ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΔΕΣΠΟΙΝΑΣ ΚΕΦΑΛΑ

Επιβλέπων : Αλέξανδρος Παπαϊωάννου
Αναπλ. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2012

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΈΑΣ ΜΑΘΗΜΑΤΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΔΕΣΠΟΙΝΑΣ ΚΕΦΑΛΑ

Επιβλέπων : Αλέξανδρος Παπαϊωάννου
Αναπλ. Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Κουκουβίνος Χ.	Παπαϊωάνου Α.	Στεφανέας Π.
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Λέκτορας Ε.Μ.Π.

Αθήνα, Ιούλιος 2012

.....

ΔΕΣΠΟΙΝΑ ΚΕΦΑΛΑ

Διπλωματούχος Σχολής Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

Περίληψη

Η κρυπτογραφία είχε σαν πεδία εφαρμογής της τον στρατό και την διπλωματία. Στην εποχή μας με την ανάπτυξη της τεχνολογίας η χρησιμότητά της κρίνεται απολύτως αναγκαία. Το πεδίο εφαρμογής ευρύ,περιλαμβάνοντας όλους τους τομείς στους οποίους η ασφαλής μετάδοση παίζει κύριο λόγο. Ψηφιακές συναλλαγές,επικοινωνίες καθώς και πλήθος άλλων εφαρμογών έχουν εισβάλλει στην καθημερινότητα μας οι οποίες πρέπει να διασφαλίσουν την εγκυρότητα τους. Έτσι δημιουργήθηκε η ανάγκη για την κατασκευή σχημάτων ψηφιακών υπογραφών. Ένα σχήμα ψηφιακής υπογραφής είναι το ανάλογο μιας χειρόγραφης υπογραφής για κάθε είδους ψηφιακή συναλλαγή ή επικοινωνία. Μια έγκυρη ψηφιακή υπογραφή διαβεβαιώνει στον παραλήπτη ενός μηνύματος ποιος είναι ο αποστολέας και αν έχει τροποποιηθεί το μήνυμα κατά την μεταφορά του.

Ο σκοπός της διπλωματικής εργασίας ήταν η περιγραφή των ψηφιακών υπογραφών στην κρυπτογραφία. Πιο συγκεκριμένα στην αρχή παρουσιάζονται μαθηματικά στοιχεία, ορισμοί και προβλήματα χρήσιμα για την μελέτη των ψηφιακών υπογραφών. Στην συνέχεια γίνεται μια ιστορική αναδρομή στην κρυπτογραφία και μια εισαγωγή στις ψηφιακές υπογραφές. Η πρώτη κατηγορία ψηφιακών υπογραφών είναι το RSA και οι σχετικές με αυτό υπογραφές με κοινό στοιχείο ότι η ασφάλεια τους βασίζεται στο πρόβλημα της παραγοντοποίησης. Μετά αναλύονται οι υπογραφές Fiat-Shamir οι οποίες παράγονται από τα αντίστοιχα σχήματα επαλήθευσης. Η επομένη κατηγορία υπογραφών που εξετάζεται είναι το DSA και οι σχετικές με αυτό υπογραφές. Ακολουθούν οι ψηφιακές υπογραφές μιας χρήσης και άλλα σχήματα ψηφιακών υπογραφών που δεν σχετίζονται με καμιά κατηγορία. Τέλος, αναλύονται υπογραφές με επιπρόσθετη λειτουργία, δηλαδή υπογραφές που συνδυάζουν ένα από τα γνωστά σχήματα υπογραφών με ένα πρωτόκολλο.

Abstract

Traditionally, cryptography was employed mainly in diplomatic and military applications. Recent technological advances have made the necessity of its use pervasive. Currently cryptography is employed widely, in every sector that demands secure transmission of information. Digital transactions, communications and many more applications, which are embedded in our daily lives, require proper validation. This was the motive for the introduction of digital signatures. Every digital signature serves the same purpose as a handwritten signature for digital transactions and communications. It ascertains to the receiver who the sender of a message was and if the message has been modified.

The purpose of this thesis is the description of digital signatures in cryptography. Initially, definitions, the mathematical foundations and characteristic problems of the field are presented. A brief review of the history of digital signature follows. Firstly RSA and related signature schemes are introduced; they share the commonality that their security is derived from the factorization problem. Then the Fiat-Shamir signatures are discussed; those are derived from respective identification schemes. The DSA and related digital signatures are exhibited. Subsequently, one-time signatures and miscellaneous schemes that don't fit any of the aforementioned categories are described. Finally, signatures with additional functionality that combine characteristics of the previous categories in one protocol are presented.

Περιεχόμενα

1 Ορισμοί-Στοιχεία θεωρίας

Σε αυτό το κομμάτι της διπλωματικής εργασίας θα παρουσιαστούν ορισμοί, αλγόριθμοι και προβλήματα χρήσιμα για την μελέτη των ψηφιακών υπογραφών.

1.1 Ακέραιοι

Ορισμός (αλγόριθμος διαίρεσης για ακεραίους): Αν a και b είναι ακέραιο με $b \geq 1$, τότε υπάρχουν μοναδικοί ακέραιοι q και r τέτοιοι ώστε

$a = qb + r$, όπου $0 \leq r < b$.

Το υπόλοιπο της διαίρεσης συμβολίζεται ως a mod b και το πηλίκο ως a div b.

Ορισμός: Ο ακέραιος c είναι κοινός διαιρέτης για το a και το b αν c|a και c|b.

Ορισμός: Ένας μη αρνητικός ακέραιος d είναι ο μέγιστος κοινός διαιρέτης των ακεραίων a και b (όχι και οι δύο μηδέν), και συμβολίζεται ως d = ΜΚΔ(a,b), αν:

i. d είναι ο κοινός διαιρέτης των a και b.
ii. Αν για το c ισχύει c|a και c|b, τότε c|d.

Αλγόριθμος-Αλγόριθμος του Ευκλείδη για τον υπολογισμό του μέγιστου κοινού διαιρέτη δύο ακεραίων
Είσοδος: δύο μη αρνητικοί ακέραιοι a και b με $a \geq b$.
Έξοδος: ο μέγιστος κοινός διαιρέτης των a και b.

1 Όσο $b \neq 1$ κάνε το ακόλουθο:
  1.1 Θέσε $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$.
2. Επέστρεψε(a).

Ο αλγόριθμος του Ευκλείδη μπορεί να επεκταθεί έτσι ώστε να υπολογίζει δύο ακεραίους x και y τέτοιους ώστε ax + by = d. Οι x, y δεν είναι μοναδικά ορισμένοι.

Αλγόριθμος-Εκτεταμένος Ευκλείδειος Αλγόριθμος
Είσοδος: δύο μη αρνητικοί ακέραιοι a και b με $a \geq b$.
Έξοδος: d = ΜΚΔ(a,b) και οι ακέραιοι x,y τέτοιοι ώστε ax + by = d.

1 Αν b = 0 τότε θέτουμε $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$ και η έξοδος είναι (d,x,y).
2 Θέτουμε $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.
3 Όσο b > 0 κάνουμε τα παρακάτω.
  3.1 $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.
  3.2 $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, $y_1 \leftarrow y$.
4 Θέτουμε $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$ και επιστρέφει (d,x,y).

Θεώρημα (Θεμελιώδες Θεώρημα της Αριθμητικής (ΘΘΑ): Κάθε ακέραιος $n \geq 2$ παραγοντοποιείται σαν ένα γινόμενο πρώτων:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

όπου p_i είναι διακριτοί πρώτοι και e_i είναι θετικοί ακέραιοι. Επιπλέον, η παραγοντοποίηση είναι μοναδική.

Ορισμός: Για $n \geq 1$, το φ(n) ορίζεται ως το πλήθος των ακεραίων που βρίσκεται στο διάστημα [1,n] και είναι σχετικά πρώτοι ως προς το n. Η συνάρτηση φ ονομάζεται συνάρτηση Euler.

Ιδιότητες συνάρτησης Euler

i. Αν p είναι πρώτος αριθμός, τότε φ(p) = p-1.
ii. Η συνάρτηση Euler είναι πολλαπλασιαστική. Με άλλα λόγια, αν ΜΚΔ(m,n) = 1, τότε $\varphi(mn) = \varphi(m)\cdot\varphi(n)$.
iii. Αν $n = p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_k^{e_k}$ είναι η αναπαράσταση του n, τότε

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$$

1.2 **Ακέραιοι modulo n**

Έστω ότι n είναι ένας θετικός ακέραιος.

Ορισμός: Αν a και b είναι ακέραιοι, ο a λέγεται ισοδύναμος του b modulo n, και συμβολίζεται με $a \equiv b \pmod n$, αν ο n διαιρεί τον (a-b).

Ορισμός: Οι ακέραιοι modulo n, συμβολίζονται $\mathbb{Z}_n$, είναι ένα σύνολο ισοδύναμων κλάσεων ακεραίων {0,1,2,...,n-1}. Όλες οι πράξεις στο $\mathbb{Z}_n$ γίνονται σε modulo n.

Κινέζικο Θεώρημα υπολοίπων: Αν οι ακέραιοι $n_1,n_2,\ldots,n_k$ είναι σχετικά πρώτοι ανά ζεύγη, τότε το σύστημα:

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

έχει μοναδική λύση modulo $n = n_1 n_2\cdot\ldots\cdot n_k$.

Αλγόριθμος-Αλγόριθμος Gauss
Η λύση x του παραπάνω θεωρήματος μπορεί να υπολογιστεί από την σχέση $x = \sum_{i=1}^{k} a_i N_i M_i \bmod n$, όπου $N_i = n/n_i$ και $M_i = N_i^{-1} \bmod n_i$.

Ορισμός: Η πολλαπλασιαστική ομάδα του $\mathbb{Z}_n$ είναι η $\mathbb{Z}_n^* = \{ a \in \mathbb{Z}_n \mid \text{ΜΚΔ}(a,n) = 1\}$. Συγκεκριμένα, αν n είναι πρώτος αριθμός, τότε $\mathbb{Z}_n^* = \{a \mid 1 \leq a \leq n-1\}$.

Ορισμός: Η τάξη της $\mathbb{Z}_n^*$ ορίζεται ως ο αριθμός των στοιχείων της.

Έστω $n \geq 2$ είναι ένας ακέραιος.

i. (Θεώρημα Euler) Αν $a \in \mathbb{Z}_n^*$, τότε $a^{\varphi(n)} \equiv 1 \pmod n$.
ii. Αν ο n είναι γινόμενο πρώτων αριθμών και αν $r \equiv s \pmod{\varphi(n)}$, τότε $a^r \equiv a^s \pmod n$ για κάθε ακέραιο a.

Μια ειδική περίπτωση του θεωρήματος Euler είναι το (μικρό) θεώρημα Fermat.

Έστω p ένας πρώτος αριθμός.

i. (Θεώρημα Fermat) Αν ΜΚΔ(a,p) = 1, τότε $a^{p-1} \equiv 1 \pmod p$.

ii. Αν $r \equiv s \pmod{p-1}$, τότε $a^r \equiv a^s \pmod{p}$ για κάθε ακέραιο a.
iii. Συγκεκριμένα, $a^p \equiv a \pmod{p}$ για κάθε ακέραιο a.

Ορισμός: Αν $a \in \mathbb{Z}_n^*$. Αν η τάξη της a είναι η φ(n), τότε το a ονομάζεται γεννήτορας ή πρωταρχικό στοιχείο της $\mathbb{Z}_n^*$. Αν η $\mathbb{Z}_n^*$ έχει γεννήτορα , τότε η $\mathbb{Z}_n^*$ ονομάζεται κυκλική. Σε μη κυκλικές ομάδες οι έννοιες γεννήτορας και πρωταρχικό στοιχείο δεν συμπίπτουν.

Ορισμός: Έστω ότι $a \in \mathbb{Z}_n^*$. Το a καλείται τετραγωνικό υπόλοιπο modulo n, αν υπάρχει $x \in \mathbb{Z}_n^*$ τέτοιο ώστε $x^2 \equiv a \pmod{n}$. Το σύνολο των τετραγωνικών υπολοίπων συμβολίζεται ως Q_n και το σύνολο των μη τετραγωνικών υπολοίπων ως $\bar{Q}_n$.

Ορισμός: Έστω ότι $a \in Q_n$. Αν $x \in \mathbb{Z}^*$ ικανοποιεί την σχέση $x^2 \equiv a \pmod{n}$, τότε το x καλείται τετραγωνική ρίζα a modulo n.

1.3 **Χρήσιμοι αλγόριθμοι**

Αλγόριθμος-Υπολογισμός αντίστροφου στο $\mathbb{Z}_n$
Είσοδος: $a \in \mathbb{Z}_n$.
Έξοδος: $a^{-1} \bmod n$, δεδομένου ότι γίνεται η αντιστροφή.

1) Χρησιμοποιούμε τον εκτεταμένο αλγόριθμο του Ευκλείδη ώστε να υπολογίσουμε τους ακεραίους x και y έτσι ώστε $ax + ny = d$, όπου $d = \text{ΜΚΔ}(a,n)$.
2) Αν $d > 1$, τότε $a^{-1} \bmod n$ δεν υπάρχει. Αλλιώς, επέστρεψε (x).

Η modular ύψωση σε δύναμη μπορεί να εκτελεστεί με τον ακόλουθο αλγόριθμο, ο οποίος χρησιμοποιείται σε πολλά κρυπτογραφικά πρωτόκολλα. Μια εκδοχή αυτού του αλγορίθμου είναι βασισμένη στην ακόλουθη παρατήρηση. Έστω ότι η δυαδική αναπαράσταση του k είναι η $\sum_{i=1}^{t} k_i 2^i$, όπου $k_i \in 0,1$. Τότε

$$a^k = \prod_{i=0}^{t} a^{k_i 2^t} = \left(a^{2^0}\right)^{k_0} \left(a^{2^1}\right)^{k_1} \cdot \ldots \cdot \left(a^{2^t}\right)^{k_t}$$

Αλγόριθμος-Ύψωση σε δύναμη στο $\mathbb{Z}_n$
Είσοδος: $a \in \mathbb{Z}_n$ και ακέραιος $0 \le k < n$ με δυαδική αναπαράσταση $k = \sum_{i=1}^{t} k_i 2^i$.
Έξοδος: $a^k \bmod n$.

1 Θέτουμε $b \leftarrow 1$. Αν $k = 0$ τότε επιστρέφουμε (b).
2 Θέτουμε $A \leftarrow a$.
3 Αν $k_0 = 1$ τότε θέτουμε $b \leftarrow a$.
4 Για i από 1 έως t κάνουμε τα ακόλουθα:
  4.1 Θέτουμε $A \leftarrow A^2 \bmod n$.
  4.2 Αν $k_i = 1$ τότε θέτουμε $b \leftarrow A \cdot b \bmod n$.
5 Επιστρέφουμε (b).

1.4 **Σύμβολα Legendre και Jacobi**

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

$$\left(\frac{a}{p}\right)=\begin{Bmatrix} 0,\alpha\nu\ p|a \\ 1,\alpha\nu\ a\in Q_n \\ -1,\alpha\nu\ a\in \bar{Q}_n \end{Bmatrix}$$

Το σύμβολο Jacobi είναι μια γενίκευση του σύμβολου Legendre για ακεραίους περιττούς αλλά όχι απαραίτητα πρώτους.

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

$$\left(\frac{a}{p}\right)=\left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\cdot\ldots\cdot\left(\frac{a}{p_k}\right)^{e_k}$$

Εδώ πρέπει να παρατηρήσουμε ότι αν ο n είναι πρώτος, τότε το σύμβολο Jacobi ταυτίζεται με το σύμβολο Legendre.

Το πρόβλημα της παραγοντοποίησης ακεραίων

Η ασφάλεια πολλών κρυπτογραφικών μεθόδων βασίζεται στο δυσεπίλυτο του προβλήματος της παραγοντοποίησης ακεραίων.

Ορισμός: Το πρόβλημα της παραγοντοποίησης ακεραίων είναι το ακόλουθο: για ένα θετικό ακέραιο n, να βρεθεί η παραγοντοποίηση του σε γινόμενο πρώτων. Με άλλα λόγια να βρεθεί $n=p_1^{e_1}\cdot p_2^{e_2}\cdot\ldots\cdot p_k^{e^k}$ όπου p_i είναι διακριτοί ανά ζεύγη πρώτοι αριθμοί και $e_i\geq 1$.

Το πρόβλημα διακριτού λογαρίθμου(DLP)

Η ασφάλεια πολλών κρυπτογραφικών τεχνικών βασίζεται στο δυσεπίλυτο του προβλήματος διακριτού λογαρίθμου. Έτσι βρίσκει εφαρμογή στην παραγωγή κλειδιού Diffie-Hellman, στο κρυπτοσύστημα και ψηφιακή υπογραφή ElGamal και σε πλήθος άλλες εφαρμογές.

Ορισμός: Έστω G μια πεπερασμένη κυκλική ομάδα τάξης n. Έστω α ένας γεννήτορας της G και $\beta\in G$. Ο διακριτός λογάριθμος του β με βάση α, συμβολίζεται $\log_\alpha\beta$, είναι ένας μοναδικός ακέραιος x, με $0\leq x\leq n-1$, τέτοιο ώστε $\beta = \alpha^x$.

Ορισμός: Το πρόβλημα διακριτού λογαρίθμου (DLP) είναι το ακόλουθο: έστω ένα πρώτος αριθμός p, ένας γεννήτορας α του $\mathbb{Z}_p^*$ και ένα στοιχείο $\beta\in\mathbb{Z}_p^*$. Να βρεθεί ένας ακέραιος x, με $0\leq x\leq p-2$, τέτοιο ώστε $\alpha^x\equiv\beta \pmod p$.

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

Οι αλγόριθμοι επίλυσης του DLP χωρίζονται σε τρεις κατηγορίες:

1) Αλγόριθμοι που λειτουργούν σε αυθαίρετες ομάδες.
2) Αλγόριθμοι που λειτουργούν σε αυθαίρετες ομάδες αλλά είναι αποδοτικοί στην περίπτωση που η τάξη της ομάδας αναλύεται σε μικρούς πρώτους παράγοντες.
3) Αλγόριθμοι που είναι αποδοτικοί σε συγκεκριμένες ομάδες.

2 Ιστορική Αναδρομή στην Κρυπτογραφία

Ίσως το πρώτο εύρημα στο οποίο είχε χρησιμοποιηθεί κρυπτογραφία είναι ο τάφος ενός ευγενούς στην Αίγυπτο στην πόλη Menet Khufu περίπου στα 1900 π.Χ. Αργότερα βρέθηκε στην Μεσοποταμία μια πλάκα στην οποία ήταν καταγεγραμμένη μια κρυπτογραφημένη φόρμουλα για την στίλβωση κεραμικών. Το 500-600 π.Χ. Εβραίοι γραμματείς χρησιμοποίησαν ένα ανεστραμμένο αλφάβητο, γνωστό ως atbash, για να διαφυλάξουν τα λεγόμενα του προφήτη Ιερεμία. Ο προφήτης Ιερεμίας άρχισε να υπαγορεύει στον Baruch γύρω στα 605 π.Χ., αλλά τα κεφάλαια τα οποία αναφέρονται σε αυτόν τον κώδικα αποδίδονται σε κάποιον "C"(ο οποίος ενδέχεται να μην είναι ο Baruch). Ο atbash είναι ένας από τους λίγους εβραϊκούς κώδικες εκείνης της εποχής.

Στην Ελλάδα εμφανίζεται η σπαρτιατική σκυτάλη η οποία ανάγεται στον 5^{ο} αιώνα π.Χ. Η σκυτάλη αυτή αποτελούνταν από ένα ξύλινο ραβδί γύρω από το οποίο τυλιγόταν μια λωρίδα από δέρμα ή περγαμηνή. Ο αποστολέας γράφει κατά μήκος της σκυτάλης το μήνυμα που θέλει να κρυπτογραφήσει. Ξετυλίγοντας την λωρίδα τα γράμματα έχουν αναδιαταχθεί, οπότε και το μήνυμα είναι χωρίς νόημα. Ο παραλήπτης για να διαβάσει το μήνυμα απλά τυλίγει την λωρίδα σε σκυτάλη με την ίδια διάμετρο.

Ο Ιούλιος Καίσαρας χρησιμοποιούσε μια απλή μετατόπιση του κανονικού αλφάβητου για να προφυλάξει τις κυβερνητικές επικοινωνίες. Αυτή η κρυπτογράφηση ήταν πιο απλή από αυτή του atbash, αλλά ήταν επαρκής μιας και εκείνη την εποχή λίγοι ήξεραν να διαβάζουν.

Ο πάπυρος του Leyden είναι ένα κωδικοποιημένο κείμενο γραμμένο στα ελληνικά στα 200 μ.Χ. Ο πάπυρος ήταν θαμμένος μαζί με τον ιδιοκτήτη του και περιγράφει αλχημείες για το πως μπορεί να παραχθεί χρυσός και άλλα μέταλλα καθώς και υφάσματα. Ο Abu al-Rahman al-Khahil ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi έγραψε το πρώτο βιβλίο αφιερωμένο στην αποκρυπτογράφηση κειμένων. Ο Yahmadi έλυσε ένα βυζαντινό κρυπτογραφημένο κείμενο γραμμένο στα ελληνικά, μαντεύοντας ότι το κείμενο ξεκινάει με την φράση "Στο όνομα του Θεού". Βασισμένος σε αυτό κατάφερε να αποκρυπτογραφήσει και το υπόλοιπο. Επίσης ο Abu Bakr Ahmad ben Ali ben Washiyya an-Nabati δημοσίευσε ένα βιβλίο με κωδικοποιημένα κείμενα τα οποία αναφέρονταν στην μαγεία.

Άλλα έγγραφα που βρέθηκαν σε κρυπτογραφημένη μορφή προέρχονται από την δυναστεία των Ghaznavid από την Περσία. Μάλιστα ένας χρονικογράφος αναφέρει ότι υψηλά ιστάμενοι είχαν το δικό τους προσωπικό κώδικα. Η έλλειψη συνέχειας των ισλαμικών κρατών και η αποτυχία να αναπτυχθεί μια μόνιμη δημόσια υπηρεσία καθώς και η δημιουργία μόνιμων πρεσβειών σε άλλες χώρες απέτρεψε την ευρύτερη χρήση της κρυπτογραφίας.

Το 1226 ένα απλοϊκό είδος κρυπτογράφησης εμφανίστηκε σε πολιτικά αρχεία στην Βενετία (τα φωνήεντα είχαν αντικατασταθεί από τελείες και σταυρούς σε μερικές διάσπαρτες λέξεις). Στην συνέχεια το 1379 ο Gabrieli di Lavinde κατόπιν αιτήματος του πάπα Κλήμη 7^{ου}, συνέθεσε ένα συνδυασμό αλφάβητου και ενός μικρού κώδικα. Παρά το γεγονός ότι ανακαλύφθηκαν στο εν τω μεταξύ πιο αποδοτικοί κώδικες, αυτός ο τρόπος κωδικοποίησης ήταν ευρέως διαδεδομένος μεταξύ των διπλωματών και μερικών πολιτών για τα επόμενα 450 χρόνια, πιθανόν λόγω της σχετικής του ευκολίας. Την ίδια εποχή ο Abd al-Rahman Ibn Khaldun έγραψε το "The Muqaddimah" στο οποίο χρησιμοποιεί ονόματα αρωμάτων, φρούτων, πουλιών ή λουλουδιών για να αντικαταστήσει γράμματα. Επίσης αλλάζει την

τυπική μορφή των γραμμάτων και εφαρμόζει αυτήν την κωδικοποίηση σε έγγραφα σχετικά με τον στρατό και την φορολογία.

Τον επόμενο αιώνα ο Shihab al-Din abu 'l-'Abbas Ahmad ben 'Ali ben Ahmad 'Abd al-Qalqashandi έγραψε μια δεκατετράτομη εγκυκλοπαίδεια η οποία περιέχει ένα τμήμα αφιερωμένο στην κρυπτογραφία. Τα είδη των κωδικών που περιγράφονται σε αυτήν είναι τόσο με μεταφορά όσο και με αντικατάσταση γραμμάτων. Κάτι όμως που εμφανίζεται για πρώτη φορά είναι οι πολλαπλές αντικαταστάσεις του ακρυπτογράφητου κειμένου. Σε αυτό το έργο επίσης παρατίθεται ένα παράδειγμα κρυπτανάλυσης που χρησιμοποιεί πίνακα με συχνότητες γραμμάτων και σύνολα γραμμάτων που δεν μπορούν να συνυπάρξουν σε μια λέξη. Μεταγενέστερα το1466 ο Leon Battista Alberti ανακαλύπτει και δημοσιεύει το πρώτο πολυαλφαβητικό κώδικα, σχεδιάζοντας έναν δίσκο για να απλοποιήσει την διαδικασία. Η αποκρυπτογράφηση του κώδικα του Alberti έγινε πολύ αργότερα στα 1800.

Το πρώτο τυπωμένο βιβλίο που εστιάζει στην κρυπτογραφία συνέγραψε ο Johannes Trithemius το 1518. Το βιβλίο αυτό περιείχε τετράγωνα γραμμάτων όπου η πρώτη γραμμή περιέχει τα 26 γράμματα του λατινικού αλφαβήτου και οι υπόλοιπες 26 είναι κυκλικές μεταθέσεις της $1^{ης}$ γραμμής κατά μια θέση κάθε γραμμή.

Η πολυαλφαβητική αντικατάσταση με χρήση διαφορετικών αλφάβητων, με αλλαγή κωδικοποίησης χωρίς περιοδικότητα, αποδίδεται στον Leon Battista Alberti. Αυτό που περιορίζει αυτήν την ανακάλυψη είναι ότι ο κρυπτογράφος πρέπει να υποδείξει, μέσα στο σώμα του κειμένου, το γράμμα που καθορίζει την επιλογή του επόμενου αλφαβήτου. Επιπλέον ήταν ο Bellaso αυτός που πρότεινε να χρησιμοποιείται μια λέξη κλειδί για την αναγνώριση του κρυπτογραφημένου αλφάβητου και δίδαξε διάφορους τρόπους ώστε ο παραλήπτης του κωδικοποιημένου μηνύματος να μην έχει ανάγκη από ανταλλαγές δίσκων ή πινάκων.

Ο Blaise de Vigenère ήταν επίσης ένας σημαντικός κρυπτογράφος, ο οποίος πρότεινε να ενσωματώσει το μήνυμα μέσα στο κλειδί. Ο πίνακας του Vigenère ήταν ασφαλής για 300 χρόνια,όμως ο Kasiski και ύστερα ο Friedman κατάφεραν να τον σπάσουν.

Το 1790 ο Thomas Jefferson, πιθανόν με συνεργασία του Dr. Robert Patterson εφηύρε το περιστροφικό κρυπτοσύστημα, το οποίο χρησιμοποιήθηκε και αργότερα με διάφορες παραλλαγές μέχρι τον δεύτερο παγκόσμιο πόλεμο από το αμερικανικό ναυτικό.

Μια άλλη σημαντική ανακάλυψη στην κρυπτογραφία ήταν αυτή του Gilbert S. Vernam το 1917. Ανακάλυψε μια πρακτική πολυαλφαβητική κρυπτογραφική μηχανή ικανή να παράγει ένα κλειδί εντελώς τυχαίο και να μην το αναπαράγει ποτέ ξανά. Η μηχανή αυτή προσφέρθηκε στην αμερικανική κυβέρνηση αλλά απορρίφθηκε. Τελικά αξιοποιήθηκε εμπορικά στα 1920.

Το σύστημα ADFGVX χρησιμοποιήθηκε από του Γερμανούς κοντά στο τέλος του πρώτου παγκοσμίου πολέμου. Πρώτα, ένα μυστικό μπερδεμένο αλφάβητο συμπλήρωνε ένα 5×5 τετράγωνο του Πολύβιου. Με βάση αυτό το τετράγωνο το κείμενο χωριζόταν σε τμήματα. Μετά, το τεμαχισμένο κείμενο υπόκειται σε μια μετάθεση κατά στήλες. Το μήνυμα γράφεται σε γραμμές κάτω από ένα κλειδί. Ύστερα, ταξινομείται αλφαβητικά το κλειδί οπότε και μεταφέρονται αναλόγως τα γράμματα του κειμένου. Τέλος, γράφεται η κάθε στήλη που έχει σχηματιστεί από την παραπάνω διαδικασία. Την αποκρυπτογράφηση αυτού του συστήματος κατάφερε ο Γάλλος λοχαγός Georges Painvin.

Ένα άλλο σύστημα που κατασκευάστηκε στο τέλος του Πρώτου Παγκοσμίου πολέμου ήταν η μηχανή Enigma. Υιοθετήθηκε από τον στρατό και τις κυβερνητικές υπηρεσίες σε πολλές

χώρες για την κρυπτογράφηση και αποκρυπτογράφηση μυστικών κειμένων.

Το 1919 ο Arvid Gerhard Damm έκανε αίτηση για δίπλωμα ευρεσιτεχνίας στην Σουηδία για μια μηχανή κρυπτογράφησης με στροφείο. Το εγχείρημα του αυτό εξελίχθηκε σε μια επιχείρηση η οποία ήταν η μόνη που είχε εμπορική επιτυχία εκείνη την εποχή. Η εταιρία αυτή λειτουργεί ακόμα,αν και αντιμετωπίζει προβλήματα μιας και κατηγορείται ότι σκόπιμα αποδυνάμωσε μια μορφή κωδικοποίησης.

Η μηχανή Enigma δεν ήταν εμπορική επιτυχία, αλλά όταν βελτιώθηκε από τους Γερμανούς έγινε η κρυπτογραφική κινητήριος δύναμη της ναζιστικής Γερμανίας. Τελικά ο Πολωνός μαθηματικός, Marian Rejewski, κατάφερε να το αποκρυπτογραφήσει έχοντας στην κατοχή του μόνο κωδικοποιημένα κείμενα και κλειδιά που είχε υποκλέψει ένας κατάσκοπος. Το οριστικό σπάσιμο του κώδικα στην πιο πολύπλοκη πολεμική του μορφή επιτεύχθηκε από τους Alan Turing, Gordon Welchman και άλλους κατά την διάρκεια του πολέμου.

Μετά τον Δεύτερο Παγκόσμιο Πόλεμο οι ρότορες αντικαταστάθηκαν από ηλεκτρονικά συστήματα. Το μοναδικό πλεονέκτημα αυτών των καινούργιων μηχανών κρυπτογράφησης ήταν η ταχύτητα. Η σύγχρονη κρυπτογραφία ξεκινάει από τον Claude Shannon, ο οποίος ήταν ο πρώτος που χρησιμοποίησε μαθηματικά συστήματα στην κρυπτογραφία. Μεταγενέστεροι του που αξίζει να αναφερθούν είναι ο Whitfield Diffie, Martin Hellman, Ron Rivest Adi Shamir και Leonard M. Adleman.

3 Ψηφιακές Υπογραφές

3.1 Εισαγωγή

Για πολλά χρόνια χρησιμοποιούνταν διάφορες μορφές υπογραφών οι οποίες συσχέτιζαν την ταυτότητα του συγγραφέα με το κείμενο. Στον Μεσαίωνα,οι ευγενείς σφράγιζαν ένα έγγραφο με ένα κέρινο αποτύπωμα του εμβλήματος τους. Ο μόνος που μπορούσε να αναπαράγει την σφραγίδα ήταν ο κάτοχος της άρα μπορούσαν να επιβεβαιώσουν την προέλευση του κειμένου. Αργότερα όταν γινόταν συναλλαγές με πιστωτικές κάρτες ο πωλητής θα έπρεπε να ελέγχει αν η υπογραφή πάνω στην κάρτα ήταν ίδια με του αγοραστή. Στην σύγχρονη εποχή με την ανάπτυξη του ηλεκτρονικού εμπορίου και των ψηφιακών κειμένων αυτές οι μέθοδοι δεν είναι πλέον επαρκής.

Ας υποθέσουμε ότι θέλουμε να υπογράψουμε ένα ψηφιακό κείμενο. Θα μπορούσαμε απλά να ψηφιοποιήσουμε την χειρόγραφη υπογραφή μας και να την επισυνάψουμε στο κείμενο. Όμως οποιοσδήποτε είχε πρόσβαση στο κείμενο θα μπορούσε να αφαιρέσει την υπογραφή μας και να την προσθέσει κάπου αλλού,για παράδειγμα σε μια επιταγή. Έτσι είναι αναγκαίο μια ψηφιακή υπογραφή να μην μπορεί να αποκοπεί από ένα μήνυμα και να επικολληθεί σε κάποιο άλλο. Συνεπώς η υπογραφή δεν είναι μονάχα συνδεδεμένη με τον υπογράφοντα αλλά και με το υπογεγραμμένο κείμενο. Επίσης η αυθεντικότητα των ψηφιακών υπογραφών πρέπει να επαληθεύεται από τους ενδιαφερόμενους. Οπότε τα σχήματα ψηφιακών υπογραφών χωρίζονται σε δύο διαδικασίες εκείνη της δημιουργίας της υπογραφής και σε αυτήν της επαλήθευσης.

