

βρίσκει την τιμή που αντιστοιχεί στο β, άρα ανακαλύπτει το b = 141421.

■

4.4.3 ΠΛΑΣΤΟΓΡΑΦΗΣΕΙΣ ΤΗΣ ΥΠΟΓΡΑΦΗΣ ElGamal

Σε αντίθεση με το RSA, δεν είναι εύκολο να πλαστογραφήσει κάποιος την υπογραφή του Α για τυχαίο μήνυμα m. Υπάρχουν, ωστόσο, οι παρακάτω τρόποι με τους οποίους μπορεί να παραχθεί μια πλαστή υπογραφή.

I. Ο Γ επιλέγει τα γ, δ και m ταυτόχρονα έτσι ώστε:

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

για i, j τέτοια ώστε $0 \le i, j \le p-2$ και ΜΚΔ(j, p-1) = 1, αφού το j^{-1} υπολογίζεται modulo (p-1).

Το (γ,δ) είναι έγκυρη υπογραφή για το ElGamal.

Πράγματι, $\beta^\gamma\gamma^\delta = \beta^{\alpha^i\beta^j}(\alpha^i\beta^j)^{-\alpha^i\beta^j j^{-1}} \bmod p = \beta^{\alpha^i\beta^j}\alpha^{-ij^{-1}}\alpha^i\beta^j\beta^{-\alpha^i\beta^j} \bmod p =$ $\alpha^{-ij^{-1}}\alpha^i \bmod p = \alpha^{-\gamma ij^{-1}} \bmod p = \alpha^m \bmod p$

Με τη μέθοδο αυτή επιτυγχάνεται μία υπαρκτή πλαστογράφηση χρησιμοποιώντας επίθεση μόνο σε κλειδί.

Παράδειγμα 4.4:

Έστω p = 467, α = 2 και β = 132. Υποθέτουμε ότι ο Γ επιλέγει i = 99 και j = 179. Τότε, j^{-1} mod (p-1) = 151 και υπολογίζει

$$\gamma = 2^{99}132^{179} \bmod 467 = 117$$

$$\delta = -117 \times 151 \bmod 466 = 41$$

$$m = 99 \times 41 \bmod 466 = 331$$

Το ζεύγος (117, 41) είναι έγκυρη υπογραφή για το μήνυμα 331. Πράγματι,

$$132^{117}117^{41} = 303 \pmod{467}$$

και $2^{331} = 303 \pmod{467}$.

■

II. Ο Γ, τώρα, έχει στην κατοχή του ένα μήνυμα υπογεγραμμένο από τον Α, το (m, (γ,δ)). Έστω οι ακέραιοι h, i και j με $0 \le h, i, j \le p-2$ και ΜΚΔ(hγ - jδ, p-1) = 1 και υπολογίζει τα

$$x = \gamma h \alpha^i \beta^j \bmod p$$

$$z = \delta x (h\gamma - j\delta)^{-1} \bmod (p-1)$$

$$m' = x(hm + i\delta)(h\gamma - j\delta)^{-1} \bmod (p-1)$$

Μπορούμε να επαληθεύσουμε ότι ισχύει:

$$\beta^x x^z = \alpha^{m'} \bmod p$$

Και σε αυτήν την περίπτωση έχουμε υπαρκτή πλαστογράφηση, αλλά με επίθεση σε γνωστό μήνυμα.

<u>Παρατηρήσεις:</u>

1) Οι πλαστογραφήσεις αυτές δεν αποτελούν σοβαρή απειλή, διότι δεν δύνανται να παράξουν υπογραφή για τυχαία επιλεγμένο μήνυμα m.

2) Οι δύο τρόποι πλαστογράφησης που περιγράψαμε μπορούν να αποφευχθούν με τη χρήση κατάλληλης συνάρτησης κατακερματισμού.

4.5 Ο ΑΛΓΟΡΙΘΜΟΣ ΨΗΦΙΑΚΗΣΗ ΥΠΟΓΡΑΦΗΣ (DSA)

Ο αλγόριθμος ψηφιακής υπογραφής (DSA) είναι μια παραλλαγή της ψηφιακής υπογραφής ElGamal που προσπαθεί να μειώσει το μέγεθος της ψηφιακής υπογραφής που παράγεται και ανήκει στην κατηγορία των σχημάτων ψηφιακών υπογραφών με παράρτημα.

Ο αλγόριθμος αυτός προτάθηκε τον Αύγουστο του 1991 απο το Αμερικάνικο Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) και υιοθετήθηκε ως πρότυπο το 1994. Αποτελεί δε, το πρώτο σχήμα ψηφιακής υπογραφής που αναγνωρίζεται από οποιαδήποτε κυβέρνηση.

Ο μηχανισμός υπογραφής απαιτεί μια συνάρτηση κατακερματισμού $h: \{0,1\} \rightarrow Z_q$, για κάθε ακέραιο q. Το DSA απαιτεί ρητά τη χρήση του Secure Hash Algorithm (SHA-1).

Υποθέτουμε παρακάτω ότι έχουμε ήδη εφαρμόσει στο μήνυμα m την SHA-1 συνάρτηση κατακερματισμού και ότι αυτό που υπογράφουμε είναι η σύνοψη του μηνύματος (message digest).

Πριν προχωρήσουμε στην περιγραφή του DSA, παραθέτουμε το παρακάτω βοηθητικό λήμμα:

Λήμμα 4.1:

Άν p πρώτος, q|p-1 και g_0 πρωταρχικό στοιχείο του $\mathbf{Z}_p^*$, το

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

είναι q-οστή ρίζα της μονάδας modulo p. Δηλαδή, $g^q = 1 \bmod p$.

Απόδειξη:

Αφού q|p-1, θα υπάρχει $\lambda \in \mathbf{Z}$, τέτοιο ώστε p-1 = λq.
Όμως τότε,

$$g^q = g_0^{\left(\frac{p-1}{q}\right)^q} = g_0^{p-1} = 1 \bmod p ,$$

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

■

Διαδικασία Παραγωγής Κλειδιού

- Ο Α επιλέγει έναν πρώτο q, έτσι ώστε $2^{159} < q < 2^{160}$.
- Επιπλέον, βρίσκει έναν πρώτο p, τέτοιον ώστε $2^{511+64t} < p < 2^{512+64t}$, όπου t ∈ {0,…,8} και q|p-1.
- Υπολογίζει κάποιον g, τέτοιον ώστε $g^q = 1 \bmod p$ (με τον τρόπο που περιγράφεται στο Λήμμα 4.1)
- Επιλέγει έναν κρυφό ακέραιο α, 1 < α < q-1, ο οποίος είναι το ιδιωτικό του κλειδί.
- Τέλος, υπολογίζει το $\beta = g^{\alpha} \bmod p$

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

Το σχήμα υπογραφής DSA

Έστω τώρα ότι ο Α επιθυμεί να στείλει στον Β ένα μήνυμα m, υπογεγραμμένο ψηφιακά με το DSA, χρησιμοποιώντας το κλειδί K = (p, q, α, g, β).

1. *Δημιουργία Υπογραφής:*

   - Ο Α επιλέγει εναν τυχαίο ακέραιο k, 1 ≤ k ≤ q-1 τον οποίο κρατάει μυστικό.
   - Υπολογίζει τα $\gamma = (g^k \bmod p) \bmod q$ και
     $\delta = (m+\alpha\gamma)k^{-1} \bmod q$.
   - Στέλνει στον Β την τριάδα (m,γ, δ), όπου m το αρχικό μήνυμα και $(\gamma,\delta)=sig_K(m,k)$ η ψηφιακή υπογραφή του Α για το τυχαία επιλεγμένο k.

2. *Επαλήθευση Υπογραφής:*

   - Ο Β ανακτά το αυθεντικό κλειδί του Α (p, q, g, β).
   - Υπολογίζει τα $e_1 = m\delta^{-1} \bmod q$ και $e_2 = \gamma\delta^{-1} \bmod q$.
   - Ελέγχει αν $(g^{e_1} \beta^{e_2} \bmod p) \bmod q = \gamma$.

   Αν ναι, $ver_K(m, \gamma, \delta)$ = αληθής και αποδέχεται την υπογραφή του Α, αλλιώς την απορρίπτει.

Απόδειξη ότι η επαλήθευση λειτουργεί:

Από τον ορισμό του δ έχουμε:

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

Έτσι,

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

Άρα παίρνουμε,

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

■

Παράδειγμα 4.5:

Έστω q = 101 και p = 78q + 1 = 7879. Το $g_0 = 3$ είναι πρωταρχικό στοιχείο του $\mathbf{Z}^*_{7879}$ άρα $g = 3^{78} \bmod 7879 = 170$.

Ο Α επιλέγει α = 75 και υπολογίζει $\beta = g^{\alpha} \bmod 7879 = 4567$. Για να υπογράψει το μήνυμα m = 22 (το οποίο ουσιαστικά ειναι η σύνοψη του μηνύματος όπως προέκυψε απο την εφαρμογή του SHA-1 σε αυτό) επιλέγει k = 50 και υπολογίζει

$$k^{-1} \bmod 101 = 50^{-1} \bmod 101 = 99 ,$$

$$\gamma = (170^{50} \bmod 7879) \bmod 101 = 2518 \bmod 101 = 94$$

και $\delta = (22 + 75\times 94)99 \bmod 101 = 97$

Η επαλήθευση της υπογραφής (94, 97) από κάποιον Β γίνεται ως εξής:

$$\delta^{-1} = 97^{-1} \bmod 101 = 25$$

$$e_1 = 22\times 25 \bmod 101 = 45$$

$$e_2 = 94\times 25 \bmod 101 = 27$$

άρα $(170^{45}4567^{27} \bmod 7879) \bmod 101 = 2518 \bmod 101 = 94$.

■

Παρατηρήσεις:

1. Αν κατά τη διαδικασία παραγωγής υπογραφής προκύψει δ = 0modq, τότε ο Α θα πρέπει να το απορρίψει και να κατασκευάσει μια νέα υπογραφή, επιλέγοντας καινούριο k. Αυτό συμβαίνει, διότι η επαλήθευση απαιτεί τον υπολογισμό του δ^{-1}modq, και αν δ = 0, το δ^{-1} δεν υπάρχει.

