ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

Μπακίρι Ένο

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΣΧΗΜΑΤΑ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ ΣΤΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Επιβλέπων:

Παπαιωάννου Αλέξανδρος

Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2010

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

Μπακίρι Ένο

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΣΧΗΜΑΤΑ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ ΣΤΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Επιβλέπων:

Παπαιωάννου Αλέξανδρος

Επίκουρος Καθηγητής Ε.Μ.Π.

Εξεταστική επιτροπή:

1. Α. Παπαιωάννου, Επίκουρος Καθηγητής Ε.Μ.Π.
   Επιβλέπων της Δ.Ε. .....
2. Θ. Ρασσιάς, Καθηγητής Ε.Μ.Π. .....
3. Ν. Πάλλα, Λέκτορας Ε.Μ.Π. .....

Αθήνα, Ιούλιος 2010

Πρόλογος

Η Ψηφιακή Υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Μια έγκυρη ψηφιακή υπογραφή δίνει στον παραλήπτη την πιστοποίηση ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά την μεταφορά. Οι ψηφιακές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού (hash function) για δημιουργία της σύνοψης (hash) σε συνδυασμό με ασυμμετρική κρυπτογραφία για κρυπτογράφηση/αποκρυπτογράφηση σύνοψης (ο συνδυασμός σύνοψης και κρυπτογράφησης με ασυμμετρική κρυπτογραφία αποδεικνύει την ακεραιότητας του εγγράφου αλλά και την απόδειξη ταυτότητας του αποστολέα).

Σε μερικές χώρες όπως τις ΗΠΑ και κάποιες χώρες της Ευρωπαϊκής ένωσης, οι ψηφιακές υπογραφές έχουν και νομική υπόσταση. Οι ψηφιακές υπογραφές σε ψηφιακά έγγραφα είναι παρόμοιες με τις αντίστοιχες χειρόγραφες υπογραφές σε έντυπα έγγραφα. Όταν οι ψηφιακές υπογραφές υλοποιούνται - εφαρμόζονται σωστά (με χρήση ασφαλών κρυπτογραφικών αλγορίθμων), είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις αντίστοιχες χειρόγραφες. Επίσης το φυσικό πρόσωπο που ψηφιακά υπογράφει το ψηφιακό έγγραφο δεν μπορεί να ισχυριστεί ότι δεν το υπόγραψε (όσο το ιδιωτικό κλειδί που χρησιμοποίησε δεν υποκλάπηκε). Κάποιες υλοποιήσεις των ψηφιακών υπογραφών προσθέτουν και την ημερομηνία υπογραφής του εγγράφου, ώστε και τον ιδιωτικό κλειδί να υποκλαπεί, η ψηφιακή υπογραφή να είναι έγκυρη. Η ψηφιακή υπογραφή μπορεί να προστεθεί σε οποιαδήποτε σειρά από bits (δηλαδή δεδομένα): παραδείγματα χρήσης είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, μηνύματα που στέλνονται στο Διαδίκτυο κλπ. Πολλοί οργανισμοί υιοθετούν την χρήση των ψηφιακών υπογραφών ώστε να αποφεύγεται η αποστολή τυπωμένων εγγράφων (επικυρωμένα με χρήση σφραγίδων και υπογραφών).

Abstract

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering.

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance. However, laws concerning electronic signatures do not always make clear whether they are digital cryptographic signatures in the sense used here, leaving the legal definition, and so their importance, somewhat confused.

Digital signatures employ a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything representable as a bitstring: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

Ευχαριστίες

Στο σημείο αυτό θα ήθελα να ευχαριστήσω ιδιαιτέρως τον επιβλέποντα επίκουρο καθηγητή του Ε.Μ.Π., Παπαϊωάννου Αλέξανδρος για την ουσιαστική βοήθεια μου προσέφερε με την άψογη συνεργασία, τις πολύτιμες συμβολές και την καθοδήγησή του σε όλη την διάρκεια της εκπόνησης αυτής της διπλωματικής εργασίας.

Υπάρχει και κάποιο άτομο στην όποια θα ήθελα να κάνω μια ιδιαίτερη αναφορά καθώς με τον τρόπο της συνέλαβε στην πραγματοποιήσει αυτής της διπλωματικής εργασίας, βοηθώντας με να ξεπεράσω πολλές περίοδος δυσκολιών και απογοητεύσεις. Θέλω να εκφράσω την βαθιά μου εκτίμηση ευγνωμοσύνη και αγάπη στην Blerta Fetahu με την όποια έζησα τα καλυτέρα χρόνια της ζωής μου.

Περιεχόμενα

Κεφάλαιο 1

Α. Στοιχειά από την θεωρία Αλγόριθμων και Πολυωνυμικού χρόνου[1] (polynomial-time algorithm)

1. Αλγόριθμος πολυωνυμικου χρόνου

Πριν προχωρήσουμε στον ορισμό του αλγορίθμου πολυωνυμικου χρόνου παραθέτουμε πρώτα κάποιους απαραίτητους ορισμούς.

Ορισμός (χρόνος εκτέλεσης) *Ο χρόνος εκτέλεσης (running time) ενός αλγορίθμου για ένα συγκεκριμένο όρισμα είναι ο αριθμός των πρωταρχικών πράξεων ή «βημάτων» που εκτελούνται.*

Ορισμός (χειρότερη περίπτωση τον χρόνου εκτέλεσης) *Η χειρότερη περίπτωση του χρόνου εκτέλεσης (worst case — running time) ενός αλγορίθμου είναι ένα άνω φράγμα του χρόνου εκτέλεσης για ένα οποιοδήποτε όρισμα και εκφράζεται ως συνάρτηση του μεγέθους του ορίσματος.*

Συνήθως δεν μας ενδιαφέρει η ακριβής μέτρηση του κόστους εκτέλεσης ενός αλγορίθμου αλλά η εύρεση μόνο της τάξης μεγέθους του κόστους. Μας ενδιαφέρει η ασυμπτωτική συμπεριφορά του αλγορίθμου. Με άλλα λόγια αναζητούμε την οριακή αυξητική τάση (rate of growth) της συνάρτησης που εκφράζει την πολυπλοκότητα του αλγορίθμου καθώς αυξάνεται το μέγεθος της εισόδου.

Ορισμός *Έστω $f: \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ και $g : N\setminus\{0\} \to N\setminus\{0\}$. Ορίζουμε το σύμβολο O ως εξής:*

$$O(g) = \{ f \mid \exists\, c > 0, n_0: \forall n > n_0 \;\; f(n) \leq cg(n)\}.$$

Αν $f \in O(g)$ συνήθως γράφουμε $f(n) = O(g(n))$ και λέμε ότι η συνάρτηση f είναι τάξης μεγέθους g.

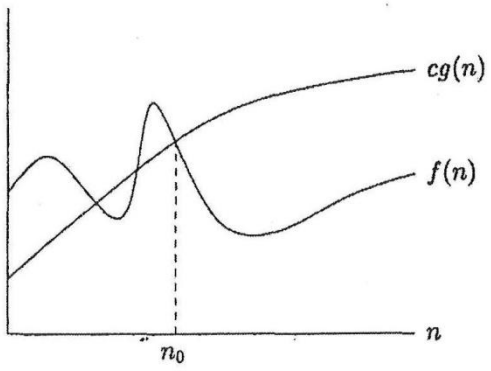
Αν $p=c_k n^k + c_{k-1}n^{k-1} + ... + c_0$, δηλαδή πολυώνυμο βαθμού k, τότε $p \in O(n^k)$ ή $p(n) = O(n^k)$.

Μπορούμε τώρα να διατυπώσουμε τον ορισμό του αλγόριθμου πολυωνυμικού χρόνου.

Ορισμός (αλγόριθμος πολυωνυμικού χρόνου) *Ένας αλγόριθμος πολυωνυμικού χρόνου είναι ένας αλγόριθμος του οποίου η συνάρτηση χειρότερης περίπτωσης του*

[1] Στην προκειμένη περίπτωση οι όροι συνάρτηση και αλγόριθμος είναι ταυτόσημοι.

χρόνου εκτέλεσης είναι της μορφής $O(n^k)$, όπου n είναι το μέγεθος του ορίσματος και k μια σταθερά.



$f = O(g)$

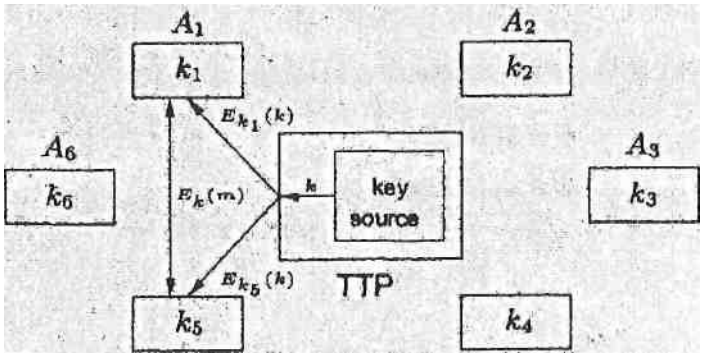
2. Έμπιστη αρχή (trusted third party-TTP)

Σκοπός μιας ψηφιακής υπογραφής είναι η λύση διαφωνιών (resolution of disputes).Για παράδειγμα, μια οντότητα Α μπορεί κάποια στιγμή να αρνηθεί ότι υπόγραψε ένα μήνυμα ή κάποια άλλη οντότητα Β Φα μπορούσε ψευδώς να ισχυριστεί ότι μια υπογραφή σε ένα μήνυμα παράχθηκε από την Α. Για να ξεπεράσουμε τέτοια προβλήματα απαιτείται μια ***έμπιστη αρχή*** *(trusted third party-TTP). Η TTP πρέπει να είναι κάποια οντότητα για την οποία όλοι οι συμμετέχοντες συμφωνούν εκ των προτέρων.*

Αν η οντότητα Α αρνηθεί ότι ένα μήνυμα m, το οποίο κατέχει η Β, υπογράφτηκε από αυτήν, τότε η Β πρέπει να μπορεί να παρουσιάσει την υπογραφή s_A του m μαζί με το μήνυμα m στην TTP. Η TTP αποφαίνεται υπέρ της Β αν V_A (m,s) =αληθής και υπέρ της Α διαφορετικά. Η Β αποδέχεται την απόφαση αν είναι σίγουρη πως η TTP έχει τον ίδιο μετασχηματισμό επαλήθευσης με την Α, V_A. Η Α αποδέχεται την απόφαση αν είναι σίγουρη πως η TTP χρησιμοποίησε το μετασχηματισμό επαλήθευσης V_A και ότι ο μετασχηματισμός υπογραφής S_A δεν αποκαλύφθηκε.

Επίσης μια TTP παίζει σημαντικό ρόλο στην επικοινωνία μεταξύ οντοτήτων εντός ενός δικτύου. Σε αυτήν την περίπτωση κάθε οντότητα A_i μοιράζεται ένα διακεκριμένο συμμετρικό κλειδί k_i με την TTP. Αν κάποια στιγμή δύο οντότητες

επιθυμήσουν να επικοινωνήσουν, τότε η TTP παράγει ένα κλειδί k και το στέλνει κρυπτογραφημένο υπό το σταθερό κλειδί κάθε οντότητας, όπως φαίνεται στο σχήμα που ακολουθεί για τις οντότητες A_1 και A_5.



Διαχείριση κλειδιού μέσω μιας έμπιστης αρχής (TTP).

3. Σχήματα πιστοποίησης ταυτότητας

Τα σχήματα πιστοποίησης ταυτότητας χρησιμοποιούνται σε συστήματα στα οποία είναι απαραίτητο να αποδειχθεί η ταυτότητα κάποιας οντότητας με ηλεκτρονικά μέσα.

Τα περισσότερα σχήματα πιστοποίησης ταυτότητας δεν είναι πάντα ασφαλή. Ένας υποκλοπέας μπορεί να υποκλέψει όλες τις απαραίτητες πληροφορίες που χρειάζεται ώστε να λειτουργήσει ως νόμιμος χρήστης του συστήματος. Ένα σχήμα πιστοποίησης ταυτότητας πρέπει να παρέχει εγγυήσεις ότι κάποιος που παρακολουθεί ένα συγκεκριμένο σύστημα δεν μπορεί κατόπιν να λειτουργεί ως νόμιμος χρήστης του. Επίσης πρέπει να είναι αδύνατο για κάποιο χρήστη του συστήματος να μπορεί να παριστάνει κάποιον άλλο χρήστη, που σημαίνει ότι όταν κάποιος χρήστης πιστοποιεί την ταυτότητα του στο σύστημα δεν πρέπει να αποκαλύπτει την πληροφορία αναγνώρισης του.

Σχήμα αναγνώρισης: πρόκληση και ανταπόκριση (challenge-and-response)

Το σχήμα πρόκληση και ανταπόκριση είναι ένα απλό σχήμα αναγνώρισης που. βασίζεται σε οποιοδήποτε κρυπτοσύστημα συμμετρικού κλειδιού (π.χ., ΒΕ3).Έστω δύο οντότητες Α,Β και ένα συμμετρικό κλειδί k. Το πρωτόκολλο έχει ως εξής:

1. *0 Β επιλέγει μία πρόκληση (challenge) e, η οποία είναι μια τυχαία δυαδική ακολουθία μήκους 64 bits και τη στέλνει στον Α.*
2. *Ο Α υπολογίζει το $y = E_k(e)$, όπου Ε ο μετασχηματισμός κρυπτογράφησης και το στέλνει στον Β.*
3. *Ο Β υπολογίζει το $y' = E_k(e)$ και πιστοποιεί ότι $y' = y$.*

Μετατρέποντας ένα σχήμα αναγνώρισης σε ένα σχήμα υπογραφής

Η ακόλουθη γενική τεχνική μπορεί να χρησιμοποιηθεί για την μετατροπή ενός σχήματος αναγνώρισης πρόκληση και ανταπόκριση σε σχήμα υπογραφής: αντικαθιστούμε την τυχαία πρόκληση e της οντότητας που επαληθεύει (Β) με την τιμή κατακερματισμού h(x||m), δηλ. της παράθεσης του μάρτυρα (witness) x και του μηνύματος m που πρόκειται να υπογραφεί.

Β. Στοιχειά από την θεωρία Αλγόριθμων και Άλγεβρα.

1. Πρωταρχικό στοιχείο (primitive element) modulo n

Ορισμός *Έστω α ∈ $\mathbb{Z}_n$*Αν η τάξη του α είναι φ(n), τότε το α λέγεται γεννήτορας ή πρωταρχικό στοιχείο του $\mathbb{Z}_n$*. Αν το $\mathbb{Z}_n$* έχει ένα γεννήτορα λέγεται κυκλικό.*

Το σύνολο $\mathbb{Z}_n$, με πράξη την πρόσθεση modulo n, σχηματίζει μια ομάδα τάξεως n. Το σύνολο $\mathbb{Z}_n$, με πράξη τον πολλαπλασιασμό modulo n δεν είναι ομάδα, αφού δεν έχουν όλα τα στοιχεία πολλαπλασιαστικό αντίστροφο. Ωστόσο, το σύνολο $\mathbb{Z}_n$ είναι ομάδα τάξεως φ(n) υπό την πράξη του πολλαπλασιασμού modulo n, με ταυτοτικό στοιχείο το 1.*

2. Συνάρτηση Euler

Ορισμός *Για n ≥ 1, το φ (n) συμβολίζει το πλήθος των ακεραίων στο διάστημα [1, n] που είναι σχετικά πρώτοι προς το n. Η συνάρτηση φ λέγεται συνάρτηση Euler.*

Πόρισμα *(ιδιότητες της συνάρτησης Euler)*

1. *Αν p είναι πρώτος, τότε φ (p) = p- 1.*
2. *Η συνάρτηση Euler είναι πολλαπλασιαστική. Αυτό σημαίνει ότι αν (m,n) = 1, τότε φ (m · n) = φ (m) · φ(n).*
3. *Αν $n = p^{e1}_1 \ p^{e2}_2 \dots p^{ek}_k$ είναι η ανάλυση του n σε πρώτους παράγοντες, τότε*

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

3. Επεκτεταμένος Ευκλείδιος αλγόριθμος (extended Euclidean algorithm)

Υπολογισμός πολλαπλασιαστικού αντιστρόφου modulo n.

Επεκτεταμένος Ευκλείδιος αλγόριθμος.

1. $no = n$
2. $b_0 = b$
3. $i_0 = 0$
4. $t = 1$
5. $q = \left\lfloor \frac{n_0}{b_0} \right\rfloor$
6. $r = no - q \times b_0$
7. ***while*** $r > 0$ ***do***

8. $temp = t_0 - q \times t$

9. ***if*** $temp > 0$ ***then*** $temp = temp \bmod n$

10. ***if*** $temp < 0$ ***then*** $temp = n - ((-temp) \bmod n)$

11. $t_0 = t$

12. $t = temp$

13. $n_0 = b_0$

14. $b_0 = r$

15. $q = \left\lfloor \frac{n_0}{b_0} \right\rfloor$

16. $r = n_0 - q \times b_0$

17. ***if*** $b_0 \neq 1$ ***then***

o b δεν έχει αντίστροφο modulo n

else

$b^{-1} = t \bmod n$

4. Θεώρημα Euler

Αν $a \in \mathbb{Z}_n^*$ *και* $(a,n) = 1$, *τότε* $a^{\varphi(n)} \equiv 1 \pmod n$.

5. Ψηφίο υψηλής και χαμηλής τάξης

Έστω ένας ακέραιος $b \geq 2$. *Τότε οποιοσδήποτε θετικός ακέραιος* α *μπορεί να εκφραστεί με μοναδικό τρόπο ως εξής:* $\alpha = a_n b^n + \alpha_{n-1} b^{n-1} + \ldots + a_1 b + \alpha_0$, *όπου* $\alpha_i \in \mathbb{Z}$ *με* $0 \leq \alpha_i \leq 6, 0 \leq i \leq n$ *και* $a_n \neq 0$.

Η αναπαράσταση ενός θετικού ακεραίου α *ως άθροισμα πολλαπλασίων δυνάμεων του b, όπως δίνεται παραπάνω, λέγεται αναπαράσταση του* α *με βάση (base ή radix) b.*

Η αναπαράσταση ενός θετικού ακεραίου α *με βάση b συνήθως γράφεται ως* $\alpha = (a_n \alpha_{n-1} \ldots a_1 \alpha_0)_b$. *Οι ακέραιοι* α_i, $0 \leq i \leq n$, *λέγονται ψηφία. Το* α_n *λέγεται το* ***πιο σημαντικό ψηφίο ή ψηφίο υψηλής τάξεως*** *(most significant or high-order dig-it).Το* α_0 *λέγεται το* ***λιγότερο σημαντικό ψηφίο ή ψηφίο χαμηλής τάξεως*** *(least significant or low-order digit). Αν b = 10,ο συνήθης συμβολισμός είναι* $\alpha = a_n \alpha_{n-1} \ldots a_1 \alpha_0$. *Αν b = 2 τότε τα ψηφία λέγονται bits (Binary digiTS).*

6. Επεξήγηση των συμβόλων ⌊ ⌋ ***και*** ⌈ ⌉

- $\lfloor x \rfloor$ *είναι ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος του x. Π.χ.,* $\lfloor 5.2 \rfloor$ *= 5 και* $\lfloor -5.2 \rfloor$ *= -6 (floor).*
- $\lceil x \rceil$ *είναι ο μικρότερος ακέραιος που είναι μεγαλύτερος ή ίσος του x. Π.χ.,* $\lceil 5.2 \rceil$*= 6 και* $\lceil -5.2 \rceil$*= -5 (ceiling).*

7. Κινεζικό θεώρημα υπολοίπων (Chinese Remainder Theorem)

Αν οι ακέραιοι $n_1,n_2,\ldots,n_k$ είναι ανά δύο πρώτοι προς αλλήλους, τότε το σύστημα των ισοτιμιών

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

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

Αλγόριθμος Gauss *Η λύση x των ταυτόχρονων ισοδυναμιών στο κινεζικό θεώρημα των υπολοίπων μπορεί να υπολογιστεί ως* $x = \sum_{i=1}^{k} a_i N_i M_i \bmod n$*, όπου* $N_i = n/n_i$ *και* $M_i = N_i^{-1} \bmod n_i$*.*

8. Σύνολο τετραγωνικών υπολοίπων modulo n

Το $\alpha \in \mathbb{Z}_n^*$[2] *λέγεται τετραγωνικό υπόλοιπο (quadratic residue - QR) modulo n, αν υπάρχει* $x \in \mathbb{Z}_n^*$ *τέτοιο ώστε να ισχύει* $x^2 \equiv a \pmod{n}$*. Αν δεν υπάρχει τέτοιο x, τότε το α λέγεται τετραγωνικό μη υπόλοιπο (quadratic non - residue - QNR) modulo n. Το σύνολο όλων των QR modulo n συμβολίζεται με* Q_n *και το σύνολο όλων των QNR με* $\overline{Qn}$*.*

Σημειώνουμε ότι από τον ορισμό $0 \notin \mathbb{Z}_n^*$ *από όπου προκύπτει ότι* $0 \notin Q_n$ *και* $0 \notin \overline{Qn}$*.*

[2] *Η* πολλαπλασιαστική ομάδα του $\mathbb{Z}_n$ είναι $\mathbb{Z}_n^*$, = $\{\alpha \in \mathbb{Z}_n \mid (a,n) = 1\}$. Συγκεκριμένα, αν ο n είναι πρώτος, τότε $\mathbb{Z}_n^* = \{\alpha \mid 1 \leq \alpha \leq n-1\}$.

9. Σύμβολο Jacobi

Ορισμός *Έστω $n \geq 3$ περιττός με ανάλυση σε πρώτους παράγοντες $n = p^{e1}_1 p^{e2}_2 \dots p^{ek}_k$. Τότε το σύμβολο Jacobi ορίζεται να είναι*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}$$

Για n πρώτο, το σύμβολο Jacobi συμπίπτει με το σύμβολο Legendre. Για. τις ιδιότητες του συμβόλου Jacobi βλ. [M0v96], κεφ.2.

10. Υπολογισμός συμβόλου Jacobi

Αλγόριθμος *Υπολογισμός συμβόλου Jacobi (και συμβόλου Legendre)*

JACOBI(a, n)

ΕΙΣΟΔΟΣ: ένας περιττός ακέραιος $n \geq 3$ και ένας ακέραιος α, $0 \leq a < n$.

ΕΞΟΔΟΣ: το σύμβολο Jacobi $\left(\frac{a}{n}\right)$ (και το σύμβολο Legendre όταν ο n είναι πρώτος).

1. *Αν α = 0 τότε επέστρεψε (0).*
2. *Αν α = 1 τότε επέστρεψε (1).*
3. *Γράψε $\alpha = 2^e a_1$, όπου a_1 περιττός.*
4. *Αν e άρτιος τότε θέσε $s \leftarrow 1$.Διαφορετικά θέσε $s \leftarrow 1$ αν $n \equiv 1$ ή $7 \pmod 8$, ή θέσε $s \leftarrow -1$ αν $n \equiv 3$ ή $5 \pmod 8$.*
5. *Αν $n \equiv 3 \pmod 4$ και $a_1 \equiv 3 \pmod 4$ τότε θέσε $s \leftarrow -s$.*
6. *Θέσε $n_1 \leftarrow n \bmod a_1$.*
7. *Αν $a_1 = 1$ τότε επέστρεψε (s) διαφορετικά επέστρεψε ($s \cdot$ JACOBI (n_1, a_1)).*

11. Υπολογισμός πολλαπλασιαστικών αντίστροφων στο $\mathbb{Z}_n$

ΕΙΣΟΔΟΣ: $a \in \mathbb{Z}_n$.

ΕΞΟΔΟΣ: $a^{-1} \bmod n$, εφόσον υπάρχει.

1. *Χρησιμοποίησε τον επεκτεταμένο Ευκλείδιο αλγόριθμο (βλ. πιο πάνω) για την εύρεση ακεραίων x και y τέτοιων ώστε $ax + ny = d$, όπου $d = (a, n)$.*
2. *Αν $d > 1$, τότε το $\alpha^{-1} \bmod n$ δεν υπάρχει. Διαφορετικά, επέστρεψε (x).*

12. Αλγόριθμος επαναλαμβανόμενου τετραγωνισμού και πολλαπλασιασμού (square-and-multiply) για εκθετοποίηση στο $\mathbb{Z}_n$

ΕΙΣΟΔΟΣ: a ∈ $\mathbb{Z}_n$ και ο ακέραιος k, 0 ≤ k < n με δυαδική αναπαράσταση k = $\sum_{i=0}^{t} k_i 2^i$.

ΕΞΟΔΟΣ: a^k mod n.

1. *Θέσε b ← 1. Αν k = 0 τότε επέστρεψε (b).*
2. *θέσε A ← α.*
3. *Αν k_0 = 1 τότε θέσε b ← a.*
4. *Για i από 1 έως t κάνε τα ακόλουθα:*
   - *4.1 Θέσε A ← A^2 mod n.*
   - *4.2 Αν k_i = 1 τότε θέσε b ← A · b mod n.*
5. *Επέστρεψε (b).*

13. Στοιχεία από τη Θεωρία Ομάδων

Ορισμός *(Διμελής πράξη) Μια διμελής πράξη * σε ένα σύνολο S είναι ένας κανόνας, με τον οποίο σε κάθε διατεταγμένο ζεύγος (α, b) στοιχείων του S αντιστοιχίζεται κάποιο στοιχείο του S.*

Με μια διμελή πράξη στο S, πρέπει να αντιστοιχίζεται σε κάθε διατεταγμένο ζεύγος (α, b) ένα στοιχείο που ανήκει και αυτό στο S. Η απαίτηση το στοιχείο αυτό να ανήκει πάλι στο S είναι γνωστή ως συνθήκη κλειστότητας. Απαιτούμε το S να είναι κλειστό ως προς μια διμελή πράξη στο S.

Ορισμός *(Ομάδα) Ομάδα < G, * > είναι ένα σύνολο G, μαζί με μια διμελή πράξη * στο G τέτοια, ώστε να ικανοποιούνται τα ακόλουθα αξιώματα:*

1. *Η διμελής πράξη * είναι προσεταιριστική.*
2. *Υπάρχει ένα στοιχείο e στο G τέτοιο, ώστε e*x = x*e = x για κάθε x ∈ G.(Αυτό το στοιχείο e λέγεται ταυτοτικό στοιχείο για την * στο G.)*
3. *Για κάθε α στο G, υπάρχει ένα στοιχείο α' στο G με την ιδιότητα α'*α = α*α' = e. (Το στοιχείο α' λέγεται αντίστροφο του α ως προς την πράξη *.)*

Το ταυτοτικό στοιχείο και τα αντίστροφα ορίζονται μονοσήμαντα σε μία ομάδα.

Ορισμός *(Αβελιανή ομάδα) Μια ομάδα G λέγεται αβελιανή αν η διμελής πράξη της είναι αντιμεταθετική. Δηλαδή, για κάθε ζεύγος (α,b) στοιχείων της ισχύει a*b = b*a.*

Ορισμός *(Δακτύλιος) Ένας δακτύλιος < R, +,· > είναι ένα σύνολο R εφοδιασμένο με δύο διμελείς πράξεις + και ·, τις οποίες αποκαλούμε πρόσθεση και πολλαπλασιασμό, ορισμένες στο R έτσι ώστε να ικανοποιούνται τα ακόλουθα αξιώματα:*

1. *< R,+ > είναι μια αβελιανή ομάδα.*
2. *Ο πολλαπλασιασμός είναι προσεταιριστικός.*
3. *Για κάθε a,b,c ∈ R ισχύει ο αριστερός επιμεριστικός νόμος, a · (b + c) = (α·b) + (α · c) και ο δεξιός επιμεριστικός νόμος, (α + b) · c = (α · c) + (b · c).*

Ορισμός *(Τάξη της G) Αν G είναι μια πεπερασμένη ομάδα, τότε η τάξη |G| της G είναι το πλήθος των στοιχείων της G. Γενικά, για κάθε πεπερασμένο σύνολο S, |S| είναι το πλήθος των στοιχείων του S.*

Ορισμός *(Επαγόμενη πράξη) Έστω G μια ομάδα και S ένα υποσύνολο της G. Αν για κάθε a,b ∈ S ισχύει ότι το γινόμενο α · b υπολογισμένο στην G ανήκει και στο S, τότε λέμε ότι το 5 είναι κλειστό ως προς την πράξη ομάδας της G. Η διμελής πράξη, που ορίζεται με αυτόν τον τρόπο στο S, λέγεται η επαγόμενη πράξη στο S από την G.*

Ορισμός *(Υποομάδα) Αν ένα υποσύνολο H μιας ομάδας G είναι κλειστό ως προς τη διμελή πράξη της G και αν το H είναι και αυτό ομάδα, τότε το H λέγεται υποομάδα της G. Θα γράφουμε $H \leq G$ ή $G \geq H$ για να συμβολίζουμε το ότι η H είναι υποομάδα της G και γράφοντας $H < G$ ή $G > H$ θα εννοούμε ότι $H \leq G$ αλλά $H \neq G$.*

Κυκλικές υποομάδες

Θεώρημα *Ένα υποσύνολο H μιας ομάδας G είναι υποομάδα της G αν και μόνον αν ισχύουν τα ακόλουθα:*

1. *Το H είναι κλειστό ως προς τη διμελή πράξη της G.*
2. *Το ταυτοτικό στοιχείο e της G ανήκει στο H.*
3. *Για κάθε α ∈ H ισχύει $α^{-1} ∈ H$.*

Μια υποομάδα της G που περιέχει το α πρέπει να περιέχει όλα τα στοιχεία της μορφής $α^n$ (ή $n · α$ για προσθετικές ομάδες), $\forall n \in \mathbb{Z}$.

Ορισμός *(Γνήσιες και μη τετριμμένες υποομάδες) Αν G είναι μια ομάδα, τότε η υποομάδα που αποτελείται από την ίδια την G λέγεται η μη γνήσια υποομάδα της G. Όλες οι άλλες υποομάδες λέγονται γνήσιες υποομάδες. Η υποομάδα {e} είναι η τετριμμένη υποομάδα της G. Όλες οι άλλες υποομάδες λέγονται μη τετριμμένες.*

Θεώρημα *Έστω G μια ομάδα και έστω α ∈ G. Τότε το σύνολο H = {a^n | n ∈ ℤ} είναι μια υποομάδα της G και μάλιστα είναι η μικρότερη υποομάδα της G που περιέχει το α, δηλαδή, κάθε υποομάδα που περιέχει το α περιέχει και την H.*

Ορισμός *(Κυκλική υποομάδα < α >) Η ομάδα H του προηγούμενου θεωρήματος λέγεται η κυκλική υποομάδα της G που παράγεται από το α και συμβολίζεται με < α >.*

Ορισμός *(Γεννήτορας, κυκλική ομάδα) Ένα στοιχείο α μιας ομάδας G παράγει την G και λέγεται γεννήτορας της G αν < α >= G. Μια ομάδα G λέγεται κυκλική αν υπάρχει κάποιο στοιχείο α στην G που παράγει την G.*

Αν η κυκλική υποομάδα < α > της G είναι πεπερασμένη, τότε η τάξη του α είναι η τάξη | < α > | αυτής της κυκλικής υποομάδας. Σε αντίθετη περίπτωση, λέμε ότι το α έχει άπειρη τάξη. Αν το α έχει πεπερασμένη τάξη m, τότε m είναι ο μικρότερος θετικός ακέραιος για τον οποίο ισχύει $a^m = e$ (όπου e το ταυτοτικό στοιχείο της G).

Κεφάλαιο 2

Εισαγωγή

2.1 Γενική ιδέα και ορισμός του σχήματος ψηφιακής υπογραφής

Οι ψηφιακές υπογραφές είναι ένας από τους σημαντικότερους κλάδους της εφαρμοσμένης κρυπτογραφίας πλήρης ονομασία τους είναι ***Σχήματα Ψηφιακής Υπογραφής*** *(Digital Signature Schemes) η απλούστερα* ***Σχήματα Υπογραφής*** *ή* ***Ψηφιακές Υπογραφές.***

Οι ψηφιακές υπογραφές έχουν πολλές εφαρμογές στην ασφάλεια πληροφοριών, συμπεριλαμβάνοντας την πιστοποίηση, δηλαδή την εξακρίβωση της προέλευσης ενός μηνύματος (authentication),την ακεραιότητα των δεδομένων, δηλαδή τη μη τροποποίηση του μηνύματος κατά τη μετάδοση (data integrity) και τη μη άρνηση μιας υπογραφής (non - repudiation),δηλαδή να αρνηθεί κάποιος ότι υπόγραψε ένα μήνυμα.

Η ιδέα και η χρησιμότητα μιας ψηφιακής υπογραφής αναγνωρίστηκε αρκετά χρόνια πριν οποιαδήποτε πρακτική εφαρμογή. Η πρώτη μέθοδος που ανακαλύφθηκε ήταν το σχήμα υπογραφής RSA, το οποίο παραμένει μία από τις πιο πρακτικές και πολύπλευρες διαθέσιμες τεχνικές. Μεταγενέστερες έρευνες είχαν ως αποτέλεσμα πολλές εναλλακτικές τεχνικές ψηφιακών υπογραφών. Μερικές έχουν σημαντικά πλεονεκτήματα όσον αφορά τη λειτουργικότητα και εφαρμογή τους.

Ο σκοπός μιας ψηφιακής υπογραφής είναι η παροχή ενός μέσου σε μια οντότητα να δεσμεύσει την ταυτότητα της με ένα ποσό πληροφορίας. Μία χειρόγραφη υπογραφή, όταν βρεθεί σε ένα έγγραφο, δηλώνει το πρόσωπο που είναι υπεύθυνο γι' αυτό. Υπάρχει μία μονοσήμαντη αντιστοιχία μεταξύ ατόμων και υπογραφών, έτσι ώστε αν προκύψει κάποιο νομικό θέμα να μπορεί εύκολα να διαπιστωθεί (με τη βοήθεια γραφολόγου) αν πράγματι μια οντότητα υπόγραψε ένα έγγραφο.

Μπορούμε λοιπόν να πούμε ότι η ψηφιακή υπογραφή αποτελεί το ψηφιακό «ταίρι» της χειρόγραφης και χρησιμοποιείται για την υπογραφή δεδομένων αποθηκευμένων σε ψηφιακή μορφή. Η απαίτηση για τη δημιουργία μίας τέτοιας υπογραφής έρχεται ως λογική συνέπεια της τεράστιας ποσότητας πληροφορίας που διακινείται πλέον μέσω του διαδικτύου. Οι ψηφιακές υπογραφές χρησιμοποιούνται επίσης σε ηλεκτρονικές συναλλαγές, στην επικοινωνία μέσω ηλεκτρονικού

ταχυδρομείου, σε ηλεκτρονικές δημοπρασίες και γενικά σε δραστηριότητες κατά τις οποίες χρειάζεται επιβεβαίωση της ταυτότητας της μίας πλευράς στην άλλη. Επίσης συχνά είναι απαραίτητο να κατοχυρωθεί η ευρεσιτεχνία (copyright) δεδομένων αποθηκευμένων σε ψηφιακή μορφή. Τέλος οι ψηφιακές υπογραφές παίζουν σημαντικό ρόλο στην ασφάλεια υπολογιστικών συστημάτων.

Πριν εμβαθύνουμε ας εξετάσουμε μερικές βασικές διαφορές μεταξύ των χειρόγραφων και των ψηφιακών υπογραφών.

Μία χειρόγραφη υπογραφή αποτελεί φυσικό κομμάτι του εγγράφου που υπογράφεται, δηλαδή επισυνάπτεται με φυσικό τρόπο στο έγγραφο έτσι ώστε κάθε γνήσιο αντίγραφο του την περιέχει. Αντιθέτως μια ψηφιακή υπογραφή δεν επισυνάπτεται φυσικά στο μήνυμα και έτσι μπορεί να αφαιρεθεί. Για να αντιμετωπιστεί αυτό το πρόβλημα πρέπει ο αλγόριθμος υπογραφής να δεσμεύει με κάποιο τρόπο το μήνυμα με την υπογραφή. Αυτό μπορεί να γίνει με την κρυπτογράφηση του υπογεγραμμένου μηνύματος. Παρακάτω θα δούμε περισσότερα για το πρόβλημα αυτό.

Η δεύτερη διαφορά αφορά την επαλήθευση. Μία χειρόγραφη υπογραφή επαληθεύεται συγκρίνοντας την με άλλες αυθεντικές υπογραφές. Βεβαίως η μέθοδος αυτή δεν είναι ιδιαίτερα ασφαλής καθώς είναι σχετικά εύκολη η πλαστογράφηση κάποιας υπογραφής. Από την άλλη πλευρά, οι ψηφιακές υπογραφές μπορούν να επαληθευθούν χρησιμοποιώντας έναν δημοσίως γνωστό αλγόριθμο επαλήθευσης. Δηλαδή ο οποιοσδήποτε μπορεί να επαληθεύσει μια ψηφιακή υπογραφή. Η χρήση ασφαλών σχημάτων υπογραφής προλαμβάνει την πιθανότητα πλαστογράφησης.

Τρίτη κατά σειρά διαφορά είναι ότι ένα αντίγραφο ενός ψηφιακά υπογεγραμμένου μηνύματος είναι πανομοιότυπο με το αρχικό, ενώ ένα αντίγραφο ενός χειρόγραφα υπογεγραμμένου εγγράφου διαφέρει συνήθως από το αρχικό. Αυτό σημαίνει ότι χρειάζεται προσοχή ώστε να εμποδίζεται η επαναχρησιμοποίηση ενός ψηφιακά υπογεγραμμένου μηνύματος. Π.χ. αν ο Α υπογράψει ένα ψηφιακό μήνυμα εξουσιοδοτώντας τον Β να αποσύρει € 100 από τον τραπεζικό του λογαριασμό (δηλαδή μια ηλεκτρονική επιταγή), το μόνο που θέλει ο Α είναι ο Β να το κάνει μία φορά. Άρα το ίδιο το μήνυμα πρέπει να περιέχει πληροφορίες, όπως ημερομηνία και ώρα, έτσι ώστε να αποφεύγεται η επαναχρησιμοποίηση του.

Ένα σχήμα ψηφιακής υπογραφής αποτελείται από δύο συστατικά μέρη: έναν ***αλγόριθμο υπογραφής (signing algorithm)*** *και έναν* ***αλγόριθμο επαλήθευσης (verification algorithm).***

Ο Α (υπογράφων) μπορεί να υπογράψει ένα μήνυμα m χρησιμοποιώντας έναν κρυφό αλγόριθμο υπογραφής S. Η προκύπτουσα υπογραφή S(m) μπορεί μελλοντικά να επαληθευθεί με τη χρήση ενός δημόσιου αλγόριθμου επαλήθευσης V. Δοθέντος ενός ζεύγους (m, s)[3] *ο αλγόριθμος επαλήθευσης επιστρέφει μια απάντηση, «αληθής» ή «ψευδής», αναλόγως με το αν η υπογραφή είναι αυθεντική ή όχι. Η διαδικασία της υπογραφής συνεπάγεται το μετασχηματισμό του μηνύματος και κάποιας πληροφορίας που διατηρείται κρυφή από μία οντότητα σε μία ετικέτα που λέγεται υπογραφή.*

Ορίζουμε τώρα πιο αυστηρά το σχήμα ψηφιακής υπογραφής.

Ορισμός 2.1 (Σχήμα Ψηφιακής Υπογραφής)

Ένα ***σχήμα ψηφιακής υπογραφής*** *είναι μία τριάδα (M,S,K), όπου ικανοποιούνται οι ακόλουθες συνθήκες:*

1. *M. είναι το πεπερασμένο σύνολο όλων των πιθανών μηνυμάτων που μπορούν να υπογραφούν.*
2. *S είναι το πεπερασμένο σύνολο όλων των υπογραφών.*
3. *K, είναι το πεπερασμένο σύνολο όλων των πιθανών κλειδιών που μπορούν να χρησιμοποιηθούν για την υπογραφή. Λέγεται* ***χώρος κλειδιών*** *(keyspace).*

∀ $k \in K$, υπάρχει ένας αλγόριθμος υπογραφής S_k και ο αντίστοιχος αλγόριθμος επαλήθευσης V_k. Κάθε S_k: $M \rightarrow S$ και $V_k : M \times S \rightarrow$ {αληθής, ψευδής} είναι συναρτήσεις τέτοιες ώστε να ικανοποιείται η ακόλουθη ισότητα για κάθε μήνυμα $m \in M$ και για κάθε υπογραφή $s \in S$:

$$V_k(m,s) = \begin{cases} \text{αληθής}, & \text{αν } s = S_k(m), \\ \text{ψευδής}, & \text{διαφορετικά.} \end{cases} \qquad (2.1)$$

[3] *s* είναι μία υπογραφή, όχι απαραίτητα η *S(m)*.

Ας περιγράψουμε συνοπτικά τις διαδικασίες υπογραφής και επαλήθευσης.

*1.**Διαδικασία υπογραφής.***

Η οντότητα Α (υπογράφων) δημιουργεί μια υπογραφή για το μήνυμα $m \in M$ ενεργώντας ως εξής:

1.1 Υπολογίζει το $s = S_A(m)$.

1.2 Μεταδίδει το ζεύγος (m,s).Το s λέγεται υπογραφή του μηνύματος m.

2.Διαδικασία επαλήθευσης.

Για να επαληθεύσει ότι μία υπογραφή s σε ένα μήνυμα m δημιουργήθηκε από τον Α, μία οντότητα Β εκτελεί τα ακόλουθα βήματα:

2.1 Αποκτά τη συνάρτηση επαλήθευσης V_A του Α.

2.2 Υπολογίζει το $u = V_A(m, s)$.

2.3 Αποδέχεται την υπογραφή αν u = αληθής και την απορρίπτει αν u = ψευδής.

Παρατήρηση 2.1 *Οι μετασχηματισμοί υπογραφής S και επαλήθευσης V χαρακτηρίζονται από ένα κλειδί. Αυτό σημαίνει ότι υπάρχει μια κλάση αλγορίθμων υπογραφής και επαλήθευσης και κάθε αλγόριθμος αναγνωρίζεται από ένα κλειδί. Έτσι ο αλγόριθμος υπογραφής S_A του Α καθορίζεται από ένα κλειδί k_A και ο Α πρέπει μόνο να διατηρεί το k_A κρυφό. Παρομοίως ο αλγόριθμος επαλήθευσης V_A του Α καθορίζεται από ένα κλειδί l_A το οποίο γίνεται δημοσίως γνωστό.*

Οι συναρτήσεις V_k και S_k πρέπει να είναι πολυωνυμικού χρόνου συναρτήσεις (polynomial - time functions) (βλ. παράρτημα). Η V_k πρέπει να είναι δημόσια και η S_k κρυφή, γνωστή μόνο στον υπογράφοντα. Πρέπει να είναι υπολογιστικά ανέφικτο για τον Ο να πλαστογραφήσει την υπογραφή του Α σε ένα μήνυμα m. Αυτό σημαίνει ότι δοθέντος του m μόνο ο Α πρέπει να μπορεί να υπολογίσει την υπογραφή s ώστε $V_A(m, s)$ = αληθής. Ένα σχήμα υπογραφής δεν είναι ποτέ απολύτως ασφαλές, αφού ο Ο μπορεί να ελέγξει όλες τις πιθανές υπογραφές s για ένα μήνυμα m χρησιμοποιώντας το δημόσιο αλγόριθμο επαλήθευσης V_A, μέχρι να βρει την σωστή υπογραφή. Δοθέντος λοιπόν επαρκούς χρόνου ο Ο μπορεί πάντα να πλαστογραφεί την υπογραφή του Α. Συνεπώς, όπως και με τα κρυπτοσυστήματα δημοσίου κλειδιού, στόχος μας είναι η εύρεση σχημάτων υπογραφής που είναι υπολογιστικά ασφαλή για όσο χρονικό διάστημα απαιτείται.

Κάθε σχήμα υπογραφής πρέπει να ικανοποιεί κάποιες βασικές ιδιότητες:

1. *Να ισχύει $V_k(m, s)$ = αληθής $\Leftrightarrow S_k(m) = s$, $\forall\ m \in M$ και $s \in S$.*
2. *Να είναι υπολογιστικά «εύκολο» για κάποιον να παράξει την υπογραφή του και για κάποιον άλλο να επαληθεύσει τη γνησιότητα της.*
3. *Να είναι υπολογιστικά ανέφικτο για οποιαδήποτε οντότητα, εκτός της Α, να βρει για οποιοδήποτε $m \in M$, ένα $s \in S$ έτσι ώστε $V_A(m, s)$ = αληθής.*

Ας επιστρέψουμε τώρα στην πρώτη διαφορά μεταξύ χειρόγραφων και ψηφιακών υπογραφών. Αναφέραμε ότι ο αλγόριθμος υπογραφής πρέπει να συνδέει με κάποιο τρόπο το μήνυμα με την υπογραφή και ότι ένας τρόπος είναι η κρυπτογράφηση του υπογεγραμμένου μηνύματος. Εδώ απαιτείται προσοχή γιατί η διαδικασία πρέπει να γίνει με τη σειρά υπογραφή → κρυπτογράφηση, γιατί αλλιώς αν ο Ο καταφέρει να υποκλέψει το υπογεγραμμένο μήνυμα του Α προς τον Β, μπορεί να αφαιρέσει την υπογραφή του Α και προσθέτοντας τη δική του να τον υποδυθεί.

Πιο συγκεκριμένα στην κρυπτογράφηση δημοσίου κλειδιού έχουμε τα ακόλουθα: Έστω ότι ο Α επιθυμεί να στείλει ένα υπογεγραμμένο, κρυπτογραφημένο μήνυμα στον Β. Δοθέντος ενός μηνύματος m ο Α υπολογίζει την υπογραφή του, $s = S_A(m)$ και έπειτα κρυπτογραφεί τα m και s χρησιμοποιώντας τον δημόσιο αλγόριθμο κρυπτογράφησης του Β, E_B. Άρα ο Α παίρνει το κρυπτοκείμενο $z = E_B(m, s)$.Το κρυπτοκείμενο z μεταδίδεται στον Β. Όταν ο Β λάβει το z πρώτα το αποκρυπτογραφεί με τον κρυφό του αλγόριθμο αποκρυπτογράφησης D_B και παίρνει το ζεύγος (m, s). Κατόπιν χρησιμοποιεί το δημόσιο αλγόριθμο επαλήθευσης του Α, V_A, για να ελέγξει αν $V_A(m, s)$ = αληθής.

Τι γίνεται όμως αν ο Α πρώτα κρυπτογραφήσει το m και στη συνέχεια υπογράψει το κρυπτοκείμενο z; Στην περίπτωση αυτή ο Α υπολογίζει την υπογραφή του, s, ως εξής: $s = S_A(E_B(m)) = S_A(z)$.0 Α μεταδίδει το ζεύγος (z, s) στον Β. Ο Β αποκρυπτογραφεί το z αποκτώντας το m και επαληθεύει την υπογραφή s με τον αλγόριθμο V_A. Ένα πιθανό πρόβλημα με αυτή την προσέγγιση είναι ότι αν ο Ο αποκτήσει το ζεύγος (z, s) μπορεί να αντικαταστήσει την υπογραφή του Α, s, με τη δική του, $s' = S_O(E_B(m))$[4] .

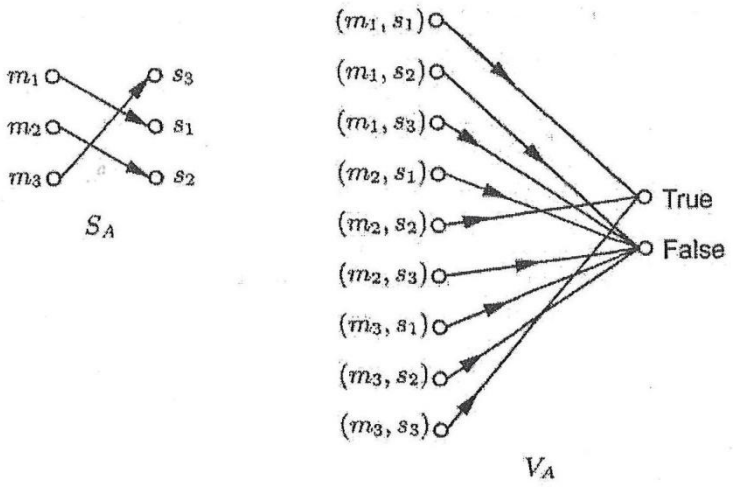
[4] Ο Ο μπορεί να υπογράψει το κρυπτοκείμενο $E_B(m)$ παρά το γεγονός ότι δεν γνωρίζει το μήνυμα m.

Αν λοιπόν ο Ο αντικαταστήσει την υπογραφή του Α με τη δική του τότε μεταδίδει το ζεύγος (z, s') στον Β.Η υπογραφή του Ο θα επαληθευθεί από τον Β με το δημόσιο αλγόριθμο επαλήθευσης του Ο, V_O και ο Β ίσως συμπεράνει ότι το αρχικό μήνυμα m προήλθε από τον Ο. Γι' αυτόν ακριβώς το λόγο προτείνεται η κρυπτογράφηση του υπογεγραμμένου μηνύματος.

Το ακόλουθο παράδειγμα κάνει πιο κατανοητή την έννοια του σχήματος ψηφιακής υπογραφής.

Παράδειγμα 2.1 (Σχήμα Ψηφιακής Υπογραφής)

Έστω $M = \{m_1,m_2,m_3\}$ και $S = \{ s_1,s_2,s_3\}$. Το αριστερό τμήμα του σχήματος 2.1 αναπαριστά μία συνάρτηση υπογραφής S_A από το M στο S, ενώ το δεξιό την αντίστοιχη συνάρτηση επαλήθευσης V_A από το M x S στο σύνολο {αληθής, ψευδής}[5]



Σχήμα 2.1 *Οι συναρτήσεις υπογραφής και επαλήθευσης ενός σχήματος ψηφιακής υπογραφής.*

Όπως είδαμε προηγουμένως πρέπει να είναι υπολογιστικά ανέφικτο για κάποιον, εκτός του Α, να βρει για κάποιο $m \in M$ ένα $s \in S$ έτσι ώστε $V_A(m,s)$ = αληθής. Κανείς μέχρι σήμερα δεν έχει αποδείξει τυπικά (μαθηματικά) ότι υπάρχουν σχήματα υπογραφής που ικανοποιούν αυτή την ιδιότητα. Υπάρχουν όμως μερικοί

[5] Ο δείκτης Α αναφέρεται στην οντότητα Α.

καλοί υποψήφιοι που προκύπτουν από τεχνικές κρυπτογράφησης δημοσίου κλειδιού.

2.2 Βασικοί ορισμοί

Παραθέτουμε κάποιους σημαντικούς για τη συνέχεια ορισμούς.

1. ***Μία ψηφιακή υπογραφή** είναι μία ακολουθία δεδομένων (data string) η οποία συνδέει ένα μήνυμα (σε ψηφιακή μορφή) με μία οντότητα προελεύσεως (originating entity).*
2. ***Ένας αλγόριθμος παραγωγής μιας ψηφιακής υπογραφής** (digital signature generation algorithm) είναι μία μέθοδος για να παραχθεί μία ψηφιακή υπογραφή.*
3. ***Ένας αλγόριθμος επαλήθευσης μιας ψηφιακής υπογραφής** (digital signature verification algorithm) είναι μία μέθοδος για να επαληθευθεί αν μία ψηφιακή υπογραφή είναι αυθεντική.*
4. ***Ένα σχήμα (ή μηχανισμός) ψηφιακής υπογραφής** (digital signature scheme (or mechanism)) αποτελείται από έναν αλγόριθμο παραγωγής της υπογραφής και τον αντίστοιχο αλγόριθμο επαλήθευσης.*
5. ***Μία διαδικασία υπογραφής** (digital signature signing process) αποτελείται από έναν (μαθηματικό) αλγόριθμο παραγωγής μίας ψηφιακής υπογραφής μαζί με μία μέθοδο διαμόρφωσης των δεδομένων σε μηνύματα που μπορούν να υπογραφούν.*
6. ***Μία διαδικασία επαλήθευσης** (digital signature verification process) αποτελείται από έναν αλγόριθμο επαλήθευσης μαζί με μία μέθοδο ανάκτησης των δεδομένων από το μήνυμα.*

Για να χρησιμοποιηθεί ένα σχήμα ψηφιακής υπογραφής στην πράξη είναι απαραίτητο να έχουμε μια διαδικασία ψηφιακής υπογραφής. Δύο τέτοιες διαδικασίες είναι γνωστές με τα ονόματα ISO/IEC 9796 και PKCS #1 (βλ.[MOV96], κεφ. 11). Παραθέτουμε τώρα τη σημειογραφία που θα χρησιμοποιήσουμε. Τα σύνολα και οι συναρτήσεις που παρατίθενται είναι όλα δημοσίως γνωστά.

- *M: Ένα σύνολο στοιχείων που λέγεται **χώρος των μηνυμάτων** (message space).*
- *M_s: Ένα σύνολο στοιχείων που λέγεται **χώρος υπογραφής** (signing space).*

- *S: Ένα σύνολο στοιχείων που λέγεται **χώρος των υπογραφών** (signature space).*
- *R: Μία 1-1 συνάρτηση από το M στο M_s που λέγεται **συνάρτηση πλεονάζουσας πληροφορίας** (redundancy function).*
- *M_R: Η εικόνα της R (δηλ., $M_R = Im(R)$).*
- *R^{-1}: Η αντίστροφη της R (δηλ., $R^{-1} : M_R \rightarrow M$).*
- *R: Ένα σύνολο στοιχείων που λέγεται το **σύνολο τοποθέτησης δεικτών για την υπογραφή** (indexing set for signing).*
- *h: Μία συνάρτηση μονής κατεύθυνσης με πεδίο ορισμού το M.*
- *M_h: Η εικόνα της h (δηλ., $h : M \rightarrow M_h$). Το $M_h \subseteq M_s$ λέγεται **χώρος των τιμών κατακερματισμού** (hash value space).*

***Σημείωση 2.1** (σχόλια επί της σημειογραφίας):*

1. *(χώρος μηνυμάτων) M είναι το σύνολο των στοιχείων στα οποία ο υπογράφων μπορεί να επισυνάψει μία ψηφιακή υπογραφή.*
2. *(χώρος υπογραφής) M_s είναι το σύνολο των στοιχείων στα οποία εφαρμόζονται οι μετασχηματισμοί υπογραφής. Οι μετασχηματισμοί υπογραφής δεν εφαρμόζονται άμεσα στο σύνολο M.*
3. *(χώρος υπογραφών) S είναι το σύνολο των στοιχείων που σχετίζονται με τα στοιχεία του χώρου μηνυμάτων M. Τα στοιχεία αυτά χρησιμοποιούνται για τη δέσμευση του υπογράφοντος με το μήνυμα.*
4. *(σύνολο τοποθέτησης δεικτών) Το σύνολο R χρησιμοποιείται για την αναγνώριση συγκεκριμένων μετασχηματισμών υπογραφής.*

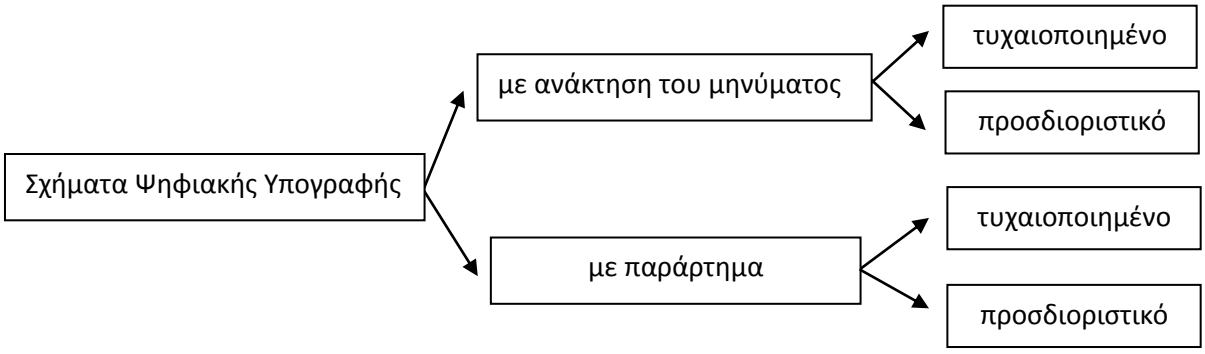
Τα σχήματα ψηφιακής υπογραφής μπορούν να διακριθούν σε δύο μεγάλες κατηγορίες:

1. ***Σχήματα ψηφιακής υπογραφής με παράρτημα** (Digital Signature Schemes with Appendix).Τα σχήματα αυτής της κατηγορίας απαιτούν το αρχικό μήνυμα ως είσοδο (όρισμα) στον αλγόριθμο επαλήθευσης.*
2. ***Σχήματα ψηφιακής υπογραφής με ανάκτηση του μηνύματος** (Digital Signature Schemes with Message Recovery). Εδώ δεν απαιτείται ως είσοδος στον αλγόριθμο επαλήθευσης το αρχικό μήνυμα. Εδώ το αρχικό μήνυμα μπορεί να ανακτηθεί από την ίδια την υπογραφή.*

Οι παραπάνω κατηγορίες μπορούν περαιτέρω να υποδιαιρεθούν αναλόγως αν |R|=1 ή όχι[6]*.*

Ορισμός 2.2 *Ένα σχήμα ψηφιακής υπογραφής (είτε με παράρτημα είτε με ανάκτηση του μηνύματος) λέγεται τυχαιοποιημένο (randomized) αν |R| > 1, αλλιώς λέγεται ντετερμινιστικό (ή προσδιοριστικό) (deterministic).*

Με τη σειρά τους τα προσδιοριστικά σχήματα ψηφιακής υπογραφής υποδιαιρούνται σε σχήματα μίας χρήσης (one-time signature schemes) και σε σχήματα πολλαπλής χρήσης (multiple — use signature schemes). Στο σχήμα που ακολουθεί απεικονίζεται η παραπάνω ταξινόμηση.



Σχήμα 2.2 *Μια ταξινόμηση των σχημάτων ψηφιακής υπογραφής.*

Πριν ολοκληρώσουμε την παράγραφο, θεωρούμε σκόπιμο να αναφέρουμε κάποια χρήσιμα στοιχεία για τη συνάρτηση πλεονάζουσας πληροφορίας R ώστε να γίνει κατανοητή η χρήση της.

Η συνάρτηση πλεονάζουσας πληροφορίας είναι μία δημοσίως γνωστή, αντιστρέψιμη συνάρτηση και χρησιμοποιείται για λόγους ασφαλείας. Ένα παράδειγμα μίας τέτοιας συνάρτησης είναι η μετατροπή ενός δυαδικού κειμένου σε τέτοια μορφή ώστε ανάμεσα σε κάθε 8 bit να εμφανίζεται η λέξη 10101. Εφαρμόζοντας ο υπογράφων σε ένα μήνυμα μία τέτοια συνάρτηση καθιστά σχεδόν αδύνατη την πλαστογράφηση της υπογραφής του, εκτός αν κάποιος «αντίπαλος» κατορθώσει να υπολογίσει το ιδιωτικό του κλειδί.

[6] Με |R| συμβολίζεται ο πληθάριθμος του R.

2.3 Κρυπτογραφικές συναρτήσεις κατακερματισμού (Cryptographic Hash Functions)

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού παίζουν θεμελιώδη ρόλο στη σύγχρονη κρυπτογραφία. Συχνά λέγονται (ανεπίσημα) και συναρτήσεις κατακερματισμού μονής κατεύθυνσης (one — way hash functions). Ενώ σχετίζονται με τις συμβατικές συναρτήσεις κατακερματισμού οι οποίες κυρίως χρησιμοποιούνται σε μη κρυπτογραφικές εφαρμογές υπολογιστών (και στις δύο περιπτώσεις μεγάλα πεδία ορισμού απεικονίζονται σε μικρότερα πεδία τιμών) έχουν αρκετές σημαντικές διαφορές. Εμείς θα περιοριστούμε στις κρυπτογραφικές συναρτήσεις κατακερματισμού οι οποίες βρίσκουν εφαρμογές στην ακεραιότητα των δεδομένων και την πιστοποίηση των μηνυμάτων.

Μία συνάρτηση κατακερματισμού δέχεται ως όρισμα ένα μήνυμα και παράγει ένα αποτέλεσμα το οποίο αναφέρεται ως τιμή κατακερματισμού. Συγκεκριμένα μία συνάρτηση κατακερματισμού h απεικονίζει ακολουθίες bit αυθαίρετου πεπερασμένου μήκους σε ακολουθίες σταθερού μήκους ,έστω n bits.Οι συναρτήσεις αυτές είναι της μορφής: $h : D \rightarrow R$, $|D| > |R|$, όπου δεν αποκλείεται $|D|=\infty$, ενώ το R είναι πεπερασμένο σύνολο.

Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται για την ακεραιότητα των δεδομένων από κοινού με σχήματα ψηφιακής υπογραφής, όπου για διάφορους λόγους ένα μήνυμα πρώτα κατακερματίζεται και στη συνέχεια η τιμή κατακερματισμού, ως αντιπρόσωπος του μηνύματος, υπογράφεται στη θέση του.

Σχετικά με την ακεραιότητα των δεδομένων οι συναρτήσεις κατακερματισμού χρησιμοποιούνται ως ακολούθως. Υπολογίζεται η τιμή κατακερματισμού που αντιστοιχεί σε κάποιο συγκεκριμένο όρισμα. Υποθέτουμε ότι η τιμή αυτή προστατεύεται με κάποιο τρόπο. Για να επαληθεύσουμε στο μέλλον ότι τα δεδομένα (όρισμα) δεν μεταβλήθηκαν, υπολογίζουμε ξανά την τιμή κατακερματισμού και συγκρίνουμε τη νέα τιμή με την αρχική.

Ορισμός 2.3 *Μία συνάρτηση κατακερματισμού είναι μία συνάρτηση h η οποία έχει τουλάχιστον τις δύο ακόλουθες ιδιότητες:*

1. ***συμπίεση*** *(compression):η h απεικονίζει ένα όρισμα x αυθαίρετου πεπερασμένου μήκους bit σε μία εικόνα h(x) σταθερού μήκους n bits.*
2. ***ευκολία στον υπολογισμό*** *(ease of computation): δοθείσης της h και ενός*

ορίσματος x, το h(x) υπολογίζεται εύκολα.

Στα παρακάτω υποθέτουμε ότι το Σ είναι ένα αλφάβητο, δηλαδή ένα σύνολο συμβόλων. Με Σ συμβολίζουμε το σύνολο όλων των συμβολοακολουθιών από το αλφάβητο Σ. Π.χ. για το δυαδικό αλφάβητο {0,1} έχουμε : {0,1}* = ϵ,0,1,00,01,10,11,001,..., όπου με ϵ συμβολίζουμε την κενή συμβολοακολουθία.*

Συναρτήσεις κατακερματισμού και συναρτήσεις συμπίεσης

Σχετικά με κρυπτογραφικές εφαρμογές υπολογιστών, όπου Σ = {0,1}, μία συνάρτηση κατακερματισμού ορίζεται μαθηματικά ως εξής: $h : \Sigma^* \rightarrow \Sigma^n$, $n \in \mathbb{N}$ (π.χ n =128 ή 160). Η πιθανότητα μία τυχαία επιλεγμένη ακολουθία να απεικονισθεί σε μία συγκεκριμένη τιμή κατακερματισμού μήκους n — bit είναι $\frac{1}{2^n}$. Οι συναρτήσεις αυτές δεν είναι 1-1 (injective).

Παράδειγμα 2.2

Η απεικόνιση που στέλνει το $b_1b_2\ldots b_k$ του {0,1} στο $(b_1 + b_2 + \cdots + b_k) \bmod 2$ είναι μία συνάρτηση κατακερματισμού. Απεικονίζει για παράδειγμα το 01101 στο 1. Εν γένει, απεικονίζει μια ακολουθία b στο 1 αν το πλήθος των μονάδων της b είναι περιττός αριθμός και στο 0 διαφορετικά.*

Οι συναρτήσεις κατακερματισμού μπορούν να παραχθούν χρησιμοποιώντας συναρτήσεις συμπίεσης. Μία συνάρτηση συμπίεσης είναι μία απεικόνιση $h : \Sigma^m \rightarrow \Sigma^n$, $n, m \in \mathbb{N}$, $m > n$. Απεικονίζει ακολουθίες σταθερού μήκους σε ακολουθίες μικρότερου μήκους.

Παράδειγμα 2.3

Η απεικόνιση που στέλνει τη λέξη $b_1b_2\ldots b_m$ του $\{0,1\}^m$ στο $(b_1+b_2+\ldots+b_k) \bmod 2$ είναι μία συνάρτηση συμπίεσης αν $m > 1$.

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού και συμπίεσης πρέπει να έχουν ιδιότητες οι οποίες εγγυώνται την ασφάλεια τους. Περιγράφουμε τώρα ανεπίσημα αυτές τις ιδιότητες. Έστω $h : \Sigma^* \rightarrow \Sigma^n$ μία συνάρτηση κατακερματισμού ή $h: \Sigma^m \rightarrow \Sigma^n$ μία συνάρτηση συμπίεσης. Συμβολίζουμε το σύνολο των ορισμάτων της h, Σ^* ή Σ^m, με D. Αν η h είναι συνάρτηση κατακερματισμού τότε $D = \Sigma^*$, ενώ αν η h είναι συνάρτηση συμπίεσης τότε $D = \Sigma^m$.

Η συνάρτηση h λέγεται συνάρτηση μονής κατεύθυνσης (one — way function) αν είναι ανέφικτη η αντιστροφή της. Είναι πολύπλοκο να περιγράψουμε τον όρο ανέφικτη με ακριβή μαθηματικό τρόπο. Γι' αυτό το λόγο δίνουμε μια διαισθητική περιγραφή. Κάθε αλγόριθμος με όρισμα ένα $y \in \Sigma^n$ *που προσπαθεί να υπολογίσει ένα x με h(x) = y σχεδόν πάντα αποτυγχάνει. Δεν είναι γνωστό αν υπάρχουν συναρτήσεις μονής κατεύθυνσης. Υπάρχουν όμως συναρτήσεις που είναι εύκολο να υπολογιστούν αλλά για τις οποίες δεν είναι γνωστοί αποδοτικοί αλγόριθμοι αντιστροφής και έτσι μπορούν να χρησιμοποιηθούν ως συναρτήσεις μονής κατεύθυνσης.*

Παράδειγμα 2.4

Αν p είναι ένας τυχαία επιλεγμένος 1024-bit πρώτος και g είναι ένα πρωταρχικό στοιχείο mod p (βλ. παράρτημα), τότε η συνάρτηση $f : \{0,2, ...,p - 2\} \rightarrow \{1, 2,...,p-1\}$, *με τύπο* $f(x) = g^x \bmod p$, *είναι εύκολο να υπολογιστεί με γρήγορη εκθετοποίηση, αλλά μία αποδοτική αντίστροφη συνάρτηση δεν είναι γνωστή επειδή είναι δύσκολο να υπολογίσουμε διακριτούς λογαρίθμους. Για αυτό το λόγο η f μπορεί να χρησιμοποιηθεί ως συνάρτηση μονής κατεύθυνσης.*

Ορισμός 2.4 *Μια σύγκρουση (collision) της h είναι ένα ζεύγος* $(x_1,x_2) \in D^2$ *για το οποίο ισχύει ότι* $x_1 \neq x_2$ *και* $h(x_1) = h(x_2)$.

Υπάρχουν συγκρούσεις σε όλες τις συναρτήσεις κατακερματισμού και συμπίεσης επειδή δεν είναι 1-1.

Παράδειγμα 2.5

Μία σύγκρουση της συνάρτησης κατακερματισμού του παραδείγματος 2.2 είναι ένα ζεύγος διακεκριμένων δυαδικών ακολουθιών με περιττό πλήθος μονάδων όπως οι (111,001).

Ορισμός 2.5 *Η συνάρτηση h λέγεται* ***ασθενώς ανθεκτική σε συγκρούσεις*** *(weak collision resistant) αν είναι ανέφικτος ο υπολογισμός μίας σύγκρουσης* (x_1,x_2) *για δοθέν* $x_1 \in D$.

Ορισμός 2.6 *Η συνάρτηση h λέγεται* ***(ισχυρώς) ανθεκτική σε συγκρούσεις*** *(strong collision resistant) αν είναι ανέφικτος ο υπολογισμός οποιασδήποτε σύγκρουσης* (x_1,x_2) *της h.*

Οι συναρτήσεις κατακερματισμού αυτού του τύπου είναι απαραίτητες για τα σχήματα ψηφιακής υπογραφής.

Μπορεί να δειχθεί ότι οι ισχυρώς ανθεκτικές συναρτήσεις κατακερματισμού είναι συναρτήσεις μονής κατεύθυνσης. Η ιδέα είναι η εξής: έστω ότι υπάρχει ένας αλγόριθμος αντιστροφής για την h. Επιλέγουμε τυχαία μια ακολουθία x_2. Χρησιμοποιώντας τον αλγόριθμο αντιστροφής υπολογίζουμε μία αντίστροφη εικόνα x_1 του $y(=h(x_2))$. Τότε το ζεύγος (x_1,x_2) είναι μία σύγκρουση της h, εκτός αν $x_1=x_2$.

Ως βασικές ιδιότητες μίας συνάρτησης κατακερματισμού αναφέραμε τη συμπίεση και την ευκολία υπολογισμού. Σε αυτές έρχονται να προστεθούν και κάποιες ακόμα:

- ***Αντίσταση 1ου ορίσματος** (preimage resistance): είναι υπολογιστικά ανέφικτο για δοθέν στοιχείο y του πεδίου τιμών της h να βρεθεί x στο πεδίο ορισμού τέτοιο ώστε $h(x) = y$.*
- ***Αντίσταση 2ου ορίσματος** (2nd — preimage resistance): είναι υπολογιστικά ανέφικτο για δοθέν στοιχείο x_1 στο πεδίο ορισμού της h να βρεθεί ένα άλλο στοιχείο x_2 τέτοιο ώστε $x_1 \neq x_2$ και $h(x_1) = h(x_2)$·*
- ***Αντίσταση συγκρούσεων** (collision resistance): είναι υπολογιστικά ανέφικτο να βρεθούν δύο διακεκριμένα ορίσματα x_1,x_2 τέτοια ώστε $h(x_1) = h(x_2)$.*

***Σημείωση 2.2** Οι όροι αντίσταση 1ου ορίσματος, αντίσταση 2ου ορίσματος και αντίσταση συγκρούσεων ταυτίζονται με τους όρους μονής κατεύθυνσης, ασθενής αντίσταση σε συγκρούσεις και ισχυρή αντίσταση σε συγκρούσεις αντίστοιχα.*

Στους ορισμούς που ακολουθούν ο όρος συνάρτηση κατακερματισμού συνεπάγεται τις ιδιότητες της συμπίεσης και της ευκολίας υπολογισμού.

***Ορισμός 2.7** Μία **συνάρτηση κατακερματισμού μονής κατεύθυνσης** (one-way hash function-OWHF) είναι μία συνάρτηση κατακερματισμού h με τις ακόλουθες επιπλέον ιδιότητες, όπως ορίστηκαν παραπάνω: αντίσταση 1ου και 2ου ορίσματος.*

***Ορισμός 2.8** Μία **συνάρτηση κατακερματισμού ανθεκτική σε συγκρούσεις** (collision resistant hash function-CRHF) είναι μία συνάρτηση κατακερματισμού h με τις ακόλουθες επιπλέον ιδιότητες, όπως ορίστηκαν παραπάνω: αντίσταση 2ου ορίσματος, αντίσταση συγκρούσεων.*

***Σημείωση 2.3** Οι όροι OWHF,CRHF ταυτίζονται με τους όρους ασθενής συνάρτηση κατακερματισμού μονής κατεύθυνσης (weak one-way hash function) και ισχυρή*

συνάρτηση κατακερματισμού μονής κατεύθυνσης (strong one-way hash function) αντίστοιχα.

2.4 Οι δύο βασικές κατηγορίες σχημάτων ψηφιακής υπογραφής

2.4.1 Σχήματα ψηφιακής υπογραφής με παράρτημα

Τα σχήματα ψηφιακής υπογραφής με παράρτημα είναι εκείνα που χρησιμοποιούνται περισσότερο στην πράξη. Βασίζονται περισσότερο σε κρυπτογραφικές συναρτήσεις κατακερματισμού παρά σε προσαρμοσμένες συναρτήσεις πλεονάζουσας πληροφορίας και είναι λιγότερο επιρρεπή σε επιθέσεις υπαρκτής πλαστογραφίας (existential forgery).

Ορισμός 2.9 *Τα σχήματα ψηφιακής υπογραφής για τα οποία απαιτείται το μήνυμα ως είσοδος στον αλγόριθμο επαλήθευσης λέγονται* ***σχήματα ψηφιακής υπογραφής με παράρτημα.***

Τέτοια σχήματα είναι τα DSS, ElGamal και Schnorr.

Αλγόριθμος 2.1

Παραγωγή κλειδιού για σχήματα ψηφιακής υπογραφής με παράρτημα.

Συνοπτικά: Κάθε οντότητα δημιουργεί ένα ιδιωτικό κλειδί για την υπογραφή μηνυμάτων και ένα αντίστοιχο δημόσιο κλειδί που χρησιμοποιείται από άλλες οντότητες για την επαλήθευση των υπογραφών.

1. *Κάθε οντότητα, έστω A, επιλέγει ένα ιδιωτικό κλειδί το οποίο ορίζει ένα σύνολο μετασχηματισμών $S_A = \{S_{A,k} : k \in R\}$. Κάθε $S_{A,k}$ είναι μία 1-1 συνάρτηση από το M_h στο S και λέγεται μετασχηματισμός υπογραφής.*
2. *Το σύνολο S_A καθορίζει μια αντίστοιχη συνάρτηση V_A από το M_h x S στο σύνολο {αληθής, ψευδής} έτσι ώστε*

$$V_A(\tilde{m}, s^*) = \begin{cases} \alpha\lambda\eta\theta\acute{\eta}\varsigma, & \alpha\nu \ SA,k\ (\widetilde{m}) = s* \\ \psi\epsilon\upsilon\delta\acute{\eta}\varsigma, & \delta\iota\alpha\phi\rho\epsilon\tau\iota\kappa\acute{\alpha} \end{cases},$$

για κάθε $\tilde{m} \in M_h$, $s^* \in S$, όπου $\tilde{m} = h(m)$ με $m \in M$. Η V_A λέγεται μετασχηματισμός επαλήθευσης και κατασκευάζεται έτσι ώστε να είναι δυνατόν να υπολογιστεί χωρίς τη γνώση του ιδιωτικού κλειδιού του υπογράφοντος.

3. *Το δημόσιο κλειδί του Α είναι ο μετασχηματισμός V_A, ενώ το ιδιωτικό του κλειδί είναι το σύνολο S_A.*

Αλγόριθμος 2.2

Παραγωγή υπογραφής και επαλήθευση.

Συνοπτικά: Η οντότητα Α παράγει μια υπογραφή $s \in S$ για ένα μήνυμα $m \in M$, η οποία. μπορεί αργότερα να επαληθευθεί από μία οντότητα Β.

1. *Παραγωγή υπογραφής . Ή οντότητα Α ενεργεί ως εξής:*

1.1 Επιλέγει ένα στοιχείο $k \in R$.

1.2 Υπολογίζει το $\tilde{m}=h(m)$ και το $s^* = S_{A,k}(\tilde{m})$.

1.3 Η υπογραφή του Α για το m είναι s. Τα m και s* είναι διαθέσιμα σε οντότητες για επαλήθευση της υπογραφής.*

2. Επαλήθευση . Η οντότητα Β ενεργεί ως ακολούθως:

2.1 Αποκτά το αυθεντικό δημόσιο κλειδί του Α, δηλ. το μετασχηματισμό επαλήθευσης V_A.

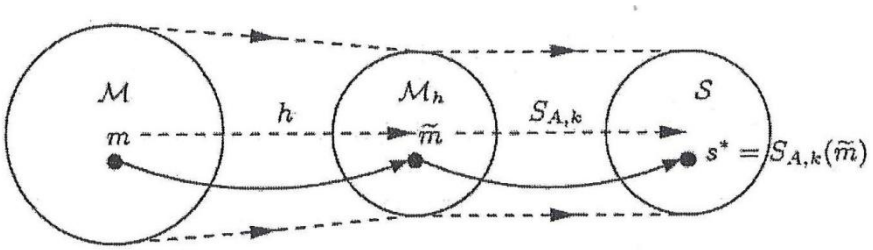
2.2 Υπολογίζει το $\tilde{m} = h(m)$ και το $u = V_A(\tilde{m}, s^*)$.

2.3 Δέχεται την υπογραφή αν και μόνον αν u = αληθής.

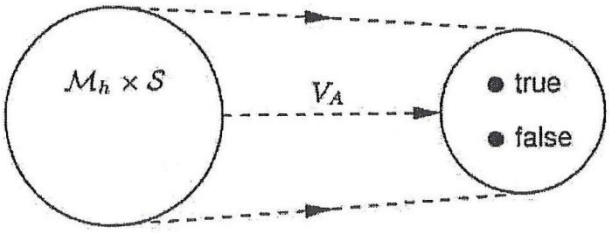
Οι ακόλουθες ιδιότητες είναι απαραίτητες για τους μετασχηματισμούς υπογραφής και επαλήθευσης:

1. *Για κάθε $k \in R$, ο μετασχηματισμός $S_{A,k}$ πρέπει να είναι αποδοτικός ως προς τον υπολογισμό του (δηλ. να είναι εύκολο για κάποιον να παράξει την υπογραφή του).*
2. *Ομοίως και για τον V_A. Δηλ. να μπορεί κάποιος εύκολα να επαληθεύσει τη γνησιότητα μιας υπογραφής.*
3. *Πρέπει να είναι υπολογιστικά ανέφικτο για κάποια οντότητα, εκτός της Α, να βρει ένα μήνυμα $m \in M$ και μία υπογραφή $s^* \in S$ τέτοια, ώστε $V_A(\tilde{m}, s^*)$ = αληθής, όπου $\tilde{m} = h(m)$.*

Το σχήμα που ακολουθεί παρέχει μία αναπαράσταση ενός σχήματος ψηφιακής υπογραφής με παράρτημα.



(i) Η διαδικασία υπογραφής



(ii) Η διαδικασία επαλήθευσης.

Σχήμα 2.3 *Οι διαδικασίες υπογραφής και επαλήθευσης ενός σχήματος ψηφιακής υπογραφής με παράρτημα.*

Σημείωση 2.4 ***(****χρήση των συναρτήσεων κατακερματισμού) Τα περισσότερα σχήματα ψηφιακής υπογραφής με ανάκτηση του μηνύματος εφαρμόζονται σε μηνύματα σταθερού μήκους, ενώ τα σχήματα με παράρτημα εφαρμόζονται σε μηνύματα αυθαίρετου μήκους. Η συνάρτηση μονής κατεύθυνσης h του αλγόριθμου 2.2 επιλέγεται τυπικά να είναι μία συνάρτηση κατακερματισμού χωρίς συγκρούσεις (collision — free hash function).Mia εναλλακτική προσέγγιση αντί του κατακερματισμού είναι το «σπάσιμο» του μηνύματος σε πακέτα (blocks) σταθερού μήκους τα οποία μπορούν να υπογραφούν ξεχωριστά χρησιμοποιώντας ένα σχήμα υπογραφής με ανάκτηση του μηνύματος. Επειδή όμως η παραγωγή υπογραφής για πολλά σχήματα είναι σχετικά αργή και επειδή η αναδιάταξη πολλών*

υπογεγραμμένων πακέτων παρουσιάζει κινδύνους σχετικά με την ασφάλεια, η μέθοδος που προτιμάται είναι ο κατακερματισμός.

2.4.2 Σχήματα ψηφιακής υπογραφής με ανάκτηση του μηνύματος

Τα σχήματα ψηφιακής υπογραφής που περιγράφονται σε αυτή την παράγραφο έχουν το χαρακτηριστικό ότι το υπογεγραμμένο μήνυμα μπορεί να ανακτηθεί από την ίδια την υπογραφή. Στην πράξη το χαρακτηριστικό αυτό χρησιμοποιείται για μικρά μηνύματα.

Ορισμός 2.10 *Ένα* ***σχήμα ψηφιακής υπογραφής με ανάκτηση του μηνύματος*** *είναι ένα σχήμα για το οποίο δεν απαιτείται εκ των προτέρων γνώση του μηνύματος για τον αλγόριθμο επαλήθευσης.*

Παραδείγματα τέτοιων σχημάτων είναι τα RSA,Rabin και Nyberg-Rueppel,που είναι σχήματα δημοσίου κλειδιού.

Αλγόριθμος 2.3

Παραγωγή κλειδιού για σχήματα ψηφιακής υπογραφής με ανάκτηση του μηνύματος.

Συνοπτικά: Κάθε οντότητα δημιουργεί ένα ιδιωτικό κλειδί για την υπογραφή μηνυμάτων και ένα αντίστοιχο δημόσιο κλειδί που χρησιμοποιείται από άλλες οντότητες για την επαλήθευση των υπογραφών.

1. *Κάθε οντότητα A επιλέγει ένα σύνολο μετασχηματισμών υπογραφής, $S_A = \{ S_{A,k} : k \in R\}$. Κάθε $S_{A,k}$ είναι μία 1-1 συνάρτηση από το M_s στο S.*
2. *Το σύνολο S_A καθορίζει μία αντίστοιχη συνάρτηση V_A με την ιδιότητα ότι $V_A \circ S_{A,k}$ είναι η ταυτοτική συνάρτηση στο Ms για κάθε $k \in R$. Ή V_A λέγεται μετασχηματισμός επαλήθευσης και κατασκευάζεται έτσι ώστε να είναι δυνατόν να υπολογιστεί χωρίς τη γνώση του ιδιωτικού κλειδιού του υπογράφοντος.*
3. *Το δημόσιο κλειδί του A είναι ο μετασχηματισμός V_A, ενώ το ιδιωτικό του κλειδί είναι το σύνολο S_A .*

Αλγόριθμος 2.4

Παραγωγή υπογραφής και επαλήθευση.

Συνοπτικά: Η οντότητα Α παράγει μία υπογραφή $s \in S$ για ένα μήνυμα $m \in M$, η οποία μπορεί αργότερα να επαληθευθεί από μία οντότητα Β. Το μήνυμα m ανακτάται από την s.

1. *Παραγωγή υπογραφής. Η οντότητα Α ενεργεί ως εξής:*

   1.1 Επιλέγει ένα στοιχείο $k \in R$.

   1.2 Υπολογίζει το $\tilde{m} = R(m)$ και το $s^* = S_{A,k}(\tilde{m})$ {R είναι μία συνάρτηση πλεονάζουσας πληροφορίας).

   1.3 Η υπογραφή του Α είναι s. Αυτή γίνεται διαθέσιμη σε οντότητες που ίσως επιθυμήσουν να την επαληθεύσουν και να ανακτήσουν το m από αυτήν.*

2. *Επαλήθευση. Η οντότητα Β ενεργεί ως ακολούθως:*

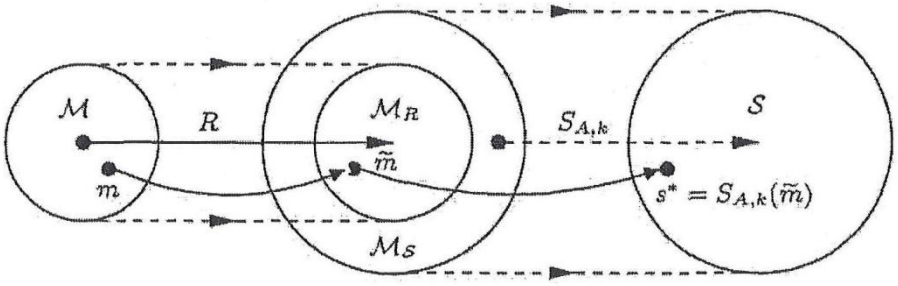
   2.1 Αποκτά το αυθεντικό δημόσιο κλειδί του Α, δηλ. το μετασχηματισμό επαλήθευσης V_A.

   2.2 Υπολογίζει το $\tilde{m} = V_A(s^*)$ (βλ. αλγόριθμο 1.3 (2)).

   2.3 Επαληθεύει ότι $\tilde{m} \in M_R$ (αν το $\tilde{m} \notin M_R$, τότε απορρίπτει την υπογραφή).

   2.4 Ανακτά το m από το $\tilde{m}$ υπολογίζοντας το $R^{-1}(\tilde{m})$.

Στο παρακάτω σχήμα απεικονίζεται ένα σχήμα ψηφιακής υπογραφής με ανάκτηση του μηνύματος.



Σχήμα 2.4 *Αναπαράσταση ενός σχήματος ψηφιακής υπογραφής με ανάκτηση του μηνύματος.*

Για τους μετασχηματισμούς υπογραφής και επαλήθευσης είναι απαραίτητες οι ακόλουθες ιδιότητες:

1. *$\forall k \in R$,ο μετασχηματισμός $S_{A,k}$ πρέπει να είναι εύκολο να υπολογιστεί.*
2. *Ομοίως και για το μετασχηματισμό επαλήθευσης V_A.*
3. *Πρέπει να είναι ανέφικτο για οποιαδήποτε άλλη οντότητα, εκτός της A, να μπορεί να υπολογίσει ένα $s^* \in S$ τέτοιο ώστε το $V_A(s^*)$ να έχει τον απαιτούμενο πλεονασμό, δηλ. $V_A(s^*) \in M_R$.*

Σημείωση 2.5 *(συνάρτηση πλεονάζουσας πληροφορίας) Η συνάρτηση πλεονάζουσας πληροφορίας R και η αντίστροφη της R^{-1} είναι δημοσίως γνωστές .Η επιλογή της κατάλληλης R είναι σημαντική για την ασφάλεια του σχήματος. Για να το καταλάβουμε αυτό ας υποθέσουμε ότι $M_R = Ms$. Έστω ότι οι R και $S_{A,k}$ είναι συναρτήσεις 1-1 και επί από το M στο M_R και από το Ms στο S, αντίστοιχα. Αυτό σημαίνει ότι $|M| = |S|$. Τότε για κάθε $s^* \in S$ συνεπάγεται ότι $V_A(s^*) \in M_R$ και είναι τετριμμένη η εύρεση μηνυμάτων m και αντίστοιχων υπογραφών s^* που θα γίνονται δεκτές από τον αλγόριθμο επαλήθευσης (αλγόριθμος 2.4, βήμα 2) ως εξής:*

1. *Επιλογή τυχαίου $k \in R$ και τυχαίου $s^* \in S$.*
2. *Υπολογισμός του $\tilde{m} = V_A(s^*)$.*
3. *Υπολογισμός του $m = R^{-1}(\tilde{m})$.*

Το στοιχείο s^* είναι μία έγκυρη υπογραφή για το μήνυμα m και δημιουργήθηκε χωρίς τη γνώση του συνόλου των μετασχηματισμών υπογραφής S_A (επίθεση υπαρκτής πλαστογραφίας) (βλ. §2.5).

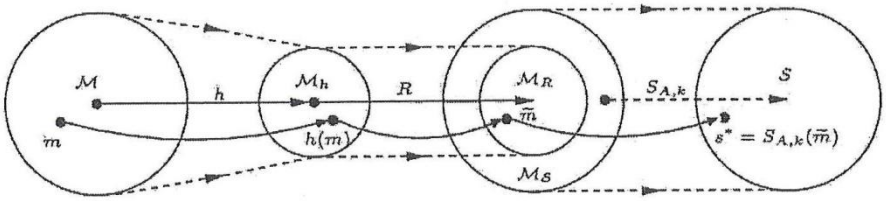
Παράδειγμα 2.6 *(συνάρτηση πλεονάζουσας πληροφορίας)*

Έστω $M = \{m : m \in \{0,1\}^n\}$ για κάποιο σταθερό θετικό ακέραιο n και $Ms = \{t : t \in \{0,1\}^{2n}\}$. Ορίζουμε $R : M \rightarrow Ms$ με τύπο $R(m) = m||m$, όπου το || δηλώνει παράθεση (concatenation)[7] Αυτό σημαίνει ότι $M_R = \{m||m : m \in M\} \subseteq Ms$. Για. μεγάλες τιμές του n, η ποσότητα $|M_R|/|M_s| = (\frac{1}{2})^n$ είναι αμελητέα μικρή. Αυτή η συνάρτηση πλεονάζουσας πληροφορίας είναι κατάλληλη εφόσον καμία συνετή επιλογή μίας υπογραφής s^* εκ μέρους ενός «αντιπάλου» θα έχει μη αμελητέα πιθανότητα ώστε $V_A(s^*) \in M_R$.

[7] Η παράθεση είναι η πράξη της συνένωσης δύο δυαδικών ακολουθιών σε μία νέα. δηλαδή αν x,y είναι δυαδικές ακολουθίες τότε $x||y = x\,y$.

Παρατήρηση 2.2 *(επιλέγοντας μία συνάρτηση πλεονάζουσας πληροφορίας) Παρ' όλο ότι η συνάρτηση πλεονάζουσας πληροφορίας R είναι δημοσίως γνωστή και η* R^{-1} *είναι εύκολο να υπολογιστεί, η επιλογή της R είναι σημαντική και δεν θα πρέπει να γίνεται ανεξάρτητα από την επιλογή των μετασχηματισμών υπογραφής του συνόλου* S_A*.*

Σημείωση 2.6 *(σχήματα με παράρτημα που προκύπτουν από σχήματα που παρέχουν ανάκτηση του μηνύματος) Κάθε σχήμα υπογραφής με ανάκτηση του μηνύματος μπορεί να μετατραπεί σε σχήμα με παράρτημα με απλό κατακερματισμό του μηνύματος και κατόπιν με την υπογραφή της τιμής κατακερματισμού. Το μήνυμα τώρα απαιτείται ως είσοδος στον αλγόριθμο επαλήθευσης. Το σχήμα 2.5 αναπαριστά αυτή την περίπτωση .Η συνάρτηση πλεονάζουσας πληροφορίας R δεν είναι πια σημαντική για την ασφάλεια του σχήματος και μπορεί να είναι οποιαδήποτε 1-1 συνάρτηση από το* M_h *στο* M_s*.*



Σχήμα 2.5 *Σχήμα υπογραφής με παράρτημα που προκύπτει από σχήμα που παρέχει ανάκτηση του μηνύματος.*

Από το σχήμα παρατηρούμε ότι αρχικά στο μήνυμα εφαρμόζεται η συνάρτηση κατακερματισμού h και στη συνέχεια στην τιμή κατακερματισμού h(m) εφαρμόζεται η συνάρτηση πλεονάζουσας πληροφορίας R. Επομένως το m είναι τώρα R(h(m)). Τέλος η υπογραφή s προκύπτει με την εφαρμογή του αλγόριθμου υπογραφής* $S_{A,k}$ *στο* $\tilde{m}$**.**

2.5 Τύποι επιθέσεων σε σχήματα υπογραφής

Σκοπός ενός «αντιπάλου» είναι η πλαστογράφηση υπογραφών, δηλαδή η παραγωγή υπογραφών οι οποίες θα γίνονται δεκτές ως υπογραφές που δημιουργήθηκαν από κάποια άλλη οντότητα. Τα ακόλουθα παρέχουν ένα σύνολο κριτηρίων για το τι σημαίνει «σπάσιμο» ενός σχήματος υπογραφής.

1. ***ολικό «σπάσιμο»*** *(total break): Ένας «αντίπαλος» είτε είναι ικανός να*

υπολογίσει το ιδιωτικό κλειδί του υπογράφοντος, είτε μπορεί να βρει έναν αποδοτικό αλγόριθμο υπογραφής λειτουργικά ισοδύναμο με τον έγκυρο αλγόριθμο υπογραφής.

2. ***επιλεκτική πλαστογραφία*** *(selective forgery): Ένας «αντίπαλος» είναι ικανός να δημιουργήσει μία έγκυρη υπογραφή για ένα συγκεκριμένο μήνυμα ή. μία συγκεκριμένη κλάση μηνυμάτων, επιλεγμένα εκ των προτέρων. Η δημιουργία της υπογραφής δεν εμπλέκει άμεσα το νόμιμο υπογράφοντα.*
3. ***υπαρκτή πλαστογραφία*** *(existential forgery): Ένας «αντίπαλος» είναι ικανός να πλαστογραφήσει μία υπογραφή για τουλάχιστον ένα μήνυμα. Ο «αντίπαλος» έχει λίγο ή καθόλου έλεγχο του μηνύματος, του οποίου την υπογραφή αποκτά και ίσως έτσι ο νόμιμος υπογράφων εμπλακεί στην απάτη.*

Υπάρχουν δύο βασικές επιθέσεις εναντίον σχημάτων υπογραφής δημοσίου κλειδιού.

1. ***επιθέσεις μόνο σε κλειδιά*** *(key — only attacks): Σε αυτές τις επιθέσεις, ένας «αντίπαλος» γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντος.*
2. ***επιθέσεις σε μηνύματα*** *(message attacks): Εδώ ένας «αντίπαλος» είναι σε θέση να εξετάσει υπογραφές αντίστοιχες είτε γνωστών, είτε επιλεγμένων μηνυμάτων.*

   Οι επιθέσεις σε μηνύματα μπορούν περαιτέρω να υποδιαιρεθούν σε τρεις κατηγορίες:

i. ***επίθεση σε γνωστό μήνυμα*** *(known — message attack): Ένας «αντίπαλος» έχει υπογραφές για ένα σύνολο μηνυμάτων τα οποία του είναι γνωστά αλλά δεν έχουν επιλεγεί από αυτόν.*

ii. ***επίθεση σε επιλεγμένο μήνυμα*** *(chosen —message attack): Ένας «αντίπαλος» αποκτά έγκυρες υπογραφές από μία επιλεγμένη λίστα μηνυμάτων πριν αποπειραθεί να «σπάσει» το σχήμα υπογραφής. Η επίθεση αυτή είναι μη - προσαρμόσιμη (non-adaptive) υπό την έννοια ότι τα μηνύματα επιλέγονται πριν ελεγχθεί οποιαδήποτε υπογραφή. Οι επιθέσεις σε επιλεγμένα μηνύματα εναντίον των σχημάτων υπογραφής, είναι ανάλογες με τις επιθέσεις σε επιλεγμένο κρυπτοκείμενο εναντίον σχημάτων κρυπτογράφησης δημοσίου κλειδιού.*

iii. ***προσαρμόσιμη επίθεση σε επιλεγμένο μήνυμα*** *(adaptive chosen — message*

attack): Ένας «αντίπαλος» μπορεί να χρησιμοποιήσει τον υπογράφοντα ως «μαντείο» (oracle). Ο «αντίπαλος» ίσως ζητήσει υπογραφές μηνυμάτων οι οποίες εξαρτώνται από το δημόσιο κλειδί του υπογράφοντος και ίσως ζητήσει υπογραφές μηνυμάτων οι οποίες εξαρτώνται από προηγουμένως αποκτηθείσες υπογραφές ή μηνύματα.

Σημείωση 2.7 *(προσαρμόσιμη επίθεση σε επιλεγμένο μήνυμα) Κατ' αρχήν, μία προσαρμόσιμη επίθεση σε επιλεγμένο μήνυμα είναι ο πιο δύσκολος τύπος επίθεσης ως προς την πρόληψη του. Είναι κατανοητό ότι δοθέντων αρκετών μηνυμάτων και αντίστοιχων υπογραφών, ένας «αντίπαλος» θα μπορούσε να συμπεράνει έναν τρόπο ώστε στη συνέχεια να πλαστογραφήσει μία υπογραφή της επιλογής του. Ενώ μια προσαρμόσιμη επίθεση σε επιλεγμένο μήνυμα ίσως να είναι πρακτικά ανέφικτη, ωστόσο ένα καλώς σχεδιασμένο σχήμα ψηφιακής υπογραφής πρέπει να προλαμβάνει αυτή την πιθανότητα.*

Σημείωση 2.8 *(ζητήματα ασφαλείας) Το επίπεδο ασφάλειας που απαιτείται σε ένα σχήμα ψηφιακής υπογραφής μπορεί να ποικίλλει αναλόγως με την εφαρμογή για την οποία προορίζεται. Για παράδειγμα, σε περιπτώσεις όπου ένας «αντίπαλος» είναι μόνο ικανός να εξαπολύσει μία επίθεση μόνο κλειδιού, ίσως να επαρκεί ο σχεδιασμός του σχήματος ώστε ο «αντίπαλος» να αποτυγχάνει στην απόπειρα επιλεκτικής πλαστογραφίας. Σε περιπτώσεις όπου ο «αντίπαλος» είναι ικανός να επιτεθεί σε μήνυμα, είναι μάλλον απαραίτητη η προφύλαξη του σχήματος απέναντι στην πιθανότητα υπαρκτής πλαστογραφίας.*

Σημείωση 2.9 *(συναρτήσεις κατακερματισμού και διαδικασίες ψηφιακής υπογραφής) Όταν μία συνάρτηση κατακερματισμού h χρησιμοποιείται σε ένα σχήμα ψηφιακής υπογραφής πρέπει να αποτελεί σταθερό κομμάτι της διαδικασίας υπογραφής έτσι ώστε ένας «αντίπαλος» να μην μπορεί να πάρει μία έγκυρη υπογραφή, να αντικαταστήσει την h με μία ασθενή συνάρτηση κατακερματισμού και κατόπιν να εξαπολύσει μία επίθεση επιλεκτικής πλαστογραφίας.*

Κεφάλαιο 3

Το RSA και σχετικά σχήματα υπογραφής

Στο κεφάλαιο αυτό περιγράφουμε τα σχήματα υπογραφής RSA και Rabin. Η ασφάλεια των σχημάτων αυτών έγκειται σε μεγάλο βαθμό στη δυσκολία του προβλήματος της παραγοντοποίησης μεγάλων ακεραίων.

3.1 Το σχήμα υπογραφής RSA

3.1.1 Το κρυπτοσύστημα RSA

Δεν θα σταθούμε πολύ στο κρυπτοσύστημα RSA αφού δεν αποτελεί αντικείμενο αυτής της εργασίας ,αλλά θα αναφέρουμε κάποια βασικά στοιχεία του, απαραίτητα για την κατανόηση του σχήματος υπογραφής RSA.

Το κρυπτοσύστημα RSA προτάθηκε το 1978 από τους Rivest, Shamir και Adleman, των οποίων και φέρει τα αρχικά.

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

Μπορούμε τώρα να περιγράψουμε το RSA. Το κρυπτοσύστημα αυτό χρησιμοποιεί υπολογισμούς στο σύνολο $\mathbb{Z}_n = \{0,1,2,...,n-1\}$, όπου n είναι το γινόμενο δύο μεγάλων τυχαία επιλεγμένων διακεκριμένων πρώτων αριθμών p,q. Για ένα τέτοιο $n=p\cdot q$ σημειώνουμε ότι $\varphi(n) = (p-1)(q-1)$,όπου φ η συνάρτηση Euler (βλ. παράρτημα).

Αλγόριθμος 3.1

Παραγωγή κλειδιού.

Συνοπτικά: Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί RSA και ένα αντίστοιχο ιδιωτικό. Κάθε οντότητα Α ενεργεί ως ακολούθως:

1. *Παράγει δύο μεγάλους διακεκριμένους τυχαίους πρώτους p και q, περίπου ίδιου μεγέθους.*
2. *Υπολογίζει $n = p\,q$ και $\varphi(n)=(p-1)(q-1)$.*
3. *Επιλέγει έναν τυχαίο ακέραιο e, $1 < e < \varphi(n)$,έτσι ώστε $(e, \varphi(n)) = 1$.*
4. *Χρησιμοποιεί τον επεκτεταμένο Ευκλείδειο αλγόριθμο (βλ. παράρτημα) για να υπολογίσει το μοναδικό ακέραιο d,$1 < d < \varphi(n)$,τέτοιο ώστε $ed \equiv 1 \pmod{\varphi(n)}$.*

5. *Το δημόσιο κλειδί του Α είναι το (n, e) και το ιδιωτικό του ο d (και οι πρώτοι p,q).*

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

Αλγόριθμος 3.2

Κρυπτογράφηση δημοσίου κλειδιού RSA.

Συνοπτικά: Ο Β κρυπτογραφεί ένα μήνυμα m για τον Α, το οποίο ο Α αποκρυπτογραφεί.

1. *Κρυπτογράφηση. Η οντότητα Β ενεργεί ως εξής:*
   - *1.1 Αποκτά, το αυθεντικό δημόσιο κλειδί του Α, (n, e).*
   - *1.2 Αναπαριστά το μήνυμα ως έναν ακέραιο m στο διάστημα [0, n-1].*
   - *1.3 Υπολογίζει $c = m^e \bmod n$.*
   - *1.4 Στέλνει το κρυπτοκείμενο c στον Α.*
2. *Αποκρυπτογράφηση. Για να ανακτήσει το απλό κείμενο m από το c, ο Α ενεργεί ως εξής:*
   - *2.1 Χρησιμοποιεί το ιδιωτικό κλειδί d για να ανακτήσει το $m = c^d \bmod n$.*

Παρατήρηση 3.1

1. *Αφού το n είναι το γινόμενο των δύο πρώτων p,q, θα ισχύει: φ(n) = (p-1)(q-1). Έτσι αν κάποιος γνωρίζει τους p,q, μπορεί εύκολα να υπολογίσει το φ(n) και άρα και το d.*
2. *Μια καλή επιλογή για τον δημόσιο εκθέτη e είναι κάποιος πρώτος αριθμός > max {p, q}.*

Δείχνουμε τώρα ότι η συνάρτηση $D(c) = c^d \bmod n$ είναι αντίστροφη της $E(m) = m^e \bmod n$, δηλαδή ότι D(E(m))= m.

Απόδειξη: *Αφού $ed \equiv 1 (\bmod \varphi(n))$, θα υπάρχει ένας ακέραιος k τέτοιος ώστε $ed = 1 + k \cdot \varphi(n)$. Έχουμε ότι: $D(E(m)) = m^{ed} \bmod n$. Συνεπώς:*

$$D(E\{m)) = m^{1+ k\varphi(n)} \bmod n = m \cdot m^{k\varphi(n)} \bmod n = m(m^{\varphi(n)})^k \bmod n = m \bmod n,$$

με την τελευταία ισότητα να προκύπτει από το θεώρημα Euler[8] (βλ. παράρτημα).

Παρατήρηση 3.2 *Ειδικά για το RSA μπορεί να δειχθεί ότι E(D(m)) = rn. Η σχέση αυτή βρίσκει εφαρμογή στο σχήμα υπογραφής.*

[8] Για να ισχύει το θεώρημα του *Euler* πρέπει (m, n) = 1,το οποίο ισχύει σχεδόν πάντα. Η πιθανότητα $(m,n) \neq 1$ είναι περίπου $1/10^{100}$

Το κρυπτοσύστημα RSA βασίζεται στη συνάρτηση $E(m)=m^e \bmod n$, η οποία δεχόμαστε (δεν έχει αποδειχθεί) ότι είναι μονής κατεύθυνσης. Δεν υπάρχει γνωστός αλγόριθμος που να αντιστρέφει αυτή τη συνάρτηση χωρίς τη γνώση του κρυφού εκθέτη αποκρυπτογράφησης d.[9]

Σημείωση 3.1 (*καθολικός έκθετης) Ο αριθμός λ = lcm (p-1, q-1), μερικές φορές καλείται καθολικός εκθέτης του n, μπορεί να χρησιμοποιηθεί αντί του φ(n)= (p-1) (q-1) στην παραγωγή κλειδιού για το RSA (αλγόριθμος 3.1). Παρατηρούμε ότι ο λ είναι κατάλληλος διαιρέτης του φ(n). Χρησιμοποιώντας τον λ μπορεί να προκύψει ένας μικρότερος εκθέτης αποκρυπτογράφησης d με αποτέλεσμα γρηγορότερη αποκρυπτογράφηση. Ωστόσο, αν οι p, q επιλεγούν τυχαία τότε ο gcd (p - 1, q - 1) αναμένεται μικρός και συνεπώς οι φ(n)και λ έχουν περίπου το ίδιο μέγεθος.*

3.1.2 Ψηφιακές υπογραφές που προκύπτουν από αντιστρεπτή κρυπτογράφηση δημοσίου κλειδιού

Η παράγραφος αυτή ασχολείται με μία κατηγορία σχημάτων ψηφιακής υπογραφής, η οποία βασίζεται σε συστήματα κρυπτογράφησης δημοσίου κλειδιού συγκεκριμένου τύπου.

Ας υποθέσουμε ότι E_e είναι ένας μετασχηματισμός κρυπτογράφησης δημοσίου κλειδιού με χώρο μηνυμάτων M και χώρο κρυπτοκειμένων C. Έστω επίσης ότι M = C. Αν D_d είναι ο μετασχηματισμός αποκρυπτογράφησης, ο αντίστοιχος του E_e, τότε αφού οι E_e, D_d είναι μεταθέσεις, θα ισχύει:

$$D_d(E_e(m)) = E_e(D_d(m)) = m, \forall m \in M. \qquad (3.1)$$

Ένα σχήμα κρυπτογράφησης δημοσίου κλειδιού αυτού του τύπου λέγεται αντιστρεπτό (reversible). Η υπόθεση ότι M = C είναι ουσιώδης ώστε η σχέση (3.1) να ισχύει $\forall m \in M$, διαφορετικά το $D_d(m)$ θα είναι άνευ σημασίας για m που δεν ανήκει στο C.

Κατασκευή ενός σχήματος ψηφιακής υπογραφής

1. Έστω M ο χώρος μηνυμάτων για το σχήμα υπογραφής.

2. Έστω C = M ο χώρος υπογραφών S.

3. Έστω (e, d) ένα ζεύγος - κλειδί για το σχήμα κρυπτογράφησης δημοσίου κλειδιού.

[9] Ο εκθέτης αποκρυπτογράφησης d είναι γνωστός και ως καταπακτή *(trapdoor)*.

4. *Ορίζουμε η συνάρτηση υπογραφής S_A να είναι ο μετασχηματισμός D_d*

Αυτό σημαίνει ότι η υπογραφή για ένα μήνυμα $m \in M$ είναι $s = D_d$.

5. *Ορίζουμε τη συνάρτηση επαλήθευσης V_A ως*

$$V_A(m, s) = \begin{cases} \text{αληθής}, & \text{αν } Ee(s) = m \\ \text{ψευδής}, & \text{διαφορετικά} \end{cases} \qquad (2.2)$$

Το σχήμα υπογραφής μπορεί περαιτέρω να απλοποιηθεί αν ο Α υπογράφει μόνο μηνύματα που έχουν μία ειδική δομή και αυτή η δομή είναι δημοσίως γνωστή[10]. Έστω M' ένα υποσύνολο του M, του οποίου τα στοιχεία έχουν μία καλώς - ορισμένη ειδική δομή, τέτοια ώστε το M' να περιέχει μόνο ένα αμελητέο κλάσμα μηνυμάτων από το σύνολο M. Για παράδειγμα, έστω ότι το M αποτελείται από όλες τις δυαδικές ακολουθίες μήκους 2t, όπου t θετικός ακέραιος. Έστω M' το υποσύνολο του M που αποτελείται από όλες τις ακολουθίες όπου τα πρώτα t bits αντιγράφονται στις τελευταίες t θέσεις (π.χ.,101101 θα ανήκει στο M' για t = 3). Αν ο Α υπογράφει μόνο μηνύματα εντός του συνόλου. M', αυτά εύκολα αναγνωρίζονται από αυτόν που επαληθεύει. Επανορίζουμε τη συνάρτηση επαλήθευσης V_A ως

$$V_A(s) = \begin{cases} \text{αληθής}, & \text{αν } Ee(s) \in M' \\ \text{ψευδής}, & \text{διαφορετικά} \end{cases} \qquad (2.3)$$

Υπό το νέο αυτό σενάριο ο Α χρειάζεται μόνο να μεταδώσει την υπογραφή s αφού το μήνυμα $m = Ee(s)$ μπορεί να ανακτηθεί εφαρμόζοντας τη συνάρτηση επαλήθευσης. Ένα τέτοιο σχήμα λέγεται σχήμα ψηφιακής υπογραφής με ανάκτηση του μηνύματος (βλ. §3.4.2) .Το χαρακτηριστικό επιλογής μηνυμάτων ειδικής δομής αναφέρεται ως επιλογή μηνυμάτων με πλεονασμό (redundancy).

Η τροποποίηση που παρουσιάστηκε προηγουμένως είναι κάτι περισσότερο από μία απλοποίηση. Είναι απολύτως κρίσιμη αν κάποιος ελπίζει να ικανοποιήσει την απαίτηση της 3ης ιδιότητας των συναρτήσεων υπογραφής και επαλήθευσης. Για να

[10] Πρόκειται για μηνύματα με πλεονασμό.

το καταλάβουμε αυτό, ας δούμε το ακόλουθο: οποιαδήποτε οντότητα Β μπορεί να επιλέξει ένα τυχαίο στοιχείο s ∈ S ως υπογραφή και να υπολογίσει το u= $Ee(s)$, αφού S = M και ο μετασχηματισμός E_e είναι δημόσια πληροφορία. Ο Β τότε παίρνει το μήνυμα m = u με την υπογραφή του m να είναι η s και μεταδίδει το ζεύγος (m,s). Είναι εύκολο να ελέγξουμε ότι η s θα γίνει δεκτή ως υπογραφή που δημιουργήθηκε για το m από τον Α, αλλά για την δημιουργία της οποίας ο Α δεν αναμείχθηκε. Σε αυτήν την περίπτωση ο Β έχει πλαστογραφήσει μια υπογραφή του Α. Αυτό είναι ένα παράδειγμα υπαρκτής πλαστογραφίας (ο Β δημιούργησε την υπογραφή του Α σε κάποιο μήνυμα πιθανώς όχι της επιλογής του)(βλ.§2.5).

Αν το M' περιέχει μόνο ένα αμελητέο κλάσμα μηνυμάτων του M, τότε η πιθανότητα κάποια οντότητα να πλαστογραφήσει την υπογραφή του Α με αυτό τον τρόπο είναι αμελητέα μικρή.

Τέλος αναφέρουμε ορισμένες ιδιότητες που πρέπει να έχουν οι ψηφιακές υπογραφές για να είναι χρήσιμες στην πράξη. Μία ψηφιακή υπογραφή πρέπει

1. *να υπολογίζεται εύκολα από τον υπογράφοντα (η συνάρτηση υπογραφής πρέπει να υπολογίζεται εύκολα),*
2. *να επαληθεύεται εύκολα από οποιονδήποτε (η συνάρτηση επαλήθευσης πρέπει να υπολογίζεται εύκολα) και*
3. *να έχει κατάλληλη διάρκεια ζωής (lifespan),δηλαδή να είναι υπολογιστικά ασφαλής σε επιθέσεις πλαστογραφίας μέχρι να πάψει να χρησιμοποιείται για τον σκοπό για τον οποίο αρχικά σχεδιάστηκε.*

3.1.3 Το σχήμα υπογραφής RSA

Ο χώρος των μηνυμάτων και των υπογραφών για το σχήμα ψηφιακής υπογραφής RSA είναι το σύνολο $\mathbb{Z}_n$ = {0,1,2,..., n - 1} όπου n είναι το γινόμενο δύο τυχαία επιλεγμένων διακεκριμένων πρώτων αριθμών, όπως και στο κρυπτοσύστημα. Εφόσον ο μετασχηματισμός κρυπτογράφησης είναι 1-1 και επί (Injection), δηλαδή M = C, οι ψηφιακές υπογραφές μπορούν να δημιουργηθούν αντιστρέφοντας τους ρόλους της κρυπτογράφησης και της αποκρυπτογράφησης, όπως είδαμε στην προηγούμενη παράγραφο. Έτσι ως μετασχηματισμός υπογραφής χρησιμοποιείται ο μετασχηματισμός αποκρυπτογράφησης του κρυπτοσυστήματος RSA, ενώ ως μετασχηματισμός επαλήθευσης χρησιμοποιείται ο μετασχηματισμός

κρυπτογράφησης. Το σχήμα υπογραφής RSA είναι ένα προσδιοριστικό σχήμα ψηφιακής υπογραφής που παρέχει ανάκτηση του μηνύματος. Ο χώρος υπογραφής Ms είναι επίσης το σύνολο $\mathbb{Z}_n$. Η συνάρτηση πλεονάζουσας πληροφορίας R: M→$\mathbb{Z}_n$, αποτελεί δημόσια πληροφορία.

Αλγόριθμος 3.3

Παραγωγή κλειδιού

Η διαδικασία παραγωγής κλειδιού για το σχήμα υπογραφής RSA είναι ίδια με αυτή του κρυπτοσυστήματος, επομένως ο αναγνώστης παραπέμπεται στον αλγόριθμο 3.1 της παραγράφου 3.1.1.

Αλγόριθμος 3.4

Παραγωγή υπογραφής και επαλήθευση.

Συνοπτικά: Η οντότητα A υπογράφει ένα μήνυμα m ∈ M. Οποιαδήποτε οντότητα B μπορεί να επαληθεύσει την υπογραφή του A και να ανακτήσει το μήνυμα m από αυτήν.

1. *Παραγωγή υπογραφής. Η οντότητα A ενεργεί ως εξής:*
   - *1.1 Υπολογίζει $\tilde{m} = R(m)$,έναν ακέραιο στο διάστημα [0, n - 1].*
   - *1.2 Υπολογίζει $s = \tilde{m} \bmod n$.*
   - *1.3 Η υπογραφή του A για το m είναι s.*

2. *Επαλήθευση. Για να επαληθεύσει την υπογραφή s του A και να ανακτήσει το μήνυμα m, ο B ενεργεί ως εξής:*
   - *2.1 Αποκτά το αυθεντικό δημόσιο κλειδί του A, (n, e).*
   - *2.2 Υπολογίζει $\tilde{m} = s^e \bmod n$.*
   - *2.3 Επαληθεύει ότι $\tilde{m} \in M_R$. Αν όχι, απορρίπτει την υπογραφή.*
   - *2.4 Ανακτά το m (= $R^{-1}(\tilde{m})$).*

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί

Αν s είναι μία υπογραφή για ένα μήνυμα m, τότε ισχύει $s=\tilde{m}^d \bmod n$, όπου $\tilde{m} = R(m)$. Αφού $ed \equiv 1 (\bmod \varphi(n))$,υπάρχει $k \in \mathbb{Z}$ τέτοιο ώστε $ed = 1 + k\varphi(n)$. Θα ισχύει ότι $s^e \equiv \tilde{m}^{ed} (\bmod n)$ και επομένως έχουμε

$$s^e \equiv \tilde{m}^{1+k\varphi(n)} (\bmod n) \equiv \tilde{m}\,\tilde{m}^{k\varphi(n)} (\bmod n) \equiv \tilde{m}\,(\tilde{m}^{\varphi(n)}) \bmod n \equiv \tilde{m} \bmod n,$$

από το θεώρημα Euler. Εν τέλει, $m = R^{-1}(\tilde{m}) = R^{-1}(R(m)) = m$.

Παράδειγμα 3.1 *(παραγωγή υπογραφής RSA με τεχνητά μικρές παραμέτρους) Παραγωγή κλειδιού. Η οντότητα Α επιλέγει τους πρώτους $p = 89$, $q = 97$ και υπολογίζει $n = p \cdot q = 8633$ και $\varphi(n) = 88 \times 96 = 8448$. Επίσης επιλέγει $e = 5$ και λύνει την ισοτιμία $ed = 5d \equiv 1 \pmod{8448}$, από την οποία προκύπτει ότι $d = 5069$. Η διαδικασία γίνετε με τον εκτεταμένο αλγόριθμο του Ευκλείδη. Το δημόσιο κλειδί του Α είναι το ζεύγος ($n = 8633$, $e = 5$) και το ιδιωτικό του κλειδί το $d = 5069$.*

Παραγωγή υπογραφής. Για λόγους απλότητας, έστω ότι $M = \mathbb{Z}_n$ και ότι η συνάρτηση πλεονάζουσας πληροφορίας $R : M \rightarrow \mathbb{Z}_n$ είναι η ταυτοτική απεικόνιση $R(m) = m$, $\forall m \in M$. Για την υπογραφή ενός μηνύματος $m = 1234$, ο Α υπολογίζει $\tilde{m} = R(m) = 1234$ και υπολογίζει την υπογραφή $s = \tilde{m}^d \bmod n = 1234^{5069} \bmod 8633 = 279$. Επαλήθευση υπογραφής. Η οντότητα Β υπολογίζει $\tilde{m} = s^e \bmod n = 279^5 \bmod 8633 = 1234$. Τέλος ο Β αποδέχεται την υπογραφή εφόσον το $\tilde{m}$ έχει τον απαιτούμενο πλεονασμό (δηλ., $\tilde{m} \in M_R$) και ανακτά το $m = R^{-1}(\tilde{m}) = 1234$.

3.1.4 Δυνατές επιθέσεις σε υπογραφές RSA

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

   Αν ένας «αντίπαλος» μπορεί να παραγοντοποιήσει το n που είναι δημόσια πληροφορία κάποιας οντότητας Α (στο εξής modulus-πληθ.: moduli) τότε μπορεί να υπολογίσει το φ(n) και κατόπιν χρησιμοποιώντας τον επεκτεταμένο Ευκλείδειο αλγόριθμο να υπολογίσει το ιδιωτικό κλειδί d από το φ(n) και τον δημόσιο εκθέτη e λύνοντας την ισοτιμία $ed \equiv 1 \pmod{\varphi(n)}$. Αυτό αποτελεί ολική κατάρρευση του συστήματος. Για να προφυλαχθεί, ο Α πρέπει να επιλέξει τους p και q έτσι ώστε η παραγοντοποίηση του n να είναι υπολογιστικά ανέφικτη.

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

   Το σχήμα υπογραφής RSA έχει την ακόλουθη πολλαπλασιαστική ιδιότητα, η οποία μερικές φορές αναφέρεται ως ομομορφική ιδιότητα (homomorphic property). Αν $s_1 = m_1^d \bmod n$ και $s_2 = m_2^d \bmod n$ είναι υπογραφές των μηνυμάτων m_1 και m_2 αντίστοιχα (ή πιο σωστά μηνυμάτων με πλεονασμό), τότε το $s = s_1 s_2 \bmod n$ έχει την ιδιότητα ότι $s = (m_1 m_2)^d \bmod n$. Αν το $m = m_1 m_2$ έχει τον κατάλληλο πλεονασμό (δηλ., $m \in M_R$), τότε το s θα είναι έγκυρη υπογραφή γι' αυτό. Επομένως είναι σημαντικό η συνάρτηση πλεονάζουσας

πληροφορίας να μην είναι πολλαπλασιαστική, δηλ. για κάθε ζεύγος $a,b \in M$, $R(a \cdot b) \neq R(a) \cdot R(b)$. *Όπως φαίνεται στο παράδειγμα που ακολουθεί, η ιδιότητα αυτή είναι απαραίτητη για την R αλλά ανεπαρκής όσον αφορά την ασφάλεια του σχήματος.*

Παράδειγμα 3.2 *(μη ασφαλής συνάρτηση πλεονάζουσας πληροφορίας) Έστω n το modulus του RSA και d το ιδιωτικό κλειδί. Έστω* $k = \lceil lg\, n \rceil$ *το μήκος bit του n και έστω t ένας σταθερός θετικός ακέραιος τέτοιος ώστε* $t < k/2$. *Έστω* $w = 2^t$ *και έστω ότι τα μηνύματα m είναι ακέραιοι στο διάστημα* $[1, n2^{-t} - 1]$. *Η συνάρτηση πλεονάζουσας πληροφορίας R έχει τύπο* $R(m) = m2^t$ *(τα λιγότερο σημαντικά t bits της δυαδικής αναπαράστασης του R(m) είναι μηδενικά)*[11]. *Για τις περισσότερες επιλογές του n, η R δεν θα έχει την πολλαπλασιαστική ιδιότητα. Η επίθεση υπαρκτής πλαστογραφίας (βλ.§2.5) έχει πιθανότητα επιτυχίας* $(\frac{1}{2})^t$. *Για τη συγκεκριμένη όμως συνάρτηση πλεονάζουσας πληροφορίας είναι πιθανή μία επίθεση επιλεκτικής πλαστογραφίας, η οποία είναι πιο επικίνδυνη.*

3.1.5 Το σχήμα υπογραφής RSA στην πράξη

1. Πρόβλημα ανάκτησης (Reblocking problem)

Μία προτεινόμενη χρήση του σχήματος RSA είναι η υπογραφή ενός μηνύματος και στη συνέχεια η κρυπτογράφηση της προκύπτουσας υπογραφής. Εδώ θα πρέπει να ενδιαφερθούμε για τα σχετικά μεγέθη των moduli που εμπλέκονται στην υλοποίηση της παραπάνω διαδικασίας. Ας υποθέσουμε ότι ο Α επιθυμεί να υπογράψει και κατόπιν να κρυπτογραφήσει ένα μήνυμα για τον Β. Έστω (n_A, e_A) *και* (n_B, e_B) *τα δημόσια κλειδιά των Α και Β αντίστοιχα. Αν* $n_A, > n_B$, *τότε υπάρχει πιθανότητα το μήνυμα να μην μπορεί να ανακτηθεί από τον Β, όπως φαίνεται στο ακόλουθο παράδειγμα.*

Παράδειγμα 3.3 *(πρόβλημα ανάκτησης)*

Έστω $n_A = 103 \times 107 = 11021$, $e_A = 5$ *και* $d_A = 4325$. *Έστω επίσης* $n_B = 4891$, $e_{B=} 5$ *και* $d_B = 1901$. *Παρατηρούμε ότι* $n_A > n_B$. *Έστω* $m = 3512$ *ένα μήνυμα με πλεονασμό το οποίο υπογράφεται με το ιδιωτικό κλειδί του Α και στη συνέχεια κρυπτογραφείται με το δημόσιο κλειδί του Β.Ο Α υπολογίζει τα ακόλουθα:*

---

[11] Δηλ., τα τελευταία t *bits* (βλ. παράρτημα).

1. $s = m^{dA} \bmod n_A = 3512^{4325} \bmod 11021 = 8485.$
2. $c = s^{eB} \bmod n_B = 8485^{5} \bmod 4891 = 3073.$

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

1. $\hat{s} = c^{dB} \bmod n_B = 3073^{1901} \bmod 4891 = 3594.$
2. $\hat{m} = \hat{s}^{eA} \bmod n_A = 3594^{5} \bmod 11021 = 6942.$

Παρατηρούμε ότι $m \neq \hat{m}$. *Ο λόγος είναι ότι η υπογραφή s είναι μεγαλύτερη από το modulus* n_B. *Εδώ η πιθανότητα εμφάνισης αυτού του προβλήματος είναι* $(n_A - n_B)/n_A \approx 0.56$.

Υπάρχουν διάφοροι τρόποι για να ξεπεράσουμε το πρόβλημα της ανάκτησης.

1. *αλλαγή της σειράς των πράξεων: Το πρόβλημα της λάθους αποκρυπτογράφησης δεν πρόκειται να εμφανιστεί αν η πράξη που χρησιμοποιεί το μικρότερο modulus εφαρμόζεται πρώτη. Αυτό σημαίνει ότι αν* $n_A > n_B$, *τότε η οντότητα Α πρέπει πρώτα να κρυπτογραφήσει το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Β και εν συνεχεία να υπογράψει το προκύπτον κρυπτοκείμενο χρησιμοποιώντας το ιδιωτικό της κλειδί. Ωστόσο η σειρά των πράξεων που προτιμάται, είναι πάντα πρώτα να υπογράφεται το μήνυμα και κατόπιν να κρυπτογραφείται η υπογραφή. Γιατί αν ο Α πρώτα κρυπτογραφήσει και ύστερα υπογράψει, ένας «αντίπαλος» Θα μπορούσε να αφαιρέσει την υπογραφή και να την αντικαταστήσει με τη δική του. Έστω και αν ο «αντίπαλος» δεν θα γνωρίζει τι υπογράφεται, ίσως υπάρξουν περιπτώσεις επωφελείς γι' αυτόν. Γι' αυτό το λόγο η αλλαγή της σειράς των πράξεων δεν αποτελεί συνετή λύση.*
2. *δύο moduli ανά οντότητα: Κάθε οντότητα πρέπει να παράγει ξεχωριστά moduli για την κρυπτογράφηση και την υπογραφή. Αν το modulus υπογραφής κάθε οντότητας είναι μικρότερο από όλα τα πιθανά moduli κρυπτογράφησης, τότε λάθος αποκρυπτογράφηση δεν συμβαίνει ποτέ. Αυτό μπορεί να διασφαλιστεί με την απαίτηση τα moduli κρυπτογράφησης να είναι αριθμοί (t + 1) -bit και τα moduli υπογραφής να είναι αριθμοί t - bit. καθορίζοντας τη μορφή του modulus: Σε αυτή τη μέθοδο, επιλέγει κάποιος τους πρώτους p και q έτσι ώστε το modulus n να έχει ειδική μορφή: το bit υψηλότερης τάξης (βλ. παράρτημα) είναι 1 και τα k επόμενα bits είναι όλα 0. Ένα t -bit modulus n της μορφής*

αυτής μπορεί να βρεθεί ως ακολούθως.Το n έχει την απαιτούμενη μορφή όταν $2^{t-1} \leq n < 2^{t-1} + 2^{t-k-1}$. *Επιλέγουμε έναν τυχαίο πρώτο p* $\lceil t/2 \rceil$ *- bit και ψάχνουμε για έναν πρώτο q στο διάστημα μεταξύ* $\left\lceil 2^{t-1}/p \right\rceil$ *και* $\left\lfloor (2^{t-1} + 2^{t-k-1})/p \right\rfloor$. *Τότε το n = pq είναι ένα modulus της απαιτούμενης μορφής (βλ. επόμενο παράδειγμα). Η επιλογή αυτή για το modulus n δεν εμποδίζει τελείως το πρόβλημα της λάθους αποκρυπτογράφησης, αλλά μπορεί να ελαττώσει την πιθανότητα εμφάνισης του σε έναν αμελητέα μικρό αριθμό.*

Παράδειγμα 3.4 *(καθορίζοντας τη μορφή του modulus)*

Ας υποθέσουμε ότι κάποιος θέλει να κατασκευάσει ένα 12-bit modulus n τέτοιο ώστε το bit υψηλότερης τάξης (βλ. παράρτημα) είναι 1 και τα επόμενα k=3 bits είναι 0. Ξεκινάμε επιλέγοντας έναν 6-bit πρώτο p = 37. Επιλέγουμε έναν πρώτο q στο διάστημα μεταξύ $\left\lceil 2^{11}/p \right\rceil$*=56 και* $\left\lfloor (2^{11} + 2^{8})/p \right\rfloor$ *= 62.Οι πιθανές τιμές για το q είναι 59 και 61. Αν επιλεγεί το q = 59 τότε n = 37 x 59 = 2183, με δυαδική αναπαράσταση 100010000111. Αν επιλεγεί το q= 61 τότε n = 37 x 61 = 2257, με δυαδική αναπαράσταση 100011010001.*

2. Συναρτήσεις πλεονάζουσας πληροφορίας

Για να αποφευχθεί μία επίθεση υπαρκτής πλαστογραφίας στο σχήμα υπογραφής RSA, απαιτείται μία κατάλληλη συνάρτηση πλεονάζουσας πληροφορίας R. Η συνετή επιλογή της R είναι κρίσιμη για την ασφάλεια του σχήματος.

Όπως είδαμε και στο τέλος της παραγράφου 2.2 εφαρμόζοντας ο υπογράφων μία τέτοια συνάρτηση σε ένα μήνυμα καθιστά σχεδόν αδύνατη την πλαστογράφηση της υπογραφής του, εκτός αν ο «αντίπαλος» κατορθώσει να παραγοντοποιήσει το δημόσιο modulus του RSA, n. Πράγματι είναι απίθανο μία τυχαία επιλεγμένη υπογραφή να δώσει ένα μήνυμα (επίθεση υπαρκτής πλαστογραφίας) με τις ιδιότητες που προσδίδει σε τυχαίο μήνυμα η συνάρτηση πλεονάζουσας πληροφορίας του νόμιμου υπογράφοντος.

3. Το σχήμα ψηφιακής υπογραφής RSA με παράρτημα

Η σημείωση 2.6 περιγράφει τον τρόπο με τον οποίο ένα οποιοδήποτε σχήμα ψηφιακής υπογραφής με ανάκτηση του μηνύματος μπορεί να τροποποιηθεί ώστε να δώσει ένα σχήμα ψηφιακής υπογραφής με παράρτημα. Για παράδειγμα, αν χρησιμοποιείται ο αλγόριθμος MD5 ([MOV96], κεφ.9) (συνάρτηση κατακερματισμού) για τον κατακερματισμό μηνυμάτων αυθαίρετου μήκους σε ακολουθίες bit μήκους 128, τότε ο αλγόριθμος 2.4 θα μπορούσε να χρησιμοποιηθεί για την υπογραφή αυτών των τιμών κατακερματισμού.

4. Χαρακτηριστικά επίδοσης της παραγωγής υπογραφής και της επαλήθευσης

Έστω n =p· q ένα 2k - bit RSA modulus,όπου p, q είναι ο καθένας k - bit πρώτοι. Ο υπολογισμός μιας υπογραφής $s = m^d \bmod n$ ενός μηνύματος πι απαιτεί $0(k^3)$ πράξεις bit. Εφόσον ο υπογράφων γνωρίζει τους p και q μπορεί να υπολογίσει $s_1 = m^d \bmod p, s_2 = m^d \bmod q$ και να καθορίσει το s χρησιμοποιώντας το κινεζικό θεώρημα των υπολοίπων. Παρ' όλο ότι η πολυπλοκότητα αυτής της διαδικασίας παραμένει $0(k^3)$, είναι αξιοσημείωτα αποδοτικότερη σε κάποιες περιπτώσεις.

Η επαλήθευση των υπογραφών είναι σημαντικά γρηγορότερη από τη διαδικασία υπογραφής αν ο δημόσιος εκθέτης επιλέγεται να είναι ένας μικρός αριθμός. Τότε η επαλήθευση απαιτεί $0(k^2)$ πράξεις bit. Προτεινόμενες τιμές για τον e στην πράξη είναι το 3 ή 2^{16+112}. Φυσικά τα p,q πρέπει να επιλέγονται έτσι ώστε (e, (p-1)(q-1))= 1.

Το σχήμα υπογραφής RSA είναι συνεπώς ιδανικό για περιπτώσεις στις οποίες η επαλήθευση των υπογραφών είναι η επικρατούσα εφαρμογή. Για παράδειγμα, όταν μια έμπιστη αρχή (trusted third party-TTP) (βλ. παράρτημα) δημιουργεί ένα πιστοποιητικό δημοσίου κλειδιού για μια οντότητα Α τότε απαιτείται μόνο μια παραγωγή υπογραφής η οποία ίσως επαληθευθεί πολλές φορές από διάφορες άλλες οντότητες.

5. Επιλογή παραμέτρων

Από το 1996, ένα ελάχιστο 768 bits προτείνεται για τα moduli υπογραφής του RSA. Ένα modulus τουλάχιστον 1024 bits προτείνεται για υπογραφές που απαιτούν μεγαλύτερες διάρκειες ζωής ή που είναι κρίσιμες για τη συνολική ασφάλεια ενός

[12] Η επιλογή του $e = 2^{16} + 1$ βασίζεται στο γεγονός ότι ο e είναι πρώτος αριθμός και ότι το $\tilde{m}^e \bmod n$ μπορεί να υπολογιστεί μόνο με 16 *modular* υψώσεις στο τετράγωνο και έναν *modular* πολλαπλασιασμό.

μεγάλου δικτύου. Είναι συνετή η ενημέρωση σχετικά με την πρόοδο στην παραγοντοποίηση των ακεραίων και βεβαίως η ανάλογη ρύθμιση των παραμέτρων.

Δεν έχουν αναφερθεί αδυναμίες στο σχήμα υπογραφής RSA όταν ο δημόσιος εκθέτης e επιλέγεται να είναι ένας μικρός αριθμός όπως το 3 ή 2^{16} + 1. Δεν ισχύει όμως το ίδιο για τον ιδιωτικό εκθέτη d αφού δεν προτείνεται ο περιορισμός του μεγέθους του για τη βελτίωση της αποδοