ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΣΙΛΟΓΙΑΝΝΗΣ ΓΕΩΡΓΙΟΣ

Υπεύθυνος Καθηγητής: Α. Παπαϊωάννου

Πρόλογος

Η διπλωματική μου εργασία αναφέρεται στον κλάδο της κρυπτογραφίας, στις ψηφιακές υπογραφές. Οι ψηφιακές υπογραφές είναι μία από τις πιο χρήσιμες ανακαλύψεις της κρυπτογραφίας. Είναι μία μέθοδος να υπογράφουμε ένα μήνυμα που είναι αποθηκευμένο σε ηλεκτρονική μορφή.

Θα παρουσιάσουμε, στο πρώτο κεφάλαιο βασικά μαθηματικά στοιχεία, στο δεύτερο γενικές πληροφορίες για τις ψηφιακές υπογραφές και στο τρίτο τα διάφορα σχήματα των ψηφιακών υπογραφών.

Ειδικότερα, στο πρώτο κεφάλαιο θα παρουσιάσουμε βασικά στοιχεία και ιδιότητες των συναρτήσεων, των πιθανοτήτων, της θεωρίας των αριθμών, της άλγεβρας, στοιχεία της θεωρίας πολυπλοκότητας, σε ποια δύσκολα μαθηματικά προβλήματα στηρίζονται οι ψηφιακές υπογραφές και ορισμένους βασικούς αλγορίθμους που θα τους χρειαστούμε στα επόμενα κεφάλαια.

Στο δεύτερο κεφάλαιο θα αναφέρουμε ορισμένες βασικές έννοιες, συμβολισμούς, τις διάφορες κατηγορίες και την ασφάλεια των ψηφιακών υπογραφών.

Τέλος στο τρίτο κεφάλαιο θα παρουσιάσουμε ορισμένα σχήματα ψηφιακών υπογραφών με τα χαρακτηριστικά τους.

Σε αρκετά σημεία της διπλωματικής μου αναφέρω απλά παραδείγματα, σημαντικά για μένα όμως, για την κατανόηση δύσκολων και πολύπλοκων εννοιών.

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω το καθηγητή κύριο Παπαϊωάννου Αλέξανδρο αλλά και όλους τους καθηγητές που είχα όπου με τη διδασκαλία τους, τις συμβουλές τους και τις παροτρύνσεις τους με βοήθησαν σε μεγάλο βαθμό, να αντεπεξέλθω στις απαιτήσεις, να αποκτήσω γνώσεις, εφόδια και ερεθίσματα που θα μου είναι χρήσιμα στο μέλλον.

Περιεχόμενα

Κεφάλαιο 1
ΜΑΘΗΜΑΤΙΚΑ ΣΤΟΙΧΕΙΑ

1. Εισαγωγή.

Σε αυτό το κεφάλαιο θα αναφέρουμε βασικές μαθηματικές έννοιες που μας είναι χρήσιμες για τη μελέτη των ψηφιακών υπογραφών.

Θα δούμε βασικούς ορισμούς και ιδιότητες των συναρτήσεων, των πιθανοτήτων, της θεωρίας αριθμών , βασικά στοιχεία της άλγεβρας όσο αφορά τις ομάδες τους δακτυλίους, τα σώματα και τις ελλειπτικές καμπύλες. Δε θα επεκταθούμε σε αποδείξεις, απλά θα αναφέρουμε τους ορισμούς και τις ιδιότητες που έχουν.

Στόχος αυτού του κεφαλαίου είναι να δούμε το μαθηματικό υπόβαθρο που υπάρχει και που στηρίζονται τα διάφορα σχήματα ψηφιακών υπογραφών που θα αναφέρουμε στα υπόλοιπα κεφάλαια.

1.1. Συναρτήσεις.

Ένα σύνολο αποτελείται από διαφορετικά αντικείμενα που ονομάζονται στοιχεία του συνόλου.

Ορισμός 1. Μία συνάρτηση ορίζεται από δύο σύνολα X και Y και ένα κανόνα f όπου απεικονίζει κάθε στοιχείο του X σε ακριβώς ένα στοιχείο στο Y. Το σύνολο X ονομάζεται πεδίο ορισμού της συνάρτησης και το σύνολο Y πεδίο τιμών. Αν το x είναι ένα στοιχείο του X ($x \in X$) η εικόνα του x είναι ένα στοιχείο του Y που το βρίσκουμε αν εφαρμόσουμε τον κανόνα f στο x. Η εικόνα y του x ορίζεται ως $y = f(x)$. Μία συνάρτηση f από το σύνολο X στο Y ορίζεται ως $f: X \rightarrow Y$. Το σύνολο όλων των στοιχείων του Y όπου σε κάθε στοιχείο του απεικονίζεται τουλάχιστο ένα στοιχείο του X με τον κανόνα f ονομάζεται εικόνα της f (Im(f)).

Ορισμός 2. Μία συνάρτηση $f: X \rightarrow Y$, είναι 1 – 1 αν κάθε στοιχείο του Y είναι εικόνα το πολύ ενός στοιχείου του X.

Ορισμός 3. Μία συνάρτηση $f: X \rightarrow Y$, είναι επί αν κάθε στοιχείο του Y είναι εικόνα τουλάχιστο ενός στοιχείου του X.

Ορισμός 4. Μία συνάρτηση $f: X \rightarrow Y$, είναι 1 – 1 και επί αν κάθε στοιχείο του Y είναι εικόνα ενός στοιχείου του X.

Ορισμός 5. Μία συνάρτηση $f: X \rightarrow Y$ που είναι 1 – 1 και επί, για κάθε στοιχείο $y \in Y$ ορίζουμε την $g: Y \rightarrow X$, με $g(y) = x$ όπου $x \in X$ και

$f(x)=y$. Η g είναι συνάρτηση και καθορίζεται από την f και λέγεται αντίστροφη της f και συμβολίζεται $g = f^{-1}$.

Υπάρχουν αρκετά είδη συναρτήσεων που έχουν σημαντικό ρόλο στην κρυπτογραφία και στις ψηφιακές υπογραφές.

Ορισμός 6. Μία συνάρτηση $f: X \to Y$ ονομάζεται one – way συνάρτηση αν το $f(x)$ είναι «εύκολα υπολογίσιμο» για όλα τα $x \in X$ αλλά για «σχεδόν όλα» τα στοιχεία $y \in \text{Im}(f)$ είναι «υπολογιστικά ανέφικτο» να βρούμε κάποιο $x \in X$ τέτοιο που $f(x)=y$. Δυστυχώς αν και υπάρχουν πολλές συναρτήσεις που πιστεύουμε ότι είναι one-way μέχρι σήμερα δεν υπάρχει απόδειξη ότι κάποια συγκεκριμένη συνάρτηση έχει αυτή την ιδιότητα.

Θα δούμε δύο παραδείγματα για να καταλάβουμε καλύτερα τι είναι one – way συναρτήσεις.

Παράδειγμα 1. Έστω X ={1,2,3,…,16} και ορίζουμε την $f(x)=r_x$ για όλα τα $x \in X$ όπου r_x είναι το υπόλοιπο όταν το 3^x διαιρεθεί με το 17. Δηλαδή

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$f(x)$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Δοθέντος ενός αριθμού από το 1 έως το 16 είναι εύκολο να βρούμε την εικόνα του με βάση την f. Αλλά είναι δυσκολότερο, αν μας δοθεί για παράδειγμα το 7, να βρούμε το x ώστε $f(x)$ =7. Βέβαια αν αντί για 7 είχαμε το 3 τότε είναι εύκολο να βρούμε ότι x =1, για αυτό το λόγο είπαμε στον ορισμό για «σχεδόν όλα» τα στοιχεία $y \in \text{Im}(f)$. Το σημαντικό στοιχείο εδώ είναι ότι υπάρχει διαφορά στην εργασία για να υπολογίσουμε το $f(x)$ και να βρούμε το x δοθέντος του $f(x)$. ∴

Παράδειγμα 2. Ένας πρώτος αριθμός είναι ένας θετικός ακέραιος μεγαλύτερος από το 1 όπου έχει θετικούς ακέραιους διαιρέτες μόνο το 1 και τον εαυτό του. Επιλέγουμε δύο πρώτους αριθμούς p =48611, q =53993 και υπολογίζουμε $n = p * q$ =2624653723 και ορίζουμε το σύνολο X ={1,2,3,…, n -1}. Ορίζουμε τη συνάρτηση f στο X, όπου $f(x)=r_x \; \forall \; x \in X$ και r_x είναι το υπόλοιπο όταν διαιρούμε το x^3 με το n. Για παράδειγμα f (2489991)=1981394214 επειδή 2489991^3 =5881949859 $* n$ + 1981394214. Για να βρούμε το $f(x)$ είναι εύκολο αλλά η αντίστροφη διαδικασία είναι πολύ πιο δύσκολη. Αν οι παράγοντες του n είναι άγνωστοι και μεγάλοι αριθμοί αυτό είναι ένα δύσκολο πρόβλημα, αλλά αν οι p και q είναι γνωστοί τότε το πρόβλημα είναι εύκολο. ∴

Ορισμός 7. Μία trapdoor one – way συνάρτηση είναι μία one – way συνάρτηση $f: X \to Y$ με μία επιπλέον ιδιότητα (που λέγεται trapdoor πληροφορία) και είναι εύκολο να βρούμε για κάθε $y \in \text{Im}(f)$ ένα $x \in X$ τέτοιο που $f(x)=y$.

Παράδειγμα trapdoor one – way συνάρτησης είναι η συνάρτηση που είδαμε στο παράδειγμα 2 με την επιπλέον πληροφορία να ξέρουμε τους παράγοντες του n (τους αριθμούς p και q).

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

Ορισμός 8. Έστω ένα πεπερασμένο σύνολο S. Μία μετάθεση $p: S \to S$ είναι μία συνάρτηση 1-1 από το S στον εαυτό του.

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

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

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

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

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

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

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

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

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

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

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

1.2. Πιθανότητες.

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

Ορισμός 1. Μία πιθανοτική κατανομή P στο S είναι μία ακολουθία αριθμών $p_1, p_2, ..., p_n$ τέτοια που όλοι οι p_i είναι μη αρνητικοί και έχουν άθροισμα 1. Η πιθανότητα να συμβεί το γεγονός s_i είναι p_i ή $P(s_i)$.

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

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

Ιδιότητα 1. Έστω $E \subseteq S$.

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

(β). $P(\overline{E})$=1-$P(E)$.

Ορισμός 4. Δύο γεγονότα E_1 και E_2 λέγονται αμοιβαίως αποκλειόμενα αν $P(E_1 \cap E_2)$=0. Δηλαδή αν συμβεί το ένα από τα δύο γεγονότα τότε το άλλο δε θα συμβεί ποτέ.

Ιδιότητα 2. Έστω δύο γεγονότα E_1 και E_2.

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

(β). $P(E_1 \cup E_2)$ + $P(E_1 \cap E_2)$= $P(E_1)$+$P(E_2)$. Δηλαδή αν τα E_1 και E_2 είναι ανεξάρτητα τότε $P(E_1 \cup E_2)$= $P(E_1)$+ $P(E_2)$.

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

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

Ορισμός 6. Δύο γεγονότα E_1 και E_2 λέγονται ανεξάρτητα αν $P(E_1 \cap E_2) = P(E_1) * P(E_2)$.

Ιδιότητα 3. (Θεώρημα του Bayes) Αν E_1 και E_2 είναι γεγονότα με $P(E_2)$>0 τότε

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

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

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

1.3. Θεωρία Αριθμών.

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

1.3.1. Ακέραιοι Αριθμοί.

Ορισμός 1. Έστω α και β ακέραιοι. Ο α διαιρεί τον β ($\alpha \mid \beta$) αν υπάρχει ένας ακέραιος γ τέτοιος που $\beta = \alpha * \gamma$.

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

(α). $\alpha \mid \alpha$.

(β). Αν $\alpha \mid \beta$ και $\beta \mid \gamma$ τότε $\alpha \mid \gamma$.

(γ). Αν $\alpha \mid \beta$ και $\alpha \mid \gamma$ τότε $\alpha \mid (\beta * x + \gamma * y)$ για όλα τα $x, y \in Z$.

(δ). Αν $\alpha \mid \beta$ και $\beta \mid \alpha$ τότε $\alpha = \pm \beta$.

Ορισμός 2. (Αλγόριθμος διαίρεσης) Αν α και β είναι ακέραιοι με $\beta \geq 1$ τότε η διαίρεση του α με το β δίδει δύο ακεραίους π (πηλίκο) και υ (υπόλοιπο) τέτοιους που $\alpha = \pi * \beta + \upsilon$, όπου $0 \leq \upsilon \leq \beta$. Οι π και υ είναι μοναδικοί, ο υ συμβολίζεται $\alpha \bmod \beta$.

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

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

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

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

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

(α). $\alpha \mid \delta$ και $\beta \mid \delta$.

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

Ιδιότητα 2. Αν α και β είναι θετικοί ακέραιοι τότε $lcd(\alpha,\beta)=\alpha*\beta/\gcd(\alpha,\beta)$.

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

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

Ιδιότητα 3. Αν ρ είναι πρώτος και $\rho \mid \alpha*\beta$ τότε $\rho \mid \alpha$ ή $\rho \mid \beta$ (ή και τα δύο).

Ιδιότητα 4. Υπάρχουν άπειροι στο πλήθος πρώτοι αριθμοί.

Ιδιότητα 5. Για κάθε ακέραιο $n \geq 2$ υπάρχει μοναδική παραγοντοποίηση του n σε γινόμενο πρώτων αριθμών

$$n = \rho_1^{e_1} * \rho_2^{e_2} * \ldots * \rho_\kappa^{e_\kappa}$$

όπου ρ_i είναι μοναδικοί διαφορετικοί πρώτοι αριθμοί και e_i είναι θετικοί ακέραιοι.

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

Ιδιότητα 6. Η συνάρτηση ϕ έχει τις ακόλουθες ιδιότητες:

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

(β). Αν $\gcd(\alpha,\beta)=1$ τότε $\phi(\alpha*\beta)=\phi(\alpha)*\phi(\beta)$.

(γ). Αν $n=\rho_1^{e_1} * \rho_2^{e_2} * \ldots * \rho_\kappa^{e_\kappa}$ είναι η παραγοντοποίηση σε πρώτους αριθμούς του n τότε

$$\phi(n)=n*(1-\frac{1}{\rho_1})*(1-\frac{1}{\rho_2})*\ldots*(1-\frac{1}{\rho_\kappa}).$$

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

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

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

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

(β). $\alpha = \alpha \bmod n$

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

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

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

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

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

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

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

Κινέζικο Θεώρημα Υπολοίπων. Αν οι ακέραιοι $n_1, n_2, ..., n_\kappa$ είναι ανά δύο σχετικώς πρώτοι τότε το σύστημα εξισώσεων

$$x = \alpha_1 \bmod n_1$$
$$x = \alpha_2 \bmod n_2 .$$
$$\vdots$$
$$x = \alpha_\kappa \bmod n_\kappa$$

έχει μία μοναδική λύση $n = n_1 * n_2 * ... * n_\kappa$.

Ιδιότητα 10. Αν $\gcd(n_1, n_2)$=1, τότε το ζευγάρι εξισώσεων $x = \alpha \bmod n_1$ και $x = \alpha \bmod n_2$ έχει μοναδική λύση $x = \alpha \bmod (n_1 n_2)$.

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

Ορισμός 14. Τάξη του Z_n^* ορίζεται ο αριθμός των στοιχείων στο Z_n^* και συμβολίζεται $|Z_n^*|$. (Συνδυάζοντας και τον Ορισμό 8 έχουμε ότι $\phi(n) = |Z_n^*|$).

Ιδιότητα 11. Έστω $n \ge 2$ είναι ένας ακέραιος τότε:

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

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

Ιδιότητα 12. Έστω p είναι πρώτος αριθμός τότε:

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

(β). Αν $r = s \ (\bmod p$ -1) τότε $\alpha^r = \alpha^s \ (\bmod p)$ για όλους τους ακέραιους α.

(γ). $\alpha^p = \alpha \ (\bmod p)$ για όλους τους ακέραιους α.

Ορισμός 15. Έστω $\alpha \in Z_n^*$. Τάξη του α ($ord(\alpha)$) είναι ο ελάχιστος θετικός ακέραιος t τέτοιος που $\alpha^t = 1 (\bmod n)$.

Ιδιότητα 13. Αν η τάξη του $\alpha \in Z_n^*$ είναι t και $\alpha^s = 1 (\bmod n)$ τότε ο t διαιρεί τον s.

Ορισμός 16. Έστω $\alpha \in Z_n^*$. Αν η τάξη του α είναι $\phi(n)$ τότε ο α είναι γεννήτορας του Z_n^*. Αν το Z_n^* έχει ένα γεννήτορα τότε το Z_n^* λέγεται κυκλικό.

Ιδιότητα 14. Ιδιότητες των γεννητόρων του Z_n^*.

(α). Το Z_n^* έχει ένα γεννήτορα αν και μόνο αν $n = 2$ ή 4 ή p^κ ή $2p^\kappa$ όπου p είναι περιττός πρώτος αριθμός και $\kappa \geq 1$.

(β). Αν α είναι γεννήτορας του Z_n^* τότε $Z_n^* = \{\alpha^i \bmod n \mid 0 \leq i \leq \phi(n) - 1\}$.

(γ). Έστω α ένας γεννήτορας του Z_n^*. Τότε $\beta = \alpha^i \bmod n$ είναι επίσης γεννήτορας του Z_n^* αν και μόνο αν $\gcd(i, \phi(n)) = 1$. Αν το Z_n^* είναι κυκλικό τότε ο αριθμός των γεννητόρων είναι $\phi(\phi(n))$.

(δ). Έστω $\alpha \in Z_n^*$, ο α είναι γεννήτορας του Z_n^* αν και μόνο αν $\alpha^{\phi(n)/p} \neq 1 (\bmod n)$ για κάθε πρώτο διαιρέτη p του $\phi(n)$.

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

Ιδιότητα 15. Έστω p είναι ένας περιττός πρώτος αριθμός και α ένας γεννήτορας του Z_p^*. Τότε $\beta \in Z_p^*$ είναι τετραγωνικό υπόλοιπο του modulo p αν και μόνο αν $\beta = \alpha^i \bmod p$ όπου i είναι ένας άρτιος ακέραιος. Έπεται ότι $|Q_p| = (p-1)/2$ και $|\overline{Q_n}| = (p-1)/2$, δηλαδή τα μισά στοιχεία στο Z_p^* είναι τετραγωνικά υπόλοιπα και τα άλλα μισά δεν είναι.

Ιδιότητα 16. Έστω n είναι το γινόμενο δύο διαφορετικών περιττών πρώτων αριθμών p και q, $n = p * q$. Τότε $\alpha \in Z_n^*$ είναι ένα τετραγωνικό υπόλοιπο του modulo n αν και μόνο αν $\alpha \in Q_p$ και $\alpha \in Q_q$.

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

Ιδιότητα 17. Για τον αριθμό των τετραγωνικών ριζών ισχύουν:

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

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

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

Ιδιότητα 18. Έστω $n = p * q$ είναι ένας Blum ακέραιος και $\alpha \in Q_n$. Τότε ο α έχει ακριβώς τέσσερις τετραγωνικές ρίζες $\bmod n$, και μόνο μία από αυτές ανήκει στο Q_n.