3.2 Χρήσιμοι ορισμοί

1. Ψηφιακή υπογραφή είναι ένα μαθηματικό σχήμα το οποίο αποδεικνύει την γνησιότητα ενός ψηφιακού κειμένου ή μηνύματος και την ταυτότητα του συγγραφέα του.
2. Αλγόριθμος παραγωγής ψηφιακών υπογραφών είναι η μέθοδος η οποία ακολουθείται για την παραγωγή ψηφιακών υπογραφών.
3. Αλγόριθμος επαλήθευσης ψηφιακών υπογραφών είναι ο αλγόριθμος που εξασφαλίζει την γνησιότητα της ψηφιακής υπογραφής.
4. Ένα σχήμα ψηφιακών υπογραφών αποτελείται από έναν αλγόριθμο παραγωγής υπογραφών και έναν σχετικό αλγόριθμο επαλήθευσης.
5. Μια διαδικασία υπογραφής ψηφιακών υπογραφών συνίσταται σε έναν αλγόριθμο παραγωγής ψηφιακών υπογραφών, σε συνδυασμό με την μέθοδο μορφοποίησης των δεδομένων σε μηνύματα.
6. Μια διαδικασία επαλήθευσης ψηφιακών υπογραφών αποτελείται από έναν αλγόριθμο επαλήθευσης,μαζί με μια μέθοδο ανάκτησης δεδομένων από το μήνυμα που χρειάζεται να υπογραφεί.

Για να παραχθούν στην πράξη σχήματα ψηφιακών υπογραφών είναι απαραίτητο να έχουμε μια διεργασία ψηφιακών υπογραφών (αυτή είναι εμπορικά τυποποιημένη). Στον επόμενο πίνακα παρατίθενται χρήσιμοι συμβολισμοί οι οποίοι είναι δημοσία γνωστοί.

3.3 **Σύμβολα**

- M: χώρος όλων των μηνυμάτων
- M_S: σύνολο στοιχείων που καλείται χώρος υπογραφής
- S: χώρος όλων των υπογραφών (signature space)
- R: συνάρτηση πλεονασμού (redundancy function)
- M_R: η εικόνα της R
- R^{-1}: η αντίστροφη εικόνα της R
- *R*: ένα σύνολο δεικτών
- h: μια μονόδρομη συνάρτηση με πεδίο ορισμού το M
- M_h : η εικόνα της h (δηλαδή h: M→M_h) το $M_h \subseteq M_S$ λέγεται τιμή του κατακερματισμού
- K: ο χώρος όλων των πιθανών κλειδιών που μπορούν να χρησιμοποιηθούν για την δημιουργία μιας ψηφιακής υπογραφής
- $sig_k(\tilde{m})$: συνάρτηση υπογραφής (signing function)
- $ver_k(\tilde{m}, s^*)$: συνάρτηση επαλήθευσης (verification function)

Παρατηρήσεις:

i. Το M είναι πεπερασμένο σύνολο όλων των πιθανών στοιχείων που μπορούν να υπογραφούν.
ii. Το M_S είναι το σύνολο στα οποία εφαρμόζονται οι μετασχηματισμοί υπογραφών. Οι μετασχηματισμοί δεν εφαρμόζονται απευθείας στο σύνολο M.
iii. Το S είναι το σύνολο των στοιχείων που σχετίζονται με τα μηνύματα στο M. Τα στοιχεία αυτά χρησιμεύουν ώστε να συνδεθεί ο υπογράφον με το κείμενο.
iv. R είναι μια συνάρτηση 1-1 με πεδίο ορισμού το M κ πεδίο τιμών το M_S, η οποία είναι επιπλέον αντιστρέψιμη και δημόσια γνωστή.
v. Το *R* χρησιμοποιείται στην αναγνώριση συγκεκριμένων μετασχηματισμών.

3.4 **Η συνάρτηση κατακερματισμού**

Η συνάρτηση κατακερματισμού χρησιμοποιείται ώστε να διασφαλιστεί η ακεραιότητα των δεδομένων και η αυθεντικότητα των μηνυμάτων. Η συνάρτηση κατακερματισμού δέχεται ως είσοδο ένα μήνυμα και παράγει ως αποτέλεσμα μια σύνοψη του μηνύματος, αποτύπωμα ή τιμή κατακερματισμού. Πιο συγκεκριμένα μια συνάρτηση κατακερματισμού δέχεται μια πεπερασμένη σειρά από bits και την μετατρέπει σε μια σειρά σταθερού μήκους. Έχει πεδίο ορισμού το D και πεδίο τιμών το R (h:D→R) και |D|>|R|. Είναι μονής κατεύθυνσης πράγμα που σημαίνει ότι η ύπαρξη συγκρούσεων (δηλαδή η πιθανότητα δυο μηνύματα να έχουν την ίδια σύνοψη) είναι εξαιρετικά μικρή. Πράγματι, αν έχουμε ως είσοδο μια t-bit συμβολοσειρά (με t>n), αν η h ήταν τυχαία με την έννοια ότι όλες οι έξοδοι ήταν ισοπίθανες, τότε περίπου 2^{t-n} θα συνοψιζόταν σε κάθε έξοδο, και δύο τυχαίες είσοδοι θα έδιναν το ίδιο αποτέλεσμα με πιθανότητα 2^{-n} (ανεξάρτητο από το t).

Σε συνδυασμό με τις ψηφιακές υπογραφές η συνάρτηση κατακερματισμού εγγυάται την

ακεραιότητα των δεδομένων. Το μήνυμα πρώτα κατακερματίζεται και μετά η τιμή του κατακερματισμού υπογράφεται αντί για το αρχικό μήνυμα. Μια ξεχωριστή κλάση συναρτήσεων κατακερματισμού ονομάζεται message authentication codes (MACs), μας βοηθάει να καταλάβουμε την αυθεντικότητα του μηνύματος με συμμετρικές τεχνικές. Ο αλγόριθμος MAC μπορεί να θεωρηθεί ως μια συνάρτηση κατακερματισμού που δέχεται δύο διακριτές εισόδους, ένα μήνυμα και ένα ιδιωτικό κλειδί και παράγει μια σταθερού μήκους έξοδο, με σκοπό να μην μπορεί κάποιος να παράγει το ίδιο αποτέλεσμα χωρίς την γνώση του κλειδιού.
Μπορούμε να εξασφαλίσουμε την ακεραιότητα των δεδομένων με τον τρόπο που περιγράφεται παρακάτω. Η τιμή του κατακερματισμού που είναι αποτέλεσμα της εφαρμογής της συνάρτησης κατακερματισμού σε ένα μήνυμα x μπορεί να υπολογισθεί την χρονική στιγμή T_1. Η ακεραιότητα της τιμής του κατακερματισμού (αλλά όχι του ίδιου του μηνύματος) είναι εξασφαλισμένη με κάποιον τρόπο. Σε κάποια ακόλουθη χρονική στιγμή T_2 διεξάγεται ο ακόλουθος έλεγχος ώστε να διαπιστωθεί άμα έχει τροποποιηθεί το μήνυμα, με άλλα λόγια αν το μήνυμα x' είναι το ίδιο με το αρχικό. Έτσι υπολογίζεται η τιμή του κατακερματισμού για το μήνυμα x' και συγκρίνεται με την τιμή κατακερματισμού του αρχικού μηνύματος. Αν είναι ίδιες τότε κάποιος μπορεί να συμπεράνει ότι οι είσοδοι στην συνάρτηση κατακερματισμού είναι ίσες, οπότε το μήνυμα x δεν έχει τροποποιηθεί. Συνεπώς το πρόβλημα που παρουσιάζεται όταν θέλουμε να επαληθεύσουμε την ακεραιότητα ενός μεγάλου μηνύματος μετατρέπεται στην διερεύνηση μιας σταθερού μεγέθους τιμής κατακερματισμού. Για να είναι αποτελεσματική μια τιμή κατακερματισμού θα πρέπει να είναι με μοναδικό τρόπο συνδεδεμένη με την είσοδο και οι συγκρούσεις να είναι υπολογιστικά δύσκολες να βρεθούν.

Ορισμός: Μια συνάρτηση κατακερματισμού είναι μια συνάρτηση, με τουλάχιστον, τις ακόλουθες ιδιότητες:
Συμπίεση-Η είσοδος της h είναι οποιουδήποτε μήκους,ενώ η έξοδος h(x) έχει πεπερασμένο, σταθερό μήκος.
Ευκολία στον υπολογισμό-Με δοσμένη την h και μια είσοδο x, η h(x) υπολογίζεται εύκολα.

3.4.1 **Βασικές ιδιότητες και ορισμοί της συνάρτησης κατακερματισμού**

Έστω συνάρτηση κατακερματισμού με εισόδους x, x' και εξόδους y,y'.

1) αντίσταση ορίσματος (preimage resistance): είναι υπολογιστικά ανέφικτο να βρεθεί ένα x' τέτοιο ώστε h(x') = y, όταν έχουμε σαν δεδομένο ένα y και δεν γνωρίζουμε την είσοδο της συνάρτησης.
2) Αντίσταση 2ου ορίσματος (2nd- preimage resistance): είναι υπολογιστικά ανέφικτο να βρεθεί μια δεύτερη είσοδος η οποία να έχει το ίδιο αποτέλεσμα με μια άλλη δοσμένη. Με άλλα λόγια είναι υπολογιστικά ανέφικτο για δοθέν x να βρεθεί ένα x' τέτοιο ώστε $x \neq x'$ και $h(x) \neq h(x')$.
3) ανθεκτική σύγκρουσης (collision resistance): είναι υπολογιστικά ανέφικτο να βρεθούν δύο διακριτές είσοδοι x, x' που κατακερματίζονται στην ίδια έξοδο, δηλαδή h(x)=h(x').
4) μη-συσχέτιση (non-correlation): τα bit εισόδου και εξόδου δεν πρέπει να είναι συσχετισμένα.

Δεν δίνονται οι ορισμοί του τι σημαίνει υπολογιστικά εύκολο ή δύσκολο, γιατί αυτό μπορεί να εξαχθεί από τα συμφραζόμενα. Για παράδειγμα το υπολογιστικά εύκολο μπορεί να σημαίνει σε πολυωνυμικό χρόνο και χώρο ή σε χρονικές μονάδες όπως τα seconds και τα milliseconds.

Ορισμός: Η συνάρτηση κατακερματισμού καλείται μοναδικής κατεύθυνσης αν ικανοποιεί τις ακόλουθες ιδιότητες: αντίσταση ορίσματος, αντίσταση 2ου ορίσματος.

Σημείωση: Παρόμοια ορίζονται και κάποιες επιπρόσθετες ιδιότητες.

- Αντίσταση κοντινής σύγκρουσης (near-collision resistance): Θα πρέπει να είναι δύσκολο να βρεθεί ζεύγος εισόδων (x,x') ώστε οι αντίστοιχες h(x), h(x') να διαφέρουν σε μικρό πλήθος bits.
- Αντίσταση μερικού ορίσματος (partial preimage resistance): τοπική μονοδρομικότητα (local one-way): Θα πρέπει να είναι το ίδιο δύσκολο να ανακτήσουμε οποιαδήποτε υπακολουθία χαρακτήρων, όσο και μια ολόκληρη είσοδο.

Αυτές οι ιδιότητες της συνάρτησης κατακερματισμού αποτρέπουν πλαστογραφήσεις. Όμως αφού η σύνοψη των μηνυμάτων είναι καθορισμένου μήκους δεν είναι τόσα όσα είναι το πλήθος των δυνατών μηνυμάτων. Άρα δημιουργούνται επιθέσεις στις ψηφιακές υπογραφές που χρησιμοποιούν την συνάρτηση κατακερματισμού.

Σημείωση: Εδώ θα πρέπει να σημειώσουμε ότι τα ονόματα Alice και Bob (βέβαια μπορούν να χρησιμοποιηθούν και άλλα ονόματα) είναι δύο αρχέτυποι χαρακτήρες που χρησιμοποιούνται τόσο στην κρυπτογραφία όσο και στην φυσική. Τα ονόματα αυτά χρησιμοποιούνται για ευκολία. Για παράδειγμα "Η Alice στέλνει στον Bob ένα κρυπτογραφημένο μήνυμα".

3.4.2 **Επιθέσεις γενεθλίων στις Ψηφιακές Υπογραφές**

Στην θεωρία πιθανοτήτων, το πρόβλημα των γενεθλίων ή το παράδοξο των γενεθλίων αναφέρεται στην πιθανότητα, σε ένα σύνολο n ατόμων τυχαία επιλεγμένων, δύο άνθρωποι να έχουν γενέθλια την ίδια μέρα. Αυτό μπορεί να εκφραστεί και στα μαθηματικά με τον εξής τρόπο. Ας υποθέσουμε ότι έχουμε n αντικείμενα και r ανθρώπους. Κάθε άνθρωπος επιλέγει ένα αντικείμενο. Η πιθανότητα να επιλεγεί το ίδιο αντικείμενο είναι:
$\Pr(\text{match}) \approx 1 - e^{-\lambda}$ όπου $r = \sqrt{\lambda n}$.
Ακολουθεί παράδειγμα με το πως μπορεί κάποιος να εκμεταλλευτεί αυτό το πρόβλημα ώστε να εξαπατήσει.

Η Alice θέλει να υπογράψει ηλεκτρονικά ένα έγγραφο και χρησιμοποιεί ένα από τα γνωστά σχήματα ψηφιακών υπογραφών ώστε να υπογράψει την σύνοψη (τιμή κατακερματισμού) του εγγράφου. Ας υποθέσουμε ότι η συνάρτηση κατακερματισμού παράγει σαν αποτέλεσμα μια έξοδο 50 bits. Όμως ανησυχεί ότι ο Fred θέλει να την εξαπατήσει και να την ωθήσει να υπογράψει ένα επιπλέον συμβόλαιο, ίσως την αγορά ενός βαλτώδους οικοπέδου, αλλά αισθάνεται ασφαλής γιατί γνωρίζει ότι η πιθανότητα ένα δόλιο συμβόλαιο να έχει την ίδια τιμή κατακερματισμού με το σωστό έγγραφο είναι 1 στα 2^{50}, το οποίο είναι περίπου 1 στα 10^{15}. Ο Fred θα δοκιμάσει διάφορα δόλια συμβόλαια, αλλά είναι σχεδόν απίθανο να βρει κάποιο με την σωστή τιμή κατακερματισμού. Ο Fred, βέβαια, έχει υπόψιν του το πρόβλημα των γενεθλίων και το χειρίζεται όπως περιγράφεται παρακάτω. Βρίσκει 30 σημεία του κειμένου στα οποία μπορεί να κάνει μικρές αλλαγές, όπως προσθέτοντας ένα κενό στο τέλος μιας γραμμής, αλλάζοντας ελαφρώς μια λέξη κ.τ.λ. Σε κάθε περίπτωση, έχει δύο επιλογές ή να κάνει μια μικρή αλλαγή ή αφήνει το έγγραφο ως έχει. Ως συνέπεια αυτού ο

Fred μπορεί να παράγει 2^{30} έγγραφα τα οποία είναι κατ' ουσίαν ίδια με το πρωτότυπο. Φυσικά, η Alice, δεν θα φέρει αντίρρηση στο να υπογράψει κάποιο από αυτά τα έγγραφα. Τώρα, ο Fred θα υπολογίσει την τιμή του κατακερματισμού όλων αυτών των κίβδηλων εκδοχών του πρωτότυπου κειμένου και θα τις αποθηκεύσει. Παρόμοια, φτιάχνει 2^{30} εκδοχές του παραποιημένου συμβολαίου και αποθηκεύει τις συνόψεις του. Έτσι για $r = 2^{30}$ και $n = 2^{50}$ έχουμε $\lambda = 2^{10} = 1024$. Όποτε η πιθανότητα να έχει το ίδιο αποτύπωμα το αρχικό με το τροποποιημένο κείμενο είναι $1-e^{-1024} \approx 1$. Ο Fred βρίσκει την εκδοχή που ταιριάζει και ζητάει από την Alice να υπογράψει την αυθεντική. Επίσης σχεδιάζει να επισυνάψει την υπογραφή της Alice και στο δόλιο συμβόλαιο. Έτσι ο Fred μπορεί να ισχυριστεί ότι η Alice συμφώνησε να αγοράσει το οικόπεδο. Αλλά η Alice είναι καθηγήτρια αγγλικών και επιμένει να αφαιρεθεί ένα κόμμα από μια πρόταση. Όποτε η Alice υπογράφει ένα κείμενο που έχει μια εντελώς διαφορετική τιμή κατακερματισμού από αυτό που έχει στην κατοχή του ο Fred. Ο Fred αποτυγχάνει γιατί είναι πρακτικά αδύνατο να βρει ένα παρόμοιο κείμενο με το αρχικό που να έχει το ίδιο αποτύπωμα.
Αυτό που έκανε ο Fred λέγεται επίθεση γενεθλίων. Στην πράξη πρέπει να χρησιμοποιείται μια συνάρτηση κατακερματισμού με διπλάσια έξοδο από αυτή που πιστεύεται ότι χρειάζεται, μιας και με την επίθεση των γενεθλίων μειώνεται στο μισό ο αριθμός των bits. Εκείνο που έκανε η Alice είναι το απαραίτητο ώστε να αποτρέψει την επίθεση στο σχήμα υπογραφής της. Συνεπώς προτού κανείς υπογράψει ένα ψηφιακό κείμενο θα ήταν καλό να το μετατρέψει ελαφρώς.

3.4.3 **Κατασκευή συναρτήσεων κατακερματισμού μίας κατεύθυνσης**

Η κατασκευή μιας κρυπτογραφικής συνάρτησης κατακερματισμού χωρίζεται σε δύο τμήματα. Το πρώτο είναι κατασκευή μιας συνάρτησης συμπίεσης η οποία δέχεται μια σταθερού μήκους είσοδο και παράγει μια μικρότερου μήκους έξοδο. Στο δεύτερο κομμάτι, δοσμένης μιας συνάρτησης συμπίεσης παράγουμε μια συνάρτηση με είσοδο αυθαίρετου μήκους.

Η συνάρτηση κατακερματισμού πρέπει να μπορεί να δέχεται ένα μήνυμα αυθαίρετου μήκους και να το μετατρέπει σε ένα σταθερού μήκους. Αυτό μπορεί να επιτευχθεί με το να χωριστεί το κείμενο σε block σταθερού μήκους και να εφαρμόσουμε διαδοχικά σε αυτά μια συνάρτηση συμπίεσης μιας κατεύθυνσης. Η συνάρτηση συμπίεσης παράγει μια τιμή κατακερματισμού ανάλογα με το περιεχόμενο του κάθε block καθώς και από την τιμή του κατακερματισμού του προηγούμενου block.

Οι σημαντικότερες συναρτήσεις κατακερματισμού και οι τεχνολογίες που χρησιμοποιούν περιγράφονται παρακάτω:

- HMAC (Hash-based Message Authentication Code): είναι μια τεχνική για τον υπολογισμό του MAC (message authentication code) χρησιμοποιώντας μια κρυπτογραφική συνάρτηση κατακερματισμού σε συνδυασμό με ένα ιδιωτικό κλειδί. Όπως με κάθε MAC, μπορεί να χρησιμοποιηθεί ταυτόχρονα για την ασφάλεια των δεδομένων και την γνησιότητα του μηνύματος. Η αποτελεσματικότητα του HMAC εξαρτάται από την "αντοχή" της συνάρτησης κατακερματισμού, το μήκος της τιμής κατακερματισμού σε bits και το μήκος και την ποιότητα του κρυπτογραφικού κλειδιού.
  Μια συνάρτηση κατακερματισμού δρα επαναλαμβανόμενα στο μήνυμα και το τεμαχίζει σε block σταθερού μήκους. Το μέγεθος της εξόδου ενός HMAC είναι ίδιο με εκείνο της συνάρτησης κατακερματισμού που έχει χρησιμοποιηθεί.
  Ο ορισμός και η ανάλυση του HMAC δημοσιεύτηκε το 1996 από τον Mihir Bellare,

Ran Canetti και Hugo Krawczyk (ο οποίος έγραψε και το RFC 2104). Σε αυτήν την δημοσίευση ορίζεται και μια μεταβλητή NMAC η οποία σπανίως χρησιμοποιείται.

- MD5 (Message Digest): Ο MD5 αλγόριθμος χρησιμοποιείται στις κρυπτογραφικές συναρτήσεις κατακερματισμού και παράγει τιμή κατακερματισμού με 128-bit. Το MD5 εφαρμόζεται σε μεγάλο εύρος εφαρμογών και συνήθως ελέγχει την ακεραιότητα των δεδομένων. Το MD5 σχεδιάστηκε από τον Ron Rivest το 1991 για να αντικαταστήσει μια προηγούμενη εκδοχή συνάρτησης κατακερματισμού την MD4. Η συνάρτηση κατακερματισμού MD5 συνήθως εκφράζεται στο δεκαεξαδικό σύστημα με 32 ψηφία.
  Όμως διαπιστώθηκε ότι ο αλγόριθμος MD5 δεν είναι ανθεκτικός στις συγκρούσεις. Το 1996, ένα ελάττωμα εμφανίστηκε στον σχεδιασμό του MD5 και παρόλο που δεν ήταν καταλυτικό, οι κρυπτογράφοι άρχισαν να προτείνουν την χρήση άλλων αλγορίθμων όπως το SHA-1 (το οποίο όμως αποδείχθηκε είναι και αυτό ευάλωτο). Το 2004, παρουσιάστηκαν πιο σοβαρά προβλήματα στο MD5 και έτσι η περαιτέρω χρήση του αλγόριθμου αμφισβητήθηκε από τους ειδικούς. Αργότερα έγιναν και άλλα σπασίματα και πλέον ο αλγόριθμος MD5 θεωρείται κρυπτογραφικά σπασμένος και ακατάλληλος για χρήση.

- SHA-1 (Secure Hash Algorithm-1): είναι μια κρυπτογραφική συνάρτηση κατακερματισμού η οποία σχεδιάστηκε από το United States National Security Agency. Υπάρχουν τρεις αλγόριθμοι SHA (SHA-0,SHA-1,SHA-2) οι οποίοι έχουν διαφορετική δομή. Ο SHA-1 είναι παρόμοιος με τον SHA-0, μόνο που είναι διορθωμένο ένα λάθος που οδηγούσε σε σημαντική αδυναμία του αρχικού SHA. Ο SHA-0 δεν χρησιμοποιήθηκε σε πολλές εφαρμογές.
  Ο SHA-1 είναι ο πιο ευρέως διαδεδομένες από τις υπάρχουσες SHA συνάρτησης κατακερματισμού καθώς χρησιμοποιείται σε πολλές εφαρμογές και πρωτόκολλα. Το 2005 βρέθηκε κάποιο πρόβλημα στην ασφάλεια του SHA-1 το οποίο σήμαινε ότι κάποια καινούργια συνάρτηση έπρεπε να κατασκευαστεί. Παρόλο που δεν έχουν εμφανιστεί επιτυχημένες επιθέσεις στο SHA-2 το SHA-3 είναι υπό κατασκευή.

3.5 **Κατηγορίες ψηφιακών υπογραφών**

Δύο είναι οι γενικές κατηγορίες ψηφιακών υπογραφών:

1) Οι ψηφιακές υπογραφές με παράρτημα (digital signature schemes with appendix), απαιτούν το αρχικό μήνυμα σαν είσοδο στον αλγόριθμο επαλήθευσης και χρησιμοποιούν την συνάρτηση κατακερματισμού. Παραδείγματα ψηφιακών υπογραφών με παράρτημα: DSA, DSS, ELGamal, Schnorr.
2) Σχήματα ψηφιακών υπογραφών με ικανότητα ανάκτησης μηνύματος, δεν απαιτούν το αρχικό μήνυμα σαν είσοδο στον αλγόριθμο επαλήθευσης. Εν αντιθέσει το αρχικό μήνυμα μπορεί να αναπαραχθεί από την ίδια την ψηφιακή υπογραφή. Παραδείγματα ψηφιακών υπογραφών με δυνατότητα ανάκτησης του μηνύματος: RSA, Rabin, Nyberg-Rueppel.

Οι κλάσεις αυτές μπορούν επιπλέον να διαιρεθούν με βάση αν το $|R| = 1$ ή όχι.

Ορισμός: Μια ψηφιακή υπογραφή (είτε με παράρτημα είτε με ανάκτηση μηνύματος) ονομάζεται τυχαιοποιημένη ψηφιακή υπογραφή αν $|R| = 1$, αλλιώς λέγεται ντετερμινιστική.

3.5.1 **Σχήματα ψηφιακής υπογραφής με παράρτημα**

Οι ψηφιακές υπογραφές με παράρτημα είναι αυτές που χρησιμοποιούνται περισσότερο στην πράξη. Βασίζονται κυρίως στην συνάρτηση κατακερματισμού και όχι στην συνάρτηση πλεονασμού. Επίσης είναι λιγότερο επιρρεπείς στις επιθέσεις υπαρκτής πλαστογραφίας (existential forgery attack), που θα περιγραφούν παρακάτω.

Παρακάτω παρουσιάζεται η διαδικασία για την παραγωγή ενός κλειδιού σε μια ψηφιακή υπογραφή με παράρτημα.
Η Alice δημιουργεί ένα ιδιωτικό κλειδί ώστε να υπογράψει το μήνυμα και ένα δημόσιο κλειδί για να το χρησιμοποιήσει ο Bob ώστε να επαληθεύσει ότι η υπογραφή είναι έγκυρη. Η Alice θα πρέπει να επιλέξει ένα ιδιωτικό κλειδί το οποίο προσδιορίζει ένα σύνολο μετασχηματισμών $sig_k=\{sig_k: k\in R\}$. Η sig_k είναι ένας μετασχηματισμός από το M_h στο S που χρησιμοποιείται για την παραγωγή των ψηφιακών υπογραφών και είναι γνωστός μόνο στον υπογράφοντα.

Η συνάρτηση υπογραφής καθορίζει έναν άλλον μετασχηματισμό $ver_k(\tilde{m}, s^*)$ από το $M_h \times S$ στο σύνολο {Αληθής,Ψευδής} και χρησιμοποιείται για να επαληθεύσει ότι η υπογραφή έχει πράγματι προκύψει από την εφαρμογή του sig_k στο $\tilde{m}$.

$$ver_k(\tilde{m}, s^*) = \begin{cases} \text{Αληθής}, \text{αν } sig_k(\tilde{m}) = s^* \\ \text{Ψευδής}, \text{αλλιώς} \end{cases}$$

όπου $\tilde{m} \in M_h$ και εδώ $\tilde{m} = h(m)$ για $m \in M$, $s^* \in S$. Αυτός ο μετασχηματισμός έχει κατασκευαστεί έτσι ώστε να μπορεί να υπολογιστεί χωρίς την γνώση του ιδιωτικού κλειδιού του υπογράφοντα. Το δημόσιο κλειδί της Alice είναι η συνάρτηση μετασχηματισμού και το ιδιωτικό της κλειδί είναι η συνάρτηση υπογραφής.

Αλγόριθμος-Παραγωγή και επαλήθευση ψηφιακών υπογραφών με παράρτημα.
Περίληψη: Η Alice δημιουργεί υπογραφή $s \in S$ για το μήνυμα $m \in M$ η οποία μπορεί να επαληθευθεί αργότερα από τον Bob.

1) Παραγωγή υπογραφής. Η Alice πρέπει:
   a) Να επιλέξει ένα στοιχείο $k \in R$.
   b) Να υπολογίσει $\tilde{m} = h(m)$ και $s^* = sig_k(\tilde{m})$.
   c) Η υπογραφή της Alice για το μήνυμα m είναι η s^*. Το m και το s^* είναι γνωστά σε αυτούς που θέλουν να επαληθεύσουν την εγκυρότητα της υπογραφής.
2) Επαλήθευση υπογραφής. Ο Bob πρέπει:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice.
   b) Να υπολογίσει $\tilde{m} = h(m)$ και το $u = ver_k(\tilde{m}, s^*)$.
   c) Να αποδεχθεί ότι η υπογραφή είναι πράγματι έγκυρη αν και μόνο αν u = αληθής.

Κάθε σχήμα ψηφιακής υπογραφής πρέπει να έχει τις εξής ιδιότητες:

1) Μόνο ο υπογράφον να μπορεί να υπολογίσει και κανείς άλλος το $s^* \in S$ για κάποιο $m \in M$ έτσι ώστε $ver_k(\tilde{m}, s^*)$ = αληθής, όπου $\tilde{m} = h(m)$.
2) Να είναι υπολογιστικά εύκολο η Alice να δημιουργήσει την υπογραφή της, αλλά και ο Bob να μπορέσει εύκολα να επαληθεύσει την εγκυρότητα της.
3) Είναι χρήσιμο επίσης στο κείμενο να περιλαμβάνονται και πληροφορίες, όπως η ημερομηνία και η ώρα, επειδή η ψηφιακή υπογραφή δεν είναι κομμάτι του κειμένου για να αποτραπεί η χρησιμοποίησή του από κάποιον άλλον αργότερα.

Σημείωση: Οι ψηφιακές υπογραφές με παράρτημα χρησιμοποιούνται για μηνύματα με

οποιοδήποτε μήκος, ενώ οι ψηφιακές υπογραφές με δυνατότητα ανάκτησης εφαρμόζονται σε μηνύματα με σταθερό μήκος. Η συνάρτηση κατακερματισμού που χρησιμοποιήθηκε στον παραπάνω αλγόριθμο είναι μοναδικής κατεύθυνσης και συνήθως επιλέγεται έτσι ώστε να είναι ανθεκτική στις συγκρούσεις. Ένας εναλλακτικός τρόπος για να υπογράψει η Alice ένα μήνυμα είναι να χωρίσει το μήνυμα σε σταθερού μήκους κομμάτια και να υπογράψει καθένα ξεχωριστά χρησιμοποιώντας σχήμα υπογραφής με ικανότητα ανάκτησης του μηνύματος. Όμως είναι σχετικά αργή η μέθοδος παραγωγής ψηφιακών υπογραφών και είναι επικίνδυνο για την ασφάλεια του μηνύματος να επαναδιατάσεις τα υπογεγραμμένα κομμάτια του.

3.5.2 **Ψηφιακές υπογραφές με ικανότητα ανάκτησης μηνύματος**

Στις ψηφιακές υπογραφές που περιγράφονται παρακάτω το αρχικό μήνυμα μπορεί να αναπαραχθεί από την υπογραφή. Όμως δεν χρησιμοποιούνται συχνά παρά μόνο σε μηνύματα με μικρό μήκος.

Ορισμός: Το σχήμα ψηφιακής υπογραφής με ικανότητα ανάκτησης του μηνύματος είναι μια ψηφιακή υπογραφή στην οποία δεν χρειάζεται να γνωρίζουμε εξαρχής το μήνυμα για να επαληθευτεί η εγκυρότητα της.

Παρακάτω παρουσιάζεται η διαδικασία για την παραγωγή ενός κλειδιού σε μια ψηφιακή υπογραφή με ικανότητα ανάκτησης μηνύματος.
Η Alice δημιουργεί ένα ιδιωτικό κλειδί για να υπογράψει το μήνυμα και ένα δημόσιο κλειδί για να το χρησιμοποιήσει ο Bob ώστε να επαληθεύσει ότι η υπογραφή είναι έγκυρη. Η Alice θα πρέπει να επιλέξει ένα ιδιωτικό κλειδί το οποίο προσδιορίζει ένα σύνολο μετασχηματισμών $sig_k=\{sig_k: k\in R\}$. Η sig_k είναι ένας μετασχηματισμός από το M_S στο S που χρησιμοποιείται για την παραγωγή των ψηφιακών υπογραφών και είναι γνωστός μόνο στον υπογράφοντα.

Η συνάρτηση υπογραφής ορίζει την συνάρτηση μετασχηματισμού ver_k και είναι κατασκευασμένη έτσι ώστε να μην χρειάζεται το ιδιωτικό κλειδί του υπογράφοντα για τον υπολογισμό της. Το δημόσιο κλειδί της Alice είναι το ver_k και το ιδιωτικό το sig_k.

Αλγόριθμος-Παραγωγή και επαλήθευση ψηφιακών υπογραφών με ικανότητα ανάκτησης του μηνύματος.
Περίληψη: Η Alice δημιουργεί την υπογραφή $s\in S$ για το μήνυμα $m\in M$ την οποία μπορεί να επαληθευθεί αργότερα από τον Bob. Το μήνυμα m μπορεί να ανακτηθεί από την υπογραφή s.

1) Παραγωγή υπογραφής. Η Alice πρέπει:
   a) Να επιλέξει ένα στοιχείο $k\in R$.
   b) Να υπολογίσει $\tilde{m} = R(m)$ και $s^* = sig_k(\tilde{m})$ (όπου R η συνάρτηση πλεονασμού).
   c) Η υπογραφή της Alice είναι η s^* και γίνεται γνωστή σε όσους θέλουν να την επαληθεύσουν και να ανακτήσουν το μήνυμα μέσω αυτής.
2) Επαλήθευση υπογραφής. Ο Bob πρέπει:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice.
   b) Να υπολογίσει $\tilde{m} = ver_k(s^*)$.
   c) Να επαληθεύσει ότι $\tilde{m}\in M_R$. Αν το $\tilde{m}$ δεν έχει αυτήν την ιδιότητα ο Bob απορρίπτει την υπογραφή.

d) Ο Bob μπορεί να ανακτήσει το μήνυμα m υπολογίζοντας το $R^{-1}(\tilde{m})$.

Απαραίτητες ιδιότητες της ψηφιακής υπογραφής με ικανότητα ανάκτησης και της συνάρτησης επαλήθευσης:

1) Θα πρέπει να είναι εύκολο να υπολογιστεί η συνάρτηση υπογραφής και επαλήθευσης.
2) Θα πρέπει να είναι υπολογιστικά ανέφικτο κάποιος άλλος εκτός από την Alice να μπορεί να βρει ένα $s^* \in S$ τέτοιο ώστε $ver_k(s^*) \in M_R$.

Σημειώσεις:

1) Η συνάρτηση πλεονασμού R και η αντίστροφη της R^{-1} είναι δημόσια γνωστά. Είναι πολύ σημαντικό να επιλεχθεί σωστά η συνάρτηση πλεονασμού για την ασφάλεια του σχήματος υπογραφής. Έτσι ας υποθέσουμε ότι $M_R = M_S$. Επίσης $R:M \rightarrow M_R$ και $sig_k:M_S \rightarrow S$ είναι 1-1 και επί. Από τα παραπάνω βγάζουμε ως συμπέρασμα ότι το M και S είναι ισοπληθικά. Οπότε για $s^* \in S$ έχουμε $ver_k(s^*) \in M_R$ και έτσι είναι εύκολο να ανακτήσουμε τα μηνύματα m και τις αντίστοιχες υπογραφές s^* που θα είναι αποδεκτά από την συνάρτηση επαλήθευσης με το εξής τρόπο:
   a) Επιλογή τυχαίου $k \in R$ και $s^* \in S$.
   b) Υπολογισμός του $\tilde{m} = ver_k(s^*)$.
   c) Υπολογισμός του $m = R^{-1}(\tilde{m})$.

   Το στοιχείο s^* είναι μια έγκυρη υπογραφή για το μήνυμα m και για την δημιουργία της δεν χρειάστηκε να είναι γνωστή η συνάρτηση υπογραφής.
2) Αν και η συνάρτηση πλεονασμού R είναι δημόσια γνωστή και παρόλο που η αντίστροφη R^{-1} της είναι εύκολο να υπολογιστεί η επιλογή της R δεν θα πρέπει να είναι ανεξάρτητη από την επιλογή των μετασχηματισμών υπογραφής του sig_k.
3) Κάθε σχήμα υπογραφής με ικανότητα ανάκτησης μηνύματος μπορεί να μετατραπεί σε σχήμα υπογραφής με παράρτημα αν βάλουμε σαν είσοδο στην συνάρτηση κατακερματισμού το μήνυμα και μετά υπογράψουμε την έξοδο. Άρα τώρα είναι απαραίτητο το μήνυμα και για τον αλγόριθμο επαλήθευσης. Όμως πλέον η συνάρτηση πλεονασμού R δεν είναι τόσο χρήσιμη για την ασφάλεια της υπογραφής και μπορεί να είναι μια οποιαδήποτε 1-1 συνάρτηση από το M_h στο M_S.

3.6 **Τύποι επιθέσεων στα σχήματα ψηφιακών υπογραφών**

Όταν αναφερόμαστε σε επιθέσεις σε σχήματα ψηφιακών υπογραφών εννοούμε την πλαστογράφηση που προσπαθεί κάποιος να επιτύχει ώστε να μας εξαπατήσει. Στην βιβλιογραφία χρησιμοποιούνται διάφοροι όροι για να περιγραφεί αυτός που επιτίθεται στην ψηφιακή υπογραφή, όπως: υποκλοπείς (interceptors), αντίπαλοι (opponents, adversaries), εχθροί (enemies), εισβολείς ή ακόμα και επιτιθέμενοι (attackers).

1) Ολικό σπάσιμο (total break). Ο αντίπαλος μπορεί να υπολογίσει το ιδιωτικό κλειδί του υπογράφοντα ή μπορεί να βρει μια συνάρτηση υπογραφής (sig_k) που να είναι πρακτικά ίδια με την αυθεντική. Έτσι μπορεί να παράγει μια έγκυρη ψηφιακή υπογραφή και να υπογράψει ένα οποιοδήποτε κείμενο.
2) Επιλεκτική πλαστογραφία (selective forgery). Με μια μη αμελητέα πιθανότητα, ο αντίπαλος μπορεί να παράγει μια έγκυρη ψηφιακή υπογραφή για ένα μήνυμα. Με άλλα λόγια, αν δοθεί στον αντίπαλο ένα μήνυμα x, μετά μπορεί να ορίσει (με κάποια πιθανότητα) μια συνάρτηση y τέτοια ώστε verk = αληθής. Το μήνυμα x δεν θα πρέπει να έχει υπογραφεί από την Alice στο παρελθόν. Σε αυτήν την περίπτωση πλαστογραφίας δεν συμμετέχει κατευθείαν ο νόμιμος υπογράφον.

3) Υπαρκτή πλαστογραφία (existential forgery). Ο αντίπαλος είναι ικανός να παράξει μια έγκυρη υπογραφή για τουλάχιστον ένα μήνυμα. Με άλλα λόγια, ο αντίπαλος μπορεί να δημιουργήσει ένα ζευγάρι (x,y) όπου x είναι το μήνυμα, y είναι η υπογραφή και verk(x,y) = αληθής. Το μήνυμα x δεν θα πρέπει να έχει υπογραφεί από την Alice στο παρελθόν. Σε αυτήν την περίπτωση επίθεσης ο αντίπαλος έχει ελάχιστο ή και καθόλου έλεγχο του μηνύματος και ο νόμιμος υπογράφον συμμετέχει στην απάτη άθελα του.

Υπάρχουν δύο βασικές επιθέσεις ενάντια σε υπογραφές με δημόσιο κλειδί.

1) Επιθέσεις μόνο σε κλειδιά (key-only attacks). Σε αυτή την περίπτωση επίθεσης, ο αντίπαλος γνωρίζει μονάχα το δημόσιο κλειδί της Alice.
2) Επιθέσεις μόνο στο μήνυμα (message attacks). Εδώ ο αντίπαλος είναι ικανός να εξετάσει τις ψηφιακές υπογραφές ανάλογα με το άμα είναι στην κατοχή του γνωστά ή άγνωστα μηνύματα. Οι επιθέσεις σε μηνύματα μπορούν επιπλέον να κατηγοριοποιηθούν σε τρεις υποκλάσεις:
   a) Επίθεση σε γνωστό μήνυμα (known-message attack). Ο αντίπαλος έχει στην κατοχή του μια λίστα από μηνύματα που έχει ήδη υπογράψει η Alice, αλλά δεν τα έχει επιλέξει ο ίδιος.
   b) Επίθεση σε επιλεγμένο μήνυμα (chosen-message attack). Σε αυτήν την περίπτωση επίθεσης ο αντίπαλος έχει στην κατοχή του έγκυρες υπογραφές από ένα κατάλογο από υπογεγραμμένα μηνύματα προτού προσπαθήσει να επιτεθεί στο σχήμα ψηφιακής υπογραφής. Αυτή η μέθοδος δεν προσαρμόζεται εύκολα σε πολλές περιπτώσεις με την έννοια ότι τα μηνύματα είναι ήδη επιλεγμένα προτού γίνουν γνωστές οι υπογραφές.
   c) Προσαρμόσιμη επίθεση σε επιλεγμένο μήνυμα (adaptive chosen-message attack). Ο αντίπαλος δέχεται υπογραφές από τυχαία μηνύματα που έχει επιλέξει, όπου η επιλογή κάθε μηνύματος μπορεί να εξαρτάται από την επιλογή των προηγούμενων μηνυμάτων.

Σημειώσεις:

- (προσαρμόσιμη επίθεση σε επιλεγμένο μήνυμα) Αυτού του είδους η επίθεση είναι η πιο ισχυρή σε σχέση με αυτές που αναφέρονται. Ο αντίπαλος μπορεί εύκολα να εξάγει ένα πρότυπο και μετά να πλαστογραφήσει την υπογραφή με δική του επιλογή αν έχει στην κατοχή του αρκετά μηνύματα και τις αντίστοιχες υπογραφές. Αν και είναι δύσκολο να προβλεφθεί αυτή η επίθεση κάθε αξιόπιστο σχήμα υπογραφής θα πρέπει να ανταποκρίνεται σε αυτή την περίσταση.
- (σχετικά με την ασφάλεια) Το επίπεδο της ασφάλειας που θα πρέπει να παρέχει μια ψηφιακή υπογραφή εξαρτάται από την εφαρμογή που καλείται να διασφαλίσει. Έτσι για παράδειγμα όταν ο αντίπαλος είναι σε θέση να επιτεθεί μόνο στο κλειδί, αρκεί να αποτραπεί η επιλεκτική πλαστογράφηση. Ενώ σε περιπτώσεις που ο αντίπαλος καταφέρνει επίθεση στο μήνυμα, πρέπει να αποφευχθεί η δυνατότατη υπαρξιακής πλαστογράφησης.
- (συναρτήσεις κατακερματισμού στις ψηφιακές υπογραφές) Η επιλογή της συνάρτησης κατακερματισμού θα πρέπει να γίνει πολύ προσεκτικά έτσι ώστε η συνάρτηση να είναι μέρος διεργασίας της υπογραφής. Αλλιώς είναι πιθανόν να δεχθούμε μια επιλεκτική πλαστογράφηση.

Γενικά κάθε σχήμα ψηφιακής υπογραφής δεν μπορεί να είναι ασφαλές άνευ όρων, μιας και ο αντίπαλος μπορεί να ελέγξει κάθε πιθανή υπογραφή για ένα δεδομένο μήνυμα,

χρησιμοποιώντας τον αλγόριθμο επαλήθευσης ver_k, μέχρι να βρει μία έγκυρη υπογραφή. Έτσι δοθέντος κάποιου χρόνου ο αντίπαλος μπορεί πάντα να πλαστογραφήσει την υπογραφή της Alice σε οποιοδήποτε μήνυμα. Συνεπώς στόχος μας είναι να κατασκευάσουμε ψηφιακές υπογραφές υπολογιστικά ασφαλής.

4 Σχήμα υπογραφής RSA και σχετικά σχήματα υπογραφών

4.1 Σχήμα υπογραφής RSA

Το σχήμα υπογραφής RSA ανακαλύφθηκε από τον Rivest, Shamir και Adleman, ήταν η πρώτη ουσιαστικά υπογραφή που χρησιμοποίησε την τεχνική του δημόσιου κλειδιού. Η ασφάλεια αυτού του συστήματος βασίζεται κυρίως στην δυσκολία που αντιμετωπίζουμε στην παραγοντοποίηση ακεραίων. Το RSA μπορούμε να το χρησιμοποιήσουμε και ως ψηφιακή υπογραφή με ικανότητα ανάκτησης μηνύματος και ως ψηφιακή υπογραφή με παράρτημα.

Στο RSA με δημόσιο κλειδί ο χώρος το μηνυμάτων και του κρυπτογραφημένου μηνύματος είναι ο $\mathbb{Z}_n$ όπου n = pq είναι το γινόμενο δύο τυχαία επιλεγμένων διακριτών πρώτων αριθμών. Επιλέγεται η συνάρτηση πλεονασμού $R:M\rightarrow \mathbb{Z}_n$ και γίνεται δημόσια γνωστή.

Αλγόριθμος-Παραγωγή κλειδιού για το κρυπτοσύστημα RSA
Περίληψη: Η Alice δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό. Η Alice θα πρέπει να κάνει τα ακόλουθα:

1) Να βρει δύο μεγάλους τυχαίους διακριτούς πρώτους αριθμούς p και q, που να έχουν περίπου το ίδιο μέγεθος.
2) Να υπολογίσει n = pq και φ(n) = (p-1)(q-1).
3) Να επιλέξει ένα τυχαίο ακέραιο e, $1 < e < \varphi$, τέτοιο ώστε $ΜΚΔ(e,\varphi) = 1$.
4) Να χρησιμοποιήσει τον εκτεταμένο αλγόριθμο του Ευκλείδη για να υπολογίσει τον μοναδικό ακέραιο d, με $1 < d < \varphi$, τέτοιο ώστε $ed \equiv 1 \pmod{\varphi}$.
5) Το δημόσιο κλειδί της Alice είναι το (n,e) και το d είναι το ιδιωτικό της.

Αλγόριθμος-Παραγωγή και επαλήθευση υπογραφής RSA
Περίληψη: Η Alice υπογράφει ένα μήνυμα $m\in M$. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice και να ανακτήσει το μήνυμα m μέσω της υπογραφής.

1. Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει $\tilde{m} = R(m)$, έναν ακέραιο που ανήκει στο διάστημα [0,n-1].
   b) Να υπολογίσει $s = \tilde{m}^d \bmod n$.
   c) Η υπογραφή της Alice για το μήνυμα m είναι η s.
2. Επαλήθευση υπογραφής. Για να επαληθευθεί η υπογραφή της Alice και να ανακτήσει ο Bob το μήνυμα m, ο Bob πρέπει:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice (n,e).
   b) Να υπολογίσει το $\tilde{m} = s^e \bmod n$.
   c) Να επαληθεύσει ότι $\tilde{m}\in M_R$, αν όχι να απορρίψει την υπογραφή.
   d) Να ανακτήσει το μήνυμα $m = R^{-1}(\tilde{m})$.

Σε αυτό το σημείο θα πρέπει να αποδειχθεί ότι η επαλήθευση της συνάρτησης λειτουργεί. Αν s είναι η ψηφιακή υπογραφή για το μήνυμα m, τότε $s = \tilde{m}^d \bmod n$ όπου $\tilde{m} = R(m)$.

Αφού $ed \equiv 1 \pmod{\varphi}$, $s^e \equiv \tilde{m}^{ed} \equiv \tilde{m} \pmod{n}$. Άρα, $R^{-1}(\tilde{m}) = R^{-1}(R(m)) = m$.

Παράδειγμα (με τεχνηέντως μικρές παραμέτρους)
Αλγόριθμος-Παραγωγή κλειδιού για το κρυπτοσύστημα RSA
Περίληψη: Η Alice δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό. Η Alice θα κάνει τα ακόλουθα:

1) Βρίσκει δύο μεγάλους τυχαίους διακριτούς πρώτους αριθμούς p = 7927 και q =6997.
2) n = 55465219 και $\varphi(n) = 7926 * 6996 = 55450296$.
3) Επιλέγει ένα τυχαίο ακέραιο e = 5.
4) Υπολογίζει $ed = 5d = 1 \pmod{55450296}$ και βρίσκει d = 44360237.
5) Το δημόσιο κλειδί της Alice είναι το (n=55465219,e=5) και το d = 44360237 είναι το ιδιωτικό της.

Αλγόριθμος-Παραγωγή και επαλήθευση υπογραφής RSA
χώρος υπογραφής $M = \mathbb{Z}_n$, συνάρτηση πλεονασμού $R:M \to \mathbb{Z}_n$ και είναι η ταυτοτική απεικόνιση R(m) = m για κάθε $m \in M$. Έστω ότι το m = 31229978.

1. Παραγωγή υπογραφής. Η Alice κάνει τα ακόλουθα:
   a) Υπολογίζει $\tilde{m} = R(m) = 31229978$.
   b) Υπολογίζει $s = \tilde{m}^d \bmod n = 31229978^{44360237} \bmod 55465219 = 30729435$.
   c) Η υπογραφή της Alice για το μήνυμα m είναι η s.
2. Επαλήθευση υπογραφής. Για να επαληθευθεί η υπογραφή της Alice και να ανακτήσει ο Bob το μήνυμα m, ο Bob:
   a) Αποκτά το αυθεντικό δημόσιο κλειδί της Alice (n,e).
   b) Υπολογίζει το $\tilde{m} = s^e \bmod n = 30729435^5 \bmod 55465219$.
   c) Επαληθεύει ότι $\tilde{m} \in M_R$.
   d) Ανακτά το μήνυμα $m = R^{-1}(\tilde{m}) = 31229978$.

4.1.1 **Επιθέσεις στις RSA ψηφιακές υπογραφές**

Παραγοντοποίηση ακεραίων

Ένα ολικό σπάσιμο της υπογραφής RSA μπορεί να επιτευχθεί αν ο αντίπαλος κατορθώσει να παραγοντοποιήσει τον ακέραιο n που έχει υπολογίσει η Alice. Κατά αυτόν τον τρόπο μπορεί να υπολογίσει το φ και στην συνέχεια χρησιμοποιώντας τον εκτεταμένο αλγόριθμο του Ευκλείδη να εξάγει το ιδιωτικό κλειδί d της Alice και το δημόσιο e λύνοντας την εξίσωση $ed \equiv 1 \pmod{\varphi}$.

Για να αποφευχθεί αυτή η περίπτωση πρέπει να γίνει προσεκτική επιλογή των πρώτων αριθμών p και q. Έτσι αυτοί οι αριθμοί θα πρέπει να έχουν το ίδιο μήκος σε bit και να είναι αρκετά μεγάλοι. Για παράδειγμα αν ένας ακέραιος με 1024-bit modulus n πρέπει να χρησιμοποιηθεί, τότε τα p, q πρέπει να έχουν περίπου 512 bits μήκος.

Έτσι δημιουργήθηκε το 1991 ένας διαγωνισμός από τα RSA-Laboratories για να βρεθεί πόσο δύσκολη είναι πραγματικά η παραγοντοποίηση μεγάλων αριθμών που χρησιμοποιούνται σαν κλειδιά στο RSA. Η παραγοντοποίηση ακεραίων με 100 ψηφία είναι

πλέον εύκολη με τους αλγόριθμους και το hardware που διαθέτουμε. Τώρα που η βιομηχανία έχει καλύτερη γνώση της κρυπτανάλυσης ο διαγωνισμός δεν είναι πλέον επίκαιρος.

Πολλαπλασιαστική ιδιότητα του RSA

Το σχήμα ψηφιακής υπογραφής RSA έχει την ακόλουθη πολλαπλασιαστική ιδιότητα:
Έστω ότι $s_1 = m_1^d \bmod n$ και $s_2 = m_2^d \bmod n$ είναι αντίστοιχα οι υπογραφές για τα μηνύματα m_1 και m_2 τότε $s = s_1 s_2 \bmod n$ και έχει την ιδιότητα $s = (m_1 m_2) \bmod n$. Αν $m = m_1 m_2$ έχει την κατάλληλη συνάρτηση πλεονασμού τότε η s είναι έγκυρη υπογραφή για το μήνυμα αυτό. Άρα είναι σημαντικό η συνάρτηση πλεονασμού να μην έχει την πολλαπλασιαστική ιδιότητα δηλαδή αν $m_1, m_2 \in M$ τότε $R(m_1 m_2) \neq R(m_1) R(m_2)$.

4.1.2 **Οι RSA ψηφιακές υπογραφές στην πράξη**

Το πρόβλημα reblocking εμφανίζεται όταν το RSA χρησιμοποιείται πρώτα για την υπογραφή και μετά την κωδικοποίηση του μηνύματος για να εξασφαλιστεί η αυθεντικότητα και η μυστικότητα του μηνύματος.

Αν υποθέσουμε ότι η Alice και ο Bob γνωρίζουν και οι δύο το δημόσιο κλειδί ο ένας του άλλου. Η Alice θέλει να στείλει ένα μήνυμα m στον Bob έτσι ώστε ο Bob να είναι σίγουρος ότι το μήνυμα είναι της Alice και η Alice να είναι σίγουρη ότι ο Bob μπορεί να διαβάσει το μήνυμα. Για να το επιτευχθεί αυτό η Alice υπολογίζει το c, αφού πρώτα υπογράψει το μήνυμα με το ιδιωτικό της κλειδί (n_A,d_A) και μετά κρυπτογραφεί την υπογραφή με το δημόσιο κλειδί του Bob (n_B,e_B). Μετά στέλνει: $c = \left(m^{d_A} \bmod n_A\right)^{e_B} \bmod n_B$ στον Bob. Μιας και το c είναι κρυπτογραφημένο με το δημόσιο κλειδί του Bob, η Alice είναι σίγουρη ότι μόνο ο Bob μπορεί να αποκρυπτογραφήσει το κρυπτοκείμενο. Με την σειρά του ο Bob αφού αποκρυπτογραφήσει το κρυπτοκείμενο με το ιδιωτικό του κλειδί, κρυπτογραφεί το αποτέλεσμα που παράγεται από αυτήν την διαδικασία με το δημόσιο κλειδί της Alice. Αν το τελικό αποτέλεσμα βγάζει νόημα, τότε ο Bob είναι σίγουρος πως η Alice έχει συντάξει το μήνυμα, αφού είναι η μοναδική που γνωρίζει το ιδιωτικό της κλειδί. Έτσι διασφαλίζεται ότι η μετάδοση είναι ασφαλής και μυστική. Όμως, δεν είναι βέβαιο ότι ο Bob μπορεί να ανακτήσει το μήνυμα m (ή έστω κάτι που να βγάζει νόημα) αν το n_A είναι μεγαλύτερο από το n_B. Σε αυτήν την περίπτωση ο Bob αποκρυπτογραφεί αυτό το κείμενο και υπολογίζει $\left(m^{d_A} \bmod n_A\right)^{e_B}\right) \bmod n_B$ το οποίο μπορεί να είναι τελείως διαφορετικό από το $\left(m^{d_A} \bmod n_A\right)^{e_B}$. Αυτό είναι το reblocking πρόβλημα όπως αρχικά διατυπώθηκε από τους Rivest, Shamir, Adleman. Όταν το $n_A > n_B$, τότε η πιθανότητα ο Bob να μην μπορεί να ανακτήσει το μήνυμα είναι $(n_A-n_B)/n_A$.

Υπάρχουν διάφοροι τρόποι για να αντιμετωπιστεί αυτό το πρόβλημα:

1) Αναδιάταξη: Η πρώτη λύση στο reblocking πρόβλημα είναι απλά η αναδιάταξη της διαδικασίας της υπογραφής και της κρυπτογράφησης ανάλογα με το πιο RSA moduli είναι μεγαλύτερο. Έτσι η Alice πρώτα υπογράφει και μετά κωδικοποιεί αν $n_A<n_B$, σε αντίθετη περίπτωση πρώτα κρυπτογραφεί και μετά υπογράφει. Αυτή η λύση με αναδιάταξη πολλές φορές καλείται προ-απόφαση (pre-judgment method).

   Τελικά η μέθοδος αυτή δεν είναι επιθυμητή για δύο λόγους. Πρώτον, αν η Alice κρυπτογραφήσει και μετά υπογράψει, κάθε παρατηρητής θα μπορούσε να αφαιρέσει την υπογραφή της Alice με το δημόσιο κλειδί της και να την αντικαταστήσει με την

δική του. Χωρίς τα κατάλληλα πρωτόκολλα αυτό μπορεί να οδηγήσει στην εξής επίθεση: Ο αντίπαλος παρεμβαίνει στην μετάδοση του μηνύματος, αφαιρεί την υπογραφή της Alice, προσθέτει την δική του, στέλνει το μήνυμα στον Bob και αργότερα ζητάει από τον Bob να στείλει πίσω το μήνυμα m. Μια δεύτερη ανεπιθύμητη συνέπεια του να κρυπτογραφείς πρώτα και μετά να υπογράφεις είναι όταν η Alice θέλει να έχει πολλούς παραλήπτες το μήνυμα της έστω $\{B_1,B_2,...,B_N\}$, με (n_i,e_i) το αντίστοιχο δημόσιο κλειδί. Όταν $n_A < n_i$ για όλα τα i=1,...,n η Alice θα πρέπει να υπογράψει μια φορά το μήνυμα και μετά να κάνει μια κρυπτογράφηση για κάθε διαφορετικό B_i. Βέβαια για κάθε modulus μικρότερο του n_A, η Alice θα πρέπει να υπολογίσει μια διαφορετική υπογραφή. Στην χειρότερη περίπτωση όταν $n_A > n_i$ για όλα τα i, η Alice θα πρέπει να υπολογίσει n κωδικοποιήσεις και n υπογραφές. Συνεπώς ο συνολικός αριθμός των κρυπτογραφήσεων/υπογραφών είναι στην χειρότερη περίπτωση (2N) σχεδόν το διπλάσιο από την καλύτερη περίπτωση (N+1).

2) Δύο moduli ανά εμπλεκόμενο: Μια δεύτερη λύση για αυτό το πρόβλημα προτάθηκε από τους Rivest, Shamir, Adleman. Αυτή η λύση απαιτεί κάθε εμπλεκόμενος να έχει δύο ζεύγη RSA κλειδιών τέτοια ώστε κάθε modulus να είναι μικρότερο από κάποιο όριο (threshold), ας υποθέσουμε h, και το άλλο modulus να είναι μεγαλύτερο. Για να στείλει η Alice ένα μήνυμα έγκυρο και με μυστικότητα, πρέπει πρώτα να υπογράψει το μήνυμα με το ιδιωτικό της κλειδί με modulus μικρότερο του h και μετά να το κρυπτογραφήσει με του Bob το δημόσιο κλειδί με modulus μεγαλύτερο του h. Κατά αυτόν τον τρόπο, το modulus που χρησιμοποιείται για την υπογραφή είναι μικρότερο από το modulus που χρησιμοποιείται για την κρυπτογράφηση και ο Bob μπορεί πάντα να ανακτήσει το αρχικό μήνυμα. Επιπροσθέτως, η Alice χρησιμοποιώντας αυτήν την μέθοδο μπορεί να στείλει το ίδιο μήνυμα σε N παραλήπτες (όπως περιγράφτηκε παραπάνω) με μια μόνο υπογραφή και N κρυπτογραφήσεις, που είναι ο ελάχιστος αριθμός κρυπτογραφήσεων/υπογραφών που απαιτούνται. Αυτή η μέθοδος καλείται τεχνική του κατωφλίου (threshold technique) για την αυθεντικότητα/μυστικότητα του μηνύματος.

3) Προκαθορισμός της μορφής του modulus. Σε αυτή την περίπτωση επιλέγεται το p και το q που είναι πρώτοι αριθμοί έτσι ώστε το modulus n να έχει μια ειδική μορφή: το υψηλότερης τάξης bit είναι το 1 και τα υπόλοιπα k που ακολουθούν είναι 0. Έτσι ένα t-bit modulus n μπορεί να βρεθεί άμα ακολουθήσουμε την παρακάτω διαδικασία. Το n θα πρέπει να είναι $2^{t-1} < n < 2^{t-1} + 2^{t-k-1}$. Μετά θα πρέπει να επιλεγεί ένας τυχαίος $\lceil t/2 \rceil - \text{bit}$ πρώτος p, και να αντίστοιχα ένα q μεταξύ του $\lfloor 2^{t-1}/p \rfloor$ και $\lfloor (2^{t-1}+2^{t-k-1})/p \rfloor$. Τότε το n = pq έχει την επιθυμητή μορφή modulus. Αυτό δεν αποτρέπει εντελώς τα λάθη στην κρυπτογράφηση, αλλά ελαττώνει την πιθανότητα αυτά να συμβούν. Αν υποθέσουμε ότι n_A είναι ένα modulus τέτοιο ώστε $s = m^{d_A} \bmod n_A$ να είναι η υπογραφή για το μήνυμα m. Επίσης ας υποθέσουμε ότι η s έχει 1 σε μια από τις k+1 θέσεις με υψηλής τάξης bit, εκτός της υψηλότερης. Τότε το s, μιας και είναι μικρότερο του n_A, πρέπει να έχει μηδενικά στις θέσεις με υψηλή τάξη, οπότε είναι μικρότερη από κάθε modulus αυτής της μορφής. Η πιθανότητα η s να μην έχει κανένα 1 στην k+1 υψηλότερης τάξης θέση, εκτός της υψηλότερης, είναι λιγότερη από $(1/2)^k$, η οποία είναι πολύ μικρότερη αν το k είναι επιλεγμένο έτσι ώστε να είναι περίπου 100.

Συνάρτηση πλεονασμού

Η επιλογή της συνάρτησης πλεονασμού είναι επίσης πολύ σημαντική για τις ψηφιακές υπογραφές RSA. Η ακατάλληλη επιλογή συνάρτησης πλεονασμού είναι κρίσιμη μιας και μπορεί να οδηγήσει σε επίθεση με υπαρκτή πλαστογραφία. Έτσι έχει δημιουργηθεί μια συνάρτηση πλεονασμού που θεωρείται ασφαλής σε διεθνές επίπεδο.

4.2 **Σχήμα ψηφιακών υπογραφών RSA με παράρτημα**

Παραπάνω έχει περιγραφεί πως μπορούμε να μετατρέψουμε τον αλγόριθμο που παράγει υπογραφές με ανάκτηση μηνύματος σε σχήμα υπογραφών με παράρτημα. Όποτε ακολουθείται η ίδια διαδικασία για την ψηφιακή υπογραφή RSA.

Χαρακτηριστικά επιδόσεων της παραγωγής και επαλήθευσης υπογραφών
Έστω p = q = k τότε:

- η παραγωγή της υπογραφής απαιτεί $O(k^3)$ bit.
- η επαλήθευση της υπογραφής, στην περίπτωση μικρού δημόσιου εκθέτη, απαιτεί $O(k^2)$.
- η προτεινόμενη τιμή για την ποσότητα e στην πράξη είναι 3 ή $2^{16}+1$. Βέβαια, τα p και q πρέπει να είναι επιλεγμένα τέτοια ώστε ΜΚΔ(e,(p-1)(q-1)) = 1.
- Το σχήμα ψηφιακών υπογραφών RSA είναι ιδανικό για τις περιπτώσεις που η επαλήθευση της υπογραφής είναι η κύρια λειτουργία που εκτελείται. Για παράδειγμα αν ένα τρίτο πρόσωπο εμπιστοσύνης παράγει ένα πιστοποιητικό με δημόσιο κλειδί για την Alice. Τότε αυτό απαιτεί την παραγωγή της υπογραφής μόνο μια φορά, αλλά η επαλήθευση της υπογραφής μπορεί να γίνει πολλές φορές από διάφορες οντότητες.

Επιλογή παραμέτρων

- το μέγεθος του modulus σε bit πρέπει να είναι τουλάχιστον 768 και για υπογραφές που χρησιμοποιούνται για περισσότερο χρόνο ή που είναι κρίσιμες για την ασφάλεια ενός δικτύου πρέπει να είναι τουλάχιστον 1024.
- Δεν έχουν εμφανιστεί αδυναμίες στην υπογραφή όταν η παράμετρος e έχει επιλέγει έτσι ώστε να είναι ένας μικρός αριθμός όπως το 3 ή το $2^{16}+1$.
- Δεν είναι απαραίτητο να περιοριστεί το μέγεθος της ιδιωτικής παραμέτρου d ώστε να βελτιωθεί η αποδοτικότητα της παραγωγής της υπογραφής.

Αποδοτικότητα εύρους ζώνης

Ορισμός: Η αποδοτικότητα εύρους ζώνης (bandwidth efficiency) στις ψηφιακές υπογραφές με ικανότητα ανάκτησης κειμένου ονομάζεται ο λόγος του λογαρίθμου (με βάση 2) μεγέθους του χώρου M_S προς τον λογάριθμο (με βάση 2) του M_R.
Για το σχήμα υπογραφής RSA (ISO/IEC 9796) η αποδοτικότητα του εύρους ζώνης είναι 5, το οποίο σημαίνει ότι με 1024-bits modulus μπορεί να υπογραφούν 512-bits μηνύματα.

Παράμετροι καθολικής εφαρμογής

- Κάθε οντότητα πρέπει να έχει το δικό του διακριτό RSA modulus, είναι επικίνδυνο να χρησιμοποιείται από όλους κοινό modulus
- Η δημόσια παράμετρος e μπορεί να είναι καθολικής χρήσης και να χρησιμοποιείται σε πολλές εφαρμογές. Σε αυτήν την περίπτωση θα πρέπει να λάβουμε υπόψιν μας τη επίθεση στην μικρή παράμετρο.

- Αν υποθέσουμε ότι n είναι ένα 2k-bit RSA modulus το οποίο χρησιμοποιείται ώστε να υπογραφούν μηνύματα μεγέθους k-bit (δηλαδή με αποδοτικότητα εύρους ζώνης ίση με 5).
- Έστω ότι η Alice θέλει να υπογράψει ένα μήνυμα m kt-bit μεγέθους:
  - Αν t = 1 το RSA με ικανότητα ανάκτησης μηνύματος είναι πιο αποδοτικό.
  - Αν t > 1 το RSA με παράρτημα είναι πιο αποδοτικό.

5 Το σχήμα υπογραφών δημοσίου κλειδιού Rabin

Στην κρυπτογραφία το σχήμα υπογραφής Rabin είναι μια μέθοδος ψηφιακής υπογραφής που αρχικά προτάθηκε από τον Michael O. Rabin το 1979. Το σχήμα υπογραφής Rabin ήταν ένα από τα πρώτα σχήματα ψηφιακής υπογραφής που προτάθηκαν, και ήταν το πρώτο που έβαλε σε συσχετισμό την δυσκολία για πλαστογράφηση με το πρόβλημα της παραγοντοποιήσης ακεραίων. Λόγω της ευκολίας και του κυρίαρχου ρόλου που κατείχε στην κρυπτογράφηση με δημόσιο κλειδί, το σχήμα αυτό καλύπτεται σε κάθε εισαγωγικό μάθημα κρυπτογραφίας. Το σχήμα υπογραφής Rabin δεν δέχεται υπαρξιακές επιθέσεις σε ένα θεωρητικό μαύρο κουτί (random oracle) αν δεχτούμε ότι το πρόβλημα της παραγοντοποίησης ακεραίων είναι δυσεπίλητο.

Το σχήμα υπογραφής Rabin είναι παρόμοιο με το RSA, όμως η παράμετρος e είναι δημόσια (εδώ θα χρησιμοποιούμε e=2). Ο χώρος υπογραφής M_S είναι το Q_n (το σύνολο των τετραγωνικών υπολοίπων) και οι υπογραφές είναι τετραγωνικές ρίζες αυτών. Επιλέγεται μια συνάρτηση πλεονασμού R: $M \rightarrow M_S$ η οποία γίνεται δημόσια γνώστη.

Αλγόριθμος-Παραγωγή του κλειδιού για το σχήμα υπογραφών δημοσίου κλειδιού Rabin
Περίληψη: Η Alice δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό κλειδί.
Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να επιλέξει δύο μεγάλους διακριτούς τυχαίους πρώτους αριθμούς p και q, περίπου το ίδιο μέγεθος.
2) Να υπολογίσει n = pq.
3) Το δημόσιο κλειδί της Alice είναι το n και το ιδιωτικό της κλειδί το (p,q).

Αλγόριθμος-Παραγωγή και επαλήθευση της υπογραφής δημοσίου κλειδιού Rabin
Περίληψη: Η Alice υπογράφει ένα μήνυμα $m \in M$. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice και να ανακτήσει το μήνυμα m από την υπογραφή.

1) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει το $\tilde{m} = R(m)$.
   b) Να υπολογίσει την τετραγωνική ρίζα s του $\tilde{m} \bmod n$.
   c) Η υπογραφή της Alice για το m είναι η s.
2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή s της Alice και να ανακτήσει το μήνυμα m, θα πρέπει να κάνει τα ακόλουθα:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί n της Alice.
   b) Να υπολογίσει $\tilde{m} = s^2 \bmod n$.
   c) Να επαληθεύσει ότι $\tilde{m} \in M_R$, αν όχι να απορρίψει την υπογραφή.
   d) Να ανακτήσει το μήνυμα $m = R^{-1}(\tilde{m})$.

Παράδειγμα (με τεχνηέντως μικρές παραμέτρους)
Αλγόριθμος-Παραγωγή του κλειδιού για το σχήμα υπογραφών δημοσίου κλειδιού Rabin
Περίληψη: Η Alice δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό κλειδί.
Η Alice πρέπει κάνει τα ακόλουθα:

1) Επιλέγει δύο μεγάλους διακριτούς τυχαίους πρώτους αριθμούς p = 7 και q =11.
2) Υπολογίζει n = 77.
3) Το δημόσιο κλειδί της Alice είναι το n = 77 και το ιδιωτικό της κλειδί (p = 7,q = 11).

Αλγόριθμος-Παραγωγή και επαλήθευση της υπογραφής δημοσίου κλειδιού Rabin
Χώρος υπογραφής $M_S = Q_{77} = \{ 1,4,9,15,16,23,36,37,53,58,60,64,67,71\}$, για διευκόλυνση θεωρούμε $M = M_S$ και η συνάρτηση πλεονασμού είναι η ταυτοτική, m = 23.

1) Παραγωγή υπογραφής. Η Alice κάνει τα ακόλουθα:
   a) Υπολογίζει το $\tilde{m} = R(m) = 23$.
   b) Υπολογίζει τις τετραγωνικές ρίζες s του $\tilde{m} \bmod 77$. Που είναι οι $s \equiv \pm 3 \pmod 7$, $s \equiv \pm 1 \pmod 7$ και άρα s=10,32,45 ή 67.
   c) Επιλέγει την υπογραφή της για το m να είναι η s = 45.
2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή s της Alice και να ανακτήσει το μήνυμα m, κάνει τα ακόλουθα:
   a) Αποκτά το αυθεντικό δημόσιο κλειδί n της Alice.
   b) Υπολογίζει $\tilde{m} = s^2 \bmod 77 = 23$.
   c) Επαληθεύει ότι $\tilde{m} \in M_R$.
   d) Ανακτά το μήνυμα $m = R^{-1}(\tilde{m}) = 23$.

Σημειώσεις:

1) Η ψηφιακή υπογραφή έχει κάποια πλεονεκτήματα σε σχέση με το σχήμα ψηφιακών υπογραφών RSA. Πρώτον, η πλαστογράφηση της υπογραφής είναι τόσο δύσκολη όσο η παραγοντοποίηση ακεραίων. Δεύτερον, η επαλήθευση της υπογραφής είναι πιο γρήγορη και κατάλληλη για εφαρμογές όπου η επαλήθευση χρησιμοποιεί μικρές συσκευές υπολογισμού.
2) Αν υπάρχει κάποιος αλγόριθμος που μπορεί να πλαστογραφήσει την υπογραφή Rabin, τότε αυτός ο αλγόριθμος μπορεί να χρησιμοποιηθεί για να παραγοντοποιηθεί το modulus που χρησιμοποιείται σε αυτό το σχήμα υπογραφής. Αυτή είναι μια επιθυμητή ιδιότητα μιας και συσχετίζει την πλαστογράφηση της ψηφιακής υπογραφής με το δυσεπίλυτο της παραγοντοποίησης ακεραίων.
   Βέβαια, αν και έχει αυτή την ιδιότητα το σχήμα αυτό δεν είναι ασφαλές σε προσαρμόσιμες επιθέσεις, όπου ο αντίπαλος ζητά από τον υπογράφοντα να χρησιμοποιήσει υπογραφές σε μηνύματα που ο ίδιος έχει επιλέξει. Για παράδειγμα, ο αντίπαλος μπορεί να επιλέξει ένα τυχαίο $s \in Q_n$, και να μεταδώσει $m = s^2 \bmod n$ στην Alice και αυτή με την σειρά της να το υπογράψει. Η Alice δίνει ως απάντηση ότι η υπογραφή της είναι η s' που είναι μια από τις τέσσερις τετραγωνικές ρίζες του m. Αν το $s' \neq \pm s \bmod n$, τότε το modulus της Alice μπορεί να παραγοντοποιηθεί.
   Συνεπώς το σχήμα υπογραφής Rabin δεν είναι χρήσιμο στην πράξη μιας και η προσαρμόσιμη επίθεση είναι αξεπέραστη. Ο υπογράφον στην αληθινή ζωή με σχήμα Rabin θα πρέπει να εμποδίσει τον αντίπαλο από το να αποκτήσει δύο διαφορετικές τετραγωνικές ρίζες από ένα μήνυμα.
3) Το πρόβλημα στο σχήμα υπογραφής δημοσίου κλειδιού Rabin είναι ότι το $\tilde{m}$ μπορεί να μην είναι τετραγωνικό υπόλοιπο. Για να ξεπεραστεί αυτό το πρόβλημα δύο περιπτώσεις υπάρχουν:
   a) Να προστεθούν κάποια τυχαία bits στο m ώστε το $\tilde{m}$ να γίνει τετραγωνικό υπόλοιπο.
   b) Να χρησιμοποιηθεί το modified Rabin σχήμα υπογραφής το οποίο έχει ειδικές συνθήκες για τους πρώτους αριθμούς p, q και την συνάρτηση πλεονασμού R.

5.1 **Modified-Rabin σχήμα υπογραφής**

Γνωρίζουμε ότι αν p, q είναι δύο διακριτοί πρώτοι αριθμοί ισοδύναμοι του 3 mod 4 και n = pq, τότε:

- Αν $MK\Delta(x,n) = 1$, τότε $x^{(p-1)(q-1)/2} \equiv 1 \pmod n$.
- Αν $x \in Q_n$ τότε το $x^{(n-p-q+5)/8}$.
- Αν x είναι ένας ακέραιος με Jacobi $\left(\frac{x}{n}\right) = 1$, και d = (n-p-q+5)/8 τότε:

$x^{2d} \bmod n = \left\{ \begin{matrix} x \,\alpha\nu\, x \in Q_n \\ n-x, \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{matrix} \right\}$.

- Αν $p \neq q \bmod 8$, τότε $\left(\frac{2}{n}\right) = -1$. Έτσι, ο πολλαπλασιασμός κάθε ακεραίου x από το 2 ή $2^{-1} \bmod n$ αντιστρέφει το σύμβολο Jacobi του x.

Σε αυτή την τροποποιημένη μορφή του σχήματος υπογραφής Rabin έχουμε κάποιους περιορισμούς. Έτσι:

- $M: \{ m \in \mathbb{Z}_n : m \leq \lfloor (n-6)/16 \rfloor \}$
- $M_S: \{ m \in \mathbb{Z}_n : m \equiv 6 \bmod 16 \}$
- $S: \{ \mathbb{Z}_n : (s^2 \bmod n) \in M_S \}$
- $R(m) = 16m + 6$ για όλα τα $m \in M$
- $M_R: \{ m \in \mathbb{Z}_n : m \equiv 6 \bmod 16 \}$

Αλγόριθμος-Παραγωγή κλειδιού για το modified-Rabin σχήμα υπογραφής
Περίληψη: Κάθε εμπλεκόμενος δημιουργεί ένα δημόσιο και ένα ιδιωτικό κλειδί. Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να διαλέξει πρώτους αριθμούς $p \equiv 3 \pmod 8$, $q \equiv 7 \pmod 8$ και να υπολογίσει την ποσότητα $n = pq$.
2) Το δημόσιο κλειδί της Alice είναι το n, το ιδιωτικό κλειδί είναι το $d = (n-p-q+5)/8$.

Αλγόριθμος-Παραγωγή και επαλήθευση του modified-Rabin σχήματος υπογραφής
Περίληψη: Η Alice υπογράφει ένα μήνυμα $m \in M$. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice και να ανακτήσει το μήνυμα m από την υπογραφή.

1) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει $\tilde{m} = R(m) = 16m + 6$.
   b) Να υπολογίσει το σύμβολο Jacobi $J = \left(\frac{\tilde{m}}{n}\right)$.
   c) Αν το $J = 1$ να υπολογίζει $s = \tilde{m}^d \bmod n$.
   d) Αν το $J = -1$ να υπολογίσει $(\tilde{m}/2)^d \bmod n$.
   e) Η υπογραφή της Alice για το μήνυμα m είναι η s.
2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή s της Alice και να ανακτήσει το μήνυμα m, θα πρέπει να κάνει τα ακόλουθα:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice.
   b) Να υπολογίσει $m' = s^2 \bmod n$.
   c) Αν $m' \equiv 6 \pmod 8$, να πάρει $\tilde{m} = m'$.
   d) Αν $m' \equiv 3 \pmod 8$, να πάρει $\tilde{m} = 2m'$.
   e) Αν $m' \equiv 7 \pmod 8$, να πάρει $\tilde{m} = n-m'$.
   f) Αν $m' \equiv 2 \pmod 8$, να πάρει $\tilde{m} = 2(n-m')$.
   g) Να επαληθεύσει ότι $\tilde{m} \in M_R$, αλλιώς να απορρίψει τη υπογραφή.
   h) Να ανακτήσει $m = R^{-1}(\tilde{m}) = (\tilde{m}-6)/16$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί: Στην φάση παραγωγής υπογραφών υπογράφει είτε το $u = \tilde{m}$ είτε το $u = \tilde{m}/2$, ανάλογα με το ποιο έχει σύμβολο Jacobi 1. Όμως ένα ακριβώς από τα $\tilde{m}$, $\tilde{m}/2$ έχει σύμβολο Jacobi 1. Η τιμή u που υπογράφεται είναι τέτοια, ώστε $u \equiv 3$ ή $6 \pmod 8$. Επίσης είναι $s^2 \bmod n = u$ ή $n - u$ ανάλογα με το αν ισχύει, ή όχι, ότι $u \in Q_n$. Αφού $n \equiv 5 \pmod 8$, οι περιπτώσεις αυτές μπορούν να διακριθούν μονοσήμαντα.

Σημειώσεις:

1) Αν χρησιμοποιείται ο προηγούμενος αλγόριθμος τότε κανένας δεν πρέπει να υπογράψει την τιμή u αν έχει σύμβολο Jacobi ίσο με -1, μιας και αυτό οδηγεί στην παραγοντοποιήση του n.
2) Το modified-Rabin δέχεται εύκολα υπαρκτή πλαστογράφηση όπως συμβαίνει και με το αρχικό σχήμα υπογραφής Rabin.

5.2 **ISO/IEC 9796**

Εκδόθηκε το 1991 από τον Διεθνή Οργανισμό Προτύπων σαν το πρώτο πρότυπο για ψηφιακές υπογραφές. Καθορίζει μια διαδικασία ψηφιακής υπογραφής η οποία χρησιμοποιεί μηχανισμό για την ανάκτηση μηνύματος. Τα κυριότερα χαρακτηριστικά του προτύπου αυτού είναι τα εξής:

- Αναφέρεται σε κρυπτογραφία με δημόσιο κλειδί.
- Ο αλγόριθμος υπογραφής δεν καθορίζεται αλλά θα πρέπει να απεικονίζει k bits σε k bits.
- Χρησιμοποιείται για την υπογραφή μηνυμάτων περιορισμένου μήκους και δεν απαιτείται κρυπτογραφική συνάρτηση κατακερματισμού.
- Παρέχει ανάκτηση μηνύματος.
- Καθορίζει το γέμισμα (padding) όπου αυτό είναι απαραίτητο.

Η διαδικασία της υπογραφής σύμφωνα με το ISO/IEC 9796 αποτελείται από πέντε βήματα που περιγράφονται περιληπτικά ως εξής:

1) παραγέμισμα: παραγεμίζουμε συμπληρώνοντας bits στο αρχικό μήνυμα έτσι ώστε το τελικό μέγεθος του μηνύματος σε bits να είναι πολλαπλάσιο του 8.
2) επέκταση μηνύματος: στο προηγούμενο αποτέλεσμα προστίθεται πολλές φόρες το ίδιο μέχρι να έχουμε το επιθυμητό αποτέλεσμα σε byte.
3) πλεονασμός: το προηγούμενο μήνυμα ανακατεύεται με άλλα byte και στην συνέχεια προσαρμόζονται κατάλληλα.
4) περικοπή και μετατροπή: σχηματίζεται ένας ενδιάμεσος ακέραιος από το μήνυμα που προκύπτει από το παραπάνω βήμα.
5) παραγωγή υπογραφής: χρησιμοποιείται ένας μηχανισμός.

Η διαδικασία επαλήθευσης σύμφωνα με το ISO/IEC 9796:

1) άνοιγμα υπογραφής-αν όχι απορρίπτεται.
2) ανάκτηση μηνύματος-αν όχι απορρίπτεται.
3) έλεγχος πλεονασμού-αν όχι απορρίπτεται.

Αν δεν έχει γίνει απόρριψη σε κάποιο βήμα η υπογραφή γίνεται αποδεκτή.

5.3 **PKCS#1**

Το PKCS#1 είναι η πρώτη οικογένεια προτύπων η οποία καλείται Κρυπτογραφικά Πρότυπα Δημοσίου Κλειδιού (Public-Key Cryptographic Standards) και δημοσιεύτηκε από τα RSA Laboratories. Τα πρότυπα αυτά μας παρέχουν πληροφορίες σχετικά με τους βασικούς ορισμούς και τρόπους κατασκευής για τον αλγόριθμο RSA. Ορίζει μαθηματικές ιδιότητες από τα δημόσια και ιδιωτικά κλειδιά, λειτουργίες της κρυπτογράφησης και των υπογραφών, καθώς και το ASN.1 (abstract syntax notation - αφηρημένος συμβολισμός σύνταξης).

Το PKCS#1 δεν χρησιμοποιεί το χαρακτηριστικό γνώρισμα της υπογραφής RSA. Απαιτεί μια συνάρτηση κατακερματισμού (MD2 ή MD5). Συνεπώς είναι ένα ψηφιακό σχήμα υπογραφής με παράρτημα.

Μορφοποίηση δεδομένων στο PKCS#1:

- Τα δεδομένα D είναι μια σειρά οκτάδων-bits, το BT είναι μια οκτάδα με δεκαεξαδική τιμή 00 ή 01. Το PS είναι μια σειρά οκτάδων "γέμισμα". Τα μορφοποιημένα δεδομένα είναι το:

  EB = 00 || BT || PS || 00 || D
- Η αρχική οκτάδα 00 βεβαιώνει ότι το EB σαν ακέραιος είναι μικρότερο του modulo n.

Διαδικασία υπογραφής για το PKCS#1

Είσοδος: μήνυμα M, ιδιωτικός εκθέτης d και το modulus n του υπογράφοντα.

1) Κατακερματισμός του μηνύματος m σε σύνοψη MD.
2) BER-κωδικοποίηση (basic encoding rules) της σύνοψης MD και του τύπου της συνάρτησης κατακερματισμού (ASN.1) προκειμένου να δώσουν μια συμβολοσειρά οκτάδων D.
3) Μορφοποίηση της D σε συμβολοσειρά οκτάδων ED.
4) Μετατροπή της ED σε ακέραιο αριθμό **m**.
5) RSA υπολογισμός, s = MD mod n.
6) Μετατροπή των οκτάδων του ακεραίου s σε συμβολοσειρά οκτάδων S.

Διαδικασία επαλήθευσης για το PKCS#1

Είσοδος: μήνυμα M, η υπογραφή S, ο δημόσιος εκθέτης e και το modulus n.

1) Μετατροπή σειράς οκτάδων S σε ακέραιο αριθμό.
   a) Απόρριψη του S εάν το μήκος του σε bit δεν είναι πολλαπλάσιο του 8.
   b) Μετατροπή του S, σε ένα ακέραιο αριθμό s.
   c) Απόρριψη υπογραφής εάν s > n.
2) RSA υπολογισμός, $m = s^e \bmod n$.
3) Μετατροπή ακέραιου αριθμού m σε συμβολοσειρά οκτάδων EB.
4) Συντακτική ανάλυση του EB σε τύπο BT, γέμισμα PS και δεδομένα D.
   a) Απόρριψη της υπογραφής αν το EB δεν μπορεί να αναλυθεί χωρίς ασάφεια.
   b) Απόρριψη της υπογραφής αν ο τύπος BT δεν είναι ένα από τα 00 ή 01.
   c) Απόρριψη της υπογραφής αν το γέμισμα PS αποτελείται από λιγότερο από 8 οκτάδες ή είναι ασύμβατο με τον τύπο BT.
5) Αποκωδικοποίηση στοιχείων.
   a) Ο BER αποκωδικοποιεί το D για να πάρει μια σύνοψη μηνυμάτων MD και ένα τύπο της συνάρτησης κατακερματισμού.
   b) Απόρριψη της υπογραφής αν ο τύπος της συνάρτησης κατακερματισμού δεν αναγνωρίζει ένα από τα MD2 ή MD5.
6) Σύνοψη και σύγκριση μηνυμάτων.
   a) Κατακερματισμός του μηνύματος M με τον επιλεγμένο αλγόριθμο MD μηνυμάτων και παράγεται ένα MD'.
   b) Αποδοχή της υπογραφής S για το M αν και μόνο αν MD' = MD.

6 Το σχήμα υπογραφής Fiat-Shamir

Τεχνικές έχουν αναπτυχθεί ώστε κάποιος να μπορεί να επιβεβαιώσει ότι η ταυτότητα κάποιου τρίτου είναι αυτή που ισχυρίζεται πως είναι και καλούνται συνήθως ταυτοποίηση, αυθεντικότητα οντότητας και επαλήθευση της ταυτότητας. Οι τεχνικές αυτές είναι στενά συνδεδεμένες, αλλά σε απλουστευμένη μορφή, με τα σχήματα ψηφιακών υπογραφών. Στα σχήματα επαλήθευσης εξετάζετε ο ισχυρισμός ότι μια ταυτότητα είναι έγκυρη το τρέχων στιγμιαίο χρονικό διάστημα. Ο ισχυρισμός αυτός ενισχύεται ή απορρίπτεται αμέσως, με τα σχετικά προνόμια ή αιτήματα να παραχωρούνται ή να απορρίπτονται σε πραγματικό χρόνο. Όμως δεν έχουν χρονική διάρκεια όπως οι υπογραφές και αμφιβολίες για την αυθεντικότητα δεν μπορούν να διατυπωθούν αργότερα και δεν προβλέπονται μελλοντικές επιθέσεις στο σχήμα.

Παρόλα αυτά σε κάποιες περιπτώσεις τα σχήματα ταυτοποίησης μπορούν να μετατραπούν σε σχήματα ψηφιακών υπογραφών. Ένα απλό σχήμα ταυτοποίησης μπορεί να περιλαμβάνει την εξής διαδικασία μαρτυρία-πρόκληση-απάντηση (witness-challenge-response). Δηλαδή η Alice μπορεί να αποδείξει την ταυτότητα της στον Bob αν ανακοινώσει ένα μυστικό που είναι γνωστό ότι συνδέεται με την Alice, χωρίς να το κάνει γνωστό στον Bob. Αυτό μπορεί να επιτευχθεί αν δοθεί μια απάντηση σε μια πρόκληση, η όποια είναι ένα τυχαίο νούμερο επιλεγμένο από την Alice. Έτσι η μετατροπή μπορεί να γίνει αν αντικατασταθεί το τυχαίο challenge e με μια μονόδρομη hash e = h (x||m), η οποία είναι συνένωση του μάρτυρα x και του μηνύματος m που πρέπει να υπογραφεί (η h παίζει το ρόλο του επαληθευτή).

Σε αυτό το κεφάλαιο θα περιγραφούν δύο σχήματα ψηφιακών υπογραφών που παράγονται κατά αυτόν τον τρόπο από το πρωτόκολλο ταυτοποίησης Fiat-Shamir.

6.1 Το σχήμα υπογραφής Feige-Fiat-Shamir

Το σχήμα υπογραφής Feige-Fiat-Shamir είναι ένα τροποποιημένο Fiat-Shamir σχήμα υπογραφής. Η ψηφιακή υπογραφή Feige-Fiat-Shamir είναι ψηφιακή υπογραφή με παράρτημα. Στο σχήμα αυτό χρησιμοποιείται μια μονόδρομη συνάρτηση κατακερματισμού, $h : \{0, 1\}^* \rightarrow \{0, 1\}^k$ για κάποιο σταθερό θετικό ακέραιο k. Το πεδίο ορισμού της συνάρτησης κατακερματισμού είναι το σύνολο όλων των συμβολοσειρών σε bit πεπερασμένου μήκους. Ενώ το πεδίο τιμών είναι ένα σύνολο συμβολοσειρών σε bit με k μήκος.

Αλγόριθμος-Παραγωγή κλειδιού για το σχήμα υπογραφής Feige-Fiat-Shamir
Περίληψη: Κάθε εμπλεκόμενος δημιουργεί ένα δημόσιο και ένα ιδιωτικό κλειδί. Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να διαλέξει δύο τυχαίους διακριτούς πρώτους αριθμούς p, q και να υπολογίσει τον ακέραιο n = pq.
2) Να επιλέξει έναν θετικό ακέραιο k και διακριτούς ακεραίους $s_1, s_2, ..., s_k \in \mathbb{Z}_n^*$.
3) Να υπολογίσει $\upsilon_j = s_j^{-2} \bmod n$, $1 \le j \le k$.
4) Το δημόσιο κλειδί της Alice είναι το $(\upsilon_1, \upsilon_2, ..., \upsilon_k)$ και το modulus n. Το ιδιωτικό κλειδί της Alice είναι το $(s_1, s_2, ..., s_k)$.

Αλγόριθμος-Παραγωγή και επαλήθευση του σχήματος υπογραφής Feige-Fiat-Shamir
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m πεπερασμένου μήκους. Ο Bob για να επαληθεύσει την υπογραφή της Alice χρησιμοποιεί το δημόσιο κλειδί της.

1) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να επιλέξει ένα τυχαίο ακέραιο r, $1 \le r \le n-1$.

b) Να υπολογίσει $u = r^2 \bmod n$.
c) Να υπολογίσει $e = (e_1, e_2,..., e_k) = h(m||u)$, όπου κάθε $e_i \in \{0,1\}$.
d) Να υπολογίσει $s = r \cdot \prod_{j=1}^{k} s_j^{e_j} \bmod n$.
e) Η υπογραφή της Alice για το μήνυμα m είναι η (e,s).

2) Επαλήθευση. Για να επαληθεύσει ο Bob ότι η υπογραφή της Alice είναι η (e,s), θα πρέπει να κάνει τα ακόλουθα:
a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice $(\upsilon_1, \upsilon_2,...,\upsilon_k)$ και το n.
b) Να υπολογίσει το $w = s^2 \cdot \prod_{j=1}^{k} \upsilon^{e_j} \bmod n$.
c) Να υπολογίσει $e' = h(m||w)$.
d) Να αποδεχθεί την υπογραφή αν και μόνο αν $e = e'$.

Απόδειξη ότι ο αλγόριθμος επαλήθευσης λειτουργεί:

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

Παράδειγμα (με τεχνηέντως μικρές παραμέτρους)
Αλγόριθμος-Παραγωγή κλειδιού για το σχήμα υπογραφής Feige-Fiat-Shamir
Περίληψη: Κάθε εμπλεκόμενος δημιουργεί ένα δημόσιο και ένα ιδιωτικό κλειδί. Η Alice κάνει τα ακόλουθα:

1) Διαλέγει δύο τυχαίους διακριτούς πρώτους αριθμούς p = 3571, q = 4532 και υπολογίζει τον ακέραιο $n = pq = 16151633$.
2) Επιλέγει έναν θετικό ακέραιο $k = 5$ και διακριτούς ακεραίους $s_1, s_2, ..., s_5 \in \mathbb{Z}_n^*$.
3) Υπολογίζει $\upsilon_j = s_j^{-2} \bmod n$, $1 \le j \le 5$.

j	1	2	3	4	5
s_j	42	73	85	101	150
$s_j^{-1} \bmod n$	4999315	885021	6270634	13113207	11090788
$\upsilon_j = s_j^{-2} \bmod n$	503594	4879739	7104483	1409171	6965302

4) Το δημόσιο κλειδί της Alice είναι το $(\upsilon_1, \upsilon_2,..., \upsilon_5)$ και το modulus n. Το ιδιωτικό κλειδί της Alice είναι το $(s_1, s_2 ,..., s_5)$.

Αλγόριθμος-Παραγωγή και επαλήθευση του σχήματος υπογραφής Feige-Fiat-Shamir
Έστω συνάρτηση κατακερματισμού $h : \{0,1\}^* \to \{0,1\}^5$.

1) Παραγωγή υπογραφής. Η Alice κάνει τα ακόλουθα:
a) Επιλέγει ένα τυχαίο ακέραιο $r = 23181$, με $1 \le r \le n-1$.
b) Υπολογίζει $u = r^2 \bmod n = 4354872$.
c) Υπολογίζει $e = (e_1, e_2,..., e_5) = h(m||u) = 10110$, όπου κάθε $e_i \in \{0,1\}$ (η τιμή αυτή είναι τυχαία επιλεγμένη για το παράδειγμα).
d) Υπολογίζει $s = r\, s_1\, s_3\, s_4 \bmod n = (23181)(42)(85)(101) \bmod n = 7978909$.
e) Η υπογραφή της Alice για το μήνυμα m είναι η (e,s).

2) Επαλήθευση. Για να επαληθεύσει ο Bob ότι η υπογραφή της Alice είναι η (e,s), κάνει τα ακόλουθα:
a) Αποκτά το αυθεντικό δημόσιο κλειδί της Alice $(\upsilon_1, \upsilon_2,...,\upsilon_5)$ και το n.
b) Υπολογίζει το $w = s^2 \upsilon_1 \upsilon_3 \upsilon_4 \bmod n = 4354872$.
c) Υπολογίζει $e' = h(m||w) = h(m||u) = e$.
d) Αποδέχεται την υπογραφή αφού $e = e'$.

Σημείωση: Με το σχήμα υπογραφής RSA και modulus με μήκος t = 768, η παραγωγή μιας υπογραφής με απλοϊκές τεχνικές είναι 1152 modular πολλαπλασιασμούς κατά μέσο όρο (δηλαδή, 768 τετραγωνισμούς και 384 πολλαπλασιασμούς). Ενώ με το σχήμα υπογραφής Feige-Fiat-Shamir η παραγωγή της υπογραφής απαιτεί k/2 modular πολλαπλασιασμούς κατά μέσο όρο. Αν η υπογραφή του μηνύματος γίνεται με βάση το σχήμα Feige-Fiat-Shamir το modulus με μήκος t = 768 και k = 128 απαιτεί 64 modular πολλαπλασιασμούς κατά μέσο όρο. Αυτό σημαίνει ότι χρειάζεται 6% λιγότερους πολλαπλασιασμούς σε σχέση με μια απλοϊκή εφαρμογή του RSA. Όμως στο σχήμα υπογραφής Feige-Fiat-Shamir για την επαλήθευση της υπογραφής απαιτούνται 64 modular πολλαπλασιασμοί, ενώ στο RSA σχήμα μόλις ένας modular πολλαπλασιασμός, αν η δημόσια παράμετρος e ισούται με 3. Σαν συμπέρασμα των παραπάνω το σχήμα υπογραφών Feige-Fiat-Shamir είναι προτιμότερο σε σχέση με το RSA να χρησιμοποιείται σε εφαρμογές όπου η παραγωγή της υπογραφής πρέπει να γίνει γρήγορα και ο χώρος αποθήκευσης του κλειδιού είναι απεριόριστος.

6.1.1 **Ασφάλεια**

1) Μια διαφορά της υπογραφής Feige-Fiat-Shamir με το σχήμα υπογραφής RSA είναι ότι το modulus n μπορεί να είναι γνωστό σε όλους τους εμπλεκόμενους με αυτή την διαδικασία. Σε αυτήν την περίπτωση, ένα έμπιστο τρίτο πρόσωπο (trusted third party-TTP) επιλέγει τους δύο διακριτούς πρώτους αριθμούς p και q καθώς και το δημόσιο και ιδιωτικό κλειδί του κάθε χρήστη.
2) Η ασφάλεια του σχήματος στηρίζεται στην δυσκολία υπολογισμού τετραγωνικών ριζών modulo n. Έχει αποδειχθεί ότι είναι ασφαλές σε προσαρμόσιμη επίθεση με επιλεγμένο μήνυμα, αν υποθέσουμε ότι το πρόβλημα της παραγοντοποίησης είναι αξεπέραστο, η συνάρτηση κατακερματισμού είναι μια τυχαία συνάρτηση και ότι τα s_i είναι διαφορετικά ανά δύο.

Η πιθανότητα επιτυχούς πλαστογράφησης είναι μικρή και στην καλύτερη περίπτωση είναι 2^{kt}. Για να ελαχιστοποιηθεί περισσότερο αυτή η πιθανότητα πλαστογράφησης (μια στο ένα εκατομμύριο) θα πρέπει να γίνει η επιλογή των παραμέτρων k και t, έτσι ώστε το γινόμενο kt να ισούται με 20.

6.1.2 **Επιλογή παραμέτρων**

Αν το n είναι ένας ακέραιος με μήκος t-bit, τότε το ιδιωτικό κλειδί όπως περιγράφεται στον παραπάνω αλγόριθμο έχει μέγεθος kt bits. Αν θέλουμε να μειώσουμε το μήκος αυτό μπορούμε να επιλέξουμε τα s_j, για $1 \le j \le k$ έτσι ώστε το μέγεθος τους να είναι t' < t. Βέβαια η επιλογή των t' πρέπει να γίνει προσεκτικά, δεν θα πρέπει να είναι πολύ μικροί αριθμοί, ώστε να είναι αδύνατο κάποιος να μπορεί να μαντέψει τα s_j. Το δημόσιο κλειδί σε αυτό το σχήμα υπογραφής έχει (k+1)t bits μέγεθος.

6.1.3 **Παραλλαγές του σχήματος υπογραφής Feige-Fiat-Shamir**

Εξατομικευμένο σχήμα υπογραφής Feige-Fiat-Shamir

Ο αλγόριθμος που έχει δοθεί παραπάνω μπορεί να τροποποιηθεί και να γίνει εξατομικευμένο. Ας υποθέσουμε ότι υπάρχει ένα έμπιστο τρίτο πρόσωπο (TTP) το οποίο έχει κατασκευάσει τα p και q καθώς και το modulus n. Το modulus n είναι κοινό για όλους τους εμπλεκόμενους με την υπογραφή. Η συμβολοσειρά σε bit I_A της Alice παραθέτει πληροφορίες σχετικά με την ταυτότητα της. Το έμπιστο τρίτο πρόσωπο υπολογίζει το εξής

$\upsilon_j = f(I^A \| j)$, με j τέτοιο ώστε $1 \le j \le k$ και f: $\{0,1\}^* \rightarrow Q_n$ μια μονόδρομη συνάρτηση κατακερματισμού. Η αναπαράσταση του j είναι στο δυαδικό σύστημα και υπολογίζει την τετραγωνική ρίζα s_j του υ_j modulo n, με j τέτοιο ώστε $1 \le j \le k$. Σε αυτήν την περίπτωση το δημόσιο κλειδί της Alice είναι η πληροφορία για την ταυτότητα της I_A, ενώ το ιδιωτικό κλειδί της είναι το (s_1, s_2,..., s_k). Το δημόσιο κλειδί έχει μεταφερθεί με ασφάλεια και μυστικότητα από το έμπιστο τρίτο πρόσωπο στην Alice. Οι συναρτήσεις f, h και το modulus n είναι παράμετροι καθολικής εφαρμογής.
Αυτή η τροποποίηση έχει το εξής πλεονέκτημα: το δημόσιο κλειδί I_A είναι μικρότερο από το δημόσιο κλειδί που παράγεται από τον αλγόριθμο που περιγράφηκε παραπάνω, το οποίο οδηγεί στην μείωση του κόστους αποθήκευσης και μετάδοσης. Όμως έχει το μειονέκτημα ότι είναι πιο ευάλωτο σε επιθέσεις σχήμα υπογραφής, διότι το ιδιωτικό κλειδί είναι γνωστό στο έμπιστο τρίτο πρόσωπο και το modulus n είναι καθολικής εφαρμογής.

Παραλλαγή μικρού πρώτου του σχήματος υπογραφής Feige-Fiat-Shamir

Η παραλλαγή αυτή έχει σαν στόχο την μείωση του μεγέθους του δημοσίου κλειδιού και την αύξηση της αποδοτικότητας του αλγόριθμου επαλήθευσης της υπογραφής. Η διαφορά του σχήματος αυτού με το παραπάνω είναι ότι η Alice παράγει μόνη της το modulus n_A και ένα σύνολο με k μικρούς πρώτους αριθμούς: $\upsilon_1, \upsilon_2, \ldots, \upsilon_k \in Q_n$. Για την παρουσίαση αυτών των μικρών πρώτων απαιτούνται περίπου 2 bytes. Το ιδιωτικό κλειδί της Alice το επιλέγει η ίδια και είναι μια από τις τετραγωνικές ρίζες s_j του υ_j^{-1} modulo n για κάθε j, με j τέτοιο ώστε $1 \le j \le k$. Το δημόσιο κλειδί της Alice αποτελείται από το n_A και τους πρώτους αριθμούς $\upsilon_1, \upsilon_2, \ldots, \upsilon_k$. Συνεπώς η επαλήθευση των υπογραφών γίνεται πιο αποδοτική, μιας και όλοι γίνονται πιο γρήγορα, αφού χρησιμοποιούνται μικρότεροι αριθμοί.