2. Παρατηρούμε ότι το μέγεθος του q είναι στα 160-bits, ενώ το μέγεθος του p μπορεί να είναι οποιοδήποτε πολλαπλάσιο του 64, συμπεριλαμβανομένων των τιμών 512 και 1024. Σημειώνεται ότι, από τον Οκτώβριο του 2001, το NIST προτείνει να χρησιμοποιούνται πρώτοι p, μεγέθους 1024-bits.

3. Ο αλγόριθμος ψηφιακής υπογραφής (DSA), μάς δίνει υπογραφές πολύ μικρότερου μεγέθους από το El Gamal, αφού όλοι οι υπολογισμοί γίνονται modulo q. Μπορούμε να δούμε ότι αυτό ισχύει, αν λάβουμε υπόψη μας ότι για πρώτο p μεγέθους 768-bits, το μήκος της υπογραφής του DSA θα είναι 320-bits, ενώ του El Gamal 1536-bits.

4. Η κατασκευή της υπογραφής του DSA είναι αρκετά πιο γρήγορη από το El Gamal, αφού οι εκθέτες είναι μικρότεροι ή ίσοι του q. Επιπλέον, σε αντίθεση με το El Gamal όπου στη διαδικασία επαλήθευσης της υπογραφής είναι αναγκαίες 3 εκθετοποιήσεις modulo p, ενώ στο DSA περιορίζονται σε 2. Εφόσον η εκθετοποίηση αποτελεί μία από τις πιο “αργές” υπολογιστικές διαδικασίες, η αλλαγή αυτή επιτυγχάνει την επαλήθευση της υπογραφής, πράγμα ιδιαίτερα βοηθητικό στην περίπτωση που χρειάζεται να επαληθεύσουμε μεγάλο αριθμό υπογραφών σε μικρό χρονικό διάστημα.

4.5.1 ΑΣΦΑΛΕΙΑ ΤΟΥ DSA

Η ασφάλεια του αλγόριθμου ψηφιακής υπογραφής DSA βασίζεται στη δυσκολία υπολογισμού του διακριτού λογάριθμου (DLP). Όλοι οι μετασχηματισμοί στο DSA γίνονται μέσα σε μια υποομάδα του $\mathbf{Z}_p^*$, μεγέθους 2^{160}, τη μοναδική κυκλική υποομάδα G_q τάξης q της $\mathbf{Z}_p^*$.

Η επίλυση του DLP είναι ιδιαίτερα δύσκολη στη G_q .

4.6 ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ SCHNORR

Μία άλλη γνωστή παραλλαγή του σχήματος υπογραφής αποτελεί το σχήμα Schnorr. Όπως και στην περίπτωση του DSA, οι υπολογισμοί γίνονται σε μια υποομάδα του $\mathbf{Z}_p^*$, τάξης q, όπου p και q πρώτοι, έτσι ώστε p-1=0modq (δηλαδή ο q διαιρεί το p-1). Τυπικά, παίρνουμε p □ 2^{1024} και q□ 2^{160}.

Επίσης, απαιτείται η χρήση μιας συνάρτησης κατακερματισμού $h : \{0,1\}^* \to \mathbf{Z}_q$, η οποία είναι μοναδικής κατεύθυνσης και ανθεκτική σε συγκρούσεις.

Η διαδικασία παραγωγής κλειδιού για το Schnorr είναι ίδια με του DSA, μόνο που δεν υπάρχουν περιορισμοί στα μεγέθη των p και q.

Το σχήμα υπογραφής Schnorr

Ο Α υπογράφει ένα μήνυμα m αυθαίρετου μήκους και το στέλνει στον Β, ο οποίος με τη σειρά του θα επαληθεύσει την προέλευσή του χρησιμοποιώντας το δημόσιο κλειδί του Α.

1. *Δημιουργία υπογραφής:*

- Ο Α επιλέγει έναν τυχαίο, μυστικό ακέραιο k, 1 ≤ k ≤ q-1.
- Υπολογίζει τα γ = h(m□g^kmodp) και δ = k + αγ modp.
- Στέλνει στον Β την τριάδα (m, γ,δ), όπου m το αρχικό μήνυμα και (γ,δ) = sig_k(m, k) η υπογραφή του Α.

2. *Επαλήθευση:*

- Ο Β αποκτά το αυθεντικό κλειδί του Α (p, q, g, β).
- Υπολογίζει το υ = $g^{\delta}\beta^{-\gamma}$modp.
- Αποδέχεται την υπογραφή του Α αν h(m□υ)=γ (δηλαδή ver_K(m, γ, δ)=Αληθής), αλλιώς την απορρίπτει.

Σημείωση 4.3: Με το σύμβολο "□" εννοούμε τη *συνένωση (concatenation)* δύο ακολουθιών π.χ. αν m = 0111 και υ = 0010, τότε m□υ = 01110010.

<u>Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί</u>

Αν η υπογραφή έχει δημιουργηθεί από τον Α, τότε
$\upsilon = g^{\delta}g^{-\alpha\gamma} = g^{k} \bmod p$.

Τότε, $h(m \| \upsilon) = h(m \| g^{k} \bmod p) = \gamma$.

■

Παράδειγμα 4.6:

Ο Α επιλέγει τους πρώτους p = 7879 και q = 101, τέτοιους ώστε ο q να διαιρεί το p-1, εδώ είναι (p-1)/q = 78. Επίσης, επιλέγει $g_0 = 3$ μία πρωταρχική ρίζα στο $\mathbf{Z}^{*}_{7879}$ και έτσι βρίσκει ότι $g = g_0^{(p-1)/q} \bmod p = 3^{78} \bmod 7879 = 170$, όπου g είναι q-στή ρίζα της μονάδας modulo p.

Ο Α επιλέγει έναν τυχαίο ακέραιο $\alpha = 75$ και υπολογίζει $\beta = g^{\alpha} \bmod p = 4567$.

Έστω τώρα ότι θέλει να υπογράψει το μήνυμα m, διαλέγοντας έναν τυχαίο ακέραιο k = 50. Πρώτα, υπολογίζει το $g^{k} \bmod p = 170^{50} \bmod 7879 = 2518$ και έπειτα το $h(m \| 2518)$, όπου h είναι μία δοσμένη συνάρτηση κατακερματισμού και το 2518 αναπαρίσταται στο δυαδικό σύστημα.

Έστω ότι βρέθηκε $\gamma = h(m \| 2518) = 96$, οπότε το δ υπολογίζεται ως $\delta = 50 + 75 \times 96 \bmod 101 = 79$. Συνεπώς, η υπογραφή του Α είναι $(\gamma, \delta) = (96,79)$.

Ο Β επαληθεύει την υπογραφή του Α υπολογίζοντας
$\upsilon = 170^{79}4567^{-96} \bmod 7879 = 2518$ και μετά ελέγχει ότι $h(m \| 2518) = 96$. Τότε, μπορεί να είναι σίγουρος ότι η υπογραφή του Α είναι γνήσια και άρα την αποδέχεται.

■

5. ΥΠΟΓΡΑΦΕΣ ΜΙΑΣ ΧΡΗΣΗΣ (One-time signatures)

Τα σχήματα υπογραφών μιας χρήσης (one-time) αποτελούν μηχανισμούς ψηφιακών υπογραφών, οι οποίοι χρησιμοποιούνται για την υπογραφή ενός μόνο μηνύματος, αλλιώς οι υπογραφές μπορεί να πλαστογραφηθούν. Αυτό σημαίνει ότι για κάθε μήνυμα που υπογράφεται απαιτείται ένα νέο δημόσιο κλειδί. Φυσικά, η επαλήθευση της υπογραφής μπορεί να πραγματοποιηθεί αυθαίρετο αριθμό φορών.

Κύριο χαρακτηριστικό όλων των σχημάτων υπογραφών μιας χρήσης είναι η χρήση κάποιας συνάρτησης κατακερματισμού μονής κατεύθυνσης (one-way function). Μια τέτοια συνάρτηση είναι, για παράδειγμα, η $f(x) = a^x \bmod p$, όπου p πρώτος και a πρωταρχικό στοιχείο του $\mathbf{Z}_p$.

Ένα σημαντικό πλεονέκτημα της πλειοψηφίας των σχημάτων αυτών είναι ότι τόσο η παραγωγή, όσο και η επαλήθευση της γνησιότητας της υπογραφής υλοποιούνται με πολύ αποδοτικούς αλγορίθμους. Αυτός είναι και ο λόγος που προτιμούνται σε συσκευές, όπως τα chipcards, όπου απαιτείται μικρή υπολογιστική ισχύ.

5.1 ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ Lamport

Το πιο διαδεδομένο από τα σχήματα υπογραφών μιας χρήσης είναι το σχήμα υπογραφής Lamport, το οποίο θα περιγράψουμε παρακάτω.

Θεωρούμε $m = \{0,1\}^k$, $S = Y^k$ και $f : Y \to Z$ μια συνάρτηση κατακερματισμού μονής κατεύθυνσης, δημόσια γνωστή. Το προς υπογραφή μήνυμα m είναι μια δυαδική ακολουθία μήκους k-bit, $k \in$. Κάθε bit του μηνύματος υπογράφεται ξεχωριστά: αν το i-οστό bit του μηνύματος έχει την τιμή j, όπου $j \in \{0,1\}$, τότε το i-οστό στοιχείο της υπογραφής είναι η τιμή $y_{i,j}$. Κάθε $z_{i,j}$ είναι η εικόνα των $y_{i,j}$ υπό τη συνάρτηση κατακερματισμού μονής κατεύθυνσης f.

Η επαλήθευση της υπογραφής περιλαμβάνει μόνο τον έλεγχο ότι κάθε στοιχείο της υπογραφής $s_{i,j}$, $i=1,...,k$ είναι όρισμα του αντίστοιχου στοιχείου του δημοσίου κλειδιού $z_{i,j}$, το οποίο αντιστοιχεί στο i-οστό bit του μηνύματος. Αυτό μπορεί να επαληθευτεί χρησιμοποιώντας τη συνάρτηση κατακερματισμού μονής κατεύθυνσης f.

Παραγωγή κλειδιού:

- Ο Α επιλέγει τυχαία 2k τιμές $y_{i,j}$ από το σύνολο Y, όπου 1 ≤ i ≤ k και $j \in \{0,1\}$.
- Υπολογίζει τα $z_{i,j}=f\left(y_{i,j}\right) \in Z$, όπου 1 ≤ i ≤ k και $j \in \{0,1\}$.
- Το δημόσιο κλειδί του Α είναι ο $k \times 2$ πίνακας $\left(z_{i,j}\right)$ και το ιδιωτικό του ο $k \times 2$ πίνακας $\left(y_{i,j}\right)$.

Το σχήμα υπογραφής Lamport

Υποθέτουμε ότι ο Α θέλει να στείλει στον Β το μήνυμα $m=\left(x_1,x_2,...,x_k\right)$, όπου $x_i \in \{0,1\}$ (δηλαδή $x_i \equiv j$) και $i=1,2,...,k$ υπογεγραμμένο ψηφιακά με το Lamport, χρησιμοποιώντας το κλειδί Κ που δημιουργήθηκε με τη διαδικασία που περιγράψαμε παραπάνω.

1. *Δημιουργία υπογραφής:*
    - Ο Α επιλέγει κατάλληλα στοιχεία $y_{i,j}$ από τον πίνακα του ιδιωτικού του κλειδιού, έτσι ώστε η ψηφιακή του υπογραφή για το μήνυμα m να είναι η $sig_K\left(x_1,x_2,...,x_k\right)=\left(y_{1,x_1},y_{2,x_2},...,y_{k,x_k}\right)=\left(s_{i,j}\right)=\vec{s}$.
    - Στέλνει στον Β το ζεύγος $\left(m,\vec{s}\right)$.

2. *Επαλήθευση υπογραφής:*
    - Ο Β αποκτά το αυθεντικό κλειδί του Α $z_{i,j}$.
    - Αποδέχεται την υπογραφή αν και μόνο αν $z_{i,j}=f\left(s_{i,j}\right)$.

Παράδειγμα 5.1:

Έστω ότι $f(x) = 3^x \bmod 7879$ δημόσια γνωστή. Ο Α επιλέγει τυχαίους αριθμούς και κατασκευάζει τον πίνακα:

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

Στη συνέχεια υπολογίζει τα $z_{i,j} = f\left(y_{i,j}\right)$ και κατασκευάζει τον πίνακα:

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

τον οποίο και δημοσιεύει.

Υποθέτουμε τώρα ότι ο Α θέλει να υπογράψει το μήνυμα $m = (1,1,0)$ και να το στείλει στον Β. Η υπογραφή του είναι η

$$\vec{s} = sig_K(1,1,0) = (y_{1,1}, y_{2,1}, y_{3,0}) = (735,2467,4285)$$

Για να επαληθεύσει την υπογραφή, ο Β υπολογίζει τα

$$f(735) = 3^{735} \bmod 7879 = 3810 = z_{1,1}$$
$$f(2467) = 3^{2467} \bmod 7879 = 4721 = z_{2,1}$$
$$f(4285) = 3^{4285} \bmod 7879 = 268 = z_{3,0}$$

Και καταλήγει στο συμπέρασμα ότι το μήνυμα προέρχεται όντως από τον Α.

■

5.1.1 ΑΣΦΑΛΕΙΑ ΤΟΥ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ Lamport

Η ασφάλεια του σχήματος υπογραφής Lamport οφείλεται στην αδυναμία κάποιου αντιπάλου Γ να αντιστρέψει τη συνάρτηση f. Είναι, ωστόσο, ιδιαίτερα σημαντικό να μη χρησιμοποιηθεί ο ίδιος πίνακας $\left(y_{i,j}\right)$ για την υπογραφή περισσοτέρων του ενός μηνυμάτων. Σε αντίθετη περίπτωση, αν ο Γ έχει στην κατοχή του 2 μηνύματα υπογεγραμμένα από τον Α, τότε μπορεί εύκολα να παράξει υπογραφές και για άλλα μηνύματα.

Παράδειγμα 5.2:

Ας υποθέσουμε ότι ο Α χρησιμοποιεί τον ίδιο πίνακα $\left(y_{i,j}\right)$ για να υπογράψει τα μηνύματα $m_1 = (0,1,1)$ και $m_2 = (1,0,1)$.

Οι υπογραφές είναι οι

$$\vec{s}_1 = sig_K(m_1) = (y_{1,0}, y_{2,1}, y_{3,1}) \text{ και } \vec{s}_2 = sig_K(m_2) = (y_{1,1}, y_{2,0}, y_{3,1})$$

Τότε ο Γ μπορεί εύκολα να παράξει υπογραφές για τα μηνύματα

$$m_3 = (1,1,1) \text{ και } m_4 = (0,0,1)$$

Οι οποίες θα είναι οι

$$(y_{1,1}, y_{2,1}, y_{3,1}) \text{ και } (y_{1,0}, y_{2,0}, y_{3,1}) \text{ αντίστοιχα.}$$ ■

<u>Σημείωση 5.1:</u> Αν και το σχήμα υπογραφής Lamport είναι εύκολο στη χρήση του, δεν είναι ιδιαίτερα εύχρηστο στην πράξη, λόγω του μεγέθους των υπογραφών που παράγει. Για παράδειγμα,αν χρησιμοποιήσουμε τη συνάρτηση κατακερματισμού του Παραδείγματος 1, τότε η ασφαλής υλοποίησή της απαιτεί το p να είναι μήκους τουλάχιστον 512-bits. Αυτό σημαίνει ότι κάθε bit του μηνύματος υπογράφεται χρησιμοποιώντας 512-bits, συνεπώς η υπογραφή είναι 512 φορές πιο μεγάλη σε σχέση με το μήνυμα.

5.2 ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ MERKLE

Το one-time σχήμα υπογραφής Merkle απαιτεί μια TTP ή κάποιο άλλο έμπιστο μέσο για την επικύρωση της αυθεντικότητας των παραμέτρων. Επιπλέον,είναι απαραίτητη η χρήση μιας συνάρτησης κατακερματισμού $h:\{0,1\}^{*}\to\{0,1\}^{l}$ με αντίσταση $1^{ου}$ ορίσματος.

Για να υπογράψει ένα δυαδικό μήνυμα m μήκους n - bit, ο Α σχηματίζει μια ακολουθία $w=m\,\square\, c$, όπου το c είναι η δυαδική αναπαράσταση του αριθμού των 0 στο m. Το c υποτίθεται ότι είναι μια ακολουθία μήκους $\lfloor \log n \rfloor +1$ bits, με τα bits υψηλής τάξης να συμπληρώνονται με 0 αν χρειαστεί. Έτσι, το w προκύπτει να είναι μήκους $t=n+\lfloor \log n \rfloor +1$ bits.

Σημείωση 5.2: Το σύμβολο $\lfloor x \rfloor$ δηλώνει τον μεγαλύτερο ακέραιο που είναι μικρότερος ή ίσος του x.

Παραγωγή κλειδιού:

- Ο Α επιλέγει $t=n+\lfloor \log n \rfloor +1$ το πλήθος τυχαίες, μυστικές ακολουθίες $k_1,k_2,...,k_t$, καθεμία εκ των οποίων έχει μήκος l - bits.
- Υπολογίζει τα $\upsilon_i=h(k_i),\ 1\le i\le t$.

Το δημόσιο κλειδί του Α είναι το $(\upsilon_1,\upsilon_2,...,\upsilon_k)$ και το ιδιωτικό του το $(k_1,k_2,...,k_t)$.

Το σχήμα υπογραφής Merkle

Υποθέτουμε ότι ο Α υπογράφει ψηφιακά ένα δυαδικό μήνυμα m μήκους n - bit και το στέλνει στον Β, ο οποίος θα επαληθέυσει τη γνησιότητα της υπογραφής χρησιμοποιώντας το δημόσιο κλειδί του Α.

1. *Δημιουργία υπογραφής:*

   - Ο Α υπολογίζει το c και αναπτύσσει $w = m \| c = (a_1, a_2, ..., a_t)$.
   - Βρίσκει τις θέσεις των συντεταγμένων στο w, έτσι ώστε $i_1 < i_2 < ... < i_u$ και $a_{i_j} = 1$, $1 \le j \le u$.
   - Η υπογραφή του Α για το μήνυμα m είναι το $(s_1, s_2, ..., s_u)$, όπου $s_j = k_{i_j}$, $1 \le j \le u$.

2. *Επαλήθευση υπογραφής:*

   - Ο Β αποκτά το αυθεντικό κλειδί του Α $(\upsilon_1, \upsilon_2, ..., \upsilon_k)$.
   - Υπολογίζει το c και σχηματίζει το $w = m \| c = (a_1, a_2, ..., a_t)$.
   - Βρίσκει τις θέσεις των συντεταγμένων στο w, έτσι ώστε $i_1 < i_2 < ... < i_u$ και $a_{i_j} = 1$, $1 \le j \le u$.
   - Αποδέχεται την υπογραφή αν και μόνο αν $\upsilon_{i_j} = h(s_j)$ για όλα τα $j = 1, 2, ..., u$.

5.2.1 ΑΣΦΑΛΕΙΑ ΤΟΥ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ MERKLE

Θα αποδείξουμε ότι δεδομένης μιας υπογραφής $(s_1, s_2, ..., s_u)$ για ένα μήνυμα m, ένας αντίπαλος Γ δεν μπορεί να παράξει καμία πλαστή υπογραφή για οποιοδήποτε άλλο μήνυμα $m' \neq m$, αν η συνάρτηση κατακερματισμού h έχει αντίσταση 1^{ου} ορίσματος.

Έχουμε ότι $w = m \| c$ και έστω $w' = m' \| c'$, όπου c' είναι ακολουθία μήκους $\lfloor \log n \rfloor + 1$ bits και αποτελεί τη δυαδική αναπαράσταση του αριθμού των 0 στο m. Αφού οποιοσδήποτε αντίπαλος Γ έχει πρόσβαση μόνο στο τμήμα του ιδιωτικού κλειδιού που αποτελείται από το $(s_1, s_2, ..., s_u)$, το σύνολο των συντεταγμένων στο m' που έχουν τιμή 1 θα πρέπει να είναι ένα υποσύνολο συντεταγμένων στο m που έχουν τιμή 1. Σε αντίθετη περίπτωση, το m' θα έχει 1 σε κάποια συντεταγμένη όπου το m έχει 0 και ο Γ θα απαιτεί ένα στοιχείο του ιδιωτικού κλειδιού, το οποίο δεν αποκαλύπτεται στην υπογραφή $(s_1, s_2, ..., s_u)$.

Άρα, το m έχει περισσότερα 1 από το m'. Αυτό σημαίνει ότι το m' έχει περισσότερα 0 από το m και επομένως $c' > c$. Τότε, το c' θα έχει 1 σε κάποια θέση όπου το c έχει 0. Το στοιχείο του ιδιωτικού κλειδιού που αντιστοιχεί σε αυτή τη θέση δεν αποκαλύπτεται στην υπογραφή $(s_1, s_2, ..., s_u)$. Παρατηρούμε, λοιπόν, ότι και σε αυτήν την περίπτωση ο αντίπαλος Γ βρίσκεται σε αδιέξοδο.

ΚΕΦΑΛΑΙΟ 6

6. ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΩΝ ΜΕ ΕΠΙΠΡΟΣΘΕΤΗ ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

Στο κεφάλαιο αυτό, θα αναπτύξουμε κάποια σχήματα ψηφιακών υπογραφών, τα οποία παρουσιάζουν συγκεκριμένες ιδιότητες, ώστε να εξυπηρετούν πρόσθετες ανάγκες των ατόμων που τα χρησιμοποιούν. Τα σχήματα αυτά, με *επιπρόσθετη λειτουργικότητα*, στις περισσότερες περιπτώσεις συνδυάζουν ένα βασικό σχήμα ψηφιακής υπογραφής (όπως π.χ. το RSA) με ένα συγκεκριμένο πρωτόκολλο. Με αυτό τον τρόπο, είναι δυνατό να επιτευχθούν αυτά τα επιπρόσθετα χαρακτηριστικά, τα οποία δε μας παρέχει η βασική μέθοδος.

6.1 ΣΧΗΜΑΤΑ ΤΥΦΛΩΝ ΥΠΟΓΡΑΦΩΝ (Blind Signature Schemes)

Τα σχήματα τυφλών υπογραφών παρουσιάστηκαν για πρώτη φορά στο συνέδριο CRYPTO το 1988 από τους D.Chaum, A.Fiat και M.Naor. Εν γένει, εξυπηρετούν ανάγκες ηλεκτρονικής επικοινωνίας, όπου η μία πλευρά επιθυμεί ανωνυμία απέναντι στην άλλη. Πρόκειται, ουσιαστικά, για ένα πρωτόκολλο επικοινωνίας ανάμεσα στον αποστολέα Α και τον υπογράφοντα Β με την παραπάνω ιδιότητα.

Ο σκοπός των τυφλών υπογραφών είναι να εμποδίζουν τον υπογράφοντα Β να γνωρίζει το μήνυμα που υπογράφει, καθώς και την υπογραφή αυτού, έτσι ώστε να μην είναι σε θέση αργότερα να συσχετίσει το υπογεγραμμένο μήνυμα με τον αποστολέα Α.

Το σκεπτικό έχει ως εξής:

Ο Α στέλνει ένα μήνυμα κρυπτογραφημένο στον Β, ο οποίος καλείται να το υπογράψει χρησιμοποιώντας κάποιο βασικό σχήμα υπογραφής και το ξαναστέλνει

στον Α. Από την υπογραφή που λαμβάνει από τον Β, ο Α υπολογίζει την υπογραφή του Β για το απλό μήνυμα. Με την ολοκλήρωση της διαδικασίας, ο Β δε γνωρίζει ούτε το μήνυμα, ούτε τη συσχετιζόμενη με αυτό υπογραφή.

Τα σχήματα τυφλών υπογραφών βρίσκουν σημαντικές εφαρμογές στις ηλεκτρονικές συναλλαγές, όπου τα το ρόλο του υπογράφοντα Β έχει μία Τράπεζα και το ρόλο του Α ένας πελάτης. Έστω ότι ο Α παίρνει από την τράπεζα ένα υπογεγραμμένο κουπόνι κατοχής μετρητών από το λογαριασμό του (electronic cash token). Αφού κάνει τις αγορές του σε κάποιο κατάστημα Κ, χρησιμοποιεί το κουπόνι για να εξοφλήσει το λογαριασμό. Όταν το κατάστημα Κ πηγαίνει στην τράπεζα για να το εξαργυρώσει, η τράπεζα δεν είναι σε θέση να το συσχετίσει με τον Α (υπό την προϋπόθεση ότι για την υπογραφή του κουπονιού έχει χρησιμοποιηθεί σχήμα τυφλής υπογραφής). Έτσι, ο Α μπορεί να παραμένει ανώνυμος και τα ποσά που ξοδεύει να μην ελέγχονται.

Για να περιγράψουμε ένα σχήμα τυφλής υπογραφής θα χρειαστούμε:

1) Ένα σχήμα ψηφιακής υπογραφής (από τα γνωστά). Θα συμβολίζουμε την υπογραφή του Β σε ένα μήνυμα με $sig_B(m)$.

2) Δύο συναρτήσεις f και g, τέτοιες ώστε $g(sig_B(f(m))) = sig_B(m)$. Η f ονομάζεται *συνάρτηση τύφλωσης* (*blinding function),* η g *συνάρτηση αποτύφλωσης (unblinding function)* και το f(m) *τυφλωμένο μήνυμα (blinded message).*

6.1.1 ΤΟ ΣΧΗΜΑ ΨΗΦΙΑΚΗΣ ΥΠΟΓΡΑΦΗΣ Chaum

Το σχήμα υπογραφής Chaum είναι βασισμένο στο σχήμα υπογραφής RSA, δημοσίου κλειδιού (n, e) και ιδιωτικού d. Αν k είναι ένας σταθερός ακέραιος με ΜΚΔ(n, k) = 1, τότε η συνάρτηση τύφλωσης $f : \mathbf{Z}_n \to \mathbf{Z}_n$ ορίζεται ως $f(m) = mk^e \bmod n$ και η συνάρτηση αποτύφλωσης $g : \mathbf{Z}_n \to \mathbf{Z}_n$ ως $g(m) = k^{-1}m \bmod n$. Γνωρίζουμε ότι η συνάρτηση υπογραφής του RSA είναι η $sig_B(m) = m^d \bmod n$, επομένως ,έχουμε ότι

$$g(sig_B(f(m))) = g(sig_B(mk^e \bmod n)) = g(m^d k^{ed} \bmod n) = g(m^d k \bmod n) =$$
$$k^{-1}m^d k \bmod n = m^d \bmod n = sig_B(m),$$

αφού $ed = 1 \bmod \varphi(n)$.

Το σχήμα υπογραφής Chaum

Υποθέτουμε ότι ο Α λαμβάνει μία υπογραφή του Β σε ένα τυφλωμένο μήνυμα $f(m)$. Από αυτήν, ο Α θα υπολογίσει την υπογραφή του στο μήνυμα m , όπου $0 \leq m \leq n-1$.

Τύφλωση

- Ο Α επιλέγει έναν τυχαίο, μυστικό ακέραιο k, τέτοιον ώστε $0 \leq k \leq n-1$ και ΜΚΔ(n, k) = 1.
- Υπολογίζει το $m^* = f(m) = mk^e \bmod n$ και το στέλνει στον Β.

Υπογραφή

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

Αποτύφλωση

- Ο Α υπολογίζει το $s = g(s^*) = k^{-1}s^* \bmod n$, το οποίο είναι η υπογραφή του Β στο μήνυμα m.

Παράδειγμα 6.1:

Έστω ότι ο Β επιλέγει τους πρώτους p = 29 και q = 17 και υπολογίζει το n = 29 × 17 = 493. Διαλέγει δημόσιο εκθέτη e = 191 (αφού είναι φ(493) = 28 × 16 = 448, 1 < e < 448 και (b, 448) = 1) και υπολογίζει τον ιδιωτικό εκθέτη d = 319, όπου ed = 1mod(φ(n)).

Ας υποθέσουμε τώρα ότι ο Α επιθυμεί την υπογραφή του Β για το μήνυμα m = 351. Επιλέγει, λοιπόν, έναν μυστικό ακέραιο k = 31, υπολογίζει το τυφλωμένο μήνυμα $m^* = mk^e \bmod n = 351 \times 31^{191} \bmod 493 = 291$ και το στέλνει στον Β.

Ο Β με τη σειρά του, υπολογίζει το $s^* = (m^*)^d \bmod n = 291^{319} \bmod 493 = 349$ και το στέλνει στον Α. Όπως έχουμε πει και προηγούμενα, το s* είναι η υπογραφή του Β για το m*.

Ο Α υπολογίζει $k^{-1} \bmod n = 31^{-1} \bmod 493 = 334$ και $s = 334 \times 349 \bmod 493 = 218$ που είναι και η υπογραφή του Β για το μήνυμα m.

Φυσικά, μπορούμε να επαληθεύσουμε ότι $m^d \bmod n = 351^{319} \bmod 493 = 218 = s$.

■

6.2 ΑΔΙΑΜΦΙΣΒΗΤΗΤΑ ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΗΣ (Undeniable Signature Schemes)

Τα αδιαμφισβήτητα σχήματα υπογραφής προτάθηκαν το 1989 από τον Chaum και τον van Antwerpen. Το κύριο χαρακτηριστικό τους είναι ότι η επαλήθευση της υπογραφής δε μπορεί να πραγματοποιηθεί χωρίς τη συνεργασια του υπογράφοντα Α. Επομένως, ο Α γνωρίζει όλες τις περιπτώσεις στις οποίες χρειάστηκε η επικύρωση της υπογραφής του για το έγγραφο που υπέγραψε. Αυτό τον προστατεύει από πιθανή επαναχρησιμοποίηση του εγγράφου του από φορείς που δεν επιθυμεί. Η επαλήθευση υπογραφής πραγματοποιείται με τη χρήση ενός πρωτοκόλλου πρόκλησης και ανταπόκρισης (challenge and response).

Θα ήταν χρήσιμο στο σημείο αυτό να παραθέσουμε δύο παραδείγματα χρήσης αδιαμφισβήτητης υπογραφής:

1. Υποθέτουμε ότι ένας πελάτης Α επιθυμεί να έχει πρόσβαση σε μια περιοχή υψηλής ασφαλείας τράπεζας Β. Η περιοχή αυτή μπορεί, για παράδειγμα, να είναι το θησαυροφυλάκιο. Η τράπεζα Β, για να του δώσει την απαιτούμενη πρόσβαση, ζητάει απο τον Α να υπογράψει ένα έγγραφο με ημερομηνία και ώρα. Εάν ο Α χρησιμοποιήσει σχήμα αδιαμφισβήτητης υπογραφής για να το υπογράψει, τότε ο Β δε θα μπορεί να αποδείξει στο μέλλον ότι η υπογραφή αυτή ανήκει στον Α, παρά μονάχα με τη συνεργασία του ίδιου του Α.

2. Έστω τώρα ότι ο Α είναι μια μεγάλη εταιρία λογισμικού, η οποία δημιουργεί ένα νέο πακέτο λογισμικού. Η Α υπογράφει το πακέτο και το πουλάει στην εταιρία Β, η οποία με τη σειρά της αποφασίζει να αντιγράψει το πακέτο και να το μεταπωλήσει σε έναν πελάτη C. Ο C δεν είναι σε θέση να επαληθεύσει τη γνησιότητα του πακέτου χωρίς τη συνεργασία του Α. Φυσικά, αυτό δεν εμποδίζει τη Β από το να επαναϋπογράψει το πακέτο και να το πουλήσει στον C σαν δικό του. Αλλά τότε, το πακέτο θα έχανε το αγοραστικό πλεονέκτημα της προέλευσης από την γνωστή εταιρία Α και επιπλέον θα ήταν εύκολο να αποδειχτεί η απάτη αυτή.

Το ερώτημα που τίθεται εδώ είναι ότι αν για την επαλήθευση μιας υπογραφής είναι απαραίτητη η συνεργασία του υπογράφοντα Α, τότε τί τον εμποδίζει να αρνηθεί ότι πράγματι ο ίδιος κατασκεύασε νωρίτερα αυτή την υπογραφή; Ο Α μπορεί να ισχυριστεί ότι μία εγκυρη υπογραφή είναι στην πραγματικότητα πλαστή και

a) είτε να αρνηθεί να συμμετέχει στην διαδικασία επαλήθευσης

b) ή να εκτελέσει το πρωτόκολλο επαλήθευσης λανθασμένα (δίνοντας πλαστά δεδομένα).

Για να αποτρέψουμε αυτό το ενδεχόμενο , στα αδιαμφισβήτητα σχήματα υπογραφών ενσωματώνεται ένα Πρωτόκολλο Αποκήρυξης (Disavowal Protocol), στο οποίο οφείλουν και την ονομασία τους. Χρησιμοποιώντας αυτό το πρωτόκολλο, είναι ιδιαίτερα δύσκολο για τον Α να αρνηθεί ότι μία υπογραφή που έχει κατασκευάσει είναι πράγματι δική του. Έτσι, ένα αδιαμφισβήτητο σχήμα υπογραφής αποτελείται από τρεις συνιστώσες: τον αλγόριθμο υπογραφής, το πρωτόκολλο επαλήθευσης και το πρωτόκολλο αποκήρυξης.

Πριν προχωρήσουμε στην περιγραφή του σχήματος Chaum και van Antwerpen, παραθέτουμε το παρακάτω λήμμα:

Δήμμα 6.1:

Αν p,q πρώτοι, τέτοιοι ώστε p = 2q+1, τότε το σύνολο G που αποτελείται από τα τετραγωνικά υπόλοιπα modulo p των στοιχείων του $\mathbf{Z}_p^*$ αποτελεί πολλαπλασιαστική υποομάδα του $\mathbf{Z}_p^*$ τάξης q.

Σημείωση 6.1: Μπορούμε να υπογίσουμε μια τέτοια υποομάδα G του $\mathbf{Z}_p$ που θα αποτελείται από τις μέχρι ταξης q δυνάμεις του $g = g_0^{1-1/q}$, όπου g_0 πρωταρχικό στοιχείο του $\mathbf{Z}_p^*$, όπως έχουμε δει σε προηγούμενο λήμμα.

Για να γίνουν πιο κατανοητά τα προηγούμενα, θα εξηγήσουμε λίγο πιο μεθοδικά τους ρόλους του p και του q. Όπως θα δούμε, οι υπολογισμοί γίνονται στην πολλαπλασιαστική υποομάδα C του $\mathbf{Z}_p^*$ πρώτης τάξης. Πιο συγκεκριμένα, πρέπει να μπορούμε να υπολογίσουμε αντιστρόφους modulo |G| (όπου με |G| συμβολίζουμε την τάξη της G) και αυτός είναι ο λόγος που |G| πρέπει να είναι πρώτος, η υποομάδα G που προκύπτει απο το Λήμμα, είναι η μεγαλύτερη δυνατή, που είναι και το επιθυμητό, αφου και τα μηνύματα και οι υπογραφές είναι στοιχεία της G.

Ας δούμε πώς πραγματοποιείται η διαδικασία παραγωγής κλειδιού για την υπογραφή ενός μηνύματος $m \in G$ με το αδιαμφισβητητο σχήμα υπογραφής Chaum και van Antwerpen.

Παραγωγή κλειδιού

- Ο Α επιλέγει πρώτους p,q , τέτοιους ώστε p = 2q+1.
- Κατασκευάζει την πολλαπλασιαστική υποομάδα G του $\mathbf{Z}_p^*$ τάξης q και υπολογίζει ένα πρωταρχικό στοιχείο της g, όπως περιγράφεται στη Σημείωση 6.1.
- Επιλέγει τυχαίο ακέραιο α, 1 < α < p-1 και υπολογίζει το $\beta = g^{\alpha} \text{mod} p$. Το δημόσιο κλειδί του Α είναι το (p,q,g,β), ενώ το ιδιωτικό του το α.

Το σχήμα υπογραφής Chaum – van Antwerpen

Έστω ότι ο Α θέλει να στείλει στον Β το μήνυμα $m \in G$, υπογεγραμμάνο ψηφιακά με το αδιαμφισβήτητο σχήμα υπογραφής Chaum – van Antwerpen, χρησιμοποιώντας το κλειδί $K = (p, \text{q}, \text{g}, \beta)$.

1. *Δημιουργία υπογραφής:*

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

2. *Επαλήθευση υπογραφής:*

   - Ο Β αποκτά το δημόσιο κλειδί του Α, $(p, \text{q}, \text{g}, \beta)$.
   - Επιλέγει τυχαίους, μυστικούς ακεραίους $e_1, e_2 \in \mathbf{Z}_p^*$.
   - Υπολογίζει το $c = s^{e_1} \beta^{e_2} \bmod p$ και το στέλνει στον Α.
   - Ο Α υπολογίζει το $d = c^{\alpha^{-1} \bmod q} \bmod p$ και το στέλνει πίσω στον Β.
   - Ο Β υπολογίζει το $d' = m^{e_1} g^{e_2} \bmod p$.
   - Αν $d = d'$, τότε $ver_K(m, d)$= Αληθής και ο Β αποδέχεται την υπογραφή ως έγκυρη, αλλιώς την απορρίπτει.

Απόδειξη ορθότητας της διαδικασίας επαλήθευσης

Έχουμε ότι $\beta = g^{\alpha} \bmod p \Rightarrow \beta^{\alpha^{-1}} = g \bmod p$.

Ομοίως, $s = m^{\alpha} \bmod p \Rightarrow s^{\alpha^{-1}} = m \bmod p$.

Άρα, $d = c^{\alpha^{-1}} \bmod p = s^{e_1 \alpha^{-1}} \beta^{e_2 a^{-1}} \bmod p = m^{e_1} g^{e_2} \bmod p = d'$.

■

Παράδειγμα 6.2:

Ο Α επιλέγει επιλέγει πρώτο p = 467 = 2 × 233 + 1, με q = 233 επίσης πρώτο. Έπειτα, επιλέγει ένα τυχαίο στοιχείο $g_0 = 2 \in \mathbf{Z}^*_{467}$ και υπολογίζει το $g = g_0^{(p-1)/q} \bmod p$ = 2^2mod267 = 4, όπου το g είναι γεννήτορας της υποομάδας G του $\mathbf{Z}^*_{467}$. Επιλέγει ακόμη α = 101 και υπολογίζει το β = 4^{101}mod467 = 449. Το δημόσιο κλειδί του Α είναι το (p, q, g, β) = (467, 233, 4, 449) και το ιδιωτικό του το α = 101.

Ο Α θέλει τώρα να υπογράψει το μήνυμα m = 119. Υπολογίζει την υπογραφή s = 119^{101}mod467 = 129 και στέλνει το υπογεγραμμένο μήνυμα (m, s) = (119, 129) στον Β. Ο Β το λαμβάνει και αποκτά το δημόσιο κλειδί του Α. Επιλέγει κρυφούς ακεραίους e_1 = 38, e_2 = 397 $\in \mathbf{Z}^*_{233}$ και υπολογίζει το c = $129^{38} \times 449^{397}$mod467 = 13, το οποίο και αποστέλλει στον Α.