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

Ιδιότητα 19. Αν $n = p * q$ είναι ένας Blum ακέραιος τότε η συνάρτηση $f: Q_n \to Q_n$ ορίζεται από τον τύπο $f(x) = x^2 \bmod n$ είναι μία μετάθεση. Η αντίστροφη της f είναι $f^{-1}(x) = x^{((p-1)(q-1)+4)/8}$.

1.3.2. Σύμβολα Legendre και Jacobi.

Ορισμός 1. Έστω p είναι ένας περιττός πρώτος και a ένας ακέραιος. Το σύμβολο Legendre $(\frac{\alpha}{p})$ ορίζεται ως εξής:

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

Ιδιότητα 1. Έστω p ένας περιττός πρώτος αριθμός και $a, \beta \in \mathrm{Z}$. Τότε το σύμβολο Legendre έχει τις ακόλουθες ιδιότητες:

(α). $(\frac{\alpha}{p}) = \alpha^{(p-1)/2} \pmod p$.

(β). $(\frac{\alpha\beta}{p}) = (\frac{\alpha}{p})(\frac{\beta}{p})$.

(γ). Αν $a = \beta \pmod p$ τότε $(\frac{\alpha}{p}) = (\frac{\beta}{p})$.

(δ). Αν q είναι περιττός πρώτος διαφορετικός από τον p τότε

$$(\frac{p}{q})=(\frac{q}{p})(-1)^{(p-1)(q-1)/4}.$$

Ορισμός 2. Έστω $n \geq 3$ περιττός με $n = p_1^{e_1} * p_2^{e_2} * ... * p_k^{e_k}$. Το σύμβολο Jabobi $(\frac{\alpha}{n})$ ορίζεται ως εξής:

$$(\frac{\alpha}{n})=(\frac{\alpha}{p_1})^{e_1}(\frac{\alpha}{p_2})^{e_2}\dots(\frac{\alpha}{p_k})^{e_k}.$$

Ιδιότητα 2. Έστω $m \geq 3$, $n \geq 3$ περιττοί ακέραιοι και $a, \beta \in Z$. Τότε το σύμβολο Jacobi έχει τις ακόλουθες ιδιότητες:

(α). $(\frac{\alpha}{n})$=0 ή 1 ή –1. Επιπλέον $(\frac{\alpha}{n})$=0 αν και μόνο αν $\gcd(a, n) \neq 1$.

(β). $(\frac{\alpha\beta}{n}) = (\frac{\alpha}{n})(\frac{\beta}{n})$.

(γ). $(\frac{\alpha}{mn}) = (\frac{\alpha}{m})(\frac{\alpha}{n})$.

(δ). Αν $a = \beta \pmod n$ τότε $(\frac{\alpha}{n})=(\frac{\beta}{n})$.

(ε). $(\frac{1}{n})$=1.

(στ). $(\frac{-1}{n})=(-1)^{(n-1)/2}$.

(ζ). $(\frac{2}{n})=(-1)^{(n^2-1)/8}$.

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

1.4. Άλγεβρα

1.4.1. Ομάδες.

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

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

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

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

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

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

Ορισμός 3. Ένα μη κενό υποσύνολο H της ομάδος G είναι υποομάδα της G αν το H είναι ομάδα και σέβεται την πράξη $*$ της G. Αν το H είναι υποομάδα της G και $H \neq G$ τότε το H λέγεται γνήσια υποομάδα της G.

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

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

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

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

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

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

Ιδιότητα 5. Έστω G είναι μία ομάδα.

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

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

1.4.2. Δακτύλιοι.

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

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

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

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

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

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

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

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

1.4.3. Σώματα.

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

Ορισμός 2. Η χαρακτηριστική ενός σώματος είναι 0 αν $\underbrace{1+1+\ldots+1}_{m \quad \phi o \rho \acute{\epsilon} \varsigma}$ δεν είναι ποτέ μηδέν για οποιοδήποτε $m \geq 1$. Αλλιώς η χαρακτηριστική του σώματος είναι ο ελάχιστος θετικός ακέραιος m τέτοιος που $\sum_{i=1}^{m} 1$ είναι ίσο με 0.

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

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

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

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

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

Ιδιότητα 4. Για κάθε δύναμη p^m του πρώτου p υπάρχει ένα μοναδικό πεπερασμένο σώμα τάξης p^m .

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

1.4.4. Ελλειπτικές Καμπύλες.

Ορισμός 1. Έστω p >3 ένας πρώτος αριθμός. Η ελλειπτική καμπύλη E $Y^2 = X^3 + \alpha X + \beta$ στο Z_p είναι το σύνολο των λύσεων $(x, y) \in Z_p \times Z_p$ της $Y^2 = X^3 + \alpha X + \beta \pmod p$, όπου α, $\beta \in Z_p$ είναι σταθερές τέτοιες που $4a^3 + 27\beta^2 \neq 0 \pmod p$ καθώς και ένα ειδικό σημείο *O* που λέγεται σημείο στο άπειρο.

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

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

Στους παρακάτω κανόνες θεωρούμε ότι P , $Q \neq O$.

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

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

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

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

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

(β). Αλλιώς $P + Q = (x_3, y_3)$ όπου

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

$y_3 = \lambda (x_1 - x_3) - y_1$ με

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \alpha\nu \quad P = Q \\ \dfrac{3x_1^2 + \alpha}{2y_1} & \alpha\nu \quad P \neq Q \end{cases}$$

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

1.5. Θεωρία Πολυπλοκότητας και Αλγόριθμοι

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

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

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

1.5.1. Θεωρία πολυπλοκότητας.

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

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

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

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

στηρίζεται σε προβλήματα που είναι NP-complete αλλά σε προβλήματα που η δυσκολία τους βρίσκεται ανάμεσα στις κλάσεις P και NP-complete.

β. Στη θεωρία πολυπλοκότητας μελετάμε τα προβλήματα στη χειρότερη τους περίπτωση (worst case) όπου και υπολογίζουμε τους χρόνους εκτέλεσης και θέλουμε αλγορίθμους με καλή απόδοση σε αυτή την περίπτωση. Στα σχήματα όμως των ψηφιακών υπογραφών αυτό δεν αρκεί. Για παράδειγμα δεν είναι αποδεκτός αυτός ο αλγόριθμος που δίνει το δικαίωμα στον αντίπαλο να αποκρυπτογραφήσει τα μισά από όλα τα πιθανά μηνύματα ακόμα και αν η αποκρυπτογράφηση των υπολοίπων θέλει εκθετικό χρόνο.

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

1.5.2. Ασυμπτωτικοί Ορισμοί.

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

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

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

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

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

Ορισμός 4.

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

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

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

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

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

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

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

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

(δ). Αν $f(n) = O(h(n))$ και $g(n) = O(l(n))$ τότε $(f*g)(n) = O(h(n)*l(n))$.

(ε). $f(n) = O(f(n))$.

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

Ιδιότητα 2.

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

(β). Για οποιαδήποτε σταθερά $c > 0$, $\log_c n = \Theta(\log n)$.

(γ). $\log(n!) = \Theta(n * \log n)$.

(δ). Για όλους τους ακεραίους $n \geq 1$,

$$\sqrt{2*\pi*n}*\left(\frac{n}{e}\right)^n \leq n! \leq \sqrt{2*\pi*n}*\left(\frac{n}{e}\right)^{n+(1/(12n))}.$$

1.5.3. Κλάσεις Πολυπλοκότητας.

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

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

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

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

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

Παράδειγμα 1. Έστω ότι έχουμε το παρακάτω πρόβλημα απόφασης: Μας δίνεται ένας θετικός ακέραιος αριθμός n και θέλουμε να βρούμε αν ο n είναι σύνθετος. Δηλαδή υπάρχουν ακέραιοι α, β >1 τέτοιοι που $n = \alpha * \beta$;

Το πρόβλημα αν ένας αριθμός είναι σύνθετος ανήκει στην κλάση NP (πρόσφατα αποδείχθηκε ότι PRIMES $\in P$)γιατί αν ο n είναι σύνθετος, τότε αυτό το γεγονός μπορεί να πιστοποιηθεί σε πολυωνυμικό χρόνο αν κάποιος μας δώσει ένα διαιρέτη του n τον α όπου 1< α < n (το πιστοποιητικό είναι ο α). ∴

Ιδιότητα 1. $P \subseteq NP$ και $P \subseteq co - NP$.

Ιδιότητα 2. Τα παρακάτω ερωτήματα είναι ανοικτά (αν και πιστεύεται ότι δεν ισχύουν, δεν έχει αποδειχθεί τίποτα):

(α). Ισχύει $P = NP$;

(β). Ισχύει $NP = co - NP$;

(γ). Ισχύει $P = NP \cap co - NP$;

Ορισμός 5. Έστω L_1 και L_2 είναι δύο προβλήματα απόφασης. Το L_1 ανάγεται σε πολυωνυμικό χρόνο στο L_2 ($L_1 \leq_P L_2$) αν υπάρχει ένας αλγόριθμος που λύνει το L_1 ο οποίος χρησιμοποιεί, σαν υπορουτίνα, ένα αλγόριθμο για την επίλυση του L_2, και ο οποίος τρέχει σε πολυωνυμικό χρόνο αν ο αλγόριθμος για το L_2 τρέχει σε πολυωνυμικό χρόνο.

Ορισμός 6. Έστω L_1 και L_2 είναι δύο προβλήματα απόφασης. Αν $L_1 \leq_P L_2$ και $L_2 \leq_P L_1$ τότε τα L_1 και L_2 είναι υπολογιστικά ισοδύναμα.

Ιδιότητα 3. Έστω L_1, L_2 και L_3 είναι προβλήματα απόφασης.

(α). Αν $L_1 \leq_P L_2$ και $L_2 \leq_P L_3$ τότε $L_1 \leq_P L_3$.

(β). Αν $L_1 \leq_P L_2$ και $L_2 \in P$ τότε $L_1 \in P$.

Ορισμός 7. Ένα πρόβλημα απόφασης L είναι NP -complete αν:

(α). Το $L \in NP$.

(β). $L_1 \leq_P L$ για κάθε $L_1 \in NP$.

Η κλάση όλων των προβλημάτων που είναι NP -complete ονομάζεται NPC .

Ορισμός 8. Ένα πρόβλημα απόφασης L είναι NP -hard αν

$L' \leq_P L$ για κάθε $L' \in NP$.

Ιδιότητα 4. Έστω L_1 και L_2 είναι δύο προβλήματα απόφασης.

(α). Αν L_1 είναι NP -complete και $L_1 \in P$, τότε $P = NP$.

(β). Αν $L_1 \in NP$, L_2 είναι NP -complete και $L_2 \leq_P L_1$, τότε L_1 είναι NP -complete.

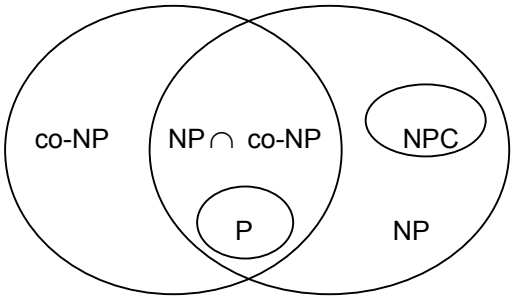
(γ). Αν L_1 είναι NP -complete και $L_1 \in co - NP$, τότε $NP = co - NP$.

Οι σχέσεις των κλάσεων μεταξύ τους φαίνονται στο σχήμα 1.

Ορισμός 9. Η κλάση πολυπλοκότητας RP περιλαμβάνει το σύνολο των προβλημάτων απόφασης L που χρησιμοποιούν ένα πιθανοτικό αλγόριθμο A που τρέχει σε πολυωνυμικό χρόνο και για κάθε είσοδο x

(α). Αν $x \in L \Rightarrow \Pr[A(x)=\text{NAI}] \geq \frac{1}{2}$.

(β). Αν $x \notin L \Rightarrow \Pr[A(x)=\text{OXI}]=0$.



Σχήμα 1.

Ορισμός 10. Η κλάση πολυπλοκότητας ZPP περιλαμβάνει το σύνολο των προβλημάτων απόφασης L που χρησιμοποιούν ένα πιθανοτικό αλγόριθμο A που τρέχει σε πολυωνυμικό χρόνο και για κάθε είσοδο x

(α). $\forall$ x Pr[A(x)=ΝΑΙ ή ΟΧΙ] $\geq \frac{1}{2}$.

(β). $\forall$ x Pr[A(x)=ΔΕΝ ΞΕΡΩ]< $\frac{1}{2}$.

Ιδιότητα 5. $ZPP = RP \cap co-RP$.

Ορισμός 11. Η κλάση πολυπλοκότητας BPP περιλαμβάνει το σύνολο των προβλημάτων απόφασης L που χρησιμοποιούν ένα πιθανοτικό αλγόριθμο A που τρέχει σε πολυωνυμικό χρόνο και για κάθε είσοδο x

(α). Αν x$\in$ L $\Rightarrow$ Pr[A(x)=ΝΑΙ] $\geq \frac{3}{4}$.

(β). Αν x $\notin$ L $\Rightarrow$ Pr[A(x)=ΝΑΙ]< $\frac{1}{4}$.

Ιδιότητα 6.

(α). $P \subseteq ZPP \subseteq RP \subseteq BPP$.

(β). $RP \subseteq NP$.

1.5.4. Δύσκολα Υπολογιστικά Μαθηματικά Προβλήματα.

Σε αυτή την ενότητα θα δούμε πάνω σε ποια μαθηματικά προβλήματα στηρίζονται τα σχήματα των ψηφιακών υπογραφών που θα μελετήσουμε αργότερα.

(α). Πρόβλημα της παραγοντοποίησης ακεραίου.

Το πρόβλημα της παραγοντοποίησης ενός ακεραίου n, είναι δοθέντος του n να βρούμε τους παράγοντες του. Ένα από τα πιο ενδιαφέροντα ανοικτά προβλήματα είναι αν το πρόβλημα της παραγοντοποίησης είναι NP-hard. Τα αντίστοιχα προβλήματα απόφασης είναι αν ο n είναι σύνθετος (COMPOSITENESS) ή αν ο n είναι πρώτος (PRIMALITY). Βέβαια φαίνεται να είναι πιο δύσκολο το να βρούμε τους πρώτους παράγοντες του n, αν ο n είναι σύνθετος

παρά να βρούμε μόνο αν ο n είναι σύνθετος ή όχι. Το ένα πρόβλημα είναι συμπλήρωμα του άλλου. Γνωρίζουμε ότι COMPOSITENESS $\in NP$ άρα το PRIMALITY $\in co-NP$ και COMPOSITENESS $\in co-NP$ και PRIMALITY $\in NP$. Δηλαδή COMPOSITENESS και PRIMALITY $\in NP \cap co-NP$. Δεν ξέρουμε αν το COMPOSITENESS είναι NP-complete. Πιστεύεται ότι το COMPOSITENESS δεν είναι NP-complete και η δυσκολία του βρίσκεται κάπου ανάμεσα στις κλάσεις P και NP-complete. Αν αποδείξουμε ότι κάποιο πρόβλημα που ανήκει $NP \cap co-NP$ είναι NP-complete τότε θα έχουμε το απρόσμενο αποτέλεσμα ότι $NP = co-NP$. Για αυτά τα προβλήματα για την επίλυση τους χρησιμοποιούμε πιθανοτικούς αλγορίθμους.

Αποδείχθηκε από το (2002) ότι PRIMES $\in P$. Αν λοιπόν κάποιο κρυπτοσύστημα στηριζόταν στη δυσκολία να βρούμε αν ένας αριθμός είναι πρώτος, αυτό το κρυπτοσύστημα θα κατέρρεε.

(β). Πρόβλημα εκθετοποίησης.

Το πρόβλημα της εκθετοποίησης, να υπολογίσουμε το $y = x^{\alpha} \pmod n$ δοθέντων των α, x, n είναι σχετικά εύκολο. Υπάρχουν όμως δύο σχετιζόμενα με αυτό προβλήματα που είναι πολύ δύσκολα.

(1). Πρόβλημα του διακριτού λογαρίθμου.

Το πρόβλημα του διακριτού λογαρίθμου είναι δοθέντων των x, y και n να βρούμε ένα εκθέτη α τέτοιο που $y = x^{\alpha} \pmod n$. Πιστεύεται ότι αυτό το πρόβλημα είναι εξαιρετικά δύσκολο και δεν έχει βρεθεί μέχρι σήμερα κάποιος αποδοτικός αλγόριθμος. Γνωρίζουμε ότι το πρόβλημα του υπολογισμού της συνάρτησης της $\phi(n)$ είναι ισοδύναμο με την παραγοντοποίηση του n, δηλαδή ένας αποδοτικός αλγόριθμος για το ένα πρόβλημα θα μας δώσει ένα αποδοτικό για το άλλο. Παραμένει ένα ενδιαφέρον ανοικτό ερώτημα να συσχετίσουμε τη δυσκολία του προβλήματος του διακριτού αλγορίθμου με αυτή του προβλήματος της παραγοντοποίησης. Πιστεύεται ότι αυτό το πρόβλημα είναι δύσκολο ακόμα και στη μέση περίπτωση (average case) π.χ. είναι δύσκολο και για τυχαίες εισόδους. Αν βρεθεί απόδειξη για αυτή την περίπτωση θα έχει σημαντικές επιπτώσεις στην κρυπτογραφία αφού θα έχει ως συνέπεια ότι η εκθετική συνάρτηση θα είναι μία one-way συνάρτηση.

(2). Το πρόβλημα εύρεσης ριζών.

Το πρόβλημα εύρεσης ριζών είναι δοθέντων των α,y και n να βρούμε ένα x τέτοιο που $y = x^{\alpha} \pmod n$. Το πρόβλημα αυτό έχει αποδειχθεί για την περίπτωση που το α=2 είναι ισοδύναμο με την παραγοντοποίηση ενός ακεραίου.

1.5.5. Αλγόριθμοι.

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

(α). Αλγόριθμος του Ευκλείδη.

(1). Όσο ισχύει $\beta \neq 0$ κάνε:

Θέσε $r \leftarrow \alpha \mod \beta$, $\alpha \leftarrow \beta$, $\beta \leftarrow$r.

(2). Επέστρεψε το (α).

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

Μπορούμε να γενικεύσουμε τον αλγόριθμο του Ευκλείδη ώστε εκτός από το μέγιστο κοινό διαιρέτη d των α , β να βρίσκει και δύο ακέραιους x , y τέτοιους που $\alpha\ x + \beta\ y = d$. Είσοδος του αλγορίθμου είναι δύο μη αρνητικοί ακέραιοι α και β με $\alpha \geq \beta$ και έξοδος είναι $\gcd(\alpha , \beta) = d$ και ακέραιοι x , y τέτοιοι που $\alpha\ x + \beta\ y = d$.

(β). Εκτεταμένος αλγόριθμος του Ευκλείδη.

(1). Αν β=0 τότε θέσε $d \leftarrow \alpha$, $x \leftarrow 1$, $y \leftarrow 0$ και επέστρεψε (d , x , y).

(2). Θέσε $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.

(3). Όσο ισχύει β >0 κάνε:

$q \leftarrow \lfloor \alpha / \beta \rfloor , r \leftarrow \alpha - q * \beta , x \leftarrow x_2 - q * x_1 ,$

$y \leftarrow y_2 - q * y_1$.

$\alpha \leftarrow \beta , \beta \leftarrow r , x_2 \leftarrow x_1 , x_1 \leftarrow x , y_2 \leftarrow y_1 , y_1 \leftarrow y$.

(4). Θέσε $d \leftarrow \alpha , x \leftarrow x_2 , y \leftarrow y_2$ και επέστρεψε (d , x , y).

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

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

(γ). Αλγόριθμος εύρεσης αντίστροφου στοιχείου.

(1). Χρησιμοποίησε τον εκτεταμένο αλγόριθμο του Ευκλείδη για να βρεις ακέραιους x και y τέτοιους που $\alpha * x + n * y = d$ με $d = \gcd(\alpha , n)$.

(2). Αν d >1 τότε δεν υπάρχει α^{-1} , αλλιώς επέστρεψε το (x).

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

(δ). Αλγόριθμος υπολογισμού $\alpha^{\kappa} \bmod n$.

Είσοδος είναι $\alpha \in Z_n$ και ένας ακέραιος κ με $0 \leq \kappa \leq$n όπου η δυαδική αναπαράσταση είναι $\kappa = \sum_{i=0}^{t} k_i * 2^i$ και έξοδος $\alpha^{\kappa} \bmod n$.

(1). Θέσε $\beta \leftarrow 1$. Αν κ =0 τότε επέστρεψε (β).

(2). Θέσε $A \leftarrow \alpha$.

(3). Αν κ_0 =1 τότε θέσε $\beta \leftarrow \alpha$.

(4). Για i =1 έως t κάνε:

Θέσε $A \leftarrow A^2 \bmod n$.

Αν κ_i =1 τότε θέσε $\beta \leftarrow A * \beta \mod n$.

(5). Επέστρεψε (β).

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

Θα δούμε τώρα ένα αλγόριθμο για να υπολογίζουμε το σύμβολο Jacobi ($J(\alpha, n)$) ή το σύμβολο Legendre. Είσοδος του αλγορίθμου είναι ένας περιττός ακέραιος $n \geq 3$ και ένας ακέραιος α με $0 \leq \alpha \leq n$ και έξοδος είναι $J(\alpha, n)$ (Αν ο n είναι πρώτος έχουμε το σύμβολο Legendre).

(ε). Αλγόριθμος υπολογισμού συμβόλου Jacobi (Legendre).

(1). Αν α =0 τότε επέστρεψε (0).

(2). Αν α =1 τότε επέστρεψε (1).

(3). Γράψε τον $\alpha = 2^e \alpha_1$, όπου α_1 είναι περιττός.

(4). Αν e είναι περιττός τότε θέσε $s \leftarrow 1$.

Αλλιώς θέσε $s \leftarrow 1$ αν n =1 ή 7 ($\bmod 8$) ή

Θέσε $s \leftarrow -1$ αν n =3 ή 5 ($\bmod 8$).

(5). Αν n =3($\bmod 4$) και α_1 =3($\bmod 4$) τότε θέσε $s \leftarrow -s$.

(6). Θέσε $n_1 \leftarrow n \mod \alpha_1$.

(7). Αν α_1 =1 τότε επέστρεψε (s). Αλλιώς επέστρεψε ($s * J(n_1, \alpha_1)$).

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

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

(στ). Αλγόριθμος υπολογισμού τετραγωνικών ριζών.

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

(1). Υπολόγισε το σύμβολο Legendre (L(α , p)) με τον αλγόριθμο (ε). Αν L(α , p)=-1 τότε επέστρεψε ότι ο α δεν έχει τετραγωνική ρίζα και σταμάτα.

(2). Επέλεξε ακεραίους β με $1 \leq \beta \leq p$ -1 τυχαία μέχρι να βρεις κάποιον με L(β , p)=-1 (Ο β δεν είναι τετραγωνικό υπόλοιπο).

(3). Με επαναλαμβανόμενες διαιρέσεις με το 2 , γράψε p -1= $2^s * t$ όπου t είναι περιττός.

(4). Υπολόγισε το $\alpha^{-1} \bmod p$ με τον αλγόριθμο (γ).

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

(6). Για i =1 έως s -1 κάνε :

Υπολόγισε $d = (r^2 * \alpha^{-1})^{2^{s-i-1}} \bmod p$.

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

Θέσε $c \leftarrow c^2 \bmod p$.

(7). Επέστρεψε (r ,- r).

Ο παραπάνω αλγόριθμος είναι πιθανοτικός και ο αναμενόμενος χρόνος εκτέλεσης είναι $O((\log n)^4)$ δυαδικές πράξεις. Δεν ξέρουμε μέχρι σήμερα κάποιο ντετερμινιστικό αλγόριθμο για αυτό το πρόβλημα (ανοικτό).

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

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

(1). Υπολόγισε $r = \alpha^{(p+1)/4} \bmod p$ (Με τον αλγόριθμο (δ)).

(2). Επέστρεψε (r ,- r).

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

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

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

(1). Υπολόγισε $d = \alpha^{(p-1)/4} \bmod p$ (Με τον αλγόριθμο (δ)).

(2). Αν d =1 τότε υπολόγισε $r = \alpha^{(p+3)/8} \bmod p$.

(3). Αν d = p -1 τότε υπολόγισε r =2α (4α)$^{(p-5)/8} \bmod p$.

(4). Επέστρεψε (r ,- r).

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

(θ). Αλγόριθμος υπολογισμού $g(x)^\kappa \bmod f(x)$.

Είσοδος του αλγορίθμου είναι $g(x) \in F_{p^m}$, k με $0 \le k \le p^m - 1$ όπου η δυαδική αναπαράσταση είναι k= $\sum_{i=0}^{t} k_i * 2^i$ (Το σώμα F_{p^m} αναπαριστάται ως $Z_p[x]/f(x)$, όπου $f(x) \in Z_p[x]$ είναι ένα ανάγωγο πολυώνυμο βαθμού m πάνω στο Z_p και έξοδος $g(x)^\kappa \bmod f(x)$.

(1). Θέσε $s(x) \leftarrow 1$. Αν κ=0 τότε επέστρεψε ($s(x)$).
(2). Θέσε $G(x) \leftarrow g(x)$.
(3). Αν κ_0=1 τότε θέσε $s(x) \leftarrow g(x)$.
(4). Για i=1 έως t κάνε:
Θέσε $G(x) \leftarrow G(x)^2 \bmod f(x)$.
Αν κ_i=1 τότε θέσε $s(x) \leftarrow G(x) * s(x) \bmod f(x)$.
(5). Επέστρεψε ($s(x)$).

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

(ι). Αλγόριθμος υπολογισμού τετραγωνικών ριζών.

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

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

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

(ια). Αλγόριθμος υπολογισμού τετραγωνικών ριζών όπου n είναι σύνθετος αριθμός και $n = p * q$ με p, q πρώτοι αριθμοί.

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

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

(5) Επέστρεψε ($\pm\ x \bmod n$, $\pm\ y \bmod n$).

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

Από αυτό τον αλγόριθμο συμπεραίνουμε ότι εάν κάποιος μπορεί να βρει τους πρώτους παράγοντες ενός αριθμού n (FACTORING) τότε το πρόβλημα εύρεσης των τετραγωνικών ριζών (SQROOT) είναι εύκολο πρόβλημα. Δηλαδή SQROOT $\leq_P$ FACTORING. Ισχύει όμως και το αντίστροφο δηλαδή FACTORING $\leq_P$ SQROOT , άρα τα δύο αυτά προβλήματα είναι ισοδύναμα.

Κεφάλαιο 2
Ψηφιακές Υπογραφές.

2. Εισαγωγή.

Ψηφιακή υπογραφή είναι μία μέθοδος να υπογράφουμε ένα μήνυμα που βρίσκεται σε ηλεκτρονική μορφή. Όπως και η απλή υπογραφή σε κάποιο έγγραφο, χρησιμοποιείται για να προσδιορίσει το άτομο που είναι υπεύθυνο για αυτό. Ένα τέτοιο μήνυμα(με ψηφιακή υπογραφή) μπορεί να μεταδοθεί μέσω ενός δικτύου υπολογιστών. Ο παραλήπτης του μηνύματος πρέπει να μπορεί να πιστοποιήσει αν η υπογραφή είναι αληθινή ή πλαστή. Το μοντέλο της ψηφιακής υπογραφής περιλαμβάνει τη δημιουργία των κλειδιών και της υπογραφής και την πιστοποίηση της υπογραφής.

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

Ενδιαφέρουσες προσεγγίσεις για τις επιθέσεις εναντίον των σχημάτων των ψηφιακών υπογραφών έγιναν από τους Goldwasser,Micali και Rivest. Πολλά από τα ψηφιακά σχήματα που έχουν ανακαλυφθεί έχει αποδειχθεί ότι είναι ανασφαλή.

Το 1991 εκδόθηκε από τον International Standards Organization (ISO) το πρώτο διεθνές πρότυπο για τις ψηφιακές υπογραφές το ISO/IEC 9796 για ψηφιακές υπογραφές με ανάκτηση του μηνύματος. Τα κύρια χαρακτηριστικά του ήταν:

(α). Βασίζεται σε κρυπτοσυστήματα δημοσίου κλειδιού.

(β). Ο αλγόριθμος δημιουργίας της ψηφιακής υπογραφής δεν είναι συγκεκριμένος, αλλά θα πρέπει να απεικονίζει k-bits σε k-bits.

(γ). Χρησιμοποιείται για την κρυπτογράφηση μηνυμάτων συγκεκριμένου μήκους και δεν απαιτεί την ύπαρξη hash συνάρτησης.

(δ). Μπορεί να υποστηρίξει σχήματα υπογραφών με ανάκτηση του μηνύματος.

(ε). Όπου απαιτείται υποστηρίζει το padding του μηνύματος.

Σχήματα υπογραφών που ικανοποιούν το ISO/IEC 9796 είναι το RSA και το τροποποιημένο σχήμα υπογραφής Rabin δημοσίου κλειδιού.

Σήμερα για τις ψηφιακές υπογραφές υπάρχουν τα παρακάτω διεθνή πρότυπα:

(α). NIST:FIPS Publication 186-2: Digital Signature Standard (DSS), January 2000.

(β). NIST:FIPS Publication 180-1: Secure Hash Standard (SHS-1), May 1995.

(γ). ISO/IEC 10118-3: Information Technology- Security Techniques- Hash Functions- Part 3: Dedicated Hash Functions, 1998.

(δ). ISO/IEC 14888-3: Information Technology- Security Techniques- Digital Signature with Appendix- Part 3: Certificate-based mechanisms, 1999.

(ε). IEEE P1363: Standard specification for public key cryptography.

(στ). ANSI X9.62-1998: Public Key Cryptography for the Financial Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

(ζ). ISO/IEC 15946-2(FCD): Information Technology- Security Techniques- Cryptographic techniques based on elliptic curves- Part 2: Digital Signatures,2000.

Σε αυτό το κεφάλαιο θα δούμε βασικές έννοιες των ψηφιακών υπογραφών και ορισμένα σχήματα ψηφιακών υπογραφών.

2.1. Βασικοί Ορισμοί και Συμβολισμοί.

Θα αρχίσουμε με τον ορισμό βασικών εννοιών με τις ψηφιακές υπογραφές.

(α). Ψηφιακή υπογραφή (ή υπογραφή) είναι μία συμβολοσειρά που συνδυάζει ένα μήνυμα με μία αυθεντική οντότητα.

(β). Αλγόριθμος δημιουργίας υπογραφής είναι μια μέθοδος παραγωγής μιας υπογραφής.

(γ). Αλγόριθμος πιστοποίησης υπογραφής είναι μια μέθοδος που πιστοποιεί αν η υπογραφή είναι αυθεντική για το συγκεκριμένο μήνυμα.

(δ). Μηχανισμός υπογραφής αποτελείται από τους αλγόριθμους δημιουργίας και πιστοποίησης υπογραφής.

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

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

Στον πίνακα που ακολουθεί φαίνονται διάφορα σύμβολα που θα χρησιμοποιήσουμε σε αυτό το κεφάλαιο.

Σύμβολο	**Ερμηνεία**
M	Ένα σύνολο στοιχείων που ονομάζεται χώρος των μηνυμάτων.
M_s	Ένα σύνολο στοιχείων που ονομάζεται χώρος των υπογραφών για τα μηνύματα $m \in M$.
S	Ένα σύνολο στοιχείων που ονομάζεται χώρος των υπογραφών
R	Μία 1-1 απεικόνιση $M \rightarrow M_s$ που ονομάζεται συνάρτηση αναγωγής.
M_R	Η εικόνα της R ($M_R = \mathrm{Im}(R)$).
R^{-1}	Η αντίστροφη συνάρτηση της R ($R^{-1}: M_R \rightarrow M$).
P	Ένα σύνολο στοιχείων που ονομάζεται πλήθος υπογραφών.
h	Μία one-way συνάρτηση με πεδίο ορισμού το M.
M_h	Η εικόνα της h ($h: M \rightarrow M_h$ και $M_h \subseteq M_s$).
Q_n	Σύνολο στοιχείων των τετραγωνικών υπολοίπων $\bmod n$.

Πίνακας 1.

- M είναι το σύνολο των στοιχείων όπου μπορούμε να επισυνάψουμε μία υπογραφή.
- M_s είναι το σύνολο των στοιχείων όπου μπορούν να εφαρμοσθούν οι μηχανισμοί της υπογραφής.
- S είναι το σύνολο των υπογραφών που σχετίζονται με τα στοιχεία του M. Αυτές οι υπογραφές χρησιμοποιούνται για να δέσουν τον υπογραφόντα με το μήνυμα.
- P χρησιμοποιείται για να προσδιορίσουμε συγκεκριμένους μηχανισμούς υπογραφής.

2.2. Κατηγορίες Υπογραφών.

Υπάρχουν δύο γενικές κατηγορίες των υπογραφών:

(α). Υπογραφή με συνημμένο το μήνυμα, όπου απαιτείται το μήνυμα να είναι είσοδος στον αλγόριθμο πιστοποίησης. Χρησιμοποιείται κυρίως για μηνύματα αυθαίρετου μήκους.

(β). Υπογραφή με ανάκτηση του μηνύματος, όπου δεν απαιτείται εδώ το μήνυμα να είναι είσοδος στον αλγόριθμο πιστοποίησης. Σε αυτή την περίπτωση το μήνυμα ανακτάται από την υπογραφή. Χρησιμοποιείται κυρίως για μηνύματα σταθερού μήκους.

Επίσης και οι δύο προηγούμενες κατηγορίες υπογραφών μπορούν να χωρισθούν ανάλογα με το πλήθος του P.

(α). Πιθανοτική υπογραφή αν $|P|>1$.

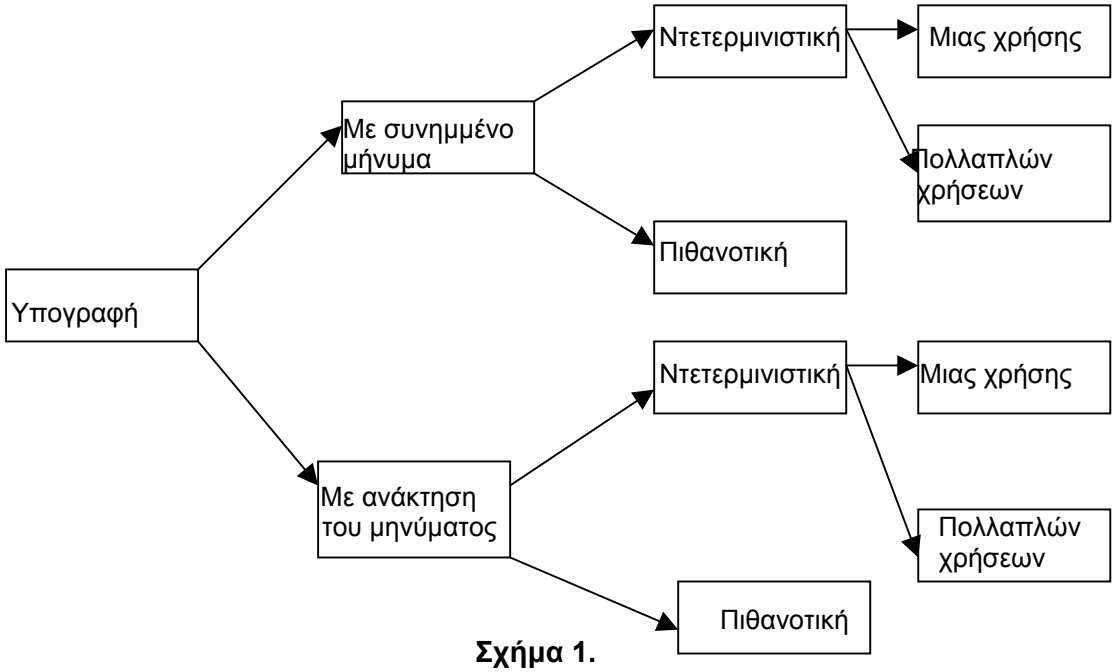
(β). Ντετερμινιστική υπογραφή αν $|P|=1$.

Η ντετερμινιστική υπογραφή διακρίνεται σε:

(α). Υπογραφή μιας χρήσης.

(β). Υπογραφή πολλών χρήσεων.

Η κατηγοριοποίηση των υπογραφών φαίνεται στο σχήμα 1.



Σχήμα 1.

2.2.1. Υπογραφή Με Συνημμένο Το Μήνυμα (Digital Signature Scheme With Appendix).

Οι υπογραφές με συνημμένο το μήνυμα είναι αυτές που χρησιμοποιούνται πιο πολύ στην πράξη. Στηρίζονται περισσότερο στις hash συναρτήσεις παρά στις συναρτήσεις αναγωγής.

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

(α). Αλγόριθμος δημιουργίας κλειδιών.

(1). Ο Α επιλέγει ένα μυστικό κλειδί και ορίζει το σύνολο $S_A = \{S_{A,\kappa} : \kappa \in P\}$ των μετασχηματισμών. Κάθε $S_{A,\kappa}$ είναι μία 1-1 απεικόνιση από το M_h στο S και ονομάζεται μετασχηματισμός υπογραφής.

(2). Το S_A ορίζει μία αντίστοιχη απεικόνιση V_A από το $M_h \times S$ στο {true,false} έτσι ώστε:

$$V_A(m', s^*) = \begin{cases} true & \alpha\nu \quad S_{A,k}(m') = s^* \\ false & \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

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

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

(β). Αλγόριθμος δημιουργίας υπογραφής.

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

(1). Επιλέγει ένα στοιχείο $\kappa \in P$.

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

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

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

Ο Β πιστοποιεί ότι η υπογραφή είναι αυθεντική.

(1). Εξασφαλίζει το δημόσιο κλειδί του Α το V_A.

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

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

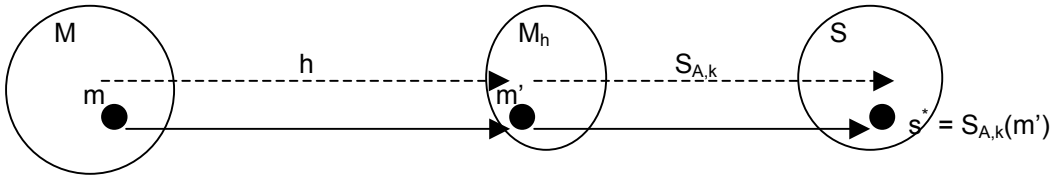
Για τους μετασχηματισμούς της υπογραφής και της πιστοποίησης θα πρέπει να ισχύουν οι παρακάτω ιδιότητες:

(α). Για κάθε $\kappa \in P$, το $S_{A,\kappa}$ θα πρέπει να υπολογίζεται εύκολα.