6.2 **Σχήμα υπογραφής GQ**

Όπως και στο σχήμα Feige-Fiat-Shamir έτσι και το σχήμα υπογραφής Guillou-Quisquater παράγεται από το αντίστοιχο πρωτόκολλο αναγνώρισης. Η μετατροπή του πρωτοκόλλου σε ψηφιακή υπογραφή έχει περιγραφεί παραπάνω και ειδικότερα αν η πρόκληση (challenge) αντικατασταθεί με μια μονόδρομη συνάρτηση κατακερματισμού. Αυτή η συνάρτηση κατακερματισμού έχει πεδίο ορισμού το $\{0,1\}^*$ και πεδίο τιμών το $\mathbb{Z}_n$, όπου n είναι θετικός ακέραιος.

Αλγόριθμος-Παραγωγή κλειδιού για το σχήμα υπογραφής GQ
Περίληψη: Κάθε χρήστης παράγει ένα δημόσιο κλειδί (n,e,J_A) και το αντίστοιχο ιδιωτικό κλειδί α. Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να επιλέξει δύο τυχαίους διακριτούς πρώτους αριθμούς p και q, να τους κρατήσει μυστικούς και να υπολογίσει το n = pq.
2) Να επιλέξει ένα ακέραιο $e \in \{1,2,...,n-1\}$ τέτοιο ώστε ο ΜΚΔ(e,(p-1)(q-1))=1.
3) Να επιλέξει έναν ακέραιο J_A, $1 < J_A < n$ με ΜΚΔ(J_A,n) = 1. Αυτός ο ακέραιος παίζει ρόλο αναγνωριστή της Alice.
4) Να ορίσει ένα $\alpha \in \mathbb{Z}_n$ τέτοιο ώστε $J_A \alpha^e \equiv 1 \pmod n$ ακολουθώντας την εξής διαδικασία:
   a) Να υπολογίσει $J_A^{-1} \bmod n$.
   b) Να υπολογίσει $d_1 = e^{-1} \bmod (p-1)$ και $d_2 = e^{-1} \bmod (q-1)$.
   c) Να υπολογίσει $\alpha_1 = (J_A^{-1})^{d_1} \bmod p$ και $\alpha_2 = (J_A^{-1})^{d_2} \bmod q$.
   d) Να βρει μια ταυτόχρονη λύση για τις εξισώσεις $\alpha \equiv \alpha_1 \pmod p$, $\alpha \equiv \alpha_2 \pmod q$.

5) Το δημόσιο κλειδί της Alice είναι το (n,e,J_A), ενώ το ιδιωτικό κλειδί της Alice είναι το α.

Σημείωση: Η δυαδική αναπαράσταση του ακεραίου J_A μπορεί να χρησιμοποιηθεί για την εκχώρηση πληροφοριών σχετικές με την Alice, όπως είναι το όνομα, η διεύθυνση,η ηλικία κ.τ.λ.)

Αλγόριθμος-Παραγωγή και Επαλήθευση του σχήματος υπογραφής GQ
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m πεπερασμένου μήκους. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να επιλέξει ένα τυχαίο ακέραιο k και να υπολογίσει το $r = k^e \bmod n$.
   b) Να υπολογίσει $l = h(m||r)$.
   c) Να υπολογίσει $s = k\alpha^l \bmod n$.
   d) Η υπογραφή της Alice για το μήνυμα m είναι το ζευγάρι (s,l).
2) Επαλήθευση. Ο Bob για να επαληθεύσει ότι η υπογραφή της Alice (s,l) στο μήνυμα m είναι αυθεντική, πρέπει να κάνει τα ακόλουθα:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice (n,e,J_A).
   b) Να υπολογίσει το $u = s^e J_A^{\,l} \bmod n$ και $l' = h(m||u)$.
   c) Να αποδεχτεί την υπογραφή αν και μόνο αν $l=l'$.

Απόδειξη ότι ο αλγόριθμος επαλήθευσης λειτουργεί:
Αν παρατηρήσουμε ότι:
$u \equiv s^e J_A^{\,l} \equiv (k\alpha^l)^e J_A^{\,l} \equiv k^e (\alpha^e J_A)^l \equiv k^e \equiv r \pmod n$. Αυτό συνεπάγεται ότι $u = r$ και άρα $l = l'$.

Παράδειγμα (με τεχνηέντως μικρές παραμέτρους)
Αλγόριθμος-Παραγωγή κλειδιού για το σχήμα υπογραφής GQ
Περίληψη: Κάθε χρήστης παράγει ένα δημόσιο κλειδί (n,e,J_A) και το αντίστοιχο ιδιωτικό κλειδί α. Η Alice πρέπει κάνει τα ακόλουθα:

1) Επιλέγει δύο τυχαίους διακριτούς μυστικούς πρώτους αριθμούς $p = 20849$ και $q = 27457$. Υπολογίζει το $n = pq = 572450993$.
2) Επιλέγει ακέραιο $e = 47$.
3) Επιλέγει ακέραιο $J_A = 1091522$.
4) Ορίζει ένα $\alpha \in \mathbb{Z}_n$ τέτοιο ώστε $J_A\alpha^e \equiv 1 \pmod n$ οπότε $\alpha = 214611724$.
5) Το δημόσιο κλειδί της Alice είναι το (n,e,J_A), ενώ το ιδιωτικό κλειδί της Alice είναι το α.

Αλγόριθμος-Παραγωγή και Επαλήθευση του σχήματος υπογραφής GQ
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα $m = 1101110001$ πεπερασμένου μήκους. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1) Παραγωγή υπογραφής. Η Alice πρέπει κάνει τα ακόλουθα:
   a) Επιλέγει ένα τυχαίο ακέραιο $k = 42134$ και υπολογίζει το $r = k^e \bmod n = 297543350$.
   b) Υπολογίζει $l = h(m||r) = 2713833$ (επιλέγουμε μια τυχαία συνάρτηση κατακερματισμού χάριν του παραδείγματος).
   c) Υπολογίζει $s = k\alpha^t \bmod n = 42134 \cdot 214611724^{2713833} \bmod n = 252000854$.
   d) Η υπογραφή της Alice για το μήνυμα m είναι το ζευγάρι (s,l).
2) Επαλήθευση. Ο Bob για να επαληθεύσει ότι η υπογραφή της Alice (s,l) στο μήνυμα m είναι αυθεντική, κάνει τα ακόλουθα:
   a) Αποκτά το αυθεντικό δημόσιο κλειδί της Alice (n,e,J_A).
   b) Υπολογίζει πρώτα το $s^e \bmod n = 252000854^{47} \bmod n = 398641962$, μετά υπολογίζει $J_A^{\,l} \bmod n = 1091522^{2713833} \bmod n = 110523867$ και τελικά

$u = s^e J_A^l \bmod n = 297543350$.

c) Αποδεχέται την υπογραφή μιας και u=r, l' = h(m||u) = h(m||r) = l.

6.2.1 **Ασφάλεια**

Για να είναι ασφαλές το σχήμα υπογραφής GQ η παράμετρος e πρέπει να είναι αρκετά μεγάλη ώστε να αποκλειστεί η πιθανότητα πλαστογραφίας βασισμένη στο παράδοξο των γενεθλίων. Η εν λόγω επίθεση μπορεί να περιγραφεί ως εξής: Ο αντίπαλος μπορεί να επιλέξει ένα μήνυμα m και να υπολογίσει το l = h(m||J_A^t) για αρκετές τιμές του t μέχρι να βρεθεί ένα l που να ταυτίζεται t (mod e). Αυτό μπορεί να επιτευχθεί μέσα σε O($\sqrt{e}$) προσπάθειες. Όταν ο αντίπαλος καταφέρει να βρει ένα τέτοιο ζεύγος (l,t) επιλέγει έναν ακέραιο x με την έξης ιδιότητα t = xe+l και υπολογίσει s = J_A^x mod n. Όμως τότε έχουμε:

$s^e J_A^t \equiv (J_A^x)^e J_A^l \equiv J_A^{xe+l} \equiv J_A^t \pmod n$

και συνεπώς ισχύει h(m|| J_A^t) = l. Αυτό έχει ως αποτέλεσμα η (s,l) να είναι μια έγκυρη πλαστογραφημένη υπογραφή για το μήνυμα m.

6.2.2 **Παράμετροι**

Το modulus n θα πρέπει να έχει μέγεθος τουλάχιστον 768 bits ώστε να είναι δύσκολη η παραγοντοποίηση ενός ακεραίου. Όπως αναφέρθηκε και προηγουμένως το e θα πρέπει να είναι αρκετά μεγάλο τουλάχιστον 128 bits. Για να μην είναι ευάλωτη σε επιθέσεις η συνάρτηση κατακερματισμού πρέπει να έχει είσοδο 128 ή 160 bits. Με τις τιμές του modulus και του e όπως αναφέρθηκαν, το δημόσιο κλειδί του σχήματος υπογραφής GQ έχει 896+u bits μέγεθος, όπου u είναι αριθμός των bits που χρειάζεται για την αναπαράσταση του J_A και το ιδιωτικό κλειδί α έχει μήκος 768 bits.

6.2.3 **Χαρακτηριστικά επιδόσεων για υπογραφές GQ**

Χρησιμοποιώντας modulus n των 768-bit, e 128-bit και συνάρτηση κατακερματισμού με έξοδο l των 128-bit, η παραγωγή της υπογραφής απαιτεί κατά μέσο όρο 384 modular πολλαπλασιασμούς. Το ίδιο περίπου απαιτεί και η επαλήθευση της υπογραφής. Το σχήμα υπογραφής GQ μπορεί να απαιτεί περισσότερους πολλαπλασιασμούς σε σχέση με το Feige-Fiat-Shamir αλλά χρησιμοποιεί σημαντικά λιγότερο αποθηκευτικό χώρο για το κλειδί.
GQ σχήμα υπογραφής με παράρτημα

Ο αλγόριθμος που έχει αναλυθεί παραπάνω μπορεί να τροποποιηθεί ώστε να έχει δυνατότητα ανάκτησης μηνύματος. Αν $M_S = \mathbb{Z}_n$ είναι ο χώρος υπογραφών και το $m \in M_S$.

1) Παραγωγή συνάρτησης.
   a) Επιλογή ενός τυχαίου k τέτοιο ώστε ΜΚΔ(k,n)=1.
   b) Υπολογισμός του $r = k^e \bmod n$ και $l = mr \bmod n$.
   c) Η υπογραφή είναι η $s = k\,\alpha^l \bmod n$.
2) Επαλήθευση συνάρτησης.
   $s^e J_A^l \equiv k^e \alpha^{el} J_A^l \equiv k^e \equiv r \pmod n$
3) Ανάκτηση μηνύματος m. Η ανάκτηση του μηνύματος m γίνεται μέσω του υπολογισμού $lr^{-1} \bmod n$.

Σημείωση: Για να αποφευχθεί μια υπαρξιακή επίθεση, όπως και σε όλα τα σχήματα ψηφιακών υπογραφών, πρέπει να επιλεχτεί μια κατάλληλα επιλεγμένη συνάρτηση πλεονασμού R.

7 Το DSA και σχετικά σχήματα υπογραφών

Οι μέθοδοι που θα περιγραφούν σε αυτό το κεφάλαιο είναι τυχαιοποιημένα σχήματα ψηφιακών υπογραφών. Επίσης όλες οι μέθοδοι που παρουσιάζονται είναι ψηφιακές υπογραφές με παράρτημα και όπως έχει αναφερθεί μπορούν να μετατραπούν σε σχήματα ψηφιακών υπογραφών με ικανότητα ανάκτησης μηνύματος.

7.1 Αλγόριθμος ψηφιακής υπογραφής (Digital Signature Algorithm-DSA)

Ο αλγόριθμος ψηφιακής υπογραφής είναι ένα ομοσπονδιακό (αμερικανικό) πρότυπο επεξεργασίας πληροφορίας (FIPS). Προτάθηκε από το εθνικό ινστιτούτο προτύπων και τεχνολογίας (NIST) τον Αύγουστο 1991, από τον David W. Kravitz, για να χρησιμοποιηθεί για το πρότυπο ψηφιακής υπογραφής (Digital Signature Standard – DSS). Μια μικρή αλλαγή πραγματοποιήθηκε το 1996 (FIPS 186-1) και το πρότυπο επεκτάθηκε περισσότερο το 2000 (FIPS 186-2) και το 2009 (FIPS 186-3).

Το σχήμα υπογραφής DSA επιβεβαιώνει την ακεραιότητα υπογεγραμμένων δεδομένων και την ταυτότητα του υπογράφοντα. Το DSA μπορεί ακόμα να χρησιμοποιηθεί ώστε ένα τρίτο πρόσωπο να επιβεβαιώσει ότι ένα έγγραφο έχει υπογραφεί από αυτόν που παρήγαγε την υπογραφή. Το DSA βρίσκει εφαρμογές στο ηλεκτρονικό ταχυδρομείο, στην αποθήκευση δεδομένων, στην ανταλλαγή ηλεκτρονικών δεδομένων, στην μεταφορά ηλεκτρονικών χρημάτων και γενικά σε εφαρμογές που απαιτούν την διασφάλιση της ακεραιότητας δεδομένων και την απόδειξη της αυθεντικότητας τους.

Ο Smid και ο Branstad αναφέρουν ότι το DSA επιλέχθηκε για πολλούς σημαντικούς λόγους: το επίπεδο της ασφάλειας που προσφέρει, μπορεί να χρησιμοποιηθεί σε πολλές εφαρμογές και η ευκολία να χρησιμοποιηθεί και εκτός ΗΠΑ. Ακόμα η επιρροή του σχήματος είναι εμφανής στην εθνική ασφάλεια και στην εφαρμογή του νόμου. Τέλος, η αποδοτικότητα του σε ένα πλήθος κυβερνητικών και εμπορικών εφαρμογών.

Το σχήμα ψηφιακής υπογραφής απαιτεί μια συνάρτηση κατακερματισμού $h : \{0,1\}^* \rightarrow \mathbb{Z}_q$ για κάποιο ακέραιο q (το DSS προτείνει την χρήση του SHA-1).

Αλγόριθμος-Παραγωγή κλειδιού για το DSA
Περίληψη: Η Alice δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό.
Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να επιλέξει έναν πρώτο αριθμό q τέτοιο ώστε $2^{159} < q < 2^{160}$.
2) Να επιλέξει έναν αριθμό t τέτοιο ώστε $0 \le t \le 8$, έναν πρώτο αριθμό p για τον οποίο να ισχύει $2^{511+64t} < p < 2^{512+64t}$ και ο αριθμός q να διαιρεί τον (p-1).
3) Να επιλέξει έναν γεννήτορα a της κυκλικής ομάδας τάξεως q της $\mathbb{Z}_p^*$. Με τον εξής τρόπο:
   a) Να επιλέξει ένα στοιχείο $g \in \mathbb{Z}_p^*$ και να υπολογίσει $a = g^{(p-1)/q} \bmod p$.
   b) Αν a = 1 τότε πηγαίνει στο βήμα 3.a.
4) Να επιλέξει ένα τυχαίο ακέραιο α τέτοιο ώστε να ανήκει στο διάστημα [1,q-1].
5) Να υπολογίσει $y = a^{\alpha} \bmod p$.
6) Το δημόσιο κλειδί της Alice είναι το (p,q,a,y) και το ιδιωτικό κλειδί της το α.

Αλγόριθμος-Παραγωγή και επαλήθευση της υπογραφής DSA

Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m πεπερασμένου μήκους. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1. Παραγωγή συνάρτησης. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να επιλέξει ένα τυχαίο ακέραιο k, $0 < k < q$ και να το κρατήσει μυστικό.
   b) Να υπολογίσει $r = (a^k \bmod p) \bmod q$.
   c) Να υπολογίσει $k^{-1} \bmod q$.
   d) Να επιλέξει $s = k^{-1} \{h(m)+\alpha r\} \bmod q$.
   e) Η υπογραφή της Alice για το μήνυμα m είναι το ζεύγος (r,s).
2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή της Alice, πρέπει να κάνει τα ακόλουθα:
   d) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice (p,q,a,y).
   e) Να επαληθεύσει ότι $0 < r < q$ και $0 < s < q$, αν δεν ισχύουν οι ανισότητες να απορρίψει την υπογραφή.
   f) Να υπολογίσει $w = s^{-1} \bmod q$ και h(m).
   g) Να υπολογίσει $u_1 = w \cdot h(m) \bmod q$ και $u_2 = rw \bmod q$.
   h) Να υπολογίσει $\upsilon = \left(a^{u_1} y^{u_2} \bmod p\right) \bmod q$.
   i) Να αποδεχθεί την υπογραφή αν και μόνο αν $\upsilon = r$.

Απόδειξη ότι ο αλγόριθμος επαλήθευσης λειτουργεί:
Έστω ότι η γνήσια υπογραφή της Alice είναι η (r,s) για το μήνυμα m. Για να επαληθευτεί αυτό πρέπει να ισχύει $h(m) \equiv -\alpha r + ks \pmod q$. Έτσι πολλαπλασιάζοντας και τις δύο μεριές της ταυτότητας με w και αναδιατάσσοντας τους όρους έχουμε $w \cdot h(m) + \alpha wr \equiv k \pmod q$. Το όποιο είναι ίδιο με $u_1 + \alpha u_2 \equiv k \pmod q$. Υψώνοντας και τις δύο πλευρές της ταυτότητας με a έχουμε $\left(a^{u_1} y^{u_2} \bmod p\right) \bmod q = (a^k \bmod p) \bmod q$. Το οποίο συνεπάγεται $\upsilon = r$ το οποίο είναι και το ζητούμενο.

Παράδειγμα (με τεχνηέντως μικρές παραμέτρους):
Αλγόριθμος-Παραγωγή κλειδιού για το DSA
Περίληψη: Η Alice δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό.
Η Alice κάνει τα ακόλουθα:

1) Επιλέγει έναν πρώτο αριθμό q = 17389.
2) Επιλέγει έναν πρώτο αριθμό p = 124540019, έτσι ώστε ο q να διαιρεί τον (p-1) και για το συγκεκριμένο παράδειγμα (p-1)/q = 7162.
3) Επιλέγει ένα στοιχείο $g \in \mathbb{Z}_p^*$ g =110217528 και υπολογίζει $a = g^{7162} \bmod p$ = 10083255. Αφού $a \neq 1$:
4) Επιλέγει ένα τυχαίο ακέραιο α = 12496.
5) Υπολογίζει $y = a^\alpha \bmod p = 10083255^{12496} \bmod 124540019 = 119946265$.
6) Το δημόσιο κλειδί της Alice είναι το (p,q,a,y) και το ιδιωτικό κλειδί της το α.

Αλγόριθμος-Παραγωγή και επαλήθευση της υπογραφής DSA
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m πεπερασμένου μήκους. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1. Παραγωγή συνάρτησης. Η Alice κάνει τα ακόλουθα:
   a) Επιλέγει ένα τυχαίο ακέραιο k = 9557.
   b) Υπολογίζει $r = (a^k \bmod p) \bmod q = (10083255^{9557} \bmod 124540019) \bmod 17389 = 34$.
   c) Υπολογίζει $k^{-1} \bmod q = 7631$.
   d) Έστω για το παράδειγμα h(m) = 5246 $s = k^{-1} \{h(m)+\alpha r\} \bmod q = (7631) \{5246+(12496)(34)\} \bmod q = 13049$.
   e) Η υπογραφή της Alice για το μήνυμα m είναι το ζεύγος (r = 34,s = 13049).
2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή της Alice, κάνει τα ακόλουθα:
   a) Αποκτά το αυθεντικό δημόσιο κλειδί της Alice (p,q,a,y).

b) Επαληθεύει ότι $0 < r < q$ και $0 < s < q$.
c) Υπολογίζει $w = s^{-1} \bmod q = 1799$.
d) Υπολογίζει $u_1 = w \cdot h(m) \bmod q = (5246)(1799) \bmod 17389 = 12716$, ακόμα $u_2 = rw \bmod q = (34)(1799) \bmod 17389 = 8999$.
e) Υπολογίζει $v = (a^{u_1} y^{u_2} \bmod p) \bmod q = (10083255^{12716}\ 119946265^{8999} \bmod 124540019) \bmod 17389 = 27039929 \bmod 17389 = 34$.
f) Αποδέχεται την υπογραφή αφού $v = r$.

7.1.1 **Ασφάλεια**

Η ασφάλεια του DSA βασίζεται στη δυσκολία του προβλήματος διακριτού λογαρίθμου μέσα σε ένα πεπερασμένο σώμα. Έρευνες πάνω στον αλγόριθμο έχουν δείξει την ύπαρξη πρώτων αριθμών οι οποίοι θα μπορούσαν να οδηγήσουν στη δημιουργία κλειδιών ευάλωτων σε επιθέσεις.

Για την ασφάλεια του DSA είναι ακόμα σημαντική η επιλογή της παραμέτρου k. Κάθε υπογραφή απαιτεί μια τυχαία διαφορετική τιμή του k. Ο αντίπαλος αν καταφέρει να αποκτήσει την τιμή k, που ο υπογράφον συστηματικά χρησιμοποιεί, μπορεί να ανακαλύψει το ιδιωτικό κλειδί και να πλαστογραφήσει την υπογραφή. Επιπλέον, αν καταφέρει να αποσπάσει δύο μηνύματα υπογεγραμμένα με το ίδιο k, μπορεί να πλαστογραφήσει την υπογραφή χωρίς να γνωρίζει την τιμή της παραμέτρου.

7.1.2 **Επιλογή παραμέτρων**

Από τον αλγόριθμο που περιγράφηκε παραπάνω το μήκος του πρώτου αριθμού q είναι σταθερός με 160 bits. Το μήκος του p μπορεί να είναι οποιαδήποτε πολλαπλάσιο του 64 μεταξύ 521 και 1024 bits. Ένας πρώτος αριθμός p μεγέθους 512 bits προστατεύει οριακά το σύστημα από μια ενδεχόμενη επίθεση. Για το μέγεθος του modulus έχει προταθεί από το 1996 να είναι τουλάχιστον 768 bits. Το πρότυπο FIPS 186 θεωρεί απαγορευτικό μέγεθος μεγαλύτερο του 1024 bits για τον πρώτο αριθμό p.

Σημειώσεις:
1) Ο αλγόριθμος ψηφιακής υπογραφής είναι μια ειδική περίπτωση του σχήματος υπογραφής el Gamal που θα περιγραφεί παρακάτω.
2) Οι πρώτοι αριθμοί p, q δεν είναι αναγκαίο να επιλεγούν κάθε φορά από τον υπογράφοντα. Βέβαια, έτσι η υπογραφή γίνεται πιο ευάλωτη σε επιθέσεις.
3) Όταν $s = 0$ παρουσιάζεται πρόβλημα στον αλγόριθμο επαλήθευσης μιας και δεν μπορούμε να υπολογίσουμε το s^{-1}. Οπότε θα πρέπει να ελέγχεται κάθε φορά αν $s \neq 0$. Αυτή η περίπτωση είναι σπάνια μιας και η πιθανότητα το $s = 0$ είναι $\left(\frac{1}{2}\right)^{160}$, αν το s είναι ένα τυχαίο στοιχείο του $\mathbb{Z}_q$. Μια άλλη παράμετρο που πρέπει να ελέγξει ο υπογράφον είναι το r. Αν το $r = 0$ ή το $s = 0$, θα πρέπει να επιλέξει μια άλλη τιμή για την παράμετρο k.
4) Σε αυτό το σχήμα η διαδικασία της υπογραφής είναι γρηγορότερη από την επαλήθευση της.

7.2 **Σχήμα υπογραφής el Gamal**

Το σχήμα υπογραφής el Gamal είναι ένα σχήμα ψηφιακής υπογραφής το οποίο βασίζεται στην δυσκολία του προβλήματος του διακριτού λογαρίθμου. Περιγράφτηκε από τον Taher el Gamal το 1984. Το σχήμα υπογραφής el Gamal δεν είναι ντετερμινιστικό (όπως και το κρυπτοσύστημα δημοσίου κλειδιού el Gamal). Αυτό συνεπάγεται ότι υπάρχουν πολλές έγκυρες υπογραφές για ένα δεδομένο μήνυμα και ότι ο αλγόριθμος επαλήθευσης θα πρέπει να δέχεται κάθε τέτοια υπογραφή ως έγκυρη. Παράγει ψηφιακές υπογραφές με παράρτημα για δυαδικά μηνύματα πεπερασμένου μήκους. Τέλος απαιτεί μια συνάρτηση κατακερματισμού h: $\{0,1\}^* \rightarrow \mathbb{Z}_p$, όπου το p είναι ένας μεγάλος πρώτος αριθμός.

Αλγόριθμος-Παραγωγή κλειδιού για το σχήμα υπογραφής el Gamal
Περίληψη: Κάθε χρήστης παράγει ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό.
Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να επιλέξει ένα μεγάλο τυχαίο πρώτο αριθμό p και έναν γεννήτορα a της πολλαπλασιαστικής ομάδας $\mathbb{Z}_p^*$.
2) Να επιλέξει ένα τυχαίο ακέραιο α, $1 \le \alpha \le p-2$.
3) Να υπολογίσει $y = a^{\alpha} \bmod p$.
4) Το δημόσιο κλειδί της Alice είναι το (p,a,y) και το ιδιωτικό της το α.

Αλγόριθμος-Παραγωγή και επαλήθευση του σχήματος υπογραφής el Gamal
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m πεπερασμένου μήκους. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να επιλέξει ένα τυχαίο μυστικό ακέραιο k, $1 \le k \le p-2$, με ΜΚΔ(k,p-1) = 1.
   b) Να υπολογίσει $r = a^k \bmod p$.
   c) Να υπολογίσει $k^{-1} \bmod (p-1)$.
   d) Να υπολογίσει $s = k^{-1} \{h(m) - \alpha r\} \bmod (p-1)$.
   e) Η υπογραφή της Alice για το m είναι το ζεύγος (r,s).
2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή της Alice (r,s) στο m, πρέπει να κάνει τα ακόλουθα:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice (p,a,y).
   b) Να επαληθεύσει ότι $1 \le r \le p-1$, αν δεν ισχύει η ανισότητα να απορρίψει την υπογραφή.
   c) Να υπολογίσει $\upsilon_1 = y^r r^s \bmod p$.
   d) Να υπολογίσει h(m) και $\upsilon_2 = a^{h(m)} \bmod p$.
   e) Να αποδεχθεί την υπογραφή αν και μόνο αν ισχύει $\upsilon_1 = \upsilon_2$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί:
Η αυθεντική υπογραφή της Alice είναι η $s = k^{-1} \{h(m) - \alpha r\} \bmod (p-1)$. Πολλαπλασιάζοντας και τις δύο μεριές της εξίσωσης με k έχουμε $sk = \{h(m) - \alpha r\} \bmod (p-1)$ από το οποίο συνεπάγεται ότι $h(m) = \alpha r + ks \pmod{(p-1)}$. Από αυτό συμπεραίνουμε ότι $a^{h(m)} \equiv a^{\alpha r+ks} \equiv (a^{\alpha})^r r^s \pmod p$. Τελικά έχουμε $\upsilon_1 = \upsilon_2$, οπότε η υπογραφή είναι έγκυρη.

Παράδειγμα (με τεχνηέντως μικρές παραμέτρους)
Αλγόριθμος-Παραγωγή κλειδιού για το σχήμα υπογραφής el Gamal
Περίληψη: Κάθε χρήστης παράγει ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό.
Η Alice κάνει τα ακόλουθα:

1) Επιλέγει ένα τυχαίο πρώτο αριθμό p = 2357 και έναν γεννήτορα a = 2 της πολλαπλασιαστικής ομάδας $\mathbb{Z}_{2357}^*$.
2) Επιλέγει ένα τυχαίο ακέραιο α = 1751.
3) Υπολογίζει $y = a^{\alpha} \bmod p = 2^{1751} \bmod 2357$.
4) Το δημόσιο κλειδί της Alice είναι το (p = 2357,a = 2,y =1185) και το ιδιωτικό της το

$\alpha = 1751$.

Αλγόριθμος-Παραγωγή και επαλήθευση του σχήματος υπογραφής el Gamal
Περίληψη: Η Alice υπογράφει ένα μήνυμα m (για ευκολία επιλέγουμε το μήνυμα να είναι ένας ακέραιος που ανήκει στο $\mathbb{Z}_p$, m = 1463). Η συνάρτηση κατακερματισμού είναι η ταυτοτική, δηλαδή h(m) = m. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1) Παραγωγή υπογραφής. Η Alice κάνει τα ακόλουθα:
   a) Επιλέγει ένα τυχαίο μυστικό ακέραιο k = 1529.
   b) Υπολογίζει $r = a^k \bmod p = 2^{1529} \bmod 2357 = 1490$.
   c) Υπολογίζει $k^{-1} \bmod (p-1) = 245$.
   d) Υπολογίζει $s = 245\ \{1463 - 1751 \cdot 1490\} \bmod 2356 = 1777$.
   e) Η υπογραφή της Alice για το m = 1436 είναι το ζεύγος (r = 1490,s = 1777).
2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή της Alice (r,s) στο m, κάνει τα ακόλουθα:
   a) Αποκτά το αυθεντικό δημόσιο κλειδί της Alice (p,a,y).
   b) Επαληθεύει ότι $1 \le r \le p-1$.
   c) Υπολογίζει $\upsilon_1 = y^r r^s \bmod p = 1185^{1490}\ 1490^{1777} \bmod 2357 = 1072$.
   d) Υπολογίζει $h(m) = 1463$ και $\upsilon_2 = a^{h(m)} \bmod p = 2^{1463} \bmod 2357 = 1072$.
   e) Αποδέχεται την υπογραφή αφού ισχύει $\upsilon_1 = \upsilon_2$.

7.2.1 **Ασφάλεια**

1) Ο αντίπαλος, για να πλαστογραφήσει μια υπογραφή, μπορεί να επιλέξει τυχαία έναν αριθμό k και να υπολογίσει $r = a^k \bmod p$ και $s = k^{-1}\{h(m) - \alpha r\} \bmod (p-1)$. Ο αντίπαλος το μόνο που μπορεί να κάνει είναι να επιλέξει μια τυχαία υπογραφή (r,s), το οποίο είναι εξαιρετικά απίθανο μιας και η πιθανότητα η πλαστογράφηση να είναι επιτυχής είναι $\frac{1}{p}$. Αυτή η ποσότητα είναι αμελητέα αν έχουμε κάνει σωστή επιλογή του p, ώστε να είναι αρκετά μεγάλος πρώτος αριθμός. Όλα τα παραπάνω ισχύουν αν υποθέσουμε ότι το πρόβλημα του διακριτού λογαρίθμου είναι δισεπίλητο.
2) Για κάθε μήνυμα που πρέπει να υπογραφεί χρειάζεται να χρησιμοποιηθεί διαφορετικό k, ώστε ο αντίπαλος να μην καταφέρει να αποκτήσει το ιδιωτικό κλειδί του υπογράφοντα. Αν χρησιμοποιηθεί το ίδιο k ώστε να υπογραφούν δύο διαφορετικά μηνύματα m_1, m_2 θα έχουμε: $s_1 = k^{-1}\{h(m_1) - \alpha r\} \bmod (p-1)$ και $s_2 = k^{-1}\{h(m_2) - \alpha r\} \bmod (p-1)$. Αφαιρώντας αυτές κατά μέλη $(s_1 - s_2)k = (h(m_1) - h(m_2)) (\bmod (p-1))$. Αν $s_1 - s_2 \neq 0 \ (\bmod (p-1))$, τότε $k = (s_1 - s_2)^{-1}(h(m_1) - h(m_2))(\bmod (p-1))$. Αφού ο αντίπαλος μπορεί να υπολογίσει το k, εύκολα να αποκτήσει και το ιδιωτικό κλειδί.
3) Οι υπογραφές el Gamal είναι επιρρεπείς στις επιθέσεις υπαρκτής πλαστογραφίας, αν δεν χρησιμοποιηθεί συνάρτηση κατακερματισμού, δηλαδή αν η εξίσωση της υπογραφής είναι $s = k^{-1}\{m - \alpha r\} \bmod (p-1)$. Τότε ο αντίπαλος μπορεί να επιλέξει οποιαδήποτε ζευγάρι ακεραίων (u,υ) με την ιδιότητα $ΜΚΔ(\upsilon, p-1) = 1$. Μετά υπολογίζει μια αυθεντική υπογραφή (r,s) από τις σχέσεις $r = a^u y^\upsilon \bmod p = a^{u+\alpha\upsilon}$ και $s = -r\upsilon^{-1} \bmod (p-1)$. Η υπογραφή αυτή είναι έγκυρη για το μήνυμα $m = su \bmod (p-1)$, μιας και $1/(a^m a^{-\alpha r})^s = a^u y^\upsilon = r$.
4) Σε ένα σημείο του αλγόριθμου επαλήθευσης πρέπει να ελεγχθεί κατά πόσο το r ικανοποιεί την ανισότητα $0 < r < p$. Αν παραληφθεί αυτός ο έλεγχος, αν ο αντίπαλος έχει στην κατοχή του μια υπογραφή της Alice μπορεί να υπογράψει μηνύματα της

δικής του επιλογής. Έστω λοιπόν, ότι έχει στην κατοχή του την υπογραφή (r,s) για το μήνυμα m. Μπορεί να διαλέξει ένα οποιοδήποτε μήνυμα m' και να υπολογίσει την τιμή κατακερματισμού και $u = h(m') \cdot (h(m))^{-1} \bmod (p-1)$, αν υποθέσουμε ότι υπάρχει η ποσότητα $(h(m))^{-1} \bmod (p-1)$. Μετά υπολογίζει $s' = su \bmod (p-1)$ και r' έτσι ώστε $r' = ru \pmod{p-1}$ και $r' = r \pmod{p}$. Το παραπάνω ισχύει αφού ισχύει το Κινεζικό Θεώρημα Υπολοίπων. Σε αυτήν την περίπτωση αν δεν υπάρχει ο έλεγχος που αναφέρθηκε το ζεύγος (r',s') γίνεται αποδεκτό από τον αλγόριθμο επαλήθευσης.