Ο Α υπολογίζει α^{-1}modq = 101^{-1}mod233 = 30 και d = $c^{\alpha^{-1} \bmod q} \bmod p$ = 13^{30}mod467 = 9 και το στέλνει στον Β. Ο Β υπολογίζει d'=$119^{38} \times 4^{397}$mod467=9=d, συνεπώς, αποδέχεται την υπογραφή ως αυθεντική.

■

ΠΡΩΤΟΚΟΛΛΟ ΑΠΟΚΗΡΥΞΗΣ

Υποθέτουμε ότι ο Α ισχυρίζεται ότι η υπογραφή s του μηνύματος m είναι πλαστή. Ο Β θα προσπαθήσει να το διαπιστώσει εκτελώντας την παρακάτω διαδικασία, η οποία στην ουσία αποτελείται από δύο αποτυχημένα "τρεξίματα" του πρωτοκόλλου επαλήθευσης και έναν τελικό έλεγχο από τον οποίο ο Β θα αποφανθεί για τον ισχυρισμό του Α.

1) Ο Β αποκτά το δημόσιο κλειδί του Α (p, q, g, β).

2) Επιλέγει τυχαίους, μυστικούς ακεραίους $e_1, e_2 \in \mathbf{Z}_p^*$, υπολογίζει το $c = s^{e_1}\beta^{e_2} \bmod p$ και το στέλνει στον Α.
3) Ο Α υπολογίζει το $d = c^{\alpha^{-1} \bmod q} \bmod p$ και το στέλνει στον Β.
4) Ο Β επαληθεύει ότι $d \neq m^{e_1} g^{e_2} \bmod p$.
5) Επιλέγει τυχαίους, μυστικούς ακεραίους $f_1, f_2 \in \mathbf{Z}_p^*$, υπολογίζει το $C = s^{f_1}\beta^{f_2} \bmod p$ και το στέλνει στον Α.
6) Ο Α υπολογίζει το $D = C^{\alpha^{-1} \bmod q} \bmod p$ και το στέλνει στον Β.
7) Ο Β επαληθεύει ότι $D \neq m^{f_1} g^{f_2} \bmod p$.
8) Συμπεραίνει ότι η s είναι όντως πλαστή υπογραφή αν και μόνο αν $(dg^{-e_2})^{f_1} = (Dg^{-f_2})^{e_1} \bmod p$.

Θεώρημα 6.1:

Αν $s \neq m^{\alpha} \bmod p$, δηλαδή η υπογραφή s είναι πλαστή και οι Α και Β ακολουθήσουν σωστά το Πρωτόκολλο Αποκήρυξης, τότε $(\mathrm{dg}^{-e_2})^{f_1} = (Dg^{-f_2})^{e_1} \bmod p$.

Απόδειξη:

Έχουμε ότι $(\mathrm{dg}^{-e_2})^{f_1} = ((\mathrm{s}^{e_1}\beta^{e_2})^{\alpha^{-1}} g^{-e_2})^{f_1} \bmod p =$ $s^{e_1\alpha^{-1}f_1}\beta^{e_2\alpha^{-1}f_1} g^{-e_2 f_1} \bmod p$ = $s^{e_1\alpha^{-1}f_1} g^{e_2 f_1} g^{-e_2 f_1} \bmod p$ = $s^{e_1\alpha^{-1}f_1} \bmod p$ (1)

αφού $d = c^{\alpha^{-1}} \bmod p$, $c = s^{e_1}\beta^{e_2} \bmod p$ και $\beta = g^{\alpha} \bmod p$.

Ομοίως, χρησιμοποιώντας τις σχέσεις $D = C^{\alpha^{-1}} \bmod p$ και $C = s^{f_1}\beta^{f_2} \bmod p$, καταλήγουμε στο ότι $(Dg^{-f_2})^{e_1} = s^{e_1\alpha^{-1}f_1} \bmod p$ (2)

Από τις σχέσεις (1) και (2) προκύπτει το ζητούμενο.

■

Παράδειγμα 6.3:

Έστω ότι το δημόσιο κλειδί του Α είναι το (p, q, g, β) = (467, 233, 4, 449), ενώ το ιδιωτικό του το α = 101. Υπογράφει, έπειτα, το μήνυμα m = 286 με την πλαστή υπογραφή s = 83 και προσπαθεί να πείσει τον Β ότι η υπογραφή δεν είναι έγκυρη.

Ο Β επιλέγει τυχαίους ακεραίους e_1 = 45 και e_2 = 237 $\in \mathbf{Z}_{233}^*$, υπολογίζει την τιμή c = $83^{45} \times 449^{237}$mod467 = 305, την οποία και αποστέλλει στον Α. Ο Α τώρα υπολογίζει το d = 305^{30}mod467 = 109 και το αποστέλλει στον Β, ο οποίος επαληθεύει ότι $m^{e_1} g^{e_2} \bmod p$ = $286^{45} \times 4^{237}$mod467 = 149 ≠ 109. Κατόπιν, ο Β επιλέγει τυχαία f_1 = 125 και f_2 = 9 $\in \mathbf{Z}_{233}^*$, υπολογίζει το C = $83^{125} \times 449^{9}$mod467 = 270 και το στέλνει στον Α.

Ο Α υπολογίζει το D = 270^{30}mod467 = 68 και το στέλνει στον Β, ο οποίος επαληθεύει ότι $m^{f_1} g^{f_2} \bmod p$ = $286^{125} \times 4^{9}$mod467 = $25 \neq 68$ υπολογίζει τα $(\mathrm{dg}^{-e_2})^{f_1} \bmod p$ =$(109 \times 4^{-237})^{125}$mod467=188,

$(Dg^{-f_2})^{e_1} \bmod p$ = $(68 \times 4^{-9})^{45}$mod467 = 188.

Εφόσον προέκυψε $(\mathrm{dg}^{-e_2})^{f_1} = (Dg^{-f_2})^{e_1} \bmod p$, ο Β συμπεραίνει ότι όντως η s είναι πλαστή υπογραφή.

■

6.2.1 ΑΣΦΑΛΕΙΑ ΤΟΥ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ Chaum – van Antwerpen

Η ασφάλεια του σχήματος υπογραφής Chaum – van Antwerpen βασίζεται στη δυσκολία επίλυσης του Προβλήματος Διακριτού Λογαρίθμου (DLP) στην υποομάδα της $\mathbf{Z}_p^*$ τάξης q. Επίσης, στο επόμενο Θεώρημα αποδεικνύεται ότι η πιθανότητα να δεχτεί ο Β μία πλαστή υπογραφή ως έγκυρη είναι εξαιρετικά μικρή. Δηλαδή, ο Α είναι σχεδόν αδύνατο να εξαπατήσει τον Β κάνοντάς τον να αποδεχτεί μία πλαστή υπογραφή ως έγκυρη.

Θεώρημα 6.2:

Αν $s \neq m^{\alpha} \bmod p$, τότε η πιθανότητα να δεχτεί ο Β το s ως έγκυρη υπογραφή για το μήνυμα m είναι το πολύ $1/q$.

Απόδειξη:

Επειδή s, β είναι και τα δύο στοιχεία της υποομάδας G και $|G| = q$, όπου q πρώτος, κάθε πρόκληση c αντιστοιχεί σε ακριβώς q διατεταγμένα ζευγάρια (e_1, e_2).

Όταν ο Α λαμβάνει μια πρόκληση c, δε μπορεί με κανένα τρόπο να βρει ποιο από τα q πιθανά ζευγάρια (e_1, e_2) χρησιμοποίησε ο Β για να την κατασκευάσει.

Ισχυρισμός: Αν $s \neq m^{\alpha} \bmod p$, τότε για την κατασκευή κάθε πιθανής απόκρισης $d \in G$, ο Α χρησιμοποιεί ακριβώς ένα από αυτά τα q διατεταγμένα ζεύγη (e_1, e_2).

Αφού το g είναι πρωταρχικό στοιχείο της G, τότε κάθε στοιχείο της G γράφεται ως κάποια δύναμη του g, όπου ο εκθέτης ορίζεται μοναδικά modulo q. Ορίζουμε $c = g^i \bmod p$, $d = g^j \bmod p$, $m = g^k \bmod p$ και $s = g^l \bmod p$, όπου $i, j, k, l \in \mathbf{Z}_q$. Γνωρίζουμε ότι

$$\left.\begin{matrix} c = s^{e_1}\beta^{e_2} \bmod p \\ d = m^{e_1} g^{e_2} \bmod p \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} g^i = g^{le_1} g^{\alpha e_2} \bmod p \\ g^j = g^{ke_1} g^{e_2} \bmod p \end{matrix}\right\} \Rightarrow \left\{\begin{matrix} i = le_1 + \alpha e_2 \bmod q \\ j = ke_1 + e_2 \bmod q \end{matrix}\right\}$$

Υποθέτουμε τώρα ότι s είναι μία πλαστή υπογραφή για το μήνυμα m, άρα $s \neq m^{\alpha} \bmod p \Rightarrow g^l \neq g^{\alpha k} \bmod p \Rightarrow l \neq \alpha k \bmod q$.

Ο πίνακας συντελεστών του συστήματος των ισοδυναμιών modulo q έχει μη μηδενική ορίζουσα, άρα το σύστημα έχει μοναδική λύση. Αυτό σημαίνει ότι κάθε $d \in G$ είναι η σωστή απόκριση για ακριβώς ένα από τα q πιθανά διατεταγμένα ζεύγη (e_1, e_2). Συνεπώς, η πιθανότητα ο Α να δώσει στον Β μία απόκριση d, τέτοια ώστε $ver_K(m, d) =$ Αληθής, είναι ακριβώς $1/q$.

■

Θα εξετάσουμε τώρα την πιθανότητα να προσπαθήσει ο Α να αποκηρύξει μία έγκυρη υπογραφή. Σε αυτή την περίπτωση, υποθέτουμε ότι ο Α εκτελεί το πρωτόκολλο επαλήθευσης λανθασμένα και κατασκευάζει πλαστά d και D. Έτσι, στο θεώρημα που ακολουθεί, υποθέτουμε μόνο ότι ο Α μπορεί να κατασκευάσει d και D, έτσι ώστε να ικανοποιούνται οι συνθήκες στα βήματα (4), (7) και (8) του Πρωτοκόλλου Αποκήρυξης.

Θεώρημα 6.3:

Αν $s = m^{\alpha} \bmod p$ και ο Β ακολουθήσει το Πρωτόκολλο Αποκήρυξης, τότε, αν ο Α δώσει πλαστά d και D, ώστε $d \neq m^{e_1} g^{e_2} \bmod p$ και $D \neq m^{f_1} g^{f_2} \bmod p$, η πιθανότητα $(dg^{-e_2})^{f_1} \neq (Dg^{-f_2})^{e_1} \bmod p$ είναι $1 - 1/q$.

Απόδειξη:

Θα κάνουμε χρήση της απαγωγής εις άτοπον.

Έστω ότι $(\mathrm{dg}^{-e_2})^{f_1} = (Dg^{-f_2})^{e_1} \bmod p$. Η σχέση αυτή, μπορεί να γραφτεί στη μορφή $D = d_0^{f_1} g^{f_2} \bmod p$, όπου $d_0 = d^{1/e_1} g^{-e_2/e_1} \bmod p$. Από το Θεώρημα 2, συνεπάγεται ότι η πιθανότητα το s να είναι μία έγκυρη υπογραφή για το d_0, είναι $1-1/q$. Υποθέτουμε τώρα ότι το s είναι μία έγκυρη υπογραφή για το m. Παρατηρούμε ότι είναι πολύ μεγάλη η πιθανότητα να ισχύει $m^{\alpha} = d_0^{\alpha} \bmod p \Rightarrow m = d_0$. Όμως, αφού $d \neq m^{e_1} g^{e_2} \bmod p \Rightarrow \mathrm{m} \neq \mathrm{d}^{1/e_1} g^{-e_2/e_1} \bmod p$. Αφού $d_0 \neq \mathrm{d}^{1/e_1} g^{-e_2/e_1} \bmod p$, έχουμε ότι $m \neq d_0$, το οποίο έρχεται σε αντίθεση με την υπόθεσή μας.

■

6.3 ΤΑ ΣΧΗΜΑΤΑ ΥΠΟΓΡΑΦΩΝ FAIL-STOP

Τα σχήματα υπογραφών Fail-Stop παρέχουν επιπλέον ασφάλεια για την περίπτωση όπου κάποιος πολύ ισχυρός αντίπαλος θα μπορούσε να πλαστογραφήσει μία υπογραφή. Πρόκειται για σχήματα ψηφιακών υπογραφών, τα οποία επιτρέπουν στον υπογράφοντα Α να αποδείξει με πολύ μεγάλη πιθανότητα ότι μία όχι πραγματικά δική του υπογραφή είναι όντως πλαστή. Πιο συγκεκριμένα, στην περίπτωση που κάποιος αντίπαλος Γ καταφέρει να πλαστογραφήσει την υπογραφή του Α, η πλαστογράφηση μπορεί να ανιχνευτεί και ο μηχανισμός υπογραφής δεν θα ξαναχρησιμοποιηθεί. Έτσι, ο χαρακτηρισμός *fail-then-stop* θα ήταν εξίσου σωστός.

Ένα σχήμα υπογραφής Fail-Stop προτάθηκε το 1992 από τους van Heyst και Pedersen. Το σχήμα αυτό, είναι ένα σχήμα υπογραφής μιας χρήσης (όπως το Lamport), το οποίο αποτελείται από τρεις συνιστώσες: τον αλγόριθμο υπογραφής, τον αλγόριθμο επαλήθευσης και έναν αλγόριθμο απόδειξης της πλαστογράφησης. Όπως και στα σχήματα πιστοποίησης ταυτότητας, πρωταρχικό ρόλο κατέχει μία Έμπιστη Αρχή (TTP).

Η TTP επιλέγει πρώτους p,q τέτοιους ώστε $p=2q+1$ και το Πρόβλημα Διακριτού Λογαρίθμου στη $\mathbf{Z}_q$ να είναι απρόσιτο. Επιπλέον, επιλέγει g πρωταρχικό στοιχείο του $\mathbf{Z}_p^*$ και τυχαίο ακέραιο $\alpha \in \mathbf{Z}_q^*$ και υπολογίζει το $\beta = g^{\alpha} \bmod p$. Τα p,q,g,β είναι δημοσίως γνωστά, ενώ ο ακέραιος a κρατείται μυστικός από την TTP.

<u>Παραγωγή κλειδιού:</u>

- Ο Α επιλέγει τυχαίους, μυστικούς ακεραίους $x_1, x_2, y_1, y_2 \in \mathbf{Z}_q$.
- Υπολογίζει τα $\gamma_1 = g^{x_1}\beta^{x_2} \bmod p$ και $\gamma_2 = g^{y_1}\beta^{y_2} \bmod p$.

Το δημόσιο κλειδί του Α είναι το (γ_1, γ_2) και το ιδιωτικό του το (x_1, x_2, y_1, y_2).

Το σχήμα υπογραφής van Heyst – Pedersen

Υποθέτουμε ότι ο Α θέλει να στείλει ένα μήνυμα $m \in \mathbf{Z}_q$, υπογεγραμμένο ψηφιακά με το σχήμα υπογραφής των van Heyst – Pedersen, χρησιμοποιώντας το κλειδί $K = (\gamma_1, \gamma_2, x_1, x_2, y_1, y_2)$.

1. *Δημιουργία υπογραφής:*

   - Ο Α υπολογίζει $s_1 = x_1 + my_1 \bmod q$ και $s_2 = x_2 + my_2 \bmod q$.
   - Στέλνει στον Β το ζεύγος (m, s), όπου $s = (s_1, s_2) = sig_K(m)$ η υπογραφή του Α για το μήνυμα m.

2. *Επαλήθευση υπογραφής:*

   - Ο Β αποκτά το δημόσιο κλειδί του Α (γ_1, γ_2).
   - Υπολογίζει $\upsilon_1 = \gamma_1 \gamma_2^m \bmod p$ και $\upsilon_2 = g^{s_1} \beta^{s_2} \bmod p$.
   - Αν $\upsilon_1 = \upsilon_2$, τότε $ver_K(m, s) =$ Αληθής και ο Β αποδέχεται την υπογραφή ως έγκυρη.

3. *Απόδειξη της πλαστογράφησης:*

   Υποθέτουμε ότι ο Α έχει στην κατοχή του μία υπογραφή $s' = (s_1', s_2')$ για ένα μήνυμα m, τέτοια ώστε $s' \neq sig_K(m)$ και $ver_K(m, s') =$Αληθής. Θα προσπαθήσει να αποδείξει ότι είναι πλαστογραφημένη. Η απόδειξη της πλαστογράφησης είναι η τιμή $\alpha = \log_g \beta$, αφού το α είναι γνωστό μόνο στην TTP.

   - Ο Α υπολογίζει την υπογραφή $s = (s_1, s_2)$ για το μήνυμα m χρησιμοποιώντας το ιδιωτικό του κλειδί (x_1, x_2, y_1, y_2).
   - Αν $s = s'$, επιστρέφει στο πρώτο βήμα και δημιουργεί νέο κλειδί.
   - Αν $s \neq s'$, υπολογίζει $\alpha_0 = (s_1 - s_1')(s_2 - s_2')^{-1} \bmod q$.
   - Αν $\alpha = \alpha_0$, τότε η υπογραφή s' είναι όντως πλαστή.

Σημείωση 6.2: Η πιθανότητα να ισχύει $s = s'$ στο δεύτερο βήμα του αλγόριθμου απόδειξης πλαστογράφησης είναι $1/q$.

Απόδειξη ορθότητας της διαδικασίας επαλήθευσης

Έχουμε ότι $\upsilon_1 = \gamma_1\gamma_2^m = (g^{x_1}\beta^{x_2})(g^{y_1}\beta^{y_2})^m = g^{x_1+my_1}\beta^{x_2+my_2} = g^{s_1}\beta^{s_2} = \upsilon_2 \bmod p$.

■

Απόδειξη ορθότητας της διαδικασίας απόδειξης πλαστογράφησης

Έχουμε ότι $s' \neq sig_K(m)$ και $ver_K(m,s') =$ Αληθής.

Αυτό σημαίνει ότι $\gamma_1\gamma_2^m = g^{s_1'}\beta^{s_2'} \bmod p$.

Επειδή s είναι η υπογραφή του Α για το μήνυμα m , ισχύει ότι $\gamma_1\gamma_2^m = g^{s_1}\beta^{s_2} \bmod p$. Επομένως,

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

Άρα $\alpha = (s_1 - s_1')(s_2 - s_2')^{-1} \bmod q = \alpha_0$.

■

Παράδειγμα 6.4:

Η Έμπιστη Αρχή ΤΤΡ επιλέγει τους πρώτους p = 3467 , q = 1733 και βρίσκει πρωταρχικό στοιχείο g = 4 του $\mathbf{Z}_{3467}^*$, τάξης 1733. Επιλέγει α = 1567 και υπολογίζει $\beta = 4^{1567} = 514$. Η ΤΤΡ γνωστοποιεί τα (p,q,g,β) = (3467, 1733, 4, 514).

Ο Α επιλέγει $x_1 = 888$, $x_2 = 1024$, $y_1 = 786$, $y_2 = 999 \in \mathbf{Z}_{1733}$ και υπολογίζει τα

$$\gamma_1 = g^{x_1}\beta^{x_2} \bmod p = 4^{888}514^{1024} \bmod 3467 = 3405 ,$$

$$\gamma_2 = g^{y_1}\beta^{y_2} \bmod p = 4^{786}514^{999} \bmod 3467 = 2281.$$

Το δημόσιο κλειδί του Α είναι το $(\gamma_1,\gamma_2) =$ (3405, 2281) και το ιδιωτικό του το (x_1,x_2,y_1,y_2) = (888, 1024, 786, 999).

Υποθέτουμε τώρα ότι ο Γ πλαστογράφησε την υπογραφή $s' = (s_1', s_2')$ = (822, 55) για το μήνυμα m' = 3383. Η υπογραφή αυτή, γίνεται αποδεκτή από τον Β γιατί ικανοποιεί τη συνθήκη επαλήθευσης. Πράγματι,

$$\upsilon_1' = \gamma_1\gamma_2^{m'} \bmod p = 3405 \times 2281^{3383} \bmod 3467 = 2282$$

$$\upsilon_2' = g^{s_1'}\beta^{s_2'} \bmod p = 4^{822} \times 514^{55} \bmod 3467 = 2282$$

Επομένως, $\upsilon_1' = \upsilon_2'$.

Για να αποδείξει την πλαστογράφηση, ο Α χρησιμοποιεί το ιδιωτικό του κλειδί και υπολογίζει την υπογραφή του $s = (s_1, s_2)$ για το m' = 3383:

$$s_1 = x_1 + m'y_1 \bmod q = 888 + 3383 \times 786 \bmod 1733 = 1504$$

$$s_2 = x_2 + m'y_2 \bmod q = 1024 + 3383 \times 999 \bmod 1733 = 1291$$

Αφού $s \neq s'$, ο Α υπολογίζει

$$\alpha_0 = (s_1 - s_1')(s_2 - s_2')^{-1} \bmod q = 682 \times 1236^{-1} \bmod 1733 = 1567 = \alpha$$

Όμως, ο α είναι γνωστός μόνο στην ΤΤΡ, συνεπώς η εύρεσή του αποτελεί απόδειξη της πλαστογράφησης.

■

6.3.1 ΑΣΦΑΛΕΙΑ ΤΟΥ ΣΧΗΜΑΤΟΣ ΥΠΟΓΡΑΦΗΣ van Heyst – Pedersen

Η ασφάλεια του σχήματος υπογραφής van Heyst – Pedersen βασίζεται στο γεγονός ότι το Πρόβλημα Διακριτού Λογαρίθμου στο $\mathbf{Z}_q$ είναι απρόσιτο, όπως έχουμε ήδη αναφέρει. Επιπλέον, θα δείξουμε ότι η πιθανότητα κάποιος αντίπαλος Γ να μπορέσει να κατασκευάσει μια πλαστή υπογραφή για ένα μήνυμα m', δεδομένης μίας υπογραφής s για ένα μήνυμα m, είναι πάρα πολύ μικρή. Θα ξεκινήσουμε δίνοντας ένα χρήσιμο ορισμό.

Ορισμός 6.1: Δύο κλειδιά $K = (\gamma_1, \gamma_2, x_1, x_2, y_1, y_2)$ και $K' = (\gamma_1', \gamma_2', x_1', x_2', y_1', y_2')$, λέγονται ***ισοδύναμα*** αν $\gamma_1 = \gamma_1'$ και $\gamma_2 = \gamma_2'$.

Παρατηρούμε ότι η συνάρτηση επαλήθευσης $ver_K(m, s)$ εξαρτάται μόνο από τις τιμές των μεταβλητών γ_1, γ_2, m και s. Για δύο ισοδύναμα κλειδιά οι τιμές αυτές συμπίπτουν. Είναι εύκολο να αποδείξουμε ότι αν K, K' είναι ισοδύναμα κλειδιά και $ver_K(m, s) =$ Αληθής, τότε $ver_{K'}(m, s) =$ Αληθής.

Το παρακάτω λήμμα μάς δείχνει ότι, δεδομένης μιας έγκυρης υπογραφής s για ένα μήνυμα m, υπάρχουν q διαφορετικά κλειδιά που θα μπορούσαν να έχουν χρησιμοποιηθεί για την παραγωγή αυτής της υπογραφής στο μήνυμα.

Λήμμα 6.2:

Αν $s = sig_K(m)$, τότε υπάρχουν ακριβώς q ισοδύναμα κλειδιά K', έτσι ώστε $s = sig_{K'}(m)$.

Απόδειξη:

Έστω (γ_1, γ_2) το δημόσιο κλειδί. Θέλουμε να προσδιορίσουμε το πλήθος όλων των πιθανών τετράδων ώστε να ικανοποιούνται οι ακόλουθες σχέσεις:

$$\gamma_1 = g^{x_1}\beta^{x_2} \bmod p$$
$$\gamma_2 = g^{y_1}\beta^{y_2} \bmod p$$
$$s_1 = x_1 + my_1 \bmod q$$
$$s_2 = x_2 + my_2 \bmod q$$

Αφού το g είναι γεννήτορας του $\mathbf{Z}_q$, τότε υπάρχουν μοναδικά $c_1, c_2, c_0 \in \mathbf{Z}_q$, τέτοια ώστε

$$\gamma_1 = g^{c_1} \bmod p$$
$$\gamma_2 = g^{c_2} \bmod p$$
$$\beta = g^{c_0} \bmod p$$

Με αντικατάσταση αυτών στις προηγούμενες σχέσεις, προκύπτει το ακόλουθο σύστημα εξισώσεων:

$$c_1 = x_1 + c_0 x_2 \bmod q$$
$$c_2 = y_2 + c_0 y_2 \bmod q$$
$$s_1 = x_1 + my_1 \bmod q$$
$$s_2 = x_2 + my_2 \bmod q$$

το οποίο σε μορφή πίνακα γράφεται ως:

$$\begin{pmatrix} 1 & c_0 & 0 & 0 \\ 0 & 0 & 1 & c_0 \\ 1 & 0 & m & 0 \\ 0 & 1 & 0 & m \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ s_1 \\ s_2 \end{pmatrix}$$

Ο βαθμός του πίνακα των συντελεστών ισούται με 3 (πρέπει να είναι τουλάχιστον 3, αφού r_1, r_2 και r_4 είναι γραμμικά ανεξάρτητες στο $\mathbf{Z}_q$ και επιπλέον, μπορεί να είναι το πολύ 3, αφού $r_1 + mr_2 - r_3 - c_0 r_4 = (0,0,0,0)$, όπου r_i είναι η i-οστή γραμμή του πίνακα). Επομένως, η διάσταση του χώρου των λύσεων ισούται με 4 - 3 = 1. Άρα, υπάρχουν ακριβώς q λύσεις για το σύστημα.

■

Για κάθε άλλο μήνυμα, όμως, $m' \neq m$, αυτά τα q διαφορετικά κλειδιά θα δώσουν διαφορετικές υπογραφές. Αποδεικνύεται ότι, δεδομένης μιας υπογραφής s για ένα μήνυμα m, η πιθανότητα ένας αντίπαλος Γ να μπορέσει να παράξει μία έγκυρη υπογραφή s' για ένα μήνυμα m' είναι ίση με $1/q$. Το αποτέλεσμα αυτό είναι ανεξάρτητο των υπολογιστικών δυνατοτήτων του αντιπάλου Γ. Η ασφάλεια εξασφαλίζεται από το γεγονός ότι ο Γ δεν μπορεί να γνωρίζει με ποιό από τα q πιθανά κλειδιά ο Α κατασκεύασε την υπογραφή του.

Παρ'όλα αυτά, σε περίπτωση που ο Γ καταφέρει τελικά να πλαστογραφήσει την υπογραφή του Α σε κάποιο μήνυμα, ο Α μπορεί να αποδείξει την πλαστογραφία με πιθανότητα $1-1/q$, ακολουθώντας τη διαδικασία απόδειξης πλαστογράφησης.

Τέλος, αν ο Α χρησιμοποιήσει το ίδιο κλειδί K για την υπογραφή δύο μηνυμάτων, η υπογραφή του μπορεί να πλαστογραφηθεί. Αυτός είναι ο λόγος που το σχήμα των van Heyst - Pedersen κατατάσεται στα σχήματα ψηφιακών υπογραφών μιας χρήσης (one-time).

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Α. Παπαϊωάννου (Επίκ. Καθηγητής Ε.Μ.Π.) - Χ. Κουκουβίνος (Καθηγητής Ε.Μ.Π.), "Κρυπτογραφία", Εκδόσεις Ε.Μ.Π. 2007.

2. Δ. Πουλάκης "Κρυπτογραφία, Η Επιστήμη της Ασφαλούς Επικοινωνίας", Εκδόσεις Ζήτη 2004.

3. W. Trappe – L. Washington "Introduction to Cryptography with coding Theory", Pearson International Edition 2006.

4. D. Stinson "Cryptography: Theory and Practice" 3rd edition, Chapman and Hall, 2006.

5. A. Menezes – P. van Oorschot – S. Vanstone "Handbook of Applied Cryptography", CRC Press 1996.

6. Ε. Ζάχος "Υπολογιστική Θεωρία Αριθμών και Κρυπτογραφία", Εκδόσεις Ε.Μ.Π. 2012.

7. John B. Fraleigh "Εισαγωγή στην Άλγεβρα", 6η Έκδοση, Πανεπιστημιακές Εκδόσεις Κρήτης 2007.

8. Ι. Στ. Βενιέρης (Καθηγητής Ε.Μ.Π.) – Ε. Νικολούζου "Τεχνολογίες Διαδικτύου", 2η Έκδοση, Εκδόσεις Τζιόλα 2006.

9. Α. Παπαϊωάννου (Επίκ. Καθηγητής Ε.Μ.Π.) - Χ. Κουκουβίνος (Καθηγητής Ε.Μ.Π.), "Θεωρία Σχεδιασμών", Εκδόσεις Ε.Μ.Π. 2004.

10. Α. Παπαϊωάννου (Επίκ. Καθηγητής Ε.Μ.Π.) – Μ. Ρασσιάς "Εισαγωγή στη Θεωρία Αριθμών", Εκδόσεις Συμεών 2010.

11. J.Kleinberg – E.Tardos, "Σχεδιασμός Αλγορίθμων", Εκδόσεις κλειδάριθμος 2008.