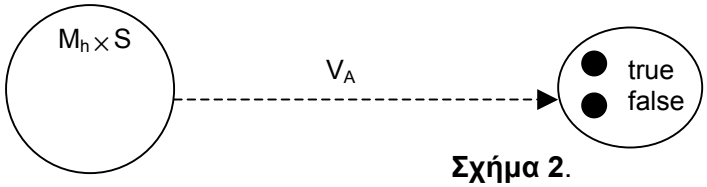
(β). Το V_A θα πρέπει να υπολογίζεται εύκολα.

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

Στα παρακάτω σχήματα φαίνονται οι διαδικασίες της υπογραφής (σχήμα 1) και της πιστοποίησης (σχήμα 2).



Σχήμα 1.



Σχήμα 2.

2.2.2. Υπογραφή Με Ανάκτηση Του Μηνύματος (Digital Signature Scheme With Message Recovery).

Οι υπογραφές με ανάκτηση του μηνύματος έχουν το χαρακτηριστικό ότι το μήνυμα ανακτάται από την υπογραφή.

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

(α). Αλγόριθμος δημιουργίας κλειδιών.

(1). Ο Α επιλέγει ένα σύνολο $S_A = \{S_{A,\kappa} : \kappa \in P\}$ των μετασχηματισμών. Κάθε $S_{A,\kappa}$ είναι μία 1-1 απεικόνιση από το M_S στο S και ονομάζεται μετασχηματισμός υπογραφής.

(2). Το S_A ορίζει μία αντίστοιχη απεικόνιση V_A με την ιδιότητα ότι $V_A \circ S_{A,\kappa}$ είναι ταυτοτική απεικόνειση στο M_S για όλα τα $\kappa \in P$. Ο V_A λέγεται μετασχηματισμός πιστοποίησης και είναι έτσι κατασκευασμένος ώστε να μπορεί να υπολογισθεί χωρίς τη γνώση του μυστικού κλειδιού του Α.

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

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α επιλέγει ένα στοιχείο $\kappa \in P$.

(2). Υπολογίζει $m' = R(m)$ και $s^* = S_{A,\kappa}(m')$. (Η R είναι η συνάρτηση αναγωγής).

(3). Η υπογραφή για το μήνυμα m είναι το s^*. Το s^* είναι διαθέσιμο στον Β για την πιστοποίηση της υπογραφής και την ανάκτηση του μηνύματος.

(γ). Αλγόριθμος πιστοποίησης της υπογραφής και ανάκτηση του μηνύματος.

Ο Β πιστοποιεί ότι η υπογραφή είναι αυθεντική.

(1). Εξασφαλίζει το δημόσιο κλειδί του Α το V_A.

(2). Υπολογίζει $m' = V_A(s^*)$.

(3). Πιστοποιεί ότι $m' \in M_R$. (Αν $m' \notin M_R$ τότε απορρίπτει την υπογραφή.)

(4). Ανακτά το m από το m' υπολογίζοντας $R^{-1}(m')$.

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

(α). Για κάθε $\kappa \in P$, το $S_{A,\kappa}$ θα πρέπει να υπολογίζεται εύκολα.

(β). Το V_A θα πρέπει να υπολογίζεται εύκολα.

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

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

(α). Επέλεξε τυχαία $\kappa \in P$ και τυχαία $s^* \in S$.

(β). Υπολόγισε $m' = V_A(s^*)$.

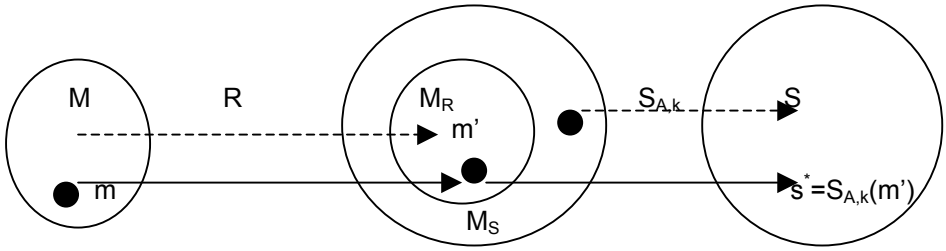
(γ). Υπολόγισε $m = R^{-1}(m')$.

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

Παράδειγμα 1. Έστω $M = \{m : m \in \{0,1\}^n\}$ για κάποιο σταθερό n και $M_S = \{t : t \in \{0,1\}^{2n}\}$ Ορίζουμε $R : M \to M_S$ με τύπο $R(m) = m \| m$, όπου || συμβολίζουμε τη συνένωση συμβολοσειρών, έτσι θα έχω $M_R = \{m \| m : m \in M\} \subseteq M_S$. Για μεγάλες τιμές του n η ποσότητα

$\frac{|M_R|}{|M_S|} = \left(\frac{1}{2}\right)^n$ έχει μηδαμινή τιμή. Αυτή η συνάρτηση αναγωγής είναι κατάλληλη ώστε καμία επιλογή του s^* από το μέρος του αντιπάλου να έχει μη μηδαμινή πιθανότητα να ισχύει $V_A(s^*) \in M_R$. ∴.

Στο παρακάτω σχήμα (σχήμα 1) φαίνεται η διαδικασία της υπογραφής με ανάκτηση του μηνύματος.



Σχήμα 1.

2.2.3. Μετατροπή σχήματος υπογραφής.

Μία υπογραφή με ανάκτηση του μηνύματος μπορεί να μετατραπεί σε υπογραφή με συνημμένο το μήνυμα, εφαρμόζοντας την hash συνάρτηση και μετά υπογράφουμε την τιμή της hash συνάρτησης. Τώρα το μήνυμα πρέπει να είναι είσοδος στον αλγόριθμο πιστοποίησης. Η συνάρτηση αναγωγής R τώρα δεν παίζει σημαντικό ρόλο για την ασφάλεια του συστήματος και μπορεί να είναι οποιαδήποτε 1-1 συνάρτηση από το M_h στο M_S.

2.3. Ασφάλεια Ψηφιακών Υπογραφών.

Στην παράγραφο 2.3.1. , θα αναφέρουμε πότε ένα κρυπτοσύστημα είναι ασφαλές. Επειδή οι ψηφιακές υπογραφές είναι τμήμα της κρυπτογραφίας και όπως είδαμε σε προηγούμενη παράγραφο το σχήμα της υπογραφής με ανάκτηση του μηνύματος δε διαφέρει ουσιαστικά από τα συστήματα κρυπτογράφησης.

Στην επόμενη παράγραφο, θα δούμε ποιες είναι οι δυνατές επιθέσεις που μπορεί να δεχθεί ένα σχήμα υπογραφής.

2.3.1. Πλήρης Ασφάλεια.

Υπάρχουν δύο προσεγγίσεις για την ασφάλεια ενός κρυπτοσυστήματος:

(α). Υπολογιστική ασφάλεια.

Η υπολογιστική ασφάλεια μετράει την υπολογιστική δύναμη που απαιτείται για να σπάσει ένα κρυπτοσύστημα. Μπορούμε να πούμε ότι ένα

κρυπτοσύστημα είναι ασφαλές αν ο βέλτιστος αλγόριθμος για να το σπάσει χρειάζεται να εκτελέσει N τουλάχιστο πράξεις όπου N είναι ένας συγκεκριμένος πολύ μεγάλος αριθμός. Το πρόβλημα είναι ότι δε γνωρίζουμε κανένα πρακτικό κρυπτοσύστημα που να είναι ασφαλές, δηλαδή δεν μπορούμε να το αποδείξουμε σύμφωνα με τον παραπάνω ορισμό. Πρακτικά λέμε ότι ένα κρυπτοσύστημα είναι υπολογιστικά ασφαλές αν χρειάζεται τεράστιο υπολογιστικό χρόνο (βέβαια αυτό διαφέρει πολύ από την απόδειξη).

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

(β). Απεριόριστη ασφάλεια.

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

2.3.2. Τύποι Επιθέσεων Σε Συστήματα Υπογραφών.

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

Υπάρχουν οι παρακάτω τύποι επιθέσεων:

(α). Κατάρρευση του συστήματος (total break). Ο αντίπαλος είναι ικανός να υπολογίσει το μυστικό κλειδί του αποστολέα ή να βρει ένα αποδοτικό αλγόριθμο ισοδύναμο με τον αυθεντικό αλγόριθμο δημιουργίας υπογραφής.

(β). Ολική πλαστογράφηση (universal forgery). Ο αντίπαλος αν και δεν μπορεί να βρει το μυστικό κλειδί του αποστολέα, μπορεί να πλαστογραφήσει οποιοδήποτε μήνυμα.

(γ). Επιλεκτική πλαστογράφηση (selective forgery). Ο αντίπαλος μπορεί να δημιουργήσει νόμιμες υπογραφές για ένα συγκεκριμένο μήνυμα ή για μια κατηγορία μηνυμάτων που έχουν επιλεγεί εκ των προτέρων. Δημιουργώντας τις υπογραφές δεν επιδρά άμεσα στο νόμιμο υπογράφοντα.

(δ). Υπαρξιακή πλαστογράφηση (existential forgery). Ο αντίπαλος είναι ικανός να πλαστογραφήσει τουλάχιστο ένα μήνυμα. Έχει λίγο ή καθόλου τον έλεγχο στο μήνυμα όπου πλαστογράφησε και ο νόμιμος υπογράφων μπορεί να εμποδίσει την απάτη.

Υπάρχουν δύο είδη επιθέσεων στα σχήματα υπογραφών δημοσίου κλειδιού:

(α). Επιθέσεις μόνο στο κλειδί (key-only attacks). Ο αντίπαλος γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντα.

(β). Επιθέσεις στο μήνυμα (message attacks). Ο αντίπαλος μπορεί να εξετάσει υπογραφές που αντιστοιχούν σε γνωστά ή σε επιλεγμένα μηνύματα και διακρίνονται σε :

(1). Επίθεση σε γνωστά μηνύματα (known-message attacks). Ο αντίπαλος έχει υπογραφές για ένα σύνολο μηνυμάτων που είναι γνωστά σε αυτόν αλλά όχι επιλεγμένα από αυτόν.

(2). Επίθεση σε επιλεγμένο μήνυμα (chosen-message attack). Ο αντίπαλος καταφέρνει να έχει νόμιμες υπογραφές για ένα επιλεγμένο σύνολο μηνυμάτων πριν προσπαθήσει να πετύχει κατάρρευση του συστήματος. Αυτή η επίθεση είναι μη προσαρμόσιμη (non-adaptive) με την έννοια ότι τα μηνύματα επιλέγονται πριν από τις υπογραφές.

(3). Επίθεση προσαρμόσιμου επιλεγμένου μηνύματος (adaptive chosen-message attack). Ο αντίπαλος μπορεί να χρησιμοποιήσει τον υπογράφοντα ως μαντείο, δηλαδή μπορεί να ζητήσει νόμιμες υπογραφές μηνυμάτων που εξαρτώνται από το δημόσιο κλειδί του υπογράφοντα ή να ζητήσει νόμιμες υπογραφές μηνυμάτων που εξαρτώνται από προηγούμενες υπογραφές ή μηνύματα.

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

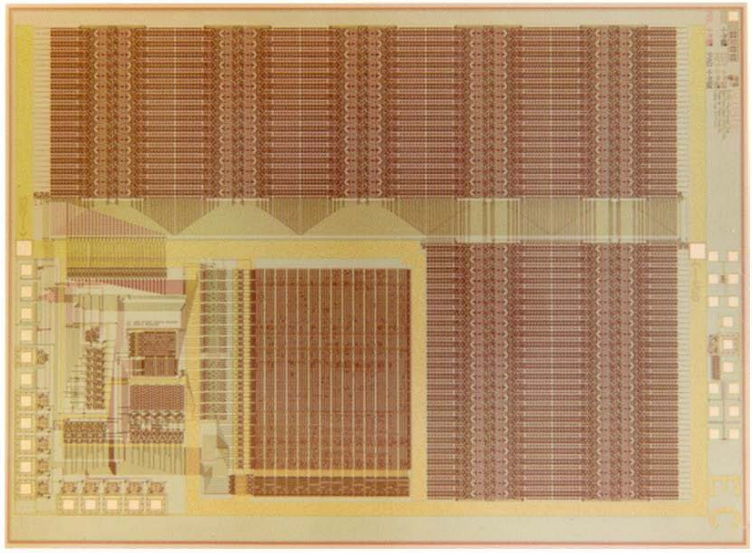
Το επίπεδο ασφάλειας που απαιτείται για κάθε σχήμα υπογραφής εξαρτάται από τις απαιτήσεις της εφαρμογής που χρησιμοποιείται. Σημαντικό ρόλο στην ασφάλεια του συστήματος έχει και η επιλογή της hash συνάρτησης όπου θα πρέπει να είναι τέτοια ώστε ο αντίπαλος να μη μπορεί να την αντικαταστήσει με κάποια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

Κεφάλαιο 3

Σχήματα Ψηφιακών Υπογραφών

3.1 Σχήμα Υπογραφής RSA.

Η ασφάλεια του σχήματος υπογραφής RSA στηρίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακέραιων αριθμών.



Φωτογραφία ενός RSA chip

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

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

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α παράγει δυο μεγάλους τυχαίους πρώτους αριθμούς p και q.

(2). Υπολογίζει $n = p * q$ και $\phi(n)$=(p -1)*(q -1)

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

(4). Με τη βοήθεια του γενικευμένου αλγορίθμου του Ευκλείδη υπολογίζει το μοναδικό ακέραιο d με 1< d < $\phi(n)$ τέτοιο που $e * d$ =1($\mathrm{mod}\ \phi(n)$).

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

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α υπολογίζει m' = $R(m)$, ένας ακέραιος στο διάστημα [0, n -1].

(2). Υπολογίζει s =(m')^d $\mathrm{mod}\ n$.

(3). Η υπογραφή του Α για το μήνυμα m είναι το s .

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

(1). Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το (n , e).

(2). Υπολογίζει m' = s^e $\mathrm{mod}\ n$.

(3). Πιστοποιεί ότι $m' \in M_R$, αλλιώς απορρίπτει την υπογραφή.

(4). Ανακτά το $m = R^{-1}(m')$.

Απόδειξη του αλγόριθμου πιστοποίησης.

Αν s είναι η υπογραφή για το μήνυμα m τότε s =(m')^d $\mathrm{mod}\ n$ με $m' = R(m)$. Επειδή $e * d$ =1($\mathrm{mod}\ \phi(n)$) , s^e =(m')^{ed} = m' ($\mathrm{mod}\ n$). Τελικά θα έχουμε ότι R^{-1} ($R(m)$)= m . ∴

Παράδειγμα 1. Θα δούμε ένα παράδειγμα για το RSA με ανάκτηση του μηνύματος. Για ευκολία στις πράξεις θα χρησιμοποιήσουμε μικρούς πρώτους αριθμούς.

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

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

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

Θα δούμε τώρα με ποιους τρόπους ένας αντίπαλος μπορεί να επιτεθεί στο σχήμα υπογραφής RSA και πως μπορούμε να τους αντιμετωπίσουμε:

(α). Παραγοντοποίηση ακεραίου.

Το πρόβλημα εύρεσης του μυστικού κλειδιού d στο RSA από το δημόσιο κλειδί (n, e) και το πρόβλημα της παραγοντοποίησης του n είναι υπολογιστικά ισοδύναμα. Αν ο αντίπαλος μπορεί να παραγοντοποιήσει το n που είναι τμήμα του δημοσίου κλειδιού του Α τότε μπορεί να υπολογίσει το $\phi(n)$ και χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη μπορεί να εξάγει το d, που είναι το μυστικό κλειδί, από το $\phi(n)$ και το e λύνοντας την $e * d = 1(\bmod \phi(n))$. Με αυτό τον τρόπο ο αντίπαλος θα προκαλέσει κατάρρευση του συστήματος αφού θα γνωρίζει το μυστικό κλειδί.

Για να αποφύγουμε μία τέτοια δυσάρεστη κατάσταση θα πρέπει να επιλέξουμε τέτοιους πρώτους p και q ώστε η παραγοντοποίηση του n να είναι υπολογιστικά ανέφικτη:

(1). Οι πρώτοι αριθμοί p και q που θα επιλέξουμε θα πρέπει να έχουν περίπου το ίδιο μήκος και να είναι 100 ψηφία ο καθένας.

(2). Η διαφορά τους $(p - q)$ δε θα πρέπει να είναι πολύ μικρή. Αν $p - q$ είναι μικρή τότε $p \approx q$ και $p \approx \sqrt{n}$. Τότε η παραγοντοποίηση του n θα μπορούσε να γίνει εύκολα δοκιμάζοντας όλους τους πιθανούς διαιρέτες που είναι περιττοί και βρίσκονται κοντά στον $\sqrt{n}$. Αν επιλεγούν τυχαία τότε η $p - q$ θα είναι κατάλληλα μεγάλη.

(3). Τέλος αρκετοί ερευνητές προτείνουν ότι οι p και q αντί να επιλέγονται τυχαία, θα πρέπει να είναι δυνατοί πρώτοι αριθμοί (strong primes). Ένας πρώτος αριθμός p λέγεται δυνατός αν ισχύουν τα παρακάτω:

α/. Ο p-1 έχει ένα μεγάλο πρώτο παράγοντα τον r.

β/. Ο p+1 έχει ένα μεγάλο πρώτο παράγοντα.

γ/. Ο r έχει ένα μεγάλο πρώτο παράγοντα.

(β). Πολλαπλασιαστική ιδιότητα του RSA.

Το σχήμα υπογραφής RSA έχει την ακόλουθη πολλαπλασιαστική ιδιότητα. Αν $s_1 = (m_1)^d \bmod n$ και $s_2 = (m_2)^d \bmod n$ είναι υπογραφές για τα μηνύματα m_1 και m_2 αντίστοιχα μετά την εφαρμογή της συνάρτησης αναγωγής, τότε $s = (s_1 * s_2) \bmod n$ έχει την ιδιότητα ότι $s = (m_1 * m_2)^d \bmod n$. Αν $m = m_1 * m_2$ έχει την ιδιότητα της συνάρτησης αναγωγής (δηλαδή $m \in M_R$) τότε το s θα είναι μία νόμιμη υπογραφή για το m. Για αυτό το

λόγο η συνάρτηση αναγωγής R δεν πρέπει να είναι πολλαπλασιαστική, δηλαδή για σχεδόν όλα τα ζευγάρια $\alpha, \beta \in M$ θα πρέπει να ισχύει $R(\alpha * \beta) \neq R(\alpha) * R(\beta)$. Θα δούμε στο παράδειγμα που ακολουθεί ότι αυτή η συνθήκη για την R είναι απαραίτητη αλλά όχι αρκετή για την ασφάλεια του συστήματος.

Παράδειγμα 2. Έστω ότι στο RSA το δημόσιο κλειδί είναι το (n, e) και το μυστικό κλειδί το d. Με κ ορίζουμε το μήκος του n (# bits στη δυαδική αναπαράσταση) και t είναι ένας σταθερός θετικός ακέραιος τέτοιος που $t < \frac{k}{2}$. Έστω $w = 2^t$ και τα μηνύματα m είναι ακέραιοι αριθμοί στο διάστημα [1, $n * 2^{-t}$ -1]. Η συνάρτηση αναγωγής R είναι $R(m) = m * 2^t$. Για τις περισσότερες επιλογές του n η R δεν έχει την πολλαπλασιαστική ιδιότητα. Είδαμε στο παράδειγμα 1 ότι η πιθανότητα επιτυχίας σε υπαρξιακή επίθεση είναι $\left(\frac{1}{2}\right)^t$, αλλά για αυτή τη συνάρτηση αναγωγής η επίθεση με επιλεκτική πλαστογράφηση (η οποία είναι πιο σοβαρή) είναι πιθανόν να γίνει. Έστω ότι ο αντίπαλος θέλει να πλαστογραφήσει μία υπογραφή για το μήνυμα m. Ο αντίπαλος γνωρίζει το n αλλά όχι το d .Μπορεί να επιτεθεί στο ακόλουθο επιλεγμένο μήνυμα για να καθορίσει την υπογραφή του m. Εφαρμόζοντας τον αλγόριθμο του Ευκλείδη στο n και στο $m' = R(m) = m * 2^t = m * w$. Σε κάθε βήμα του αλγορίθμου ακέραιοι x, y και r υπολογίζονται ώστε $x * n + y * m' = r$. Μπορεί να αποδειχθεί ότι σε κάποιο βήμα υπάρχει ένα y και ένα r τέτοια που $|y| < \frac{n}{w}$ και $r < \frac{n}{w}$ αν $w \leq \sqrt{n}$ **.** Αν $y > 0$ τότε $m_2 = r * w$ και $m_3 = y * w$. Αν $y < 0$ τότε $m_2 = r * w$ και $m_3 = -y * w$. Και στις δύο περιπτώσεις τα μηνύματα m_2 και m_3 έχουν την απαιτούμενη ιδιότητα της συνάρτησης αναγωγής. Αν υπογράψει με $s_2 = (m_2)^d \mod n$ και $s_3 = (m_3)^d \mod n$ τότε ο αντίπαλος μπορεί να υπολογίσει μία υπογραφή για το m ως ακολούθως:

- Αν $y > 0$ υπολογίζει $\frac{s_2}{s_3} = \frac{m_2^d}{m_3^d} = \left(\frac{r * w}{y * w}\right)^d = \left(\frac{r}{y}\right)^d = (m')^d \mod n$.
- Αν $y < 0$ υπολογίζει $\frac{s_2}{-s_3} = \frac{m_2^d}{(-m_3)^d} = \left(\frac{r * w}{y * w}\right)^d = \left(\frac{r}{y}\right)^d = (m')^d \mod n$.

Και στις δύο περιπτώσεις ο αντίπαλος έχει καταφέρει να υπογράψει ένα μήνυμα. Η επιλογή της κατάλληλης συνάρτησης αναγωγής R παίζει σπουδαίο ρόλο στην ασφάλεια του συστήματος. ∴

Ένας προτεινόμενος τρόπος για τη χρησιμοποίηση του RSA είναι να υπογράψουμε το μήνυμα και μετά να κρυπτογραφήσουμε το αποτέλεσμα της υπογραφής. Ας υποθέσουμε ότι ο Α θέλει να υπογράψει και μετά να κρυπτογραφήσει ένα μήνυμα για τον Β. Έστω ότι (n_A, e_A) και (n_B, e_B) είναι τα δημόσια κλειδιά των Α και Β αντίστοιχα. Αν $n_A > n_B$ τότε υπάρχει περίπτωση το μήνυμα να μην μπορεί να ανακτηθεί από τον Β όπως θα δούμε στο ακόλουθο παράδειγμα.

Παράδειγμα 3. Έστω n_A=8387×7499=62894113, e_A=5 και d_A=37726937, και n_B=55465219, e_B=5 και d_B=44360237. Παρατηρούμε ότι $n_A > n_B$. Έστω ότι m=1368797 είναι ένα μήνυμα που έχει εφαρμοσθεί η συνάρτηση αναγωγής και θα υπογραφεί με το μυστικό κλειδί του Α και θα κρυπτογραφηθεί με το δημόσιο κλειδί του Β.

(α). Ο Α υπολογίζει:

$$s = m^{d_A} \bmod n_A = 1368797^{37726937} \bmod 62894113 = 59847900.$$

$$c = s^{e_B} \bmod n_B = 59847900^5 \bmod 55465219 = 38842235.$$

(β). Για να ανακτήσει το μήνυμα και να πιστοποιήσει την υπογραφή ο Β υπολογίζει:

$$s' = c^{d_B} \bmod n_B = 38842235^{44360237} \bmod 55465219 = 4382681.$$

$$m' = (s')^{e_A} \bmod n_A = 4382681^5 \bmod 62894113 = 54383568.$$

Παρατηρούμε ότι $m \neq m'$. Ο λόγος για αυτό είναι ότι το s είναι μεγαλύτερο από το n_B. Η πιθανότητα να συμβεί αυτή η ανωμαλία είναι $\frac{n_A - n_B}{n_A} \approx 0.12$.∴.

Θα δούμε πως μπορούμε να αντιμετωπίσουμε αυτό το πρόβλημα (reblocking problem):

(α).Αναδιάταξη ενεργειών(reordering).

Το πρόβλημα δεν θα συνέβαινε αν χρησιμοποιούσαμε στη διαδικασία πρώτα το μικρότερο n_i ($n_i = \min(n_A, n_B)$). Αν $n_A > n_B$ τότε ο Α θα έπρεπε πρώτα να κρυπτογραφήσει το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Β και μετά να υπογράψει το αποτέλεσμα της κρυπτογράφησης με το μυστικό κλειδί του Α. Βέβαια αυτή η σειρά δεν είναι λογική αφού πρώτα υπογράφουμε το μήνυμα και μετά το κρυπτογραφούμε . Έτσι αν ο Α έκανε τη διαδικασία με αυτή τη σειρά ο αντίπαλος θα μπορούσε να αφαιρέσει την υπογραφή και να την αντικαταστήσει με μία δική του. Παρά το γεγονός ότι ο αντίπαλος δεν ξέρει τι υπογράφει μερικές φορές είναι πλεονέκτημα για αυτόν. Έτσι η αναδιάταξη δεν είναι η προτεινόμενη λύση.

(β). Διαχωρισμός των n_i (two moduli per entity).

Κάθε άτομο έχει δύο ξεχωριστούς σύνθετους αριθμούς (n_i) για κρυπτογράφηση και για δημιουργία υπογραφής όπου όλοι οι σύνθετοι αριθμοί για δημιουργία υπογραφής είναι μικρότεροι από τους σύνθετους αριθμούς για κρυπτογράφηση. Τότε λάθος στην αποκρυπτογράφηση δεν θα γίνει ποτέ. Αυτό μπορεί να επιτευχθεί απαιτώντας το μήκος των σύνθετων αριθμών για υπογραφή να έχει μήκος το πολύ t και το μήκος των σύνθετων αριθμών για κρυπτογράφηση να είναι τουλάχιστο t+1.

(γ). Συγκεκριμένη διάταξη n_i (prescribing the form of the modulus).

Με αυτή τη μέθοδο διαλέγουμε πρώτους p και q ώστε οι n_i να έχουν μία συγκεκριμένη μορφή: Το μεγαλύτερο bit είναι 1 και τα επόμενα κ bits είναι 0. Έστω ότι θέλουμε να βρούμε ένα αριθμό n μεγέθους t bits. Για τον n θέλουμε $2^{t-1} \le n \le 2^{t-1} + 2^{t-\kappa-1}$. Επιλέγω ένα τυχαίο πρώτο p με $\left\lceil \frac{t}{2} \right\rceil$ bits και ψάχνω για ένα πρώτο q να βρίσκεται ανάμεσα στους $\left\lceil \frac{2^{t-1}}{p} \right\rceil$ και $\left\lfloor \frac{(2^{t-1} + 2^{t-k-1})}{p} \right\rfloor$.

Τότε ο $n = p * q$ ικανοποιεί τη μορφή που θέλουμε. Η επιλογή του n με αυτό τον τρόπο δεν μας εξασφαλίζει ότι δε θα εμφανισθεί το πρόβλημα μας αλλά μειώνει σημαντικά την πιθανότητα να εμφανισθεί. Έστω ότι επιλέγουμε με αυτό τον τρόπο τον n_A και $s = m^{d_A} \bmod n_A$ είναι η υπογραφή για το μήνυμα m. Έστω ότι ο s έχει ένα 1 σε μία από τις κ+1 θέσεις από αριστερά εκτός από την πρώτη θέση. Τότε ο s επειδή είναι μικρότερος από τον n_A πρέπει να έχει ένα 0 στην πιο αριστερή θέση άρα θα είναι μικρότερος από οποιονδήποτε άλλο n_i με παρόμοιο τύπο. Η πιθανότητα ότι ο s δεν έχει κανένα 1 στις κ+1 θέσεις από αριστερά εκτός από την πιο αριστερή είναι $\left(\frac{1}{2}\right)^k$ όπου είναι μηδαμινή αν επιλεγεί ο κ να είναι πολύ μεγάλος (π.χ. 100). Στο παρακάτω παράδειγμα βλέπουμε πως κάνουμε την επιλογή τέτοιου n.

Παράδειγμα 4. Έστω ότι θέλουμε να κατασκευάσουμε ένα 12-bit αριθμό n τέτοιο που το πρώτο bit είναι 1 και τα επόμενα κ=3 bits είναι 0. Θα βρω ένα 6-bit πρώτο αριθμό p=37. Επιλέγω ένα πρώτο q να βρίσκεται ανάμεσα στους $\left\lceil \frac{2^{11}}{p} \right\rceil$=56 και $\left\lfloor \frac{(2^{11}+2^8)}{p} \right\rfloor$=62. Οι πιθανοί q είναι οι 59 και 61. Αν q=59 τότε n=37∗59=2183 έχοντας δυαδική αναπαράσταση 100010000111. Αν q=61 τότε n=37∗61=2257 έχοντας δυαδική αναπαράσταση 100011010001.∴

Αν $n = p * q$ είναι αριθμός μήκους 2κ-bit με p και q αριθμοί μήκους κ-bit ο καθένας, για την υπογραφή $s = m^d \bmod n$ για το μήνυμα m απαιτούνται $O(\kappa^3)$ δυαδικές πράξεις. Επειδή ο υπογράφων γνωρίζει τους p και q μπορεί να υπολογίσει $s_1 = m^d \bmod n$ και $s_2 = m^d \bmod n$ και να καθορίσει το s χρησιμοποιώντας το Κινέζικο θεώρημα, με την πολυπλοκότητα αυτής της διαδικασίας να είναι πάλι $O(\kappa^3)$.

Η πιστοποίηση της υπογραφής είναι πιο γρήγορη αν επιλεγεί ο e να είναι μικρός αριθμός. Αν γίνει αυτό τότε για την πιστοποίηση απαιτούνται $O(\kappa^2)$ δυαδικές πράξεις. Προτεινόμενες τιμές για το e είναι το 3 ή 2^{16}+1 και φυσικά θα πρέπει $\gcd(e,(p-1)(q-1))=1$.

Το πλάτος της αποδοτικότητας(Bandwidth Efficiency) του σχήματος υπογραφής του RSA δίνεται από τον τύπο $BE = \frac{\log_2 |M_S|}{\log_2 |M_R|}$ για συγκεκριμένη συνάρτηση αναγωγής R.
Καλύτερο πλάτος αποδοτικότητας έχουμε όταν χρησιμοποιούμε το σχήμα της υπογραφής RSA με συνημμένο το μήνυμα αν το μήνυμα είναι αυθαίρετου μήκους, ενώ αν το μήκος του μηνύματος είναι μικρότερο από κ-bits (με n να είναι 2κ-bit) προτιμάται το σχήμα της υπογραφής RSA με ανάκτηση του μηνύματος.

Έστω ότι θέλουμε να υπογράψουμε ένα μήνυμα $m = \kappa * t$ και έχουμε επιλέξει το n να είναι μεγέθους 2κ-bit. Επειδή το σχήμα της υπογραφής με ανάκτηση του μηνύματος χρησιμοποιείται για μηνύματα σταθερού μήκους (έστω μεγέθους t) θα πρέπει να διαμερίσουμε το m σε κ-bit blocks έτσι ώστε $m = m_1 || m_2 || \ldots || m_t$ και να υπογράψουμε κάθε block ανεξάρτητα (αυτή η μέθοδος δεν προτείνεται). Εναλλακτικά θα μπορούσαμε να εφαρμόσουμε μία hash συνάρτηση που να αντιστοιχίζει το m σε

ένα δυαδικό αριθμό μήκους $w \le \kappa$ και να υπογράψουμε μετά την τιμή της hash συνάρτησης.

3.2 Σχήμα Υπογραφής Rabin Δημοσίου Κλειδιού.

Αυτό το σχήμα υπογραφής είναι παρόμοιο με το RSA αλλά ο αριθμός e, που είναι τμήμα του δημοσίου κλειδιού, είναι άρτιος. Για λόγους απλότητας θα θεωρήσουμε ότι e=2. Επίσης ισχύουν ότι $M_S = Q_n$ και οι υπογραφές είναι τετραγωνικές ρίζες αυτών. Η συνάρτηση αναγωγής $R : M \rightarrow M_S$ είναι δημόσια γνωστή.

(α). Αλγόριθμος δημιουργίας κλειδιού.

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

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α υπολογίζει $m' = R(m)$.
(2). Υπολογίζει μία τετραγωνική ρίζα s του $m' \bmod n$
(3). Η υπογραφή του Α για το μήνυμα m είναι το s.

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

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

Στο παρακάτω παράδειγμα θα δούμε μία απλή εφαρμογή.

Παράδειγμα 1. Έστω ότι ο Α επιλέγει p=7, q=11 και υπολογίζει n=77. Το δημόσιο κλειδί του Α είναι n=77 και το μυστικό κλειδί είναι το (p, q)=(7,11). Ξέρουμε ότι $M_S = Q_n$, άρα Q_{77}={1,4,9,15,16,23,25,36,37,53,58,60,64,67,71}. Για λόγους απλότητας θεωρούμε ότι $M = M_S$ και η συνάρτηση αναγωγής είναι η ταυτοτική συνάρτηση, δηλαδή $m' = R(m) = m$. Έστω ότι το μήνυμα μας είναι m=23. Ο Α υπολογίζει $R(m) = m'$=23 και βρίσκει μία τετραγωνική ρίζα του $m' \bmod 77$. Αν s είναι μία τέτοια τετραγωνική ρίζα τότε $s = \pm 3 (\bmod 7)$ και $s = \pm 1 (\bmod 11)$ άρα s=10,32,45 ή 67. Επιλέγει ο Α η υπογραφή να είναι το s=45.
Ο Β υπολογίζει $m' = s^2 \bmod 77$=23. Επειδή $m' \in M_R$ ο Β αποδέχεται την υπογραφή και ανακτά το m από τη σχέση $m = R^{-1}(m')$=23.

Όπως είδαμε και στο RSA, η επιλογή της συνάρτησης αναγωγής R παίζει σπουδαίο ρόλο στην ασφάλεια του συστήματος. Αν για παράδειγμα υποθέσουμε ότι $M = M_S = Q_n$ και $R(m) = m$ για όλα τα $m \in M$ τότε ο αντίπαλος μπορεί να επιλέξει ένα οποιοδήποτε ακέραιο $s \in Z_n^*$ και υπολογίζει $m' = s^2 \bmod n$ τότε το s είναι μία νόμιμη υπογραφή για το m', χωρίς να ξέρει τίποτα για το μυστικό κλειδί. Σε αυτή την περίπτωση έχουμε επίθεση με υπαρξιακή πλαστογράφηση.

Με την εφαρμογή της συνάρτησης αναγωγής R σε ένα μήνυμα m, έχουμε ότι $m' = R(m)$. Δεν υπάρχει καμία εγγύηση ότι το m' είναι τετραγωνικό υπόλοιπο του $\bmod ulo\ n$ και έτσι ο υπολογισμός της τετραγωνικής ρίζας θα είναι αδύνατος. Μία λύση θα είναι να προσθέσουμε ένα τυχαίο μικρό αριθμό στο m και να υπολογίσουμε πάλι το $R(m)$ ελπίζοντας τώρα ότι $R(m) \in Q_n$. Θα δούμε παρακάτω μία ντετερμινιστική μέθοδο, που είναι προτιμότερη για την αντιμετώπιση αυτού του προβλήματος.

Αυτό το σχήμα υπογραφής που θα δούμε λέγεται τροποποιημένο σχήμα υπογραφής Rabin δημοσίου κλειδιού και στηρίζεται στην επιλογή πρώτων αριθμών p και q με κάποια ιδιαίτερα χαρακτηριστικά.

Επιλέγουμε δύο πρώτους αριθμούς p και q έτσι ώστε $p = 3 \bmod 4$ και $q = 3 \bmod 4$ και $n = p * q$. Για αυτούς τους πρώτους αριθμούς ισχύουν τα παρακάτω:

(α). Αν $\gcd(x, n) = 1$ τότε $x^{(p-1)(q-1)/2} = 1 (\bmod n)$.

(β). Αν $x \in Q_n$ τότε $x^{(n-p-q+6)/8} \bmod n$ είναι μία τετραγωνική ρίζα του $x \bmod n$.

(γ). Έστω x είναι ένας ακέραιος έχοντας σύμβολο Jacobi $JS = (\frac{x}{n}) = 1$ και έστω $d = (n - p - q + 5)/8$. Τότε

$$x^{2d} \bmod n = \begin{cases} x & \alpha\nu \quad x \in Q_n \\ n - x & \alpha\nu \quad x \notin Q_n \end{cases}$$

(δ). Αν $p \neq q \pmod 8$ τότε $JS = (\frac{2}{n}) = -1$. Έτσι ο πολλαπλασιασμός του x με το 2 ή με $2^{-1} \bmod n$ αντιστρέφει το JS του x.(Οι ακέραιοι του τύπου $n = p * q$ όπου $p \equiv q \equiv 3 (\bmod 4)$ και $p \neq q$ λέγονται **Williams** ακέραιοι.)

Εκμεταλλευόμενοι τις παραπάνω ιδιότητες των p και q θα ορίσουμε το τροποποιημένο σχήμα αλλάζοντας τους ορισμούς ορισμένων συμβόλων που φαίνονται στον πίνακα 1.

Σύμβολο	Περιγραφή
M	$\{m \in Z_n : m \le \lfloor (n-6)/16 \rfloor\}$
M_S	$\{m \in Z_n : m = 6 (\mathrm{mod}\ 16)\}$
S	$\{ s \in Z_n : s^2 \bmod n) \in M_S\}$
R	$R\ (m)=16m+6$ για όλα τα $m \in M$
M_R	$\{ m \in Z_n : m = 6 (\mathrm{mod}\ 16)\}$

Πίνακας 1.

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α παράγει δυο μεγάλους τυχαίους πρώτους αριθμούς $p = 3 (\mathrm{mod}\ 8)$ και $q = 7 (\mathrm{mod}\ 8)$ και υπολογίζει $n = p * q$.

(2). Το δημόσιο κλειδί του Α είναι το n και το μυστικό κλειδί είναι το $d = (n - p - q + 5)/8$.

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α υπολογίζει $m' = R(m) = 16m + 6$.

(2). Υπολογίζει το σύμβολο Jacobi $JS = (\frac{m'}{n})$.

(3). Αν $JS = 1$ τότε υπολογίζει $s = (m')^d \bmod n$.

(4). Αν $JS = -1$ τότε υπολογίζει $s = (\frac{m'}{2})^d \bmod n$.(Αν $JS \neq 1$ ή –1 τότε $JS = 0$ δηλαδή $\gcd(m', n) \neq 1$. Αυτό μας οδηγεί στην παραγοντοποίηση του n. Η πιθανότητα να συμβεί αυτό είναι μηδαμινή).

(5). Η υπογραφή του Α για το m είναι το s.

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

(1). Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το n.

(2). Υπολογίζει $m'' = s^2 \bmod n$.

(3). Αν $m'' = 6 (\mathrm{mod}\ 8)$ τότε $m' = m''$.

(4). Αν $m'' = 3 (\mathrm{mod}\ 8)$ τότε $m' = 2m''$.

(5). Αν $m'' = 7 (\mathrm{mod}\ 8)$ τότε $m' = n - m''$.

(6). Αν $m'' = 2 (\mathrm{mod}\ 8)$ τότε $m' = 2(n - m'')$.

(7). Πιστοποιεί ότι $m' \in M_R$, αλλιώς απορρίπτει την υπογραφή.

(8). Ανακτά το $m = R^{-1}(m') = (m' - 6)/16$.

Απόδειξη του αλγόριθμου πιστοποίησης.

Στον αλγόριθμο δημιουργίας υπογραφής ο Α υπογράφει το $u = m'$ ή $u = m'/2$ ανάλογα ποιο από τα δύο έχει $JS = 1$. Από τις ιδιότητες των πρώτων αριθμών που είδαμε στην παράγραφο αυτή (από τη (δ)), έχουμε ότι ένας από τους $m', m'/2$ έχει $JS = 1$. Η τιμή u που υπογράφεται είναι τέτοια ώστε $u = 3$ ή $6 (\mathrm{mod}\ 8)$.

Από την (γ) έχουμε ότι $s^2 \bmod n = u$ ή $n-u$ (εξαρτάται ποιο από το αν $u \in Q_n$ Επειδή n =5$(\bmod 8)$ αυτές οι περιπτώσεις μπορούν μοναδικά να διαχωριστούν.∴

Παράδειγμα 2. Έστω ότι ο Α επιλέγει p =19 και q =31, και υπολογίζει $n = p * q$ =589 και d =$(n-p-q+5)/8$=68 Το δημόσιο κλειδί του Α είναι το n =589 και το μυστικό κλειδί το d =68. Το σύνολο M_S περιλαμβάνει τα στοιχεία που φαίνονται στον πίνακα 2 με τα αντίστοιχα τους JS .

m	6	22	54	70	86	102	118	134	150	166	182	198	214	230	246
$(\frac{m}{589})$	-1	1	-1	-1	1	1	1	1	1	1	-1	1	1	1	1
m	262	278	294	326	358	374	390	406	422	438	454	470	486		
$(\frac{m}{589})$	-1	-1	-1	-1	-1	-1	-1	-1	1	1	1	-1	-1		
m	502	518	534	550	566	582									
$(\frac{m}{589})$	1	-1	-1	-1	1	1									

Πίνακας 2.

Έστω ότι m =12. Ο Α υπολογίζει m'= R (12)=198, JS =$(\frac{m'}{n})$=$(\frac{198}{589})$=1 και s =$198^{68} \bmod 589$=102. Η υπογραφή του Α για το m =12 είναι s =102.

Ο Β υπολογίζει m'' = $s^2 \bmod n$ =$102^2 \bmod 589$=391. Επειδή m'' =7$(\bmod 8)$ ο Β υπολογίζει m'= n - m'' =589-391=198. Τελικά ο Β υπολογίζει $m = R^{-1}(m')$= (198-6)/16=12 και αποδέχεται την υπογραφή.

Με τον αλγόριθμο που περιγράψαμε κανείς δε θα υπέγραφε ένα μήνυμα με τιμή u έχοντας JS =-1 επειδή αυτό οδηγεί στην παραγοντοποίηση του n. Παρατηρούμε ότι το $y = u^{2d} = s^2$ πρέπει να έχει JS =1, αλλά $y^2 = (u^2)^{2d} = u^2 (\bmod n)$ από την (γ). Έτσι $(u-y)(u+y)$=0$(\bmod n)$. Επειδή οι u, y πρέπει να έχουν αντίθετα JS , θα έχουμε ότι $\gcd(u-y, n)$= p ή q .

Η επίθεση με υπαρξιακή πλαστογράφηση εξακολουθεί να υφίσταται. Αρκεί ο αντίπαλος να βρει ένα s τέτοιο που $1 \le s \le n$-1 ώστε είτε s^2 είτε $2s^2$ είτε $2(n - s^2) \bmod n$ να ισούται με $6 \bmod 16$. Σε οποιαδήποτε από αυτές τις περιπτώσεις το s είναι νόμιμη υπογραφή για $m' = s^2 \bmod n$.

3.3. Σχήματα Υπογραφών Από Πρωτόκολλα Μηδενικής Γνώσης.

Θα δούμε σε αυτή την ενότητα τα σχήματα υπογραφών Feige-Fiat-Shamir και Guillou-Quisquarter.

3.3.1 Σχήμα υπογραφής Feige-Fiat-Shamir.

Το σχήμα υπογραφής Feige-Fiat-Shamir είναι ένα τροποποιημένο σχήμα του Fiat-Shamir και χρησιμοποιεί μία one-way hash συνάρτηση $h:\{0,1\}^{\pi} \rightarrow \{0,1\}^{\kappa}$ για κάποιο συγκεκριμένο θετικό ακέραιο κ. Το $\{0,1\}^{\kappa}$ ορίζει το σύνολο των μηνυμάτων μεγέθους κ και το $\{0,1\}^{\pi}$ το σύνολο όλων των μηνυμάτων. Θα δούμε το σχήμα υπογραφής με συνημμένο το μήνυμα. Η μέθοδος αυτή είναι πιθανοτική.

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α παράγει δυο μεγάλους τυχαίους πρώτους αριθμούς p και q και υπολογίζει $n = p * q$.

(2). Επιλέγει ένα θετικό ακέραιο κ και διαφορετικούς τυχαίους ακεραίους $s_1, s_2, ..., s_{\kappa} \in Z_n^*$.

(3). Υπολογίζει $u_i = (s_j)^{-2} \bmod n$ με $1 \le j \le \kappa$.

(5). Το δημόσιο κλειδί του Α είναι $(n, u_1, ..., u_{\kappa})$ και το μυστικό κλειδί είναι $(s_1, s_2, ..., s_{\kappa})$.

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α επιλέγει ένα τυχαίο ακέραιο r με $1 \le r \le n$ -1.
(2). Υπολογίζει $u = r^2 \bmod n$.
(3). Υπολογίζει $e = (e_1, e_2, ...e_{\kappa}) = h(m \,||\, u)$ για κάθε $e_i \in \{0,1\}$.
(4). Υπολογίζει $s = r * \prod_{j=1}^{k} s_j^{e_j} \bmod n.$
(3). Η υπογραφή του Α για το μήνυμα m είναι το ζευγάρι (e, s).

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

(1). Ο Β Εξασφαλίζει το δημόσιο κλειδί του Α το $(n, u_1, ..., u_{\kappa})$.
(2). Υπολογίζει $w = s^2 * \prod_{j=1}^{k} u_j^{e_j} \bmod n.$
(3). Υπολογίζει $e' = h(m \,||\, w)$.
(4). Αποδέχεται την υπογραφή αν και μόνο αν $e = e'$.

Απόδειξη του αλγόριθμου πιστοποίησης.

Έχουμε ότι

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

Επειδή $w = u$ θα έχουμε ότι $e = e'$ ∴.

Παράδειγμα 1. Ο Α επιλέγει πρώτους αριθμούς p =3571 και q =4523 και υπολογίζει $n = p * q$ =16151633. Στον πίνακα 1 φαίνονται η επιλογή των s_j (το μυστικό κλειδί του Α) και των ακεραίων u_j (το δημόσιο κλειδί του Α) με τις ενδιάμεσες τιμές των $(s_j)^{-1}$.

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

Πίνακας 1.

Έστω ότι h:$\{0,1\}^{\pi} \rightarrow \{0,1\}^5$ είναι η hash συνάρτηση. Ο Α επιλέγει ένα τυχαίο ακέραιο r =23181 και υπολογίζει $u = r^2 \bmod n$ =4354872. Για να υπογράψει ένα μήνυμα m ο Α υπολογίζει $e = h(m \| u)$=10110 . Ο Α υπολογίζει $s = r * s_1 * s_3 * s_4 \bmod n$ =(23181)(42)(85)(101) $\bmod n$ =7978909, η υπογραφή για το m είναι (e =10110, s =7978909).

Ο Β υπολογίζει $s^2 \bmod n$ =2926875 και
$u_1 * u_3 * u_4 \bmod n$ =(503594)(7104483)(1409171) $\bmod n$ =15668174.

Ο Β υπολογίζει $w = s^2 * u_1 * u_3 * u_4 \bmod n$ =4354872.

Επειδή $w = u$ έχουμε ότι $e' = h(m \| w) = h(m \| u)$=e και ο Β αποδέχεται την υπογραφή∴.

Η ασφάλεια του σχήματος βασίζεται στον υπολογισμό των τετραγωνικών ριζών $\bmod n$. Έχει αποδειχθεί ότι για να είναι ασφαλές το σχήμα ενάντια στην επίθεση προσαρμόσιμου επιλεγμένου μηνύματος, η hash συνάρτηση h πρέπει να είναι τυχαία και τα s_j διαφορετικά μεταξύ τους.

3.3.2 Σχήμα υπογραφής Guillou-Quisquarter.

Σε αυτό το σχήμα θεωρούμε ότι h:$\{0,1\}^{\pi} \rightarrow Z_n$ είναι η hash συνάρτηση και n είναι θετικός ακέραιος αριθμός.

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α παράγει δυο μεγάλους τυχαίους πρώτους αριθμούς p και q και υπολογίζει $n = p * q$.

(2). Επιλέγει ένα θετικό ακέραιο $e \in \{1,2,\ldots,n\text{-}1\}$ τέτοιο που $\gcd(e,(p\text{-}1)(q\text{-}1))=1$.

(3). Επιλέγει ένα θετικό ακέραιο J_A με $1<J_A<n$ όπου είναι η ταυτότητα του Α και $\gcd(J_A, n)=1$.

(4). Καθορίζει ένα ακέραιο $\alpha \in Z_n$ τέτοιο που $J_A * \alpha^e = 1 (\mathrm{mod}\, n)$ ως εξής:

α/. Υπολογίζει $(J_A)^{-1} \bmod n$.

β/. Υπολογίζει $d_1 = e^{-1} \bmod (p\text{-}1)$ και $d_2 = e^{-1} \bmod (q\text{-}1)$.

γ/. Υπολογίζει $\alpha_1 = (J_A^{-1})^{d_1} \bmod p$ και $\alpha_2 = (J_A^{-1})^{d_2} \bmod q$.

δ/. Βρίσκει μία λύση για το α τέτοια που $\alpha = \alpha_1 \pmod p$ και $\alpha = \alpha_2 \pmod q$.

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

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α επιλέγει ένα τυχαίο ακέραιο κ και υπολογίζει $r = \kappa^e \bmod n$.
(2). Υπολογίζει $u = h(m \| r)$.
(3). Υπολογίζει $s = \kappa * \alpha^u \bmod n$.
(4). Η υπογραφή του Α για το μήνυμα m είναι το ζευγάρι (s, u).

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

(1). Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το (n, e, J_A).
(2). Υπολογίζει $w = s^e * J_A^u \bmod n$ και $u' = h(m \| w)$.
(3). Αποδέχεται την υπογραφή αν και μόνο αν $u = u'$.

Απόδειξη του αλγόριθμου πιστοποίησης.

Παρατηρούμε ότι $w = s^e * J_A^u = (\kappa * \alpha^u)^e * J_A^u = \kappa^e * (\alpha^e * J_A)^u = \kappa^e = r (\mathrm{mod}\, n)$. Επειδή $w = r$ έχουμε ότι $u = u'$.

Παράδειγμα 1. Ο Α επιλέγει πρώτους p =20849 και q =27457 και υπολογίζει $n = p * q$ =572450993. Επιλέγει ένα ακέραιο e =47 και J_A =1091522 και βρίσκει τον α ώστε $\alpha^e * J_A = 1 (\mathrm{mod}\, n)$ με α =214611724. Το δημόσιο κλειδί του Α είναι (n =572450993, e =47, J_A =1091522) και μυστικό κλειδί α =214611724.

Για να υπογράψει το μήνυμα m =1101110001 επιλέγει ένα τυχαίο κ =42134 και υπολογίζει $r = \kappa^e \bmod n$ =297543350. Ο Α υπολογίζει $u = h(m \| r)$ =2713833 και $s = \kappa * \alpha^u \bmod n$ =(42134) $214611724^{2713833} \bmod n$ =252000854. Η υπογραφή του Α για το μήνυμα m είναι το ζευγάρι (s =252000854, u =2713833).

Ο Β υπολογίζει $s^e \bmod n$ =252000854$^{47} \bmod n$ =398641962,

$J_A^u \bmod n$ =1091522$^{2713833} \bmod n$ =110523867 και τελικά

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

Επειδή $w = r * u' = h(m \,||\, w) = h(m \,||\, r)$ ο Β αποδέχεται την υπογραφή.

Ο αριθμός e πρέπει να είναι αρκετά μεγάλος ώστε να αποκλείσουμε την πιθανότητα της πλαστογράφησης. Ο αντίπαλος επιλέγει ένα μήνυμα m και υπολογίζει $u = h\ (m \,||\, J_A^t)$ για αρκετές τιμές του t μέχρι να ισχύει για κάποιο t $u = t \ (\bmod e)$, αυτό αναμένεται να γίνει σε Ο($\sqrt{e}$) προσπάθειες. Έχοντας καθορίσει ένα τέτοιο ζευγάρι (u,t) , ο αντίπαλος καθορίζει ένα ακέραιο x τέτοιο που $t = x * e + u$ και υπολογίζει $s = J_A^x \bmod n$.

Παρατηρούμε ότι $s^e * J_A^u = (J_A^x)^e \, J_A^u = J_A^{xe+u} = J_A^t \ (\bmod n)$ και $h\ (m \,||\, J_A^t) = u$. Έτσι το ζευγάρι (s,u) είναι μία νόμιμη (πλαστογραφημένη) υπογραφή για το μήνυμα m.

Μπορούμε να χρησιμοποιήσουμε αυτό το σχήμα και για υπογραφή με ανάκτηση του μηνύματος. Θα έχουμε ότι $M_S = Z_n$ και $m \in M_S$. Στη δημιουργία της υπογραφής επιλέγουμε ένα τυχαίο κ τέτοιο που $\gcd(\kappa, n) = 1$ και υπολογίζουμε $r = \kappa^e \bmod n$ και $u = m \bmod n$. Η υπογραφή είναι $s = \kappa * \alpha^u \bmod n$. Η πιστοποίηση δίνει $s^e * J_A^u = \kappa^e * \alpha^{eu} * J_A^u = \kappa^e = r (\bmod n)$. Το μήνυμα m μπορεί να ανακτηθεί από το $u * r^{-1} \bmod n$. Όπως είπαμε και σε προηγούμενα σχήματα με ανάκτηση του μηνύματος η επιλογή κατάλληλης συνάρτησης αναγωγής R παίζει σπουδαίο ρόλο στην ασφάλεια του συστήματος.

3.4. Σχήματα Υπογραφών DSA, ElGamal, Schnorr και Ελλειπτικών Καμπυλών.

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

3.4.1. Σχήμα Υπογραφής DSA.

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

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α επιλέγει ένα πρώτο αριθμό q τέτοιο που $2^{159}<q<2^{160}$.

(2). Διαλέγει t έτσι ώστε $0\le t\le 8$ και επιλέγει ένα πρώτο αριθμό p όπου $2^{511+64t}<p<2^{512+64t}$ με την ιδιότητα ότι ο q διαιρεί τον (p-1).

(3). Επιλέγει ένα γεννήτορα α της μοναδικής κυκλικής ομάδος τάξης q στο Z_p^*.

α/. Επιλέγει ένα στοιχείο $g \in Z_p^*$ και υπολογίζει $\alpha = g^{(p-1)/q} \bmod p$.

β/. Αν α =1τότε εκτέλεσε το προηγούμενο βήμα.

(4). Επιλέγει ένα τυχαίο ακέραιο a τέτοιο που $1\le a\le q$ -1.

(5). Υπολογίζει $y=\alpha^{a} \bmod p$.

(6). Το δημόσιο κλειδί του Α είναι (p, q, α, y) και το μυστικό κλειδί είναι το a.

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α επιλέγει ένα τυχαίο μυστικό ακέραιο κ με $0<\kappa<q$.

(2). Υπολογίζει $r=(\alpha^{\kappa} \bmod p) \bmod q$.

(3). Υπολογίζει $\kappa^{-1} \bmod q$.

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

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

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

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

(2). Πιστοποιεί ότι $0<r<q$ και $0<s<q$ αλλιώς απορρίπτει την υπογραφή.

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

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

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

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

Απόδειξη του αλγόριθμου πιστοποίησης.

Αν (r, s) είναι η υπογραφή του μηνύματος m τότε θα ισχύει $h(m)=-ar+\kappa s \pmod q$. Πολλαπλασιάζοντας και τα δύο μέλη με w θα έχουμε $wh(m)+arw=\kappa \pmod q$. Αλλά ξέρουμε ότι $u_1+au_2=\kappa \pmod q$. Τελικά $(a^{u_1}y^{u_2} \bmod p) \bmod q=(\alpha^{\kappa} \bmod p) \bmod q$. Άρα $v=r$ ∴.

Παράδειγμα 1. Ο Α επιλέγει πρώτους p =124540019 και q =17389 τέτοιους που ο q διαιρεί τον (p -1). Επιλέγει ένα τυχαίο στοιχείο g =110217528 $\in Z_p^*$ και

υπολογίζει $\alpha = g^{17389} \bmod p$ =10083255. Επειδή $\alpha \neq 1$, ο α είναι ένας γεννήτορας της μοναδικής κυκλικής υποομάδας τάξης q στο Z_p^*. Επιλέγει ένα τυχαίο αριθμό a=12496 τέτοιο που $1 \leq a \leq q$ -1 και υπολογίζει $y = \alpha^a \bmod p$ =$10083255^{12496} \bmod 124540019$=119946265. Το δημόσιο κλειδί του Α είναι (p =124540019, q =17389, α =10083255, y =119946265) και το μυστικό κλειδί είναι το a=12496.

Για να υπογράψει το μήνυμα m επιλέγει ένα τυχαίο ακέραιο κ =9557 και υπολογίζει $r = (\alpha^\kappa \bmod p) \bmod q$ =$(10083255^{9557} \bmod 124540019) \bmod 17389$ = $27039929 \bmod 17389$ =34. Ο Α υπολογίζει $\kappa^{-1} \bmod q$ =7631, $h(m)$=5246 και τελικά $s = (7631)\{5246+(12496)(34)\} \bmod q$ =13049. Η υπογραφή για το m είναι το ζευγάρι (r =34, s =13049).

Ο Β υπολογίζει $w = s^{-1} \bmod q$ =1799 , $u_1 = w * h(m) \bmod q$ = $(5246)(1799) \bmod 17389$ = 12716 και $u_2 = r * w \bmod q$ =$(34)(1799) \bmod 17389$= 8999. Ο Β υπολογίζει $v = (a^{u_1} y^{u_2} \bmod p) \bmod q$ = $10083255^{12716} * 119946265^{8999} \bmod 124540019) \bmod 17389$= $27039929 \bmod 17389$=34. Επειδή $v = r$ ο Β αποδέχεται την υπογραφή.∴

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

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

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

3.4.2 Σχήμα Υπογραφής ElGamal.

Το σχήμα υπογραφής ElGamal είναι πιθανοτικό. Δημιουργεί υπογραφές με συνημμένο το μήνυμα με μηνύματα σε δυαδική μορφή αυθαίρετου μήκους και χρησιμοποιεί μία hash συνάρτηση $h:\{0,1\}^\pi \rightarrow Z_p$, όπου p είναι ένας μεγάλος πρώτος αριθμός.

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α επιλέγει ένα μεγάλο πρώτο αριθμό p και ένα γεννήτορα α της πολλαπλασιαστικής ομάδος Z_p^*.

(2). Επιλέγει ένα τυχαίο ακέραιο a με $1 \leq a \leq p$ -2.

(3). Υπολογίζει $y = \alpha^a \bmod p$.

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

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α επιλέγει ένα τυχαίο μυστικό ακέραιο κ με $1 \le \kappa \le p$ -2 με $\gcd(\kappa, p\text{-}1)=1$.

(2). Υπολογίζει $r = \alpha^{\kappa} \pmod p$.

(3). Υπολογίζει $\kappa^{-1} \bmod (p\text{-}1)$.

(4). Υπολογίζει $s = \kappa^{-1}\{h(m)\text{-a}r\} \bmod (p\text{-}1)$.

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

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

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

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

(3). Υπολογίζει $v_1 = y^r * r^s \bmod p$.

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

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

Απόδειξη του αλγόριθμου πιστοποίησης.

Αν η υπογραφή δημιουργήθηκε από τον Α τότε $s = \kappa^{-1}\{h(m)\text{-a}r\} \bmod (p\text{-}1)$.
Πολλαπλασιάζοντας και τα δύο μέλη με κ θα έχουμε $\kappa * s = (h(m)\text{-a}r) \pmod{(p\text{-}1)} \Leftrightarrow h(m) = (\text{a}r + \kappa s) \pmod{(p\text{-}1)}$. Τελικά θα έχουμε $\alpha^{h(m)} = \alpha^{\text{a}r+\kappa s} = (\alpha^{\text{a}})^r r^s \pmod p$. Άρα $v_1 = v_2 \therefore$

Παράδειγμα 1. Ο Α επιλέγει πρώτο αριθμό p =2357 και ένα γεννήτορα α =2 της Z^*_{2357}. Ο Α επιλέγει ένα μυστικό κλειδί a=1751 και υπολογίζει $y = \alpha^{\text{a}} \bmod p = 2^{1751} \bmod 2357 = 1185$. Το δημόσιο κλειδί του Α είναι (p =2357, α =2, y =1185). Για απλότητα θεωρούμε ότι τα μηνύματα είναι ακέραιοι από το Z_p και $h(m) = m$. Για να υπογράψει ο Α ένα μήνυμα m =1463, επιλέγει ένα τυχαίο ακέραιο κ =1529, υπολογίζει $r = (\alpha^{\kappa} \bmod p) = 2^{1529} \bmod 2357 = 1490$ και $\kappa^{-1} \bmod (p\text{-}1) = 245$. Τελικά ο Α υπολογίζει $s = 245\{1463\text{-}1751(1490)\} \bmod 2356 = 1777$. Η υπογραφή του Α για το μήνυμα m =1463 είναι το ζευγάρι (r =1490, s =1777).
Ο Β υπολογίζει $v_1 = 1185^{1490} * 1490^{1777} \bmod 2357 = 1072$, $h(m) = 1463$ και $v_2 = 2^{1463} \bmod 2357 = 1072$. Ο Β αποδέχεται την υπογραφή επειδή $v_1 = v_2$.

Ένας αντίπαλος μπορεί να προσπαθήσει να πλαστογραφήσει την υπογραφή του Α για το μήνυμα m επιλέγοντας ένα τυχαίο ακέραιο κ και υπολογίζοντας $r = \alpha^{\kappa} \bmod p$. Ο αντίπαλος πρέπει να καθορίσει το $s = \kappa^{-1}\{h(m)\text{-a}r\} \bmod (p\text{-}1)$. Αν το πρόβλημα του διακριτού λογαρίθμου είναι υπολογιστικά ανέφικτο τότε το μόνο

που μπορεί να κάνει είναι να το επιλέξει τυχαία, όπότε η πιθανότητα επιτυχίας είναι μόνο $\frac{1}{p}$ που είναι μηδαμινή για μεγάλο p.

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

Αν δεν χρησιμοποιήσουμε hash συνάρτηση τότε $s = \kappa^{-1}\{m - a r\} \bmod (p-1)$. Η επίθεση από τον αντίπαλο με υπαρξιακή πλαστογράφηση μπορεί εύκολα να πραγματοποιηθεί. Ο αντίπαλος επιλέγει ένα ζευγάρι ακεραίων (u, v) με $\gcd(v, p-1)=1$. Υπολογίζει $r = \alpha^u * y^v \bmod p = \alpha^{u + a v} \bmod p$ και $s = -r v^{-1} \bmod (p-1)$. Το ζευγάρι (r, s) είναι μία νόμιμη υπογραφή για το μήνυμα $m = s * u \bmod (p-1)$ επειδή $(\alpha^m \alpha^{-a r})^{s^{-1}} = \alpha^u * y^v = r$.

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

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

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α επιλέγει μία κατάλληλη κυκλική ομάδα G με n στοιχεία και ένα γεννήτορα α.

(2). Επιλέγει ένα τυχαίο μυστικό ακέραιο a με $1 \leq a \leq n-1$. Υπολογίζει το στοιχείο της ομάδος $y = \alpha^a$.

(3). Το δημόσιο κλειδί του Α είναι (α, y) με τον ορισμό της πράξης της ομάδος και το μυστικό κλειδί είναι το a.

(β). Αλγόριθμος δημιουργίας υπογραφής.

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

(2). Υπολογίζει το στοιχείο της ομάδας $r = \alpha^{\kappa}$.

(3). Υπολογίζει $\kappa^{-1} \bmod n$.

(4). Υπολογίζει $h(m)$ και $h(r)$.

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

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

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

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

(2). Υπολογίζει $h(m)$ και $h(r)$.

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

(4). Υπολογίζει $v_2 = \alpha^{h(m)}$.

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

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

i	α^i
0	00001
1	00010
2	00100
3	01000
4	10000
5	00101
6	01010
7	10100

i	α^i
8	01101
9	11010
10	10001
11	00111
12	01110
13	11100
14	11101
15	11111

i	α^i
16	11011
17	10011
18	00011
19	00110
20	01100
21	11000
22	10101
23	01111

i	α^i
24	11110
25	11001
26	10111
27	01011
28	10110
29	01001
30	10010

Πίνακας 1.

Το στοιχείο α =(00010) είναι ένας γεννήτορας για την $G = F_{2^5}^*$, η πολλαπλασιαστική κυκλική ομάδα του σώματος. Η τάξη της ομάδος είναι n=31. Έστω ότι $h: \{0,1\}^{\pi} \rightarrow Z_{31}$ είναι η hash συνάρτηση. Ο Α επιλέγει ένα μυστικό κλειδί a=19 και υπολογίζει $y = \alpha^a$ =$(00010)^{19}$=(00110). Το δημόσιο κλειδί του Α είναι (α =(00010), y =(00110)). Για να υπογράψει το μήνυμα m =10110101 ο Α επιλέγει ένα τυχαίο ακέραιο κ =24 και υπολογίζει $r = \alpha^{24}$ =(11110) και $\kappa^{-1} \bmod 31$=22. Ο Α υπολογίζει $h(m)$=16 και $h(r)$=7 και s =22 * {16-(19)(7)} $\bmod 31$=30. Η υπογραφή του Α για το μήνυμα m είναι (r =(11110), s =30). Ο Β υπολογίζει $h(m)$=16 , $h(r)$=7 , $v_1 = y^{h(r)} * r^s$ = $(00110)^7$ * $(11110)^{30}$=(11011) και $v_2 = \alpha^{h(m)} = \alpha^{16}$=(11011). Ο Β αποδέχεται την υπογραφή επειδή $v_1 = v_2$.

Μία από τις πιο σημαντικές εφαρμογές του γενικευμένου σχήματος υπογραφής ElGamal είναι η περίπτωση όπου η πεπερασμένη αβελιανή ομάδα G είναι κατασκευασμένη από το σύνολο των στοιχείων μιας ελλειπτικής καμπύλης

πάνω σε ένα πεπερασμένο σώμα F_q (θα δούμε αυτό το σχήμα υπογραφής σε επόμενη παράγραφο).

3.4.3. Σχήμα υπογραφής Schnorr.

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

(α). Αλγόριθμος δημιουργίας κλειδιού.

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

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α επιλέγει ένα τυχαίο μυστικό ακέραιο κ με $1 \le \kappa \le q$-1.

(2). Υπολογίζει $r = \alpha^{\kappa} \bmod p$, $e = h(m \| r)$ και s =a$e + \kappa \bmod q$.

(3). Η υπογραφή του Α για το μήνυμα m είναι το ζευγάρι (s, e).

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

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

(2). Υπολογίζει $v = \alpha^s y^{-e} \bmod p$ και $e' = h(m \| v)$.

(5). Αποδέχεται την υπογραφή αν και μόνο αν $e' = e$.

Απόδειξη του αλγόριθμου πιστοποίησης.

Αν η υπογραφή δημιουργήθηκε από τον Α τότε $v = \alpha^s y^{-e} = \alpha^s \alpha^{\text{a}e} = \alpha^{\kappa} = r \pmod p$. Έτσι $h(m \| v) = h(m \| r)$ και $e' = e$.

Παράδειγμα 1. Ο Α επιλέγει πρώτους αριθμούς p=129841 και q=541 ((p-1)/ q=240). Μετά επιλέγει ένα τυχαίο ακέραιο g=26346 $\in Z_p^*$ και υπολογίζει α=$26346^{240} \bmod p$=26. Επειδή $\alpha \neq 1$, ο α είναι γεννήτορας της μοναδικής κυκλικής υποομάδας τάξης 541 στο Z_p^*. Επιλέγει ένα μυστικό ακέραιο a=423 και υπολογίζει y=$26^{423} \bmod p$=115917. Το δημόσιο κλειδί του Α είναι (p=129841, q=541, α=26, y=115917). Για να υπογράψει το μήνυμα m=11101101 επιλέγει ένα τυχαίο αριθμό κ=327 τέτοιο που $1 \le \kappa \le 540$ και υπολογίζει r=$26^{327} \bmod p$=49375 και $e = h(m \| r)$=155 . Τελικά ο Α υπολογίζει s=$423 * 155 + 327 \bmod 541$=431. Η υπογραφή για το μήνυμα m είναι (s=431, e=155).
Ο Β υπολογίζει v=$26^{431} * 115917^{-155} \bmod p$=49375 και $e' = h(m \| v)$=155. Ο Β αποδέχεται την υπογραφή επειδή $e' = e$.

3.4.4. Σχήμα Υπογραφής Ελλειπτικών Καμπυλών.

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

(α). Η πολύ μεγάλη ευκαμψία στην επιλογή της ομάδος (δηλαδή για κάθε δύναμη του πρώτου αριθμού q υπάρχει μόνο μία πολλαπλασιαστική ομάδα F_q^*, αλλά υπάρχουν πολλές ελλειπτικές καμπύλες E/F_q).

(β). Η έλλειψη κατάλληλων αλγορίθμων (subexponential time) για να σπάσουν ένα τέτοιο κρυπτοσύστημα αν η E είναι κατάλληλα επιλεγμένη.

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

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α επιλέγει ένα τυχαίο ακέραιο x με 1< x < q -1.

(2). Υπολογίζει $Q = x * P$.

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

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α επιλέγει ένα τυχαίο ακέραιο κ με 1< κ < q -1.

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

(3). Υπολογίζει $\kappa^{-1} \bmod q$.

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

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

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

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

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

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

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

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

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

Απόδειξη του αλγόριθμου πιστοποίησης.

$$u_1 * P + u_2 * Q = (u_1 + u_2 * x)\ P = s^{-1}\ (H\ (m) + x * r)\ P = \kappa * P.$$

Κανείς δεν γνωρίζει κάποια μέθοδο για να βρει τους (r, s) χωρίς να γνωρίζει τους κ και x.

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

3.5. Άλλα Σχήματα Υπογραφών.

3.5.1 Σχήματα Υπογραφών Μιας Χρήσης (One-time Digital Signatures).

Σχήματα υπογραφών μιας χρήσης είναι μηχανισμοί ψηφιακών υπογραφών όπου μπορούν να χρησιμοποιηθούν για να υπογράψουν το πολύ ένα μήνυμα, αλλιώς οι υπογραφές μπορούν να πλαστογραφηθούν. Ένα νέο δημόσιο κλειδί απαιτείται για κάθε μήνυμα που υπογράφεται. Το πλεονέκτημα των υπογραφών μιας χρήσης είναι ότι η δημιουργία και η πιστοποίηση των υπογραφών είναι πολύ εύκολη. Είναι χρήσιμες σε εφαρμογές με μικρή υπολογιστική πολυπλοκότητα. Τέτοια σχήματα μιας χρήσης είναι το Rabin, το Merkle και το Goldwasser,Micali, Rivest (GMR).

Εφαρμογή των σχημάτων υπογραφών μιας χρήσης είναι τα on-line/off-line σχήματα υπογραφών.

3.5.2 Σχήματα Υπογραφών Με Τρία Μέρη (Arbitrated Digital Signatures).

Ένα σχήμα υπογραφής με τρία μέρη είναι ένας μηχανισμός υπογραφής όπου απαιτείται η ύπαρξη ενός τρίτου έμπιστου ατόμου (TTP) στη διαδικασία της δημιουργίας και της πιστοποίησης της υπογραφής.

Έχουμε ένα αλγόριθμο συμμετρικής κρυπτογράφησης $E = \{E_\kappa : \kappa \in \mathrm{K}\}$ όπου K είναι ο χώρος των κλειδιών. Υποθέτουμε η είσοδος και η έξοδος για κάθε E_κ είναι συμβολοσειρές μήκους l-bits και $h : \{0,1\}^{\pi} \rightarrow \{0,1\}^{l}$ είναι μία one-way hash συνάρτηση. Το TTP επιλέγει ένα κλειδί $\kappa_{\mathrm{T}} \in \mathrm{K}$ και το κρατάει μυστικό. Για να πιστοποιήσει μία υπογραφή πρέπει να γνωρίζει το μυστικό κλειδί του Α.

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α επιλέγει ένα τυχαίο μυστικό κλειδί $\kappa_{\mathrm{A}} \in \mathrm{K}$.

(2). Με κάποιο μυστικό τρόπο μεταδίδει το κ_A στον TTP.

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α υπολογίζει $H = h(m)$.
(2). Κρυπτογραφεί το H με τον αλγόριθμο Ε και παίρνει $u = E_{k_A}(H)$.
(3). Στέλνει το u με τη συμβολοσειρά αυθεντικότητας I_A στον TTP.
(4). Ο TTP υπολογίζει $E_{k_A}^{-1}$ και παίρνει το H.
(5). Ο TTP υπολογίζει $s = E_{k_T}(H \| I_A)$ και στέλνει το s στον Α.
(6). Η υπογραφή του Α για το μήνυμα m είναι το s.

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

(1). Ο Β υπολογίζει $v = E_{k_B}(s)$.
(2). Στέλνει το v με τη συμβολοσειρά αυθεντικότητας I_B στον TTP.
(3). Ο TTP υπολογίζει $E_{k_B}^{-1}(v)$ για να πάρει το s.
(4). Ο TTP υπολογίζει $E_{k_T}^{-1}(s)$ για να πάρει το $H \| I_A$.
(5). Ο TTP υπολογίζει $w = E_{k_B}(H \| I_A)$ και στέλνει το w στον Β.
(6). Ο Β υπολογίζει $E_{k_B}^{-1}(w)$ για να πάρει το $H \| I_A$.
(7). Ο Β υπολογίζει $H' = h(m)$.
(8). Ο Β δέχεται την υπογραφή αν και μόνο αν $H' = H$.

3.5.3. Σχήμα υπογραφής ESIGN.

Είναι ένα σχήμα υπογραφής με συνημμένο το μήνυμα και απαιτεί μία one-way hash συνάρτηση $h:\{0,1\}^{\pi} \rightarrow Z_n$.

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο Α επιλέγει τυχαίους μεγάλους πρώτους p και q με $p \geq q$.
(2). Υπολογίζει $n = p^2 * q$.
(3). Επιλέγει ένα θετικό ακέραιο κ με $\kappa \geq 4$.
(4). Το δημόσιο κλειδί του Α είναι το (n, κ) και το μυστικό κλειδί το (p, q).

(β). Αλγόριθμος δημιουργίας υπογραφής.

(1). Ο Α υπολογίζει $v = h(m)$.
(2). Επιλέγει ένα τυχαίο μυστικό ακέραιο x με $0 \leq x \leq p * q$.

(3).Υπολογίζει $w = \left| ((v - x^k) \bmod n)/(pq) \right|$ και

$y = w * (\kappa * x^{\kappa-1})^{-1} \bmod p$.

(4). Υπολογίζει $s = (x + y * p * q) \bmod n$.

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

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

(1). Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το (n, κ).

(2). Υπολογίζει $u = s^{\kappa} \bmod n$ και $z = h(m)$.

(3). Αν $z \le u \le z + 2^{\left\lceil \frac{2}{3}\log n \right\rceil}$ δέχεται την υπογραφή, αλλιώς την απορρίπτει.

Απόδειξη του αλγόριθμου πιστοποίησης.

Παρατηρούμε ότι $s^{\kappa} = (x + y * p * q)^{\kappa} = \sum_{i=0}^{k} \binom{k}{i} x^{k-i} (ypq)^i$

$= x^{\kappa} + \kappa * y * p * q * x^{\kappa-1} (\bmod n)$. Αλλά $\kappa * x^{\kappa-1} * y = w (\bmod p)$ και έτσι $\kappa * x^{\kappa-1} * y = w + l * p$ για κάποιο $l \in Z$. Επειδή

$s^{\kappa} = x^{\kappa} + p * q\,(w + l * p) = x^{\kappa} + p * q * w =$

$x^{\kappa} + p * q \left\lceil \frac{(h(m) - x^k) \bmod n}{pq} \right\rceil = x^{\kappa} + p * q \left(\frac{h(m) - x^k + jn + \varepsilon}{pq} \right) (\bmod n)$ όπου

$\varepsilon = (x^{\kappa} - h(m)) \bmod pq$.

Έτσι $s^{\kappa} = x^{\kappa} + h(m) - x^{\kappa} + \varepsilon = h(m) + \varepsilon \pmod n$. Επειδή $0 \le \varepsilon \le p * q$ έχουμε ότι

$h(m) \le s^{\kappa} \bmod n \le h(m) + p * q$

$\le h(m) + 2^{\left\lceil \frac{2}{3}\log n \right\rceil}$, οπότε ο Β δέχεται την υπογραφή.

3.5.4. Τυφλά Σχήματα Υπογραφών (Blind Signature Schemes).

Είναι ένας μηχανισμός μεταξύ του αποστολέα (Α) και του υπογράφοντα (Β). Ο Α στέλνει ένα τμήμα πληροφορίας στον Β, το οποίο το υπογράφει ο Β και το επιστρέφει στον Α. Από αυτή την υπογραφή ο Α μπορεί να υπολογίσει την υπογραφή του Β για ένα μήνυμα m της επιλογής του Α. Ο Β δεν γνωρίζει ούτε το μήνυμα m ούτε την υπογραφή που σχετίζεται με αυτό το μήνυμα.

Στόχος αυτού του σχήματος είναι να εμποδίσει τον Β από το να παρατηρήσει το μήνυμα που υπογράφει και την υπογραφή του, ώστε αργότερα να είναι αδύνατο για αυτόν να συσχετίσει το υπογεγραμμένο μήνυμα με τον αποστολέα Α.

Τα τυφλά σχήματα υπογραφής έχουν εφαρμογές όπου ο αποστολέας Α (πελάτης) δεν θέλει ο υπογράφων Β (τράπεζα) να είναι ικανός να συσχετίσει ένα μήνυμα m και μία υπογραφή $S_B(m)$ για το m με τον Α. Αυτό είναι χρήσιμο για εφαρμογές ηλεκτρονικών πληρωμών όπου ένα μήνυμα m μπορεί να αντιπροσωπεύει ένα ποσό που ο Α μπορεί να χρησιμοποιήσει. Όταν τα m και

$S_B(m)$ παρουσιάζονται στον Β για πληρωμή, ο Β δεν μπορεί να συμπεράνει πιο τμήμα είναι το μήνυμα δοθέντος της υπογραφής. Αυτό επιτρέπει στον Α να είναι ανώνυμος .

Ένα σχήμα τυφλής υπογραφής πρέπει να έχει τα ακόλουθα χαρακτηριστικά:

(α). Ένα μηχανισμό υπογραφής για τον υπογράφοντα Β. Το $S_B(x)$ ορίζει την υπογραφή του Β στο x.

(β). Συναρτήσεις f και g (γνωστές μόνο στον αποστολέα) τέτοιες που $g(S_B(f(m)))= S_B(m)$. Η f λέγεται συνάρτηση τύφλωσης(blinding function) , η g συνάρτηση επαναφοράς(unblinding function) και το $f(m)$ τυφλό μήνυμα(blinded message).

Παράδειγμα 1. Θα δούμε ένα παράδειγμα όπου η συνάρτηση τύφλωσης f βασίζεται στο RSA. Έστω $n = p*q$ είναι το γινόμενο δύο μεγάλων πρώτων αριθμών. Ο αλγόριθμος δημιουργίας της υπογραφής για τον Β (S_B) είναι ο αλγόριθμος που είδαμε στο RSA (4.5.1) με δημόσιο κλειδί (n,e) και μυστικό κλειδί το d. Έστω κ είναι κάποιος ακέραιος με $\gcd(n,\kappa)$=1. Η συνάρτηση τύφλωσης $f: Z_n \rightarrow Z_n$ ορίζεται από τον τύπο $f(m)= m * \kappa^e \bmod n$ και η συνάρτηση επαναφοράς $g: Z_n \rightarrow Z_n$ ορίζεται από τον τύπο $g(m)= \kappa^{-1} * m \bmod n$. Για αυτή την επιλογή των f, g και S_B έχουμε ότι $g(S_B(f(m)))= g(S_B(m * \kappa^e \bmod n))= g(m^d * \kappa \bmod n)= m^d \bmod n = S_B(m)$.

Τέλος θα δούμε ένα πρωτόκολλο τυφλής υπογραφής του Chaum.

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

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

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

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

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

3.5.5. Γνήσια Σχήματα Υπογραφών (Undeniable Signature Schemes).

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

Οι εφαρμογές αυτών των σχημάτων είναι πολλές:

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

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

Θα δούμε ένα σχήμα γνήσιας υπογραφής.

(α). Αλγόριθμος δημιουργίας κλειδιού.

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

(2). Επιλέγει ένα τυχαίο ακέραιο α της υποομάδας, τάξης q στο Z_p^*.

(3). Αν α =1, τότε πήγαινε στο βήμα 2.

(4). Επιλέγει ένα τυχαίο ακέραιο $\kappa \in$ {1,2,…, q -1} και υπολογίζει $y = \alpha^{\kappa} \bmod p$.

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

(β). Αλγόριθμος δημιουργίας υπογραφής.

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

(1). Ο Α υπολογίζει $s = m^{\kappa} \bmod p$.

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

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

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

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

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

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

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

Απόδειξη του αλγόριθμου πιστοποίησης.

$$w = (z)^{\kappa^{-1}} = (s^{x_1} * y^{x_2})^{\kappa^{-1}} = (m^{\kappa x_1} * \alpha^{\kappa x_2})^{\kappa^{-1}} = m^{x_1} * \alpha^{x_2} = w' \bmod p \therefore$$

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

(α). Να αρνηθεί να πάρει μέρος στη διαδικασία πιστοποίησης της υπογραφής.

(β). Να εκτελέσει την πιστοποίηση λανθασμένα.

(γ). Να ισχυρισθεί ότι η υπογραφή είναι πλαστογραφημένη αν και έχει πετύχει η διαδικασία πιστοποίησης.

3.5.6. Σχήμα Υπογραφής Εύρεσης Πλαστογράφησης (Fail-Stop Signature Schemes).

Σε αυτό το σχήμα της υπογραφής ο Α μπορεί να αποδείξει ότι μία υπογραφή είναι πλαστή. Αυτό γίνεται δείχνοντας ότι ο βασικός μηχανισμός που δημιουργεί την υπογραφή είναι δεσμευτικός. Η ικανότητα να αποδείξουμε ότι η υπογραφή είναι πλαστή δε στηρίζεται σε κάποια κρυπτογραφική υπόθεση αλλά ότι μπορεί να αποτύχει με μικρή πιθανότητα. Η πιθανότητα αποτυχίας είναι ανεξάρτητη από την υπολογιστική δύναμη του πλαστογράφου. Το βασικό πλεονέκτημα αυτού του σχήματος είναι ότι ακόμα και ένας δυνατός υπολογιστικά πλαστογράφος μπορέσει να πλαστογραφήσει μία απλή υπογραφή, η πλαστογράφηση μπορεί να ανακαλυφθεί και ο συγκεκριμένος μηχανισμός δημιουργίας της υπογραφής δε θα χρησιμοποιηθεί στο μέλλον.

Είναι ένα σχήμα υπογραφής μιας χρήσης αλλά μπορεί να γενικευθεί ώστε να επιτρέπονται περισσότερες υπογραφές χρησιμοποιώντας δέντρα αυθεντικότητας.

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

(α). Αν ο υπογράφων υπογράψει ένα μήνυμα με το δεσμευτικό μηχανισμό τότε αυτός που θα πιστοποιήσει την υπογραφή πρέπει να τη δεχτεί ως έγκυρη.

(β). Ο πλαστογράφος δε μπορεί να κατασκευάσει υπογραφές που να περάσουν από τον αλγόριθμο πιστοποίησης χωρίς να χρειασθεί εκθετικό χρόνο εργασίας.

(γ). Αν ο πλαστογράφος καταφέρει να κατασκευάσει μία υπογραφή που περάσει από τον αλγόριθμο πιστοποίησης τότε με μεγάλη πιθανότητα ο αληθινός υπογράφων μπορεί να αποδείξει την πλαστογράφηση.

(δ). Ο υπογράφων δε μπορεί να κατασκευάσει υπογραφές που μετά από την πάροδο κάποιου χρονικού διαστήματος να ισχυρισθεί ότι είναι πλαστές.

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

(α). Αλγόριθμος δημιουργίας κλειδιού.

(1). Ο TTP κάνει τα εξής:

α/. Επιλέγει πρώτους p και q τέτοιους που ο q διαιρεί τον (p -1)

β/. Επιλέγει ένα τυχαίο ακέραιο α της υποομάδας, τάξης q στο Z_p^*.

γ/. Αν α =1 τότε πήγαινε στο βήμα β.

δ/. Επιλέγει ένα τυχαίο ακέραιο a με $1 \le a \le q$ -1 και υπολογίζει $\beta = \alpha^a \bmod p$. Ο ακέραιος a κρατιέται μυστικός από τον ΤΤΡ.

ε/. Στέλνει στον Α το (p, q, α, β).

(2) Ο Α κάνει τα εξής:

α/. Επιλέγει τυχαία ακέραιους x_1, x_2, y_1, y_2 από το διάστημα [0, q -1].

β/. Υπολογίζει $\beta_1 = \alpha^{x_1} * \beta^{x_2} \bmod p$ και $\beta_2 = \alpha^{y_1} * \beta^{y_2} \bmod p$.

γ/. Το δημόσιο κλειδί του Α είναι $(\beta_1, \beta_2, p, q, \alpha, \beta)$ και το μυστικό κλειδί $\bar{x} = (x_1, x_2, y_1, y_2)$.

(β). Αλγόριθμος δημιουργίας υπογραφής.

Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου στην υποομάδα τάξης q στο Z_p^*. Το μήνυμα $m \in$ [0, q -1]

(1). Ο Α υπολογίζει $s_{1,m} = x_1 + my_1 \bmod q$ και $s_{2,m} = x_2 + my_2 \bmod q$.

(2). Η υπογραφή του Α για το μήνυμα m είναι $(s_{1,m}, s_{2,m})$.

(γ). Αλγόριθμος πιστοποίησης της υπογραφής.

(1). Ο Β εξασφαλίζει το δημόσιο κλειδί του Α το $(\beta_1, \beta_2, p, q, \alpha, \beta)$.

(2). Υπολογίζει $v_1 = \beta_1 * \beta_2^m \bmod p$ και $v_2 = a^{s_{1,m}} * \beta^{s_{2,m}} \bmod p$.

(3). Ο Β δέχεται την υπογραφή αν και μόνο αν $v_1 = v_2$.

Απόδειξη του αλγόριθμου πιστοποίησης.

$v_1 = \beta_1 * \beta_2^m = (\alpha^{x_1} * \beta^{x_2})(\alpha^{y_1} * \beta^{y_2})^m = \alpha^{x_1 + my_1} * \beta^{x_2 + my_2} = a^{s_{1,m}} * \beta^{s_{2,m}} = v_2 \ (\bmod p)$.

Ιδιότητα του σχήματος υπογραφής. Έστω ότι το δημόσιο κλειδί είναι $(\beta_1, \beta_2, p, q, \alpha, \beta)$ και το μυστικό κλειδί είναι $\bar{x} = (x_1, x_2, y_1, y_2)$.

(α). Υπάρχουν ακριβώς q^2 τετράδες $\bar{x}' = (x_1', x_2', y_1', y_2')$ με $x_1', x_2', y_1', y_2' \in Z_q$ όπου έχουν το ίδιο αποτέλεσμα με το (β_1, β_2) του τμήματος του δημοσίου κλειδιού.

(β). Έστω T το σύνολο αυτών των τετράδων για το (β_1, β_2). Για κάθε $m \in Z_q$ υπάρχουν ακριβώς q τετράδες στο T όπου δίνουν την ίδια υπογραφή $(s_{1,m}, s_{2,m})$ για το m. Έτσι οι q^2 τετράδες του T δίνουν ακριβώς q διαφορετικές υπογραφές για το m.

(γ). Έστω $m' \in Z_q$ είναι ένα μήνυμα διαφορετικό από το m. Τότε οι q τετράδες του T που δίνουν του Α τις υπογραφές ($s_{1,m}$, $s_{2,m}$) για το m, δίνουν διαφορετικές υπογραφές για το m'.

Παράδειγμα 1. Έστω p=29 και q=7 και α=16 είναι ένας γεννήτορας της υποομάδας τάξης q στο Z_p^*. Παίρνουμε $\beta = \alpha^5 \bmod 29$=23. Υποθέτουμε ότι το μυστικό κλειδί του Α είναι $\bar{x}$=(x_1, x_2, y_1, y_2)=(2,3,5,2) και το δημόσιο κλειδί είναι $\beta_1 = \alpha^2 * \beta^3 \bmod 29$=7, $\beta_2 = \alpha^5 * \beta^2 \bmod 29$=16. Στον πίνακα 1 βλέπουμε τις q^2=49 τετράδες που δίνουν το ίδιο δημόσιο κλειδί.

1603	2303	3003	4403	5103	6503	0203
1610	2310	3010	4410	5110	6510	0210
1624	2324	3024	4424	5124	6524	0224
1631	2331	3031	4431	5131	6531	0231
1645	2345	3045	4445	5145	6545	0245
1652	2352	3052	4452	5152	6552	0252
1666	2366	3066	4466	5166	6566	0266

Πίνακας 1.

Αν οι 49 τετράδες του παραπάνω πίνακα χρησιμοποιηθούν για την υπογραφή του μηνύματος m=1, τότε υπάρχουν ακριβώς q=7 υπογραφές ($s_{1,m}$, $s_{2,m}$). Στον πίνακα 2 βλέπουμε τις πιθανές και εκείνες τις τετράδες που δημιουργούν κάθε υπογραφή.

Υπογραφές	(2,6)	(3,3)	(4,0)	(5,4)	(6,1)	(0,5)	(1,2)
Τετράδες	1610	1624	1631	1645	1652	1666	1603
	2303	2310	2324	2331	2345	2352	2366
	3066	3003	3010	3024	3031	3045	3052
	4452	4466	4403	4410	4424	4431	4445
	5145	5152	5166	5103	5110	5124	5131
	6531	6545	6552	6566	6503	6510	6524
	0224	0231	0245	0252	0266	0203	0210

Πίνακας 2.

Τέλος στον πίνακα 3 βλέπουμε για κάθε μήνυμα $m' \in Z_7$, όλες τις υπογραφές για τις 7 τετράδες όπου η υπογραφή του Α είναι (0,5) για το μήνυμα m=1.

	m'						
Τετράδα	0	1	2	3	4	5	6
1666	16	05	64	53	42	31	20
2352	23	05	50	32	14	66	41
3045	30	05	43	11	56	24	62
4431	44	05	36	60	21	52	13
5124	51	05	22	46	63	10	34
6510	65	05	15	25	35	45	55
0203	02	05	01	04	00	03	06

Πίνακας 3.

Έστω ότι ο πλαστογράφος θέλει να βρει την υπογραφή του Α για κάποιο μήνυμα m'. Υπάρχουν δύο περιπτώσεις που θα εξετάσουμε:

(α). Ο πλαστογράφος έχει πρόσβαση μόνο στο δημόσιο κλειδί του Α. Από την ιδιότητα του σχήματος αυτού, η πιθανότητα ότι η υπογραφή που θα κατασκευάσει να είναι ίδια με την υπογραφή του Α για το μήνυμα m'είναι ίση με $\frac{q}{q^2}=\frac{1}{q}$. Αυτή η πιθανότητα είναι ανεξάρτητη από την υπολογιστική δύναμη του πλαστογράφου.

(β). Αν ο πλαστογράφος έχει πρόσβαση σε ένα μήνυμα m και στην αυθεντική υπογραφή του, τότε η πιθανότητα να κατασκευάσει μία πλαστογραφημένη υπογραφή για ένα μήνυμα m' είναι πάλι $\frac{1}{q}$ όπου πάλι αυτή η πιθανότητα είναι ανεξάρτητη από την υπολογιστική δύναμη του πλαστογράφου.

Θα δούμε τώρα με πιο τρόπο ο Α θα μπορέσει να αποδείξει με μεγάλη πιθανότητα ότι μία υπογραφή είναι πλαστή. Υποθέτουμε ότι ο πλαστογράφος έχει πλαστογραφήσει μία υπογραφή του Α για ένα μήνυμα και έχει περάσει με επιτυχία τον αλγόριθμο πιστοποίησης. Ο παρακάτω αλγόριθμος απόδειξης της πλαστογραφίας μας δείχνει πως ο Α θα χρησιμοποιήσει την πλαστή υπογραφή για να βρει το μυστικό ακέραιο a που είχαμε υποθέσει στην αρχή ότι τον γνωρίζει μόνο ο TTP.

Αλγόριθμος **απόδειξης** της πλαστογραφίας.

Για να αποδείξουμε ότι η υπογραφή $s'=(s'_{1,m},\ s'_{2,m})$ είναι πλαστή για ένα μήνυμα m , ο Α θα βρει το $a=\log_{\alpha}\beta$. Ο Α κάνει τα εξής:

(α). Υπολογίζει μία υπογραφή $s=(s_{1,m},s_{2,m})$ για το μήνυμα m χρησιμοποιώντας το δικό του μυστικό κλειδί $\bar{x}=(x_1,x_2,y_1,y_2)$.

(β). Αν $s=s'$ τότε τέλος.

(γ). Υπολογίζει $a=(s_{1,m}-s'_{1,m})*(s'_{2,m}-s_{2,m})^{-1} \bmod q$.

Απόδειξη του αλγόριθμου απόδειξης της πλαστογραφίας.

Η πιθανότητα να ισχύει $s=s'$ είναι $\frac{1}{q}$. Από τον αλγόριθμο πιστοποίησης έχουμε ότι

$\alpha^{s_{1,m}}*\beta^{s_{2,m}}=\alpha^{s'_{1,m}}*\beta^{s'_{2,m}} \pmod p$ ή $\alpha^{s_{1,m}-s'_{1,m}}=\alpha^{a(s'_{2,m}-s_{2,m})} \pmod p$

ή $s_{1,m}-s'_{1,m}=a(s'_{2,m}-s_{2,m}) \pmod q$.

Τελικά έχουμε ότι $a=(s_{1,m}-s'_{1,m})*(s'_{2,m}-s_{2,m})^{-1} \bmod q$.

Βιβλιογραφία

1. Applied Cryptography 2nd edition – B. Schneier
2. Guide to Elliptic Curve Cryptography – D. Hankerson, A. Menezes, S. Vanstone
3. Handbook of Applied Cryptography – Alfred Menezes, Paul van Oorschot, Scott Vanstone
4. Cryptography Theory and practice 3rd edition – Douglas Stinson
5. Cryptology Unlocked – Reinhard Wobst
6. Contemporary Cryptography – Rolf Oppliger
7. Modern Cryptography Theory and Practice – Wenbo Mao
8. Cryptology Smarties – Peter Skvarenina
9. Introduction to Cryptography with Coding Theory – Wade Trappe, Lawrence Washington
10. M. Agrawal, N. Kayal, N. Saxena “Primes is in P”
11. T. ElGamal “Cryptography and logarithms over finite fields” PhD thesis, Stanford University, 1984.
12. Κρυπτογραφία – Χ. Κουκουβίνος , Α. Παπαϊωάννου
13. Σημειώσεις στη Θεωρία Αριθμών και την Κρυπτογραφία – Ε. Ζάχος
14. Κρυπτογραφία η Επιστήμη της Ασφαλούς Επικοινωνίας – Δ. Πουλάκης