7.2.2 **Επιθέσεις βασισμένες στην επιλογή παραμέτρων**

1) Ο πρώτος αριθμός p θα πρέπει να είναι αρκετά μεγάλος ώστε να μην είναι δυνατή η λύση του προβλήματος του διακριτού λογαρίθμου.
2) Για τον ίδιο λόγο το p-1 θα πρέπει να διαιρείται με έναν πρώτο αριθμό q.
3) Για να αποφευχθεί μια επίθεση στο σχήμα υπογραφής el Gamal θα πρέπει να γίνει προσεκτικά η επιλογή του γεννήτορα της υποομάδας. Αν υποθέσουμε ότι $p \equiv 1 \pmod 4$ και γεννήτορας a. Ο a θα πρέπει να διαιρεί το (p-1) και να είναι δυνατός ο υπολογισμός λογαρίθμων στην υποομάδα S τάξεως a της $\mathbb{Z}_p^*$. Με αυτά σαν δεδομένα ο αντίπαλος μπορεί να πλαστογραφήσει μια υπογραφή χωρίς να γνωρίζει το ιδιωτικό κλειδί της Alice. Ο αλγόριθμος επαλήθευσης μπορεί να δεχτεί μια πλαστή υπογραφή ως αυθεντική αν ο αντίπαλος επιχειρήσει την ακόλουθη διαδικασία (υποθέτοντας ότι $p-1 = aq$). Αρχικά υπολογίζει $t – (p – 3)/2$ και θέτει $r = q$. Βρίσκει z με την ιδιότητα $a^{qz} \equiv y^q \pmod p$. Ο αντίπαλος μπορεί να βρει έναν τέτοιο αριθμό, διότι a^q και y^q είναι στοιχεία της ομάδας S και το a^p είναι γεννήτορας αυτής. Ύστερα υπολογίζει $s = t \cdot (h(m) - qz) \bmod (p-1)$. Το ζεύγος (r,s) είναι μια αυθεντική υπογραφή για ένα μήνυμα m.
   Ο αλγόριθμος επαλήθευσης αποδέχεται την υπογραφή επειδή ικανοποιείται η σχέση $r^s y^r \equiv a^{h(m)} \pmod p$. Κατ ' αρχάς, παρατηρούμε ότι $aq \equiv -1 \pmod p$, $a \equiv -q^{-1} \pmod p$ και $q^{(p-1)/2} \equiv -1 \pmod p$ (επειδή a είναι γεννήτορας της ομάδας και $q \equiv a^{-1} \pmod p$). Από τις ταυτότητες αυτές έχουμε $q \equiv q^{(p-1)/2} q^{-1} \equiv -q^{-1} \equiv a \pmod p$. Τελικά προκύπτει $r^s y^r \equiv (q^t)^{(h(m)-qz)}\ y^q \equiv a^{h(m)} a^{-qz} y^q \equiv a^{h(m)} y^{-q} y^q = a^{h(m)} \pmod p$. Για να αποτρέψουμε αυτού του είδους την επίθεση το a αρκεί να επιλεγεί ως γεννήτορας μιας υποομάδας της $\mathbb{Z}_p^*$ με τάξη έναν πρώτο αριθμό και όχι γεννήτορας της ίδιας της $\mathbb{Z}_p^*$.

7.2.3 **Επιλογή παραμέτρων**

Μια οριακή τιμή, για την ασφάλεια του σχήματος υπογραφής, για το μέγεθος του modulus p είναι 512 bits. Το 1996, προτάθηκε το ελάχιστο μέγεθος του modulus p να είναι 768 bits. Αν θέλουμε να εξασφαλίσουμε ότι η υπογραφή δεν θα δεχτεί επίθεση σε βάθος χρόνου το μέγεθος του modulus που πρέπει να επιλέξουμε είναι 1024 bits ή και μεγαλύτερο.

7.2.4 **Σύγκριση υπογραφών DSA-ElGamal**

Στο σχήμα υπογραφής DSA οι υπολογισμοί γίνονται modulo q και έτσι το μέγεθος της υπογραφής είναι πολύ μικρότερο από το αντίστοιχο της ElGamal. Έτσι αν υποθέσουμε ότι p είναι ένας πρώτος μεγέθους 768 bit, το ElGamal θα παράγει μια υπογραφή με μήκος 1536 bit. Ενώ το DSA θα σχηματίσει μια υπογραφή μεγέθους 320 bit.

7.2.5 **Παραλλαγές του σχήματος υπογραφής ElGamal**

Υπάρχουν διάφορες παραλλαγές του σχήματος υπογραφής ElGamal που βασίζονται στην αλλαγή της εξίσωσης υπογραφής. Έτσι έχουμε τον παρακάτω πίνακα που περιγράφει αυτές τις παραλλαγές.

u	υ	w	Εξίσωση υπογραφής	Επαλήθευση
h(m)	r	s	$h(m)=\alpha r+ks$	$a^{h(m)}=(a^{\alpha})^r$
h(m)	s	r	$h(m)=\alpha r+ks$	$a^{h(m)}=(a^{\alpha})^s r^r$
s	r	h(m)	$s=\alpha r+kh(m)$	$a^s=(a^{\alpha})^r r^{h(m)}$
s	h(m)	r	$s=\alpha h(m)+kr$	$a^s=(a^{\alpha})^{h(m)}r^r$
r	s	h(m)	$r=\alpha s+kh(m)$	$a^r=(a^{\alpha})^s r^{h(m)}$
r	h(m)	s	$r=\alpha h(m)+ks$	$a^r=(a^{\alpha})^{h(m)}r^s$

Άλλη παραλλαγή του σχήματος ElGamal είναι το γενικευμένο σχήμα υπογραφής ElGamal. Το σχήμα που παρουσιάστηκε αρχικά βασιζόταν στην πολλαπλασιαστική ομάδα $\mathbb{Z}_p^*$, μπορεί να μετατραπεί σε σχήμα που χρησιμοποιεί κάθε πεπερασμένη αβελιανή ομάδα.

7.3 **Σχήμα ψηφιακής υπογραφής Schnorr**

Το σχήμα υπογραφής Schnorr προτάθηκε από τον Claus Schnorr και προέρχεται από το αντίστοιχο πρωτόκολλο αναγνώρισης και είναι μια παραλλαγή του σχήματος υπογραφής ElGamal. Οι υπολογισμοί σε αυτή την μέθοδο πραγματοποιούνται στην κυκλική υποομάδα $\mathbb{Z}_p^*$ τάξης q, όπου p είναι ένας μεγάλος πρώτος αριθμός. Η συνάρτηση κατακερματισμού που χρησιμοποιείται στο σχήμα υπογραφής είναι $h:\{0,1\}^* \rightarrow \mathbb{Z}_q$. Ο αλγόριθμος παραγωγής κλειδιού είναι παρόμοιος με αυτόν του DSA. Η διαφορά είναι ότι δεν υπάρχουν περιορισμοί στο μέγεθος των αριθμών p και q.

Αλγόριθμος-Παραγωγής και επαλήθευσης του σχήματος ψηφιακής υπογραφής Schnorr
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m πεπερασμένου μήκους. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να επιλέξει έναν τυχαίο μυστικό ακέραιο k, $1 \le k \le q-1$.
   b) Να υπολογίσει $r = a^k \bmod p$, $e=h(m||r)$ και $s = \alpha e + k \bmod q$.
   c) Η υπογραφή της Alice για το μήνυμα m είναι το ζεύγος (s,e).
2) Επαλήθευση .Ο Bob για να επαληθεύσει, ότι η υπογραφή της Alice είναι η (s,e) για το m, πρέπει να κάνει τα ακόλουθα:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί (p,q,a,y).
   b) Να υπολογίσει $\upsilon = a^s y^{-e} \bmod p$ και $e' = h(m||\upsilon)$.
   c) Να αποδεχτεί την υπογραφή αν και μόνο αν $e' = e$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί:
Η υπογραφή θα είναι της Alice αν $\upsilon \equiv a^s y^{-e} \equiv a^s a^{-\alpha e} \equiv a^k \equiv r \pmod p$, οπότε $h(m||\upsilon) = h(m||r)$ και $e' = e$ (υπενθύμιση: $y = a^{\alpha} \bmod p$).

Παράδειγμα (με τεχνηέντως μικρές παραμέτρους):

Αλγόριθμος-Παραγωγή κλειδιού για το Schnorr
Περίληψη: Η Alice δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό.
Η Alice κάνει τα ακόλουθα:

1) Επιλέγει έναν πρώτο αριθμό q = 541.
2) Επιλέγει έναν πρώτο αριθμό p = 129841, έτσι ώστε ο q να διαιρεί τον (p-1) και για το συγκεκριμένο παράδειγμα (p-1)/q = 240.
3) Επιλέγει ένα στοιχείο $g \in \mathbb{Z}_p^*$ g = 26346 και υπολογίζει a = 26346^{240} mod p = 26. Αφού a ≠ 1:
4) Επιλέγει ένα τυχαίο ακέραιο α = 423.
5) Υπολογίζει y = a^{α} mod p = 26^{423} mod p = 115917.
6) Το δημόσιο κλειδί της Alice είναι το (p,q,a,y) και το ιδιωτικό κλειδί της το α.

Αλγόριθμος-Παραγωγής και επαλήθευσης του σχήματος ψηφιακής υπογραφής Schnorr
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m = 11101101. Ο Bob επαληθεύει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1) Παραγωγή υπογραφής. Η Alice πρέπει κάνει τα ακόλουθα:
   a) Επιλέγει έναν τυχαίο μυστικό ακέραιο k = 327, $1 \le k \le 540$.
   b) Να υπολογίσει r = a^k mod p = 26^{327} mod p = 49375, e = h(m||r) = 155 (η επιλογή της συνάρτησης κατακερματισμού είναι για το συγκεκριμένο παράδειγμα) και s = αe + kmod q = $423 \cdot 155 + 327$ mod 541 = 431.
   c) Η υπογραφή της Alice για το μήνυμα m είναι το ζεύγος (s = 431,e = 155).
2) Επαλήθευση .Ο Bob για να επαληθεύσει, ότι η υπογραφή της Alice είναι η (s,e) για το m, πρέπει κάνει τα ακόλουθα:
   a) Αποκτά το αυθεντικό δημόσιο κλειδί (p,q,a,y).
   b) Υπολογίζει υ = $a^s y^{-e}$ mod p = $26^{431} \cdot 115917^{-155}$ mod p και e' = h(m||υ) = 155.
   c) Αποδέχεται την υπογραφή μιας και e' = e.

Σημειώση: Χρησιμοποιώντας την υποομάδα τάξεως q δεν βελτιώνει κατά πολύ την υπολογιστική αποδοτικότητα του σχήματος υπογραφής σε σχέση με το ElGamal. Όμως παρέχει υπογραφές μικρότερες σε μέγεθος.

7.4 **Το σχήμα υπογραφής ElGamal με ικανότητα ανάκτησης κειμένου**

Το πλεονέκτημα με τα σχήματα υπογραφών που χρησιμοποιούν ανάκτηση μηνύματος είναι ότι είναι κατάλληλα για επικοινωνίες που απαιτούν μικρότερο εύρος ζώνης για το υπογεγραμμένο μήνυμα. Το σχήμα υπογραφής Nyberg-Rueppel είναι ένα τροποποιημένο σχήμα ElGamal, το οποίο υποστηρίζει ανάκτηση μηνύματος.

Σε αυτό το σχήμα υπογραφής, ο χώρος των υπογραφών είναι $M_S = \mathbb{Z}_p^*$ και ο χώρος όλων των υπογραφών ο $S = \mathbb{Z}_p \times \mathbb{Z}_q$, όπου p, q είναι πρώτοι αριθμοί και το q διαιρεί το (p-1). Η συνάρτηση πλεονασμού είναι η R: M→MS. Τέλος, όπως και στην υπογραφή Schnorr, ο αλγόριθμος για την παραγωγή του κλειδιού είναι ο ίδιος με τον DSA. Η μόνη διαφορά είναι ότι δεν υπάρχουν περιορισμοί στο μέγεθος του p και q.

Αλγόριθμος-Παραγωγή και επαλήθευση του σχήματος υπογραφής Nyberg-Rueppel
Περίληψη: Η Alice υπογράφει ένα μήνυμα $m \in M$. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice και να ανακτήσει το μήνυμα m από την υπογραφή.

0) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει $\tilde{m} = R(m)$.
   b) Να επιλέξει ένα τυχαίο μυστικό ακέραιο k, $1 \le k \le q-1$, και να υπολογίσει r = a^{-k} mod p.
   c) Να υπολογίσει e = $\tilde{m}$ r mod p.

d) Να υπολογίσει $s = \alpha e + k \bmod q$.
e) Η υπογραφή της Alice για το μήνυμα m είναι το ζεύγος (e,s).

2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή της Alice πρέπει να κάνει τα ακόλουθα:
a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice (p,q,α,y).
b) Να επαληθεύσει ότι $0 < e < p$, αν δεν ισχύει η ανισότητα να απορρίψει την υπογραφή.
c) Να επαληθεύσει ότι $0 \leq s < q$, αν δεν ισχύει η ανισότητα να απορρίψει την υπογραφή.
d) Να υπολογίσει $\upsilon = a^s y^{-e} \bmod p$ και $\tilde{m} = \upsilon e \bmod p$.
e) Να επαληθεύσει ότι $\tilde{m} \in M_R$, αν δεν ισχύει αυτό να απορρίψει την υπογραφή.
f) Να ανακτήσει μέσω της υπογραφής το μήνυμα $m = R^{-1}(\tilde{m})$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί:
Αν η Alice δημιουργήσει μια υπογραφή, τότε $\upsilon \equiv a^s y^{-e} \equiv a^{s-\alpha e} \equiv a^k \pmod p$. Οπότε $\upsilon e \equiv a^k \tilde{m} a^{-k} \equiv \tilde{m} \pmod p$, δηλαδή το ζητούμενο.

Παράδειγμα (με τεχνηέντως μικρές παραμέτρους):
Αλγόριθμος-Παραγωγή κλειδιού για το σχήμα υπογραφής Nyberg-Rueppel
Περίληψη: Η Alice δημιουργεί ένα δημόσιο κλειδί και το αντίστοιχο ιδιωτικό.
Η Alice κάνει τα ακόλουθα:

1) Επιλέγει έναν πρώτο αριθμό $q = 3571$.
2) Επιλέγει έναν πρώτο αριθμό $p = 1256993$, έτσι ώστε ο q να διαιρεί τον (p-1) και για το συγκεκριμένο παράδειγμα $(p-1)/q = 352$.
3) Επιλέγει ένα στοιχείο $g \in \mathbb{Z}_p^*$ $g = 42077$ και υπολογίζει $a = 42077^{352} \bmod p = 441238$. Αφού $a \neq 1$:
4) Επιλέγει ένα τυχαίο ακέραιο $\alpha = 2774$.
5) Υπολογίζει $y = a^{\alpha} \bmod p = 1013657$.
6) Το δημόσιο κλειδί της Alice είναι το (p,q,a,y) και το ιδιωτικό κλειδί της το α.

Αλγόριθμος-Παραγωγή και επαλήθευση του σχήματος υπογραφής Nyberg-Rueppel
Περίληψη: Η Alice υπογράφει ένα μήνυμα $m \in M$. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice και να ανακτήσει το μήνυμα m από την υπογραφή.

1) Παραγωγή υπογραφής. Η Alice κάνει τα ακόλουθα:
a) Υπολογίζει $\tilde{m} = R(m) = 1147892$ (η τιμή αυτή είναι για το παράδειγμα).
b) Επιλέγει ένα τυχαίο μυστικό ακέραιο $k = 1001$ και υπολογίζει $r = a^{-k} \bmod p = 441238^{-1001} \bmod p = 1188935$.
c) Υπολογίζει $e = \tilde{m} r \bmod p = 138207$.
d) Υπολογίζει $s = \alpha e + k \bmod q = (2774)(138207) + 1001 \bmod q = 1088$.
e) Η υπογραφή της Alice για το μήνυμα m είναι το ζεύγος (e,s).

2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή της Alice κάνει τα ακόλουθα:
a) Αποκτά το αυθεντικό δημόσιο κλειδί της Alice (p,q,α,y).
b) Επαληθεύει ότι $0 < e < p$.
c) Επαληθεύει ότι $0 \leq s < q$.
d) Υπολογίζει $\upsilon = a^s y^{-e} \bmod p = 441238^{1088}\ 1013657^{-138207} \bmod 1256993 = 504308$ και $\tilde{m} = \upsilon e \bmod p = 1147892$.
e) Επαληθεύει ότι $\tilde{m} \in M_R$.
f) Ανακτά μέσω της υπογραφής το μήνυμα $m = R(\tilde{m})^{-1}$.

7.4.1 **Ασφάλεια**

1) Επειδή το σχήμα αυτό είναι μια παραλλαγή του σχήματος υπογραφής ElGamal τα ίδια που ισχύουν για αυτό ισχύουν και για το Nyberg-Rueppel. Ακόμα, όπως και στο DSA η ασφάλεια του βασίζεται σε δύο διαφορετικά προβλήματα διακριτού λογαρίθμου.
2) Το σχήμα αυτό είναι ευάλωτο σε επιθέσεις στις οποίες ο αντίπαλος μπορεί να αντικαταστήσει το δημόσιο κλειδί της Alice με ένα πλαστό. Έτσι σε αυτό το σχήμα πρέπει να γίνει καλή επιλογή της συνάρτησης πλεονασμού. Κάποιοι υποστηρίζουν ότι αυτό δεν είναι αναγκαίο. Βέβαια, όταν ο αντίπαλος έχει στην κατοχή του μια έγκυρη υπογραφή για ένα μήνυμα δεν είναι δύσκολο να τροποποιήσει την δοσμένη υπογραφή για να κατασκευάσει μια πλαστή υπογραφή για ένα γνωστό μήνυμα.
3) Ένας άλλος λόγος που πρέπει να γίνει προσεκτική η επιλογή της συνάρτησης πλεονασμού ώστε να μην είναι δυνατή μια υπαρξιακή επίθεση. Η επίθεση που μπορεί να πραγματοποιηθεί είναι η ακόλουθη. Έστω ότι $m \in M$, $\tilde{m} = R(m)$ και η υπογραφή για το m είναι η (e,s). Για ένα τυχαίο επιλεγμένο ακέραιο k, $e = \tilde{m}\, a^{-k} \bmod p$ και $s = ae + k$. Αν υποθέσουμε ότι $\tilde{m}^* = \tilde{m}\, a^l \bmod p$, για κάποιο ακέραιο l. Έστω τώρα ότι $s^* = s + l \bmod q$ και $\tilde{m}^* \in M_R$. Σε αυτήν την περίπτωση η (e, s^*) είναι μια αυθεντική υπογραφή για το μήνυμα $m^* = R^{-1}(\tilde{m}^*)$. Αυτό το συμπέρασμα εξάγεται από τον αλγόριθμο επαλήθευσης $v \equiv a^{s^*} y^{-e} \equiv a^{s+l} a^{-\alpha e} \equiv a^{k+l} \pmod p$ και $ve \equiv a^{k+l}\, \tilde{m}\, a^{-k} \equiv \tilde{m}\, a^l \equiv \tilde{m}^* \pmod p$. Αφού $\tilde{m}^* \in M_R$, η πλαστή υπογραφή (e, s^*) θα γίνει αποδεχτή από τον αλγόριθμο επαλήθευσης ως έγκυρη υπογραφή για το μήνυμα m^*.
4) Ένα σημείο που είναι σημαντικό στον αλγόριθμο επαλήθευσης είναι ο έλεγχος για το αν ισχύει η ανισότητα $0 < e < p$. Αν υποθέσουμε ότι η υπογραφή της Alice είναι η (e,s) για το μήνυμα m. Τότε $e = \tilde{m}^r \bmod p$ και $s = \alpha e + k \bmod q$. Ο αντίπαλος μπορεί να υπολογίσει την υπογραφή για ένα μήνυμα της δικής του επιλογής $\tilde{m}^*$. Με την βοήθεια του Κινεζικού θεωρήματος υπολοίπων, μπορεί να υπολογίσει $e^* \equiv \tilde{m}^{*r} \pmod p$ και $e^* \equiv e \pmod q$. Αν $0 < e^* < p$ η υπογραφή (e^*, s) είναι αποδεκτή από τον αλγόριθμο επαλήθευσης.

8 Υπογραφές μιας χρήσης

Οι ψηφιακές υπογραφές μιας χρήσης είναι γνωστές εδώ και τουλάχιστον δύο δεκαετίες και έχουν μελετηθεί κυρίως για την θεωρητική τους αξία. Αυτά τα σχήματα υπογραφών επιτρέπουν την υπογραφή ενός μόνο μηνύματος. Το πλεονέκτημα τους είναι ότι είναι σχετικά γρήγορες. Βέβαια, αυτά τα σχήματα τείνουν να είναι δυσκίνητα όταν είναι να υπογραφούν πολλά μηνύματα, γιατί τα επιπλέον δεδομένα απαιτούν υπογραφή και επαλήθευση τους για κάθε μήνυμα. Σε αντίθεση, με τα συνηθισμένα σχήματα ψηφιακής υπογραφής όπως το RSA, το ίδιο κλειδί μπορεί να χρησιμοποιηθεί για την υπογραφή πολλαπλών μηνυμάτων. Οι δημόσιες πληροφορίες που είναι αναγκαίες για την επαλήθευση υπογραφών μιας χρήσης αναφέρονται σαν παράμετροι επικύρωσης. Τα σχήματα υπογραφών μιας χρήσης βρίσκουν εφαρμογή σε έξυπνες κάρτες που δεν χρειάζονται υψηλή υπολογιστική πολυπλοκότητα.

8.1 Ψηφιακή υπογραφή μιας χρήσης Rabin

Η ψηφιακή υπογραφή μιας χρήσης Rabin είναι ένα από τα πρώτα σχήματα αυτού του είδους. Στο σχήμα αυτό για να πραγματοποιηθεί η επαλήθευση χρειάζεται την συνεισφορά του υπογράφοντα και αυτού που θέλει να επαληθεύσει την υπογραφή. Όπως και κάθε σχήμα ψηφιακής υπογραφής αυτού του είδους επιτρέπει την υπογραφή ενός μόνο μηνύματος. Η διαφορά με άλλα σχήματα είναι ότι ο αλγόριθμος επαλήθευσης μπορεί να πραγματοποιηθεί μονάχα μία φορά.

Χρήσιμα σύμβολα:

- M_0 : 0^l είναι η συμβολοσειρά από 0 μήκους l.
- $M_0(i)$: $0^{l-e}||b_{e-1}...b_1b_0$ όπου τα b_i είναι η δυαδική αναπαράσταση του i.
- K : ένα σύνολο των συμβολοσειρών με l-bit μέγεθος.
- E : ένα σύνολο μετασχηματισμών κρυπτογράφησης.
- E_t : ένας μετασχηματισμός κρυπτογράφησης στον E με $t \in K$. Το E_t απεικονίζει συμβολοσειρές των l-bit σε συμβολοσειρές των l-bit.
- h : μια μονόδρομη συνάρτηση κατακερματισμού με πεδίο ορισμού $\{0,1\}^*$ και πεδίο τιμών $\{0,1\}^l$ και είναι δημόσια γνωστή.
- n : ένα σταθερός θετικός αριθμός και είναι μια παράμετρος ασφαλείας.

Αλγόριθμος-Παραγωγή κλειδιού ψηφιακής υπογραφής μιας χρήσης Rabin
Περίληψη: Η Alice επιλέγει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού E, παράγει 2n τυχαίες συμβολοσειρές και ένα σύνολο παραμέτρων επικύρωσης.
Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να επιλέξει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού E.
2) Να παράγει 2n τυχαίες μυστικές συμβολοσειρές $k_1, k_2, ..., k_{2n} \in K$, η κάθε μια με μέγεθος l-bit.
3) Να υπολογίσει $y_i = E_{k_i}(M_0(i)),\ 1 \le i \le 2n$.
4) Το δημόσιο κλειδί της Alice είναι $(y_1,y_2,...,y_{2n})$ και το ιδιωτικό κλειδί της $(k_1,k_2,...,k_{2n})$.

Αλγόριθμος-Παραγωγή και επαλήθευση της ψηφιακής υπογραφής μιας χρήσης Rabin
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m πεπερασμένου μήκους. Η επαλήθευση υπογραφών γίνεται με την συνεργασία της Alice.

1) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει h(m).
   b) Να υπολογίσει $s_i = E_{k_i}(h(m)),\ 1 \le i \le 2n$.
   c) Η υπογραφή της Alice για το m είναι $(s_1,s_2,...,s_{2n})$.
2) Επαλήθευση. Ο Bob για να επαληθεύσει ότι η υπογραφή της Alice είναι η $(s_1,s_2,...,s_{2n})$ για το m, πρέπει να κάνει τα ακόλουθα:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice $(y_1,y_2,...,y_{2n})$.
   b) Να υπολογίσει την h(m).
   c) Να επιλέξει n διακριτούς αριθμούς r_j, $1 \le r_j \le 2n$, για $1 \le j \le n$.
   d) Να ζητήσει από την Alice τα κλειδιά k_{r_j} , $1 \le j \le n$.
   e) Να επαληθεύσει την αυθεντικότητα των κλειδιών αυτών υπολογίζοντας $z_j = E_{k_{r_j}}(M_0(r_j))$ και να ελέγξει ότι $z_j = y_{r_j}$, για κάθε $1 \le j \le n$.
   f) Να επαληθεύσει ότι $s_{r_j} = E_{k_{r_j}}(h(m)), 1 \le j \le n$.

Σημείωση: Το μέγεθος των κλειδιών σε αυτό το σχήμα εξαρτάται από το E_t το οποίο δίνει ως έξοδο l-bit. Οπότε το δημόσιο και ιδιωτικό κλειδί αποτελείται από 2nl bits το κάθε ένα. Έτσι για παράδειγμα αν n = 80 και l =64, τα κλειδιά που θα παραχθούν θα έχουν μήκος 1280 bytes το κάθε ένα.

8.1.1 **Ασφάλεια**

Στο σχήμα ψηφιακής υπογραφής Rabin μιας χρήσης μπορεί να προκύψουν κάποιες αντιδικίες μεταξύ της Alice και του Bob. Οι αντιδικίες αυτές εμφανίζονται όταν η Alice θεωρήσει ότι πλαστογραφήθηκε η υπογραφή της, ενώ ο Bob θεωρεί ότι είναι αυθεντική. Για την επίλυση αυτού, εμπλέκεται ένα τρίτο έμπιστο πρόσωπο και πραγματοποιείται η παρακάτω διαδικασία:

1) Ο Bob δίνει το μήνυμα m και την υπογραφή της Alice $(s_1,s_2,...,s_{2n})$ σε ένα τρίτο έμπιστο πρόσωπο (TTP).
2) Ο TTP αποκτά τα $k_1,k_2,...,k_{2n}$ από την Alice.
3) Ο TTP επαληθεύει την αυθεντικότητα του ιδιωτικού κλειδιού υπολογίζοντας $z_i = E_{k_i}(M_0(i))$ και ελέγχει αν $y_i = z_i$, $1 \le i \le 2n$. Αν αυτός ο έλεγχος αποτύχει, ο TTP ενημερώνει τον Bob ότι η υπογραφή είναι έγκυρη και τον δικαιώνει.
4) Ο TTP υπολογίζει $u_i = E_{k_i}(h(m)), 1 \le i \le 2n$. Μετά ελέγχει αν $u_i = s_i$ για το πολύ n τιμές του i και ενημερώνει την Alice ότι η υπογραφή της έχει πλαστογραφηθεί και την δικαιώνει. Αν για n+1 ή και για περισσότερες τιμές του i προκύπτει $u_i = s_i$, η υπογραφή θεωρείται αυθεντική και ο TTP δικαιώνει τον Bob.

Η διαδικασία αυτή βασίζεται στον εξής συλλογισμό. Η Alice μπορεί να δημιουργήσει μια υπογραφή και για κάποιον λόγο στο μέλλον να αμφισβητήσει την αυθεντικότητα της. Τότε θα πρέπει να διασφαλίσει ότι $u_i = s_i$ για ακριβώς n τιμές του i και να ευελπιστεί ότι ο Bob θα επιλέξει ακριβώς αυτές τις τιμές (αυτό συμβαίνει με πολύ μικρή πιθανότητα). Από την πλευρά του Bob, άμα προσπαθήσει να διαπράξει αυτός πλαστογραφία για ένα μήνυμα m', θα πρέπει να δημιουργήσει τουλάχιστον ένα παραπάνω κλειδί k'. Δημιουργεί αυτό το κλειδί έτσι ώστε τουλάχιστον n+1 τιμές του i να προκύψει $u_i = s_i$. Ένας άλλος τρόπος για να επιτύχει τον σκοπό του μπορεί να προσδιορίσει κατάλληλο m' για το οποίο ισχύει h(m) = h(m'). Για να αποτραπεί αυτή η απάτη θα πρέπει να επιλεγεί προσεκτικά ο αλγόριθμος παραγωγής συμμετρικού κλειδιού και η συνάρτηση κατακερματισμού.

8.2 **Το σχήμα ψηφιακών υπογραφών μιας χρήσης Merkle**

Το σχήμα ψηφιακών υπογραφών μιας χρήσης Merkle αναπτύχθηκε από τον Ralph Merkle στα τέλη της δεκαετίας του 70. Το πλεονέκτημα αυτού του σχήματος είναι ότι θεωρείται ασφαλής σε επιθέσεις από κβαντικούς υπολογιστές. Οι παραδοσιακοί αλγόριθμοι δημοσίου κλειδιού, όπως το RSA και ElGamal θα ήταν ευάλωτα σε επιθέσεις από ένα κβαντικό υπολογιστή, αν μπορούσε να κατασκευαστεί κατάλληλα. Το σχήμα ψηφιακών υπογραφών μιας χρήσης Merkle βασίζεται στην ύπαρξη μιας ασφαλούς συνάρτησης κατακερματισμού, πράγμα που το καθιστά ανθεκτικό σε επιθέσεις με κβαντικό υπολογιστή.

Σε αντίθεση με το σχήμα Rabin, που μόλις περιγράφηκε, ο αλγόριθμος επαλήθευσης δεν χρειάζεται την συνεισφορά του υπογράφοντα. Εδώ, η επαλήθευση της διαδικασίας ανατίθεται στο TTP ή σε κάποιο άλλο έμπιστο μέσο.

Αλγόριθμος-Παραγωγής κλειδιού για το σχήμα ψηφιακών υπογραφών μιας χρήσης Merkle
Περίληψη: Η Alice για να υπογράψει ένα μήνυμα μεγέθους n bit, παράγει $t = n + \lfloor logn \rfloor + 1$ παραμέτρους επικύρωσης.
Η Alice θα πρέπει να κάνει τα ακόλουθα:

1) Να επιλέξει t τυχαίες μυστικές συμβολοσειρές $k_1,k_2,...,k_t$ η κάθε μια με μήκος l bit.
2) Να υπολογίσει $\upsilon_i = h(k_i)$, για $1 \le i \le t$. Η συνάρτηση κατακερματισμού θα πρέπει να επιλεγεί έτσι ώστε να έχει αντίσταση ορίσματος και $h: \{0,1\}^* \rightarrow \{0,1\}^l$.
3) Το δημόσιο κλειδί της Alice είναι το $(\upsilon_1,\upsilon_2,...,\upsilon_t)$ και το ιδιωτικό της το $(k_1,k_2,...,k_t)$.

Για την υπογραφή ενός μηνύματος σε αυτό το σχήμα πρέπει να σχηματίσουμε μια συμβολοσειρά w= m||c. Το c ορίζεται ως η δυαδική αναπαράσταση για τον αριθμό των 0 σε ένα μήνυμα m. Επίσης, το c θα πρέπει να επιλεχτεί ώστε να έχει μήκος $\lfloor \log n \rfloor + 1$. Άρα το w έχει μήκος ίσο με t.

Αλγόριθμος-Παραγωγή και επαλήθευση του σχήματος ψηφιακών υπογραφών μιας χρήσης Merkle
Περίληψη: Η Alice υπογράφει ένα δυαδικό μήνυμα m με μήκος n bit. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1) Παραγωγή υπογραφής. Η Alice θα πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει το c, δηλαδή την δυαδική αναπαράσταση του αριθμού των μηδενικών του μηνύματος .
   b) Να σχηματίσει $w = m||c = (\alpha_1\alpha_2...\alpha_t)$.
   c) Να προσδιορίσει τις θέσεις $i_1 < i_2 < ... < i_u$ στο w για τις οποίες ισχύει $\alpha_{i_j} = 1$, $1 \le j \le u$.
   d) Έστω $s_j = k_{i_j}, 1 \le j \le u$.
   e) Η υπογραφή της Alice για το m είναι η $(s_1,s_2,...,s_u)$.
2) Επαλήθευση. Ο Bob για να επαληθεύσει την υπογραφή της Alice $(s_1,s_2,...,s_u)$ για το μήνυμα m:
   a) Να αποκτήσει το δημόσιο κλειδί της Alice $(\upsilon_1,\upsilon_2,...,\upsilon_t)$.
   b) Να υπολογίσει το c.
   c) Να σχηματίσει $w = m||c = (\alpha_1\alpha_2...\alpha_t)$.
   d) Να προσδιορίσει τις θέσεις $i_1 < i_2 < ... < i_u$ στο w για τις οποίες ισχύει $\alpha_{i_j} = 1$,

$1 \le j \le u$.

e) Να αποδεχτεί αν και μόνο αν $\upsilon_{i_j} = h(s_j)$ για κάθε $1 \le j \le u$.

8.2.1 **Ασφάλεια**

Τα δεδομένα είναι το μήνυμα m, η συμβολοσειρά w = m||c, η υπογραφή για το m $(s_1,s_2,...,s_u)$ και η συνάρτηση κατακερματισμού h με αντίσταση ορίσματος. Επειδή η συνάρτηση κατακερματισμού έχει επιλεγεί κατά αυτόν τον τρόπο, συμπεραίνουμε ότι δεν μπορεί να πλαστογραφηθεί μια υπογραφή για m' ≠ m. Αν υποθέσουμε ότι w' = m'||c', όπου c' είναι η δυαδική αναπαράσταση του αριθμού των 0 για το μήνυμα m'. Ο αντίπαλος έχει στην κατοχή του την υπογραφή $(s_1,s_2,...,s_u)$ η οποία αποτελείται από τα στοιχεία του ιδιωτικού κλειδιού που αντιστοιχούν στις θέσεις των μονάδων του w. Για να σχηματίσει μια υπογραφή για το μήνυμα m' πρέπει να δηλώσει τις θέσεις των μονάδων στο w'. Το m', όμως περιέχεται στο w' θα πρέπει οι θέσεις των μονάδων στο m' να είναι υποσύνολο των θέσεων των μονάδων στο m. Σε άλλη περίπτωση θα χρειαζόταν να γνωρίζει επιπλέον στοιχεία του ιδιωτικού κλειδιού. Άρα το m' θα είχε περισσότερα μηδενικά από το m, με άλλα λόγια c' > c. Αυτό έχει σαν συνέπεια ότι ο c' ως μεγαλύτερος αριθμός από των c θα περιλαμβάνει το ψηφίο 1 σε τουλάχιστον μια θέση που ο c έχει 0 στην δυαδική τους αναπαράσταση. Όμως το c' περιέχεται στο w'. Συνεπώς ο αντίπαλος χρειάζεται ένα στοιχείο του ιδιωτικού κλειδιού, το οποίο αντιστοιχεί στην θέση αυτή, αλλά ο υπογράφον δεν του έχει αποκαλύψει.

8.2.2 **Χρήσιμα στοιχεία**

Για την αποθήκευση του δημοσίου και ιδιωτικού κλειδιού, για ένα μήνυμα m με μήκος n bit το οποίο έχει k μονάδες, απαιτούνται $l \cdot (n + \lfloor \log n \rfloor + 1)$ bits αντίστοιχα. Η υπογραφή καταλαμβάνει $l \cdot (k + k')$ bits του αποθηκευτικού χώρου, όπου το k' είναι αριθμός των μονάδων στην δυαδική αναπαράσταση του n-k. Για παράδειγμα, αν n = 128, l = 64 και k = 72, τότε το δημόσιο και το ιδιωτικό κλειδί απαιτούν 8704bits και η ψηφιακή υπογραφή 4800bits.

Για να ελαττωθεί σημαντικά το μήκος τα k_i σχηματίζονται από μια μοναδική seed value (όταν κάποιος θέλει να παράγει τυχαίους αριθμούς, το seed value είναι η αρχική τιμή που ξεκινάει και επεκτείνεται η διαδικασία). Έτσι για παράδειγμα, αν k' είναι μια συμβολοσείρα με μήκος τουλάχιστον l bits τότε τα $k_i = h(k'||i)$, για $1 \le i \le t$.

Για την παραγωγή της υπογραφής δεν χρειάζονται υπολογισμοί, όποτε είναι πολύ γρήγορη. Η επαλήθευση της υπογραφής χρειάζεται τον υπολογισμό της συνάρτησης κατακερματισμού h για λιγότερες από $n + \lfloor \log n \rfloor + 1$ τιμές.

Βελτίωση αποδοτικότητας

Όπως αναφέρθηκε και παραπάνω για την αποθήκευση του δημόσιου και ιδιωτικού κλειδιού απαιτούνται $l \cdot (n + \lfloor \log n \rfloor + 1)$ bits για το κάθε ένα. Το δημόσιο κλειδί είναι αναγκαίο να είναι τόσο μεγάλο γιατί ο αλγόριθμος επαλήθευσης εξετάζει μεμονωμένα bits του μηνύματος. Έτσι, θα μπορούσε να βελτιωθεί ο αλγόριθμος υπογραφής αν κάθε φορά εξέταζε παραπάνω του ενός bit την φορά. Αυτό μπορεί να γίνει ακολουθώντας την παρακάτω διαδικασία.

Αλγόριθμος-Παραγωγή κλειδιού και υπογραφή για το τροποποιημένο σχήμα υπογραφών μιας χρήσης Merkle

Περίληψη:Έστω ότι η Alice επιθυμεί να υπογράψει ένα μήνυμα m μήκους kt bits. Τότε το m θα μπορούσε να αναπαρασταθεί με τον εξής τρόπο $m = m_1||m_2||...||m_t$, όπου κάθε m_i έχει μήκος k bits και αναπαριστούν έναν ακέραιο μεταξύ 0 και 2^k-1. Πρέπει να κάνει τα ακόλουθα:

1) Να ορίσει $U=\sum_{i=1}^{t}(2^k-1)\le t2^k$. Το U μπορεί να αναπαρασταθεί με $\log U\le\lfloor \log t\rfloor+1+k$ bits. Το U μπορεί να αναπαρασταθεί δυαδικά ως $U = u_1||u_2||...||u_3$ όπου κάθε u_i έχει μήκος k bits, αν το $r=\lceil(\lfloor \log t\rfloor+1+k)/k\rceil$.
2) Να σχηματίσει μια συμβολοσειρά $w = m_1||m_2||...m_t||u_1||u_2||...||u_r$.
3) Να παράγει t+r τυχαίους ακέραιους αριθμούς $k_1,k_2,...,k_{t+r}$ και να υπολογίσει $\upsilon_i=h^{2^k-1}(k_i),1\le i\le t$ και $s_i=h^{u_i}(k_{t+i}),1\le i\le r$.
4) Το δημόσιο κλειδί της Alice είναι το $(k_1,k_2,...,k_{t+r})$ και το ιδιωτικό της το $(\upsilon_1,\upsilon_2,...,\upsilon_{t+r})$.
5) Η υπογραφή της Alice για το μήνυμα m είναι η $(s_1,s_2,...,s_{t+r})$, όπου $s_i = h^{m_i}(k_i)$, $1\le i\le t$ και $s_i = h^{u_i}(k_{t+i})$, $1\le i\le r$.

Σημειώσεις:

i. Το h^c είναι η c-πλή σύνθεση της h με τον εαυτό της.
ii. Τα επιπλέον bit που προστίθενται σε αυτό το σχήμα παίζουν τον ρόλο ενός αθροίσματος ελέγχου (check-sum). Δοθέντος ενός στοιχείου $s_i = h^a(k_j)$, ένας αντίπαλος μπορεί εύκολα να υπολογίσει την τιμή $h^{a+\delta}(k_j)$ για $0 \le \delta \le 2^k - a$, όμως δεν είναι ικανός να υπολογίσει την τιμή $h^{a-\delta}$, για οποιοδήποτε $\delta > 0$, αν η h είναι μια μονόδρομη συνάρτηση κατακερματισμού. Για να πλαστογραφήσει μια υπογραφή σε ένα νέο μήνυμα, το μόνο που μπορεί να κάνει ο αντίπαλος είναι να ελαττώσει την τιμή του αθροίσματος ελέγχου, το οποίο θα καταστήσει αδύνατο για αυτόν, τον υπολογισμό των απαιτούμενων τιμών κατακερματισμού στα προσαρτημένα kr bit.

Παράδειγμα

Αλγόριθμος-Παραγωγή κλειδιού και υπογραφής για το τροποποιημένο σχήμα υπογραφών μιας χρήσης Merkle

Περίληψη:Η Alice υπογράφει ένα μήνυμα $m = m_1||m_2||m_3||m_4$, όπου $m_1 = 1011$, $m_2 = 0111$, $m_3 = 1010$, $m_4 = 1101$ και είναι οι δυαδικές αναπαραστάσεις του 11, 7, 10 και 13 αντίστοιχα. Κάνει τα ακόλουθα:

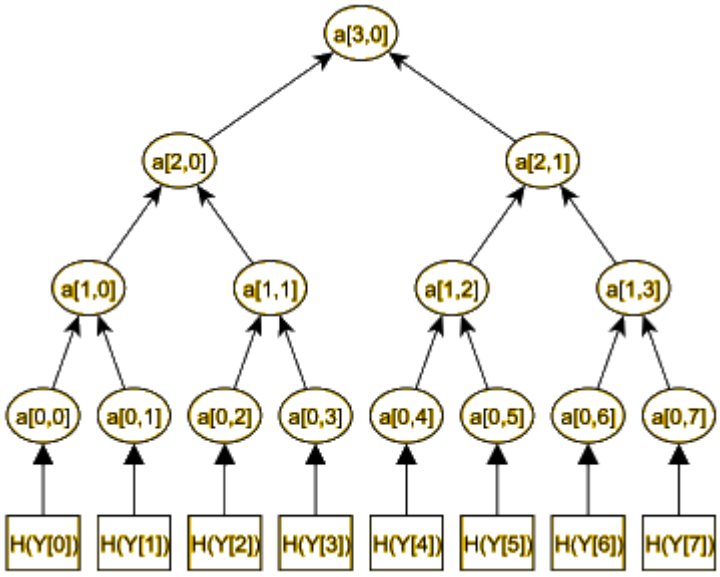
1) Ορίζει $U = (16-m_1)+(16-m_2)+(16-m_3)+(16-m_4) = 5+9+6+3 =23$. Το U μπορεί να αναπαρασταθεί δυαδιακά ως U = 10111.
2) Σχηματίζει μια συμβολοσειρά w = m||00010111.
3) Παράγει 6 τυχαίους ακέραιους αριθμούς $k_1,k_2,...,k_6$.
4) Η υπογραφή της Alice για το μήνυμα m είναι η $(s_1,s_2,...,s_6)$, όπου $s_1 = h^{11}(k_1)$, $s_2 = h^7(k_2)$, $s_3 = h^{10}(k_3)$, $s_4 = h^{13}(k_4)$, $s_5 = h^1(k_5)$, $s_6 = h^7(k_6)$.

Σημείωση: Αν ο αντίπαλος προσπαθήσει να τροποποιήσει το μήνυμα, μπορεί να εφαρμόσει την συνάρτηση κατακερματισμού σε μερικά μόνο s_i. Τότε το άθροισμα των στοιχείων που αποτελούν ένα μήνυμα αυξάνεται, το οποίο έχει ως αποτέλεσμα την μείωση του $t2^d-\sum m_i$. Ο αντίπαλος δεν μπορεί να τροποποιήσει τα δύο τελευταία τμήματα μιας και πρέπει να υπολογιστεί η h^{-1} για να μειώσει τον αποτέλεσμα του αθροίσματος. Όμως, η συνάρτηση κατακερματισμού έχει επιλεγεί έτσι ώστε να έχει αντίσταση ορίσματος και έτσι δεν μπορεί να υπολογιστεί η αντίστροφή της συνάρτηση από τον αντίπαλο.

8.2.3 **Σχήμα υπογραφής Merkle με δέντρα κατακερματισμού**

Το μεγαλύτερο πρόβλημα για τα σχήματα υπογραφών μιας χρήσης είναι η διαχείριση του κλειδιού. Η ανταλλαγή του δημοσίου κλειδιού είναι πολύπλοκη. Πρέπει να είναι εγγυημένο ότι το δημόσιο κλειδί ανήκει στον υπογράφοντα και ότι δεν έχει τροποποιηθεί. Έτσι είναι απαραίτητο να χρησιμοποιηθούν ελάχιστα δημόσια κλειδιά και επιπλέον να έχουν μικρό μήκος. Αλλά στα σχήματα ψηφιακών υπογραφών μιας χρήσης, ένα καινούργιο δημόσιο κλειδί παράγεται για κάθε υπογραφή, το οποίο είναι μεγάλο. Για να γίνουν ποιο χρήσιμα αυτά τα σχήματα πρέπει να μειωθεί ο αριθμός των δημόσιων κλειδιών και το μήκος τους. Έτσι ο Merkle παρουσίασε το σχήμα υπογραφής Merkle, με το οποίο ένα δημόσιο κλειδί χρησιμοποιείται για την υπογραφή πολλών μηνυμάτων.

Το σχήμα υπογραφής Merkle μπορεί να χρησιμοποιηθεί για να υπογραφεί ένας πεπερασμένος αριθμός μηνυμάτων με ένα δημόσιο κλειδί. Ο αριθμός των μηνυμάτων πρέπει να είναι δύναμη του δύο, ώστε ο πιθανός αριθμός να είναι $N = 2^n$. Το πρώτο βήμα είναι η παραγωγή του ιδιωτικού κλειδιού X_i και του δημοσίου Y_i για 2^n ψηφιακές υπογραφές μιας χρήσης. Για κάθε δημόσιο κλειδί Y_i, με $1 \leq i \leq 2^n$, πρέπει να υπολογιστεί η τιμή $h_i = h(Y_i)$. Με αυτές τις τιμές κατακερματισμού h_i σχηματίζεται ένα δένδρο Merkle. Ένας κόμβος του δένδρου αυτού ονομάζεται α_{ij}, όπου το i δηλώνει το επίπεδο του κόμβου. Το επίπεδο του κόμβου προσδιορίζεται από την απόσταση του από το φύλλο ενός δένδρου. Έτσι, το φύλλο ενός δένδρου είναι στο επίπεδο i = 0 και η ρίζα του είναι στο επίπεδο i = n. Οι κόμβοι του ίδιου επιπέδου αριθμούνται από αριστερά προς τα δεξιά, έτσι ώστε το αριστερότερο στοιχείο να είναι το $\alpha_{i,0}$ στο επίπεδο i. Το Merkle δένδρο είναι ένα δυαδικό δένδρο του οποίου τα φύλλα είναι οι τιμές κατακερματισμού h_i, έτσι ώστε $h_i = \alpha_{0,i}$. Κάθε εσωτερικός κόμβος είναι η συνένωση της τιμής κατακερματισμού των δύο παιδιών του. Συνεπώς $\alpha_{1,0} = h(\alpha_{0,0}||\alpha_{0,1})$ και $\alpha_{2,0} = h(\alpha_{1,0},\alpha_{1,1})$. Ένα παράδειγμα τέτοιου δένδρου είναι το παρακάτω.

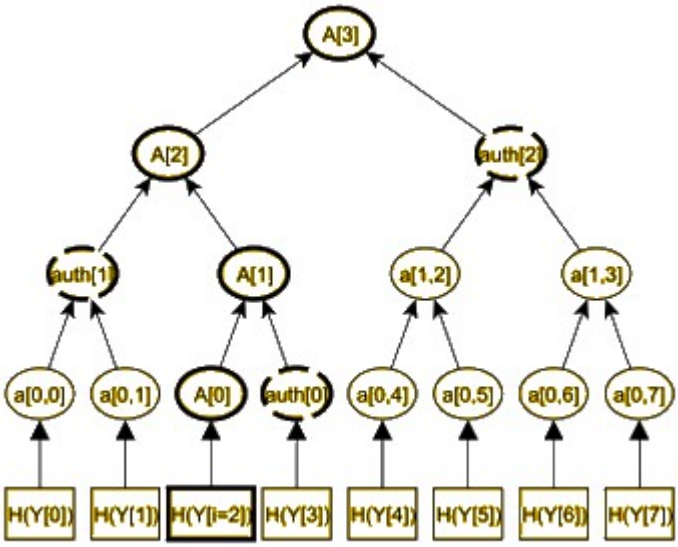


Κατά αυτόν τον τρόπο κατασκευάζεται ένα δένδρο Merkle με 2^n φύλλα και 2^{n+1}-1 κόμβους. Η ρίζα του δένδρου $\alpha_{n,0}$ είναι το δημόσιο κλειδί του σχήματος υπογραφής Merkle.

Παραγωγή υπογραφής

Για να υπογράψουμε ένα μήνυμα m με το σχήμα υπογραφής Merkle, το μήνυμα m πρώτα υπογράφεται με ένα σχήμα μιας χρήσης και έτσι έχουμε την υπογραφή sig'. Αυτό γίνεται με την χρησιμοποίηση του ζεύγους δημοσίου και ιδιωτικού κλειδιού (X_i,Y_i). Το αντίστοιχο φύλλο του δένδρου κατακερματισμού για το μιας χρήσης κλειδί Y_i είναι το $\alpha_{0,i} = h(Y_i)$. Το

μονοπάτι του δένδρου από τον κόμβο $\alpha_{0,i}$ στην ρίζα το ονομάζουμε Α. Το μονοπάτι Α αποτελείται από n+1 κόμβους, $A_0,...,A_n$, με $A_0 = \alpha_{0,i}$ να είναι το φύλλο και $A_n = \alpha_{n,0}$ να είναι η ρίζα του δένδρου. Για να υπολογίσουμε το μονοπάτι Α, χρειάζεται να γνωρίζουμε όλους τους κόμβους $A_1,...,A_n$. Γνωρίζουμε ότι το A_i είναι το παιδί του A_{i+1}. Για να υπολογίσουμε τον επόμενο κόμβο στο μονοπάτι Α, πρέπει να γνωρίζουμε και τα δύο παιδιά του A_{i+1}. Όποτε χρειαζόμαστε τον αδερφό του A_i. Καλούμε αυτόν τον κόμβο $auth_i$, έτσι ώστε $A_{i+1} = h(A_i||auth_i)$. Συνεπώς n κόμβοι $auth_0,...,auth_{n-1}$ απαιτούνται, ώστε να υπολογιστεί κάθε κόμβος του μονοπατιού Α. Αυτοί οι κόμβοι σε συνδυασμό με την υπογραφή sig' είναι η υπογραφή για το m, $sig = (sig'||auth_0||...||auth_{n-1})$. Ένα παράδειγμα τέτοιου μονοπατιού είναι το παρακάτω.



Επαλήθευση υπογραφή

Ο Bob γνωρίζει το δημόσιο κλειδί της Alice, το μήνυμα m και την υπογραφή $sig = (sig'||auth_0||...||auth_{n-1})$. Στην αρχή ο Bob επαληθεύει αν είναι αυθεντική η υπογραφή μιας χρήσης sig' για το μήνυμα m. Αν η sig' είναι η αυθεντική υπογραφή για το m, ο Bob υπολογίζει $A_0 = h(Y_i)$ εφαρμόζοντας την συνάρτηση κατακερματισμού στο δημόσιο κλειδί της υπογραφής μιας χρήσης. Για j=1,...,n-1 οι κόμβοι A_j του μονοπατιού Α υπολογίζονται από την σχέση $A_j = h(\alpha_{j-1}||b_{j-1})$. Αν A_n ισούται με το δημόσιο κλειδί του σχήματος Merkle, η υπογραφή είναι έγκυρη.

8.3 **Το σχήμα ψηφιακής υπογραφής GMR**

Το σχήμα υπογραφής GMR οφείλεται στους Goldwasser, Micali και Rivest. Είναι ένα σχήμα ψηφιακής υπογραφής βασισμένο στην δυσκολία του υπολογισμού της παραγοντοποίησης ακεραίων. Το σχήμα έχει την ιδιότητα ότι είναι ανθεκτικό σε προσαρμόσιμες επιθέσεις με επιλεγμένο μήνυμα. Αυτό είναι εντυπωσιακό, μιας και οι ιδιότητες η πλαστογράφηση να είναι ισοδύναμη με την παραγοντοποίηση και η ανθεκτικότητα σε προσαρμόσιμες επιθέσεις με επιλεγμένο μήνυμα θεωρούταν αντιφατικές.

Γενικά, σε αυτό το τμήμα θα παρουσιαστεί η κατασκευή ενός σχήματος υπογραφής, η οποία βασίζεται στην ύπαρξη "claw-free" ζεύγος μεταθέσεων-μια δυνητικά ασθενέστερη

υπόθεση σε σχέση με την παραγοντοποίηση ακεραίων.

Σε αυτό το σχήμα η παραγωγή υπογραφής και η επαλήθευση της είναι σχετικά γρήγορες και οι υπογραφές είναι συμπαγείς.

"Claw-free" ζεύγος μεταθέσεων

Το σχήμα υπογραφής αυτό βασίζεται στην ύπαρξη ενός ζεύγους μεταθέσεων "claw-free". Με άλλα λόγια βασίζεται στην δυσκολία να βρεθεί μια τριπλέτα x, y, z , τέτοια ώστε $f_0(x) = f_1(y) = z$, όπου f_0 και f_1 είναι μεταθέσεις με κοινό πεδίο ορισμού.

Ορισμός: Έστω G ένας αλγόριθμος, με είσοδο 1^k και έξοδο την διατεταγμένη πεντάδα αλγόριθμων $(d,f_0,f_0^{-1},f_1,f_1^{-1})$. Ο G ονομάζεται γεννήτορας claw-free ζεύγος μεταθέσεων, αν υπάρχει ένα πολυώνυμο p, τέτοιο ώστε:

1) Ο αλγόριθμος d να σταματάει μετά από p(k) βήματα και να ορίζει μια ομοιόμορφη κατανομή στο πεπερασμένο σύνολο D = [d( )].
2) Οι αλγόριθμοι f_0, f_0^{-1},f_1 και f_1^{-1} να σταματούν μετά από p(k) βήματα, αν η είσοδος είναι $x \in D$. (Για διαφορετικές εισόδους, που δεν ανήκουν στον D, αυτοί οι αλγόριθμοι είτε πέφτουν σε βρόχο για πάντα είτε σταματούν με ένα μήνυμα λάθους). Επιπλέον, οι συναρτήσεις $x \rightarrow f_0(x)$ και $x \rightarrow f_0^{-1}(x)$ είναι μεταθέσεις του D οι οποίες είναι ανάστροφη η μια της άλλης, όπως και οι $x \rightarrow f_1(x)$, $x \rightarrow f_1^{-1}$.
3) Για όλους τους αλγόριθμους (που δημιουργούν claw-free ζεύγη) $I(\cdot,\cdot,\cdot,\cdot)$, για κάθε c και αρκετά μεγάλο k:
$P(f_0(x)) = f_1(y) = z|(d,f_0,f_0^{-1},f_1,f_1^{-1}) \leftarrow G(1^k);(x,y,z) \leftarrow I(1^k,d,f_0,f_1)) < k^{-c}$.

Ορισμός: Το $f = (d,f_0,f_1)$ ονομάζεται claw-free ζεύγος μεταθέσεων (ή εν συντομία claw-free ζεύγος) αν $(d, f_0, f_0^{-1}, f_1, f_1^{-1}) \in [G(1^k)]$ για κάποιο k και το G να είναι ένας γεννήτορας claw-free ζευγών μεταθέσεων.

Στο σχήμα υπογραφής GMR ο χώρος μηνυμάτων είναι ο M και υποσύνολο του $\{0,1\}^+$.

Αλγόριθμος-Παραγωγή κλειδιού για το σχήμα υπογραφής GMR
Υποθέτουμε την ύπαρξη του γεννήτορα G των claw-free ζευγών μεταθέσεων και χωρίς βλάβη της γενικότητας ότι το όριο B του αριθμού των υπογραφών είναι δύναμη του 2 ($B = 2^b$). Ο αλγόριθμος έχει σαν είσοδο το 1^k και 2^b. Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να τρέξει δύο φορές τον αλγόριθμο G με είσοδο 1^k για να επιλέξει μυστικά και τυχαία δύο πεντάδες:
$(d_f,f_0,f_0^{-1},f_1,f_1^{-1})$ και $(d_g, g_0, g_0^{-1}, g_1, g_1^{-1}) \in [G(1^k)]$.
2) Να επιλέξει ένα τυχαίο μυστικό αριθμό $r_\epsilon^f \in D_f$ (domain f).
3) Το δημόσιο κλειδί της Alice είναι το $(f,r_\epsilon^f,g,2^b)$, όπου f είναι ένα claw-free ζεύγος (d_f,f_0,f_1) και g είναι ένα claw-free ζεύγος (d_g,g_0,g_1). Το ιδιωτικό κλειδί της Alice είναι το (f^{-1},g^{-1}).

Ορισμός: Το αντικείμενο f είναι το $(t,r;c_1,c_2,...,c_m)$.

- Όπου t είναι η ετικέτα του αντικειμένου.
- Όπου r είναι η ρίζα του αντικειμένου.
- Και τα c_i είναι τα παιδιά του αντικειμένου. Σημειώνουμε ότι τα παιδιά είναι διατεταγμένα, ώστε να μπορούμε να μιλάμε για πρώτο, δεύτερο παιδί κ.τ.λ.

Ορισμός: Μια σειρά από αντικείμενα f $L_1,...,L_b$ είναι μια αλυσίδα f η οποία ξεκινάει από το y αν , για i = 1,...,b-1 η ρίζα του L_{i+1} είναι ένα από τα παιδιά του L_i και y είναι η ρίζα του L_1. Λέμε ότι η αλυσίδα τελειώνει στο x αν x είναι ένα από τα παιδιά του αντικειμένου L_b.

Ορισμός: Έστω i είναι μια δυαδική συμβολοσειρά με μήκος b και f ένα claw-free ζεύγος. Ονομάζουμε f-i-δένδρο T αν:

1) αν η συμβολοσειρά j έχει μήκος b, τότε T(j) είναι το αντικείμενο f με ακριβώς δύο παιδιά και το ένα από τα δύο είναι η κενή συμβολοσειρά ϵ. Αυτά τα αντικείμενα f καλούνται γέφυρες.
2) Αν η συμβολοσειρά j έχει λιγότερο μήκος από b, τότε T(j) είναι ένα αντικείμενο f με δύο ακριβώς παιδιά, c_0 και c_1 και είναι και τα δύο μη κενές συμβολοσειρές.

Η υπογραφή για το μήνυμα m και το αντίστοιχο δημόσιο κλειδί $(f,r_\epsilon^f,g,2^b)$ αποτελείται από:

a) Μια αλυσίδα f μήκους b+1, η οποία ξεκινάει από συμβολοσειρά r_ϵ^f και τελειώνει στην r^g.
b) Ένα αντικείμενο g με την r^g για ρίζα και m το μοναδικό παιδί της.

Για την υπογραφή η Alice δημιουργεί ένα f-1^b-δένδρο T, το οποίο έχει 2^b φύλλα. Η ρίζα του δένδρου είναι η r^f. Οι εσωτερικοί κόμβοι είναι τυχαία επιλεγμένα στοιχεία του D_f. Τα φύλλα του T είναι τυχαία επιλεγμένα στοιχεία του D_g.

Για την υπογραφή του m_i, δηλαδή του i-στου μηνύματος σε χρονολογική σειρά, η Alice υπολογίζει ένα αντικείμενο G_i του οποίου η ρίζα είναι το $r_i^g \in D_g$ το i-στο φύλλο του T και του οποίου το μοναδικό παιδί είναι το μήνυμα m_i. Μετά, εξάγει την υπογραφή για το m_i, G_i και την αλυσίδα f στο δένδρο T ξεκινώντας με ρίζα r_ϵ^f και τελευταίο φύλλο το r_i^g.

Στην πραγματικότητα δεν είναι αποδοτικό η Alice να κατασκευάσει ολόκληρο το δένδρο T. Θα πρέπει να "μεγαλώσει" το δένδρο T όσο χρειάζεται και να προσπαθήσει να βελτιστοποιήσει την χρησιμοποίηση του χώρου και του χρόνου. Στην υπογραφή αυτή η Alice θα πρέπει να θυμάται το δημόσιο κλειδί της και την τελευταία υπογραφή της ώστε να παράγει την επόμενη. Άρα στον αλγόριθμο που ακολουθεί έχουμε υποθέσει ότι η Alice έχει υπογράψει ήδη τα μηνύματα $m_0,m_1,...,m_{i-1}$ και έχει αποθηκεύσει τον αριθμό τον προηγούμενων υπογραφών και την τελευταία υπογραφή που έχει κατασκευάσει.

Αλγόριθμος-Παραγωγής υπογραφής GMR

Για να κατασκευάσει η Alice την υπογραφή για το μήνυμα m_i, δηλαδή το i-στο μήνυμα, η Alice θα πρέπει να κάνει τα ακόλουθα:

1) (Έξοδος αντικείμενο f)
   a) (Έξοδος αντικείμενα f κοινά με τις προηγούμενες υπογραφές). Αν $i = 0^b$ αυτό το βήμα παραλείπεται και πηγαίνει στο βήμα b. Αλλιώς, για κάθε συμβολοσειρά j που είναι κοινή με το πρόθεμα του i και i-1, δίνει έξοδο ένα αντικείμενο f $(t_j^f,r_j^f,r_{j0}^f,r_{j1}^f)$ το οποίο είναι κομμάτι της υπογραφής του μηνύματος m_{i-1}, ώστε να αυξήσει το μέγεθος του j.
   b) (Έξοδος ένα νέο αντικείμενο f του f-δένδρου) Για κάθε συμβολοσειρά j που είναι πρόθεμα του i, αλλά όχι πρόθεμα του i-1, η Alice δημιουργεί ένα αντικείμενο f T(j), για να αυξήσει το μήκος του j. Το αντικείμενο f $T(j)=(t_j^f,r_j^f,r_{j0}^f,r_{j1}^f)$ δημιουργείται ως εξής: Αν $j = \epsilon$ η ρίζα του r_j^f είναι η r_ϵ^f από το δημόσιο κλειδί. Σε άλλη περίπτωση είναι το k-οστό παιδί του τελευταίου αντικειμένου f που έχει κατασκευαστεί, όπου k είναι το τελευταίο bit της συμβολοσειράς j. Τα παιδιά r_{j0}^f και r_{j1}^f του αντικειμένου f με ρίζα r_j^f έχουν επιλεγεί τυχαία από το πεδίο ορισμού D_f. Η ετικέτα $t_j^f = f^{-1}_{(r_{j0}^f, r_{j1}^f)}(r_j^f)$ υπολογίζεται χρησιμοποιώντας τις f_0^{-1} και f_1^{-1} του δημοσίου κλειδιού. Εδώ πρέπει να σημειώσουμε ότι η έξοδος (είτε του a βήματος είτε του b) έχει το r_i^f σαν μοναδικό παιδί.

c) (Έξοδος γέφυρα)Η επόμενη έξοδος που παράγει η Alice είναι ένα αντικείμενο f με ρίζα r_i^f και με παιδιά την κενή συμβολοσειρά ϵ και το r_i^f, ένα τυχαία επιλεγμένο στοιχείο του D_g. Η ετικέτα t_i^f του αντικειμένου χρησιμοποιεί τις f_0^{-1} και f_1^{-1}.

2) (Έξοδος αντικείμενο g). Τέλος η Alice κατασκευάζει το αντικείμενο g: $G_i = (t_i^g, r_i^g, m_j)$. Η ετικέτα αυτού του αντικειμένου t_i^g υπολογίζεται με την χρήση του g^{-1}.
3) Το αποτέλεσμα όλων των παραπάνω αποτελεί την υπογραφή της Alice για το m_i.

Αλγόριθμος-Επαλήθευση υπογραφής GMR

Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice πρέπει να κάνει τα ακόλουθα:

1) Να αποκτήσει το δημόσιο κλειδί της Alice $(f, r_\epsilon^f, g, 2^b)$.
2) Να επαληθεύσει ότι για τα b+1 στοιχεία της υπογραφής του m_i:
   a) Τα αντικείμενα f σχηματίζουν μια αλυσίδα f η οποία ξεκινάει από το r_ϵ^f και τελειώνει με το r_i^g.
   b) Το αντικείμενο g στην υπογραφή έχει σαν ρίζα το r_i^g και σαν μοναδικό παιδί το m_i.
3) Να αποδεχτεί την υπογραφή ως αυθεντική αν ισχύουν όλα τα παραπάνω.

Αποδοτικότητα

Έστω ότι το $f = (d_f, f_0, f_1)$ είναι ένα claw-free ζεύγος μήκους k, τότε ένα στοιχείο του D_f ορίζεται από μια συμβολοσειρά με μήκος k bit. Τότε ο χρόνος που χρειάζεται για να κατασκευαστεί η υπογραφή για το μήνυμα m μήκους l είναι O(bk).

Το μήκος της υπογραφής για το μήνυμα m είναι το O(bk+l), οπού l είναι το μήκος του μηνύματος, αν το m είναι μέρος της υπογραφής σαν το παιδί του αντικειμένου g. Αν το m είναι γνωστό στον παραλήπτη, το αντικείμενο g δεν είναι ανάγκη να περιλαμβάνει το m και αρκεί να έχουμε την ρίζα και την ετικέτα του. Σε αυτήν την περίπτωση η υπογραφή μπορεί να έχει μήκος O(bk), το οποίο είναι ανεξάρτητο του μεγέθους του μηνύματος m και πιθανόν η υπογραφή να ήταν πολύ μικρότερη.

Η μνήμη που απαιτείται για τον αλγόριθμο της υπογραφής είναι O(bk), μιας και χρειάζεται να αποθηκευτεί η πιο πρόσφατη υπογραφή.

9 Άλλα σχήματα ψηφιακών υπογραφών

Τα σχήματα υπογραφών που παρουσιάζονται σε αυτή την ενότητα δεν συσχετίζονται με καμιά κατηγορία ψηφιακών υπογραφών.

9.1 Σχήμα ψηφιακών υπογραφών με διαιτησία

Το σχήμα ψηφιακών υπογραφών με διαιτησία κατασκευάστηκε από τους Davies και Price και είναι βασισμένο στην εργασία των Needham και Schroeder. Για την παραγωγή και επαλήθευση της υπογραφής επεμβαίνει ένα τρίτο έμπιστο πρόσωπο (TTP)-διαιτητής.

Στον αλγόριθμο αυτό χρησιμοποιείται αλγόριθμος κρυπτογράφησης συμμετρικού κλειδιού $E = \{E_k : k \in K\}$, όπου K είναι ο χώρος των κλειδιών. Έστω ότι οι είσοδοι και οι έξοδοι του E_k είναι συμβολοσειρές με μέγεθος l bits και ότι η συνάρτηση κατακερματισμού είναι η μονόδρομη $h: \{0,1\}^* \rightarrow \{0,1\}^l$. Σε αυτό το σχήμα υπογραφής ο TTP είναι αυτός που επιλέγει το μυστικό κλειδί $k_T \in K$. Στην διαδικασία της επαλήθευσης της υπογραφής η Alice μοιράζεται το ίδιο συμμετρικό κλειδί με το TTP.

Αλγόριθμος-Παραγωγή κλειδιού για το σχήμα υπογραφής με διαιτησία
Περίληψη: Η Alice διαλέγει ένα κλειδί και το ανακοινώνει (μυστικά) στο TTP.
Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να επιλέξει ένα τυχαίο μυστικό κλειδί $k_A \in K$.
2) Με μυστικότητα εμπιστεύεται το κλειδί αυτό στο TTP.

Αλγόριθμος-Παραγωγή και επαλήθευση του σχήματος ψηφιακής υπογραφής με διαιτησία
Περίληψη: Η Alice δημιουργεί μια υπογραφή χρησιμοποιώντας τον E_{k_A}. Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice σε συνεργασία με το TTP.

1) Παραγωγή υπογραφής. Η Alice για να υπογράψει ένα μήνυμα m, πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει H = h(m).
   b) Να κρυπτογραφήσει το H με τον E για να βρει $u = E_{k_A}(H)$.
   c) Να στείλει το u μαζί με μια συμβολοσειρά αναγνώρισης I_A στο TTP.
   d) Με την σειρά του το TTP υπολογίζει $E_{k_A}^{-1}(u)$, ώστε να αποκτήσει το H.
   e) Ο TTP υπολογίζει $s = E_{k_T}(H||I_A)$ και στέλνει το αποτέλεσμα στην Alice.
   f) Η υπογραφή της Alice για το m είναι η s.
2) Επαλήθευση. Ο Bob μπορεί να επαλήθευση ότι η υπογραφή της Alice για το m είναι η s, αν ακολουθήσει την εξής διαδικασία:
   a) Να υπολογίσει $\upsilon = E_{k_B}(s)$.
   b) Να στείλει το υ και μια συμβολοσειρά αναγνώρισης I_B στο TTP.
   c) Με τη σειρά του ο TTP υπολογίζει $E_{k_B}^{-1}(\upsilon)$, ώστε να αποκτήσει την s.
   d) Ο TTP υπολογίζει $E_{k_T}^{-1}(s)$, ώστε να αποκτήσει $H||I_A$.
   e) Ο TTP υπολογίσει $w = E_{k_T}(H||I_A)$ και στέλνει το αποτέλεσμα στον Bob.
   f) Ο Bob υπολογίζει $E_{k_B}^{-1}(w)$, ώστε να αποκτήσει το $H||I_A$.
   g) Ο Bob υπολογίζει H' = h(m) για το μήνυμα m.
   h) Ο Bob αποδέχεται την υπογραφή αν και μόνο αν H' = H.

9.1.1 **Ασφάλεια**

Η ασφάλεια του σχήματος ψηφιακής υπογραφής εξαρτάται από το σχήμα κρυπτογράφησης συμμετρικού κλειδιού που επιλέγεται και στην διανομή των κλειδιών με μυστικότητα και ασφάλεια.

9.2 **ESIGN**

Το ESIGN (συντομογραφία του Efficient digital SIGNature) σχήμα υπογραφής προτάθηκε το 1985 από τον Tatsuaki Okamoto. Έχει αποδειχθεί ότι είναι ασφαλές σε επιθέσεις υπαρκτής πλαστογραφίας σε επιλεγμένο μήνυμα, αν υποθέσουμε ότι το πρόβλημα της προσέγγισης τις e-οστης ρίζας (approximate e-th root-AER) είναι δύσκολο και ότι η επιλογή της συνάρτησης κατακερματισμού είναι τυχαία. Οι παράμετροι που χρησιμοποιούνται είναι για να διασφαλίσουν την ασφάλεια σε επιθέσεις που σχετίζονται με την παραγοντοποίηση ακεραίων.

Αλγόριθμος-Παραγωγή κλειδιού για την ESIGN
Περίληψη:Η Alice δημιουργεί το δημόσιο και το αντίστοιχο ιδιωτικό κλειδί της.
Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να επιλέξει δύο τυχαίους διακριτούς πρώτους p, q με μέγεθος k bit και να υπολογίσει $n = p^2q$.
2) Να επιλέξει έναν ακέραιο $e > 4$.
3) Το δημόσιο κλειδί της Alice είναι το (n,e,k) και το ιδιωτικό της είναι το (p,q).

Επιπλέον, πρέπει να ορίσει μια συνάρτηση κατακερματισμού h' με μέγεθος εξόδου k bits.

Αλγόριθμος-Παραγωγή και επαλήθευση την ESIGN
Περίληψη: Η Alice υπογράφει το μήνυμα m με την βοήθεια του ιδιωτικού της κλειδιού.
Ο Bob μπορεί να επαληθεύσει την υπογραφή της Alice χρησιμοποιώντας το δημόσιο κλειδί της.

1) Παραγωγή υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει h'(m) και το h(m) εξάγεται από το h'(m) διαγράφοντας το πιο σημαντικό bit.
   b) Να επιλέξει ένα r τυχαία από το $\{ r \in \mathbb{Z}_{pq} : MK\Delta(r,p) = 1\}$.
   c) Να θέσει $z = (0||h(m)||0^{2k})$ και $\alpha = (I(z)-r^e) \bmod n$, όπου η συνάρτηση I μετατρέπει μια δυαδική συμβολοσειρά σε ακέραιο.
   d) Θέτει (w_0,w_1) τέτοιο ώστε $w_0 = \left\lceil \frac{a}{pq} \right\rceil$, $w_1 = w_0pq - \alpha$.
   e) Αν $w_1 \geq 2^{k-1}$, τότε να επιστρέψει στο βήμα b.
   f) Να θέσει $t = \frac{w_0}{er^{e-1}}$ και $s = B_{3k}[(r+tpq) \bmod n]$, όπου $B_{3k}[X]$ μετατρέπει ένα ακέραιο X σε μια δυαδική συμβολοσειρά με μήκος 3k (και αν είναι αναγκαίο να προστεθούν κάποια μηδενικά στην αρχή).
   g) Η υπογραφή της Alice για το m είναι η s.
2) Επαλήθευση. Ο Bob μπορεί να επαλήθευση ότι η υπογραφή της Alice για το m είναι η s, αν ακολουθήσει την εξής διαδικασία:
   a) Να αποκτήσει το αυθεντικό κλειδί της Alice (n,e,k).
   b) Να υπολογίσει h'(m) και το h(m) εξάγεται από το h'(m) διαγράφοντας το πιο σημαντικό bit.
   c) Να ελέγξει αν η ακόλουθη εξίσωση ισχύει:
   $[B_{3k}[I(s)^e \bmod n]]^k = 0||h(m)$
   όπου η συνάρτηση $[X]^k$ υποδεικνύει τα k πιο σημαντικά bits της εξόδου X.

d) Ο Bob αποδέχεται την υπογραφή αν ισχύει η εξίσωση.

Σημειώσεις:

1) Ο αλγόριθμος παραγωγής της υπογραφής υπολογίζει τον ακέραιο s έτσι ώστε το s^e mod n να βρίσκεται σε συγκεκριμένο διάστημα το οποίο καθορίζεται από το μήνυμα. Ο αλγόριθμος επαλήθευσης της υπογραφής αποδεικνύει ότι πράγματι το s^e mod n βρίσκεται στο καθορισμένο διάστημα.
2) Για να γίνει πιο γρήγορη η διαδικασία της παραγωγής της υπογραφής το βήμα e μπορεί να είναι προαιρετικό. Η συνθήκη $w_1 \geq 2^{2^{k-1}}$ εξασφαλίζει ότι η τιμή $w_1 = s^e - I(z)$ είναι ομοιόμορφα κατανεμημένη στο διάστημα $[0, 2^{2^{k-1}} - 1]$. Βέβαια, δεν είναι γνωστή κάποια αδυναμία στο σχήμα υπογραφής αν αυτός ο έλεγχος παραληφθεί.
3) Οι Fujioka, Okamoto και Miyaguchi περιέγραψαν μια εφαρμογή του ESIGN για e = 32. Με αυτή την εφαρμογή διαπίστωσαν ότι το ESIGN είναι είκοσι φορές πιο γρήγορο από το σχήμα υπογραφής RSA (με $e = 2^{16}+1$) με ανάλογο κλειδί και μήκος υπογραφής.

9.2.1 **Ασφάλεια**

Όπως αναφέρθηκε η ασφάλεια του ESIGN βασίζεται στην υπόθεση AER η οποία ορίζεται ως εξής: Έστω $n = p^2q$, όπου p και q είναι πρώτοι αριθμοί με το ίδιο μήκος. Το AER πρόβλημα είναι να βρεθεί x δοθέντων n, e, y τέτοιο ώστε $[x^e \bmod n]^{|n|/3} = [y]^{|n|/3}$. Η υπόθεση AER είναι ότι δεν υπάρχει αποδοτικός αλγόριθμος ο οποίος να μπορεί να λύσει το AER πρόβλημα.

Στο αρχικό σχήμα ESIGN είχε προταθεί το e = 2 ως κατάλληλη τιμή για το δημόσιο κλειδί. Ο Brickell και ο DeLaurentis υπέδειξαν ότι αυτή η επιλογή δεν είναι ασφαλής. Η επίθεση τους επεκτείνεται και στην περίπτωση που e = 3. Ο Okamoto τότε πρότεινε $e \geq 4$ και με αυτήν την τιμή δεν έχει διαπιστωθεί αδυναμία στο σχήμα.

Για την ασφάλεια του ESIGN παίζει ρόλο η επιλογή της συνάρτησης κατακερματισμού. Έτσι η συνάρτηση κατακερματισμού πρέπει να είναι ανθεκτική σε συγκρούσεις και αντίσταση ορίσματος.

Τέλος το n πρέπει να επιλεγεί κατάλληλα, ώστε $n = p^2q$ όπου p,q είναι τυχαία επιλεγμένοι του ίδιου μήκους τουλάχιστον 320 (ώστε n να έχει μήκος τουλάχιστον 960). Τότε όλοι οι γνωστοί αλγόριθμοι για την παραγοντοποίηση του n αποτυγχάνουν.

9.2.2 **Παράμετροι**

Οι προτεινόμενοι παράμετροι για το σχήμα ESIGN είναι οι ακόλουθοι:

- k: μεγαλύτερος ή ίσος με 320bits (έτσι ώστε n να είναι μεγαλύτερος από 960bits)
- e: μεγαλύτερος ή ίσος του 8.

10 Υπογραφές με επιπρόσθετη λειτουργία

Σε αυτή την ενότητα εξετάζονται υπογραφές οι οποίες συνδυάζουν ένα από τα γνωστά σχήματα υπογραφών με ένα πρωτόκολλο ώστε η υπογραφή να έχει επιπλέον ιδιότητες που δεν παρέχει η βασική έκδοση.

10.1 Σχήματα τυφλών υπογραφών

Οι τυφλές υπογραφές παρουσιάστηκαν από τον David Chaum, ο οποίος περιέγραψε την έννοια, τις επιθυμητές ιδιότητες που πρέπει να περιλαμβάνουν αυτά τα σχήματα καθώς και ένα πρωτόκολλο μη ανιχνεύσιμων πληρωμών. Κυρίως χρησιμοποιούνται για ηλεκτρονικές επικοινωνίες στην περίπτωση που η μια πλευρά επιθυμεί ανωνυμία απέναντι στην άλλη.

Η βασική ιδέα των τυφλών σχημάτων υπογραφών είναι η ακόλουθη. Ο αποστολέας στέλνει κάποιες πληροφορίες στον υπογράφοντα. Με την σειρά του ο υπογράφον υπογράφει αυτές τις πληροφορίες και τις επιστρέφει στον αποστολέα.

Οι επόμενες τρεις συναρτήσεις είναι χρήσιμες για την κατασκευή τυφλών υπογραφών:

1) Μια εξίσωση υπογραφής s' γνωστή μόνο στον υπογράφοντα, και η αντίστοιχη δημόσια γνωστή s, αντίστροφη της s', έτσι ώστε s(s'(x)) = x. Η s είναι έτσι κατασκευασμένη ώστε να μην μπορεί να μας δώσει κανένα στοιχείο για την s'.
2) Μια συνάρτηση c και η αντίστροφή της c', και οι δύο γνωστές μόνο στον αποστολέα, έτσι ώστε c'(s'(c(x)) = s'(x), και οι c(x) και s' να μην παρέχουν κανένα στοιχείο για το x.
3) Μια συνάρτηση r, η οποία ελέγχει αν υπάρχει αρκετός πλεονασμός ώστε να είναι αδύνατη η πλαστογράφηση μιας υπογραφής.

Πρωτόκολλο

1) Ο αποστολέας επιλέγει ένα τυχαίο x έτσι ώστε η r(x), σχηματίζει την c(x) και μεταδίδει την c(x) στον υπογράφοντα.
2) Ο υπογράφον υπογράφει την c(x) με εφαρμογή της s' και επιστρέφει την υπογεγραμμένη s'(c(x)) στον αποστολέα.
3) Ο αποστολέας υπολογίζει c'(s'(c(x))) = s'(x).
4) Καθένας μπορεί να ελέγξει ότι η s'(x) έχει δημιουργηθεί από τον υπογράφοντα, εφαρμόζοντας το δημόσιο κλειδί s του υπογράφοντα και να ελέγξει ότι r(s(s'(x)).

10.2 Αδιαμφισβήτητα σχήματα υπογραφής

Τα αδιαμφισβήτητα σχήματα υπογραφής, τα οποία επινόησαν οι Chaum και van Antwerpen, είναι υπογραφές που χρειάζονται την συνεργασία του υπογράφοντα ώστε να επιτευχθεί η επαλήθευση της. Βέβαια, αν μια υπογραφή μπορεί μόνο με την βοήθεια του υπογράφοντα, ενδέχεται ένας αντίπαλος να αρνηθεί να πιστοποιήσει την αυθεντικότητα ενός γνήσιου εγγράφου. Για να αποτραπεί αυτή η περίπτωση, στα σχήματα ψηφιακής υπογραφής προστίθεται ένα καινούργιο στοιχείο, το πρωτόκολλο αποκήρυξης.

Τα σχήματα αυτά χρησιμοποιούν κρυπτογράφηση δημοσίου κλειδιού και βασίζονται στο πρόβλημα του διακριτού λογαρίθμου. Η διαδικασία της υπογραφής είναι παρόμοια με τα άλλα σχήματα που εξαρτώνται από το πρόβλημα διακριτού λογαρίθμου. Η επαλήθευση της

υπογραφής πραγματοποιείται με την χρήση ενός πρωτοκόλλου πρόκλησης-απάντησης. Όπου αυτός που πραγματοποιεί την επαλήθευση στέλνει μια πρόκληση στον υπογράφοντα και βλέπει την απάντηση ώστε να επαληθεύσει την υπογραφή. Το πρωτόκολλο αποκήρυξης ακολουθεί παρόμοια διαδικασία. Η πιθανότητα ένας ανέντιμος υπογράφον να καταφέρει να παραπλανήσει αυτόν που πραγματοποιεί την επαλήθευση, κατά την διαδικασία της επαλήθευσης ή της αποκήρυξης, είναι 1/p (όπου p είναι ο πρώτος αριθμός που χρησιμοποιείται για την κατασκευή του ιδιωτικού κλειδιού). Αν το ιδιωτικό κλειδί έχει μήκος 768 bits, υπάρχει μονάχα μια μικρή πιθανότητα ο υπογράφον να αποκηρύξει ένα έγγραφο που έχει υπογράψει.

Παράδειγμα:(χρήση αδιαμφισβήτητων υπογραφών). Έστω ότι ο Α είναι πελάτης της τράπεζας Β και θέλει να αποκτήσει πρόσβαση σε στοιχεία με υψηλή ασφάλεια. Η τράπεζα για να επιτρέψει την πρόσβαση του Α σε αυτά τα στοιχεία τον υποχρεώνει να υπογράψει ένα έγγραφο με ημερομηνία και ώρα. Αν ο Α υπογράψει το κείμενο χρησιμοποιώντας αδιαμφισβήτητη υπογραφή, τότε η τράπεζα δεν είναι ικανή να αποδείξει σε κανέναν ότι η υπογραφή ανήκει στον Α, χωρίς την άμεση ανάμειξη του Α στην διαδικασία της επαλήθευσης.

Αλγόριθμος-Παραγωγή κλειδιού για το αδιαμφισβήτητο σχήμα υπογραφής Chaum-van Antwerpen
Περίληψη: Η Alice επιλέγει το ιδιωτικό και το αντίστοιχο δημόσιο κλειδί της.
Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να επιλέξει έναν τυχαίο πρώτο αριθμό p = 2q+1, όπου ο q είναι επίσης πρώτος αριθμός.
2) (Να επιλέξει έναν γεννήτορα a της υποομάδας $\mathbb{Z}_p^*$, τάξης q)
   a) Να επιλέξει ένα τυχαίο στοιχείο $b \in \mathbb{Z}_p^*$ και να υπολογίσει $a = b^{(p-1)/q} \bmod p$.
   b) Αν a = 1 να επιστρέψει στο 2)a).
3) Να επιλέξει έναν τυχαίο ακέραιο $\alpha \in 1,2,\ldots,q-1$ και να υπολογίσει $y = a^{\alpha} \bmod p$.
4) Το δημόσιο κλειδί της Alice είναι το (p,a,y) και το ιδιωτικό της είναι το α.

Αλγόριθμος-Παραγωγή και επαλήθευση για το αδιαμφισβήτητο σχήμα υπογραφής Chaum-van Antwerpen
Περίληψη: Η Alice υπογράφει ένα μήνυμα m το οποίο ανήκει στην υποομάδα $\mathbb{Z}_p^*$,τάξης q. Ο Bob μπορεί να επαληθεύσει την υπογραφή με την συνεργασία της Alice.

0) Παραγωγή της υπογραφής. Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει $s = m^{\alpha} \bmod p$.
   b) Η υπογραφή της Alice για το μήνυμα m είναι η s.
2) Επαλήθευση. Το πρωτόκολλο για τον Bob ώστε να επαληθεύσει την υπογραφή s της Alice στο μήνυμα m είναι το ακόλουθο:
   a) Ο Bob αποκτά το αυθεντικό δημόσιο κλειδί της Alice (p,a,y).
   b) Ο Bob επιλέγει τυχαίους μυστικούς ακεραίους $x_1, x_2 \in \{1,2,...,q-1\}$.
   c) Ο Bob υπολογίζει $z = s^{x_1} y^{x_2} \bmod p$ και στέλνει το αποτέλεσμα στην Alice.
   d) Η Alice υπολογίζει $w = (z)^{\alpha^{-1}} \bmod p$ (όπου $\alpha\alpha^{-1} \equiv 1 (\bmod q)$) και στέλνει το αποτέλεσμα στον Bob.
   e) Ο Bob υπολογίζει $w' = m^{x_1} \alpha^{x_2} \bmod p$ και αποδέχεται την υπογραφή αν και μόνο αν w = w'.

Απόδειξη ότι ο αλγόριθμος επαλήθευσης λειτουργεί:
$w \equiv (z)^{\alpha^{-1}} \equiv (s^{x_1} y^{x_2})^{\alpha^{-1}} \equiv (m^{\alpha x_1} a^{\alpha x_2})^{\alpha^{-1}} \equiv m^{x_1} \alpha^{x_2} \equiv w' \bmod p$, δηλαδή το ζητούμενο.

Πρωτόκολλο αποκήρυξης

Περίληψη: Το πρωτόκολλο αποκήρυξης καθορίζει αν η Alice προσπαθεί να αποκηρύξει μια έγκυρη υπογραφή s ή αν η υπογραφή είναι μια απάτη.

1) Ο Bob αποκτά το δημόσιο αυθεντικό κλειδί της Alice (p,a,y).
2) Ο Bob επιλέγει μυστικούς ακέραιους $x_1, x_2 \in \{1,2,...,q-1\}$, υπολογίζει $z = s^{x_1} y^{x_2} \bmod p$ και στέλνει το αποτέλεσμα στην Alice.
3) Η Alice υπολογίζει $w = (z)^{\alpha^{-1}} \bmod p$ (όπου $\alpha\alpha^{-1} \equiv 1 (\bmod q)$)και στέλνει το αποτέλεσμα στον Bob.
4) Αν $w = m^{x_1} \alpha^{x_2} \bmod p$, ο Bob αποδέχεται την υπογραφή s και το πρωτόκολλο τερματίζει.
5) Ο Bob επιλέγει μυστικούς ακέραιους $x'_1, x'_2 \in \{1,2,...,q-1\}$, υπολογίζει $z' = s^{x'_1} y^{x'_2} \bmod p$ και στέλνει το αποτέλεσμα στην Alice.
6) Η Alice υπολογίζει $w' = (z')^{\alpha^{-1}} \bmod p$ και στέλνει το αποτέλεσμα στον Bob.
7) Αν $w' = s^{x'_1} y^{x'_2} \bmod p$, ο Bob αποδέχεται την υπογραφή s και το πρωτόκολλο τερματίζει.
8) Ο Bob υπολογίζει $c = (w\alpha^{-x_2})^{x'_1} \bmod p$ και $c = (w\alpha^{-x_1})^{x'_2} \bmod p$. Αν c = c', ο Bob συμπεραίνει ότι η s είναι απάτη, αλλιώς συμπεραίνει ότι η υπογραφή είναι έγκυρη και ότι η Alice προσπαθεί να αποκηρύξει την υπογραφή της s.

Παράδειγμα(με τεχνηέντως μικρές παραμέτρους)

Αλγόριθμος-Παραγωγή κλειδιού για το αδιαμφισβήτητο σχήμα υπογραφής Chaum-van Antwerpen

Περίληψη: Η Alice επιλέγει το ιδιωτικό και το αντίστοιχο δημόσιο κλειδί της.

Η Alice κάνει τα ακόλουθα:

1) Επιλέγει έναν τυχαίο πρώτο αριθμό p = 2q+1 = 467, όπου ο q = 233.
2) Επιλέγει ένα τυχαίο στοιχείο b = 2 και υπολογίζει $a = b^{(p-1)/q} \bmod p = 4$.
3) Επιλέγει έναν τυχαίο ακέραιο α = 101 και να υπολογίσει $y = a^{\alpha} \bmod p = 449$.
4) Το δημόσιο κλειδί της Alice είναι το (p = 467,a = 233,y = 499) και το ιδιωτικό της είναι το α = 101.

Αλγόριθμος-Παραγωγή και επαλήθευση για το αδιαμφισβήτητο σχήμα υπογραφής Chaum-van Antwerpen

Περίληψη: Η Alice υπογράφει ένα μήνυμα m = 119 το οποίο ανήκει στην υποομάδα $\mathbb{Z}_p^*$, τάξης q. Ο Bob μπορεί επαληθεύει την υπογραφή με την συνεργασία της Alice.

1) Παραγωγή της υπογραφής. Η Alice κάνει τα ακόλουθα:
   a) Υπολογίζει $s = m^{\alpha} \bmod p = 129$.
   b) Η υπογραφή της Alice για το μήνυμα m είναι η s.
2) Επαλήθευση. Το πρωτόκολλο για τον Bob ώστε να επαληθεύσει την υπογραφή s της Alice στο μήνυμα m είναι το ακόλουθο:
   a) Ο Bob αποκτά το αυθεντικό δημόσιο κλειδί της Alice (p,a,y).
   b) Ο Bob επιλέγει τυχαίους μυστικούς ακεραίους $x_1 = 38$, $x_2 = 397$.
   c) Ο Bob υπολογίζει $z = s^{x_1} y^{x_2} \bmod p = 13$ και στέλνει το αποτέλεσμα στην Alice.
   d) Η Alice υπολογίζει $w = (z)^{\alpha^{-1}} \bmod p = 9$ και στέλνει το αποτέλεσμα στον Bob.
   e) Ο Bob υπολογίζει $w' = m^{x_1} \alpha^{x_2} \bmod p = 9$ και αποδέχεται την υπογραφή μιας και w = w'.

10.3 **Fail-stop υπογραφές**

Οι fail-stop υπογραφές παρουσιάστηκαν για πρώτη φορά από τους Waidner και Pfitzmann. Όμως πιο αποδοτικές τεχνικές σχεδιάστηκαν από τους van Heijst και Pedersen. Οι υπογραφές αυτές δημιουργήθηκαν ώστε να μειώσουν την πιθανότητα ένας αντίπαλος να πλαστογραφήσει την υπογραφή κάποιου. Είναι μια παραλλαγή των υπογραφών μιας χρήσης που κάθε φορά μόνο ένα μήνυμα μπορεί να υπογραφεί και να προστατευτεί με ένα κλειδί. Το σχήμα βασίζεται στο πρόβλημα διακριτού λογαρίθμου. Πιο συγκεκριμένα, αν ένας αντίπαλος μπορεί να πλαστογραφήσει μια υπογραφή, τότε ο αυθεντικός υπογράφον μπορεί να αποδείξει την απάτη παρουσιάζοντας την λύση ενός δύσκολου προβλήματος. Τότε η ικανότητα του αντιπάλου να λύσει αυτό το πρόβλημα μεταφέρεται στον υπογράφοντα. Ακόμα, ο υπογράφον δεν μπορεί να κατασκευάσει μια υπογραφή και αργότερα να θεωρηθούν πλαστογραφία. Τέλος, ο όρος fail-stop αναφέρεται στο γεγονός ότι ο υπογράφον μπορεί να ανιχνεύσει και να σταματήσει την πλαστογραφία.

Σχήμα υπογραφής fail-stop των van Heijst-Pedersen

Αλγόριθμος-Παραγωγή κλειδιού
Περίληψη: Η παραγωγή κλειδιού είναι συνεργασία μεταξύ της Alice και ενός έμπιστου τρίτου προσώπου.

1) Το TTP πρέπει να κάνει τα ακόλουθα:
   a) Να επιλέξει δύο πρώτους αριθμούς p και q, έτσι ώστε q να διαιρεί το (p-1) και το πρόβλημα διακριτού λογαρίθμου στο $\mathbb{Z}_p^*$ είναι μη επιλύσιμο.
   b) (Να επιλέξει έναν γεννήτορα α της κυκλικής υποομάδας G του $\mathbb{Z}_p^*$ τάξης q.)
      i. Να επιλέξει ένα τυχαίο στοιχείο $g \in \mathbb{Z}_p^*$ και να υπολογίσει $\alpha = g^{(p-1)/q} \bmod p$.
      ii. Αν α = 1 επανέρχεται στο προηγούμενο βήμα (i).
   c) Να επιλέξει ένα τυχαίο ακέραιο a, $1 \le a \le q-1$ και να υπολογίσει $b = \alpha^a \bmod p$. Ο ακέραιος a κρατιέται μυστικός από τον TTP.
   d) Να στείλει το (p,q,α,β) με ασφάλεια στην Alice.
2) Η Alice πρέπει να κάνει τα ακόλουθα:
   a) Να επιλέξει ακέραιους x_1,x_2,y_1,y_2 από το διάστημα [0,q-1] και να τους κρατήσει μυστικούς.
   b) Να υπολογίσει $\beta_1 = \alpha^{x_1}\beta^{x_2}$ και $\beta_2 = \alpha^{y_1}\beta^{y_2} \bmod p$.
   c) Το δημόσιο κλειδί της Alice είναι το $(\beta_1,\beta_2,p,q,\alpha,\beta)$ και το ιδιωτικό κλειδί της $\tilde{x} = (x_1, x_2, y_1, y_2)$.

Αλγόριθμος-Παραγωγή και επαλήθευση
Περίληψη: Θα περιγραφεί ένα σχήμα υπογραφής μιας χρήσης του οποίου η ασφάλεια βασίζεται στο πρόβλημα διακριτού λογαρίθμου στην υποομάδα τάξης q στο $\mathbb{Z}_p^*$.

1) Παραγωγή υπογραφής. Η Alice για να υπογράψει το μήνυμα $m \in [0, q-1]$, πρέπει να κάνει τα ακόλουθα:
   a) Να υπολογίσει $s_{1,m} = x_1 + my_1 \bmod q$ και $s_{2,m} = x_2 + my_2 \bmod q$.
   b) Η υπογραφή της Alice για το μήνυμα m είναι η $(s_{1,m},s_{2,m})$.
2) Επαλήθευση. Ο Bob για να επαληθεύσει ότι η υπογραφή της Alice για το m είναι η $(s_{1,m},s_{2,m})$, πρέπει να κάνει τα ακόλουθα:
   a) Να αποκτήσει το αυθεντικό δημόσιο κλειδί της Alice $(\beta_1,\beta_2,p,q,\alpha,\beta)$.
   b) Να υπολογίσει $\upsilon_1 = \beta_1\beta_2^m \bmod p$ και $\upsilon_2 = \alpha^{s_{1,m}}\beta^{s_{2,m}} \bmod p$.
   c) Να αποδεχτεί την υπογραφή αν και μόνο αν $\upsilon_1 = \upsilon_2$.

Απόδειξη ότι ο αλγόριθμος επαλήθευσης λειτουργεί:

$$\upsilon_1 \equiv \beta_1 \beta_2^{\,m} \equiv (\alpha^{x_1}\beta^{x_2})(\alpha^{y_1}\beta^{y_2})^m \equiv \alpha^{x_1+my_1}\beta^{x_2+my_2} \equiv \alpha^{s_{1,m}}\beta^{s_{2,m}} \equiv \upsilon_2 \pmod p$$

Αν τώρα υποθέσουμε ότι η Alice θέλει να αποδείξει ότι η υπογραφή της έχει πλαστογραφηθεί. Ο επόμενος αλγόριθμος δείχνει πως η Alice, με μεγάλη πιθανότητα, μπορεί να χρησιμοποιήσει την πλαστογραφημένη υπογραφή για να εξάγει το μυστικό αριθμό a. Όμως, αυτός ο αριθμός είναι υποτίθεται γνωστός μόνο στο TTP και έτσι το παραπάνω αποτελεί απόδειξη ότι η υπογραφή είναι απάτη.

Αλγόριθμος-Απόδειξη πλαστογραφίας

Περίληψη: Η Alice για να αποδείξει ότι η υπογραφή s' = ($s'_{1,m}, s'_{2,m}$) για το μήνυμα m είναι μια απάτη ανακαλύπτει τον $a = \log_\alpha \beta$. Η Alice πρέπει να κάνει τα ακόλουθα:

1) Να υπολογίσει μια υπογραφή $s = (s_{1,m}, s_{2,m})$ για το μήνυμα m χρησιμοποιώντας το ιδιωτικό κλειδί $\tilde{m}$.
2) Αν s = s' να επιστρέψει στο βήμα 1.
3) Να υπολογίσει $a = (s_{1,m} - s'_{1,m})(s_{2,m} - s'_{2,m}) \bmod q$.

11 ΒΙΒΛΙΟΓΡΑΦΙΑ

Chaum D., “Blind signatures for untraceable payments”, Springer-Verlag, 1998

Goldwasser S., Micali S., Rivest R., “ A digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks”, 1995

Kahn D., “The Codebreakers”, Macmillan, 1967

Menezes A., Qu M., Stinson D., Wang Y., “Evaluation of Security Level of Cryptography: ESIGN Signature Scheme”, Certicom Search, 2001

Menezes A., van Oorschot P., Vanstone S.,”Handbook of Applied Cryptography”,1996

Stinson D.”Cryptography Theory and Practice”, third ed., Chapman and Hall, 2006

Trappe W., Washington L.”Introduction to Cryptography with Coding Theory”, Pearson education international, 2006

Wenbo M., “Modern Cryptography: Theory and Practice”, Prentice Hall PTR, 2003

Ζάχος Ε., “Αλγόριθμοι και πολυπλοκότητα”, Ε.Μ.Π., 2003

Ζάχος Ε., “Εισαγωγή στη Θεωρία Αριθμών και Κρυπτολογία”, Ε.Μ.Π., 2005

Κουκουβίνος Χ., Παπαϊωαννου Α., “Κρυπτογραφία”, Ε.Μ.Π., 2007

Πουλάκης Δ., “Κρυπτογραφία η Επιστήμη της Ασφαλούς Επικοινωνίας”, ΖΗΤΗ, 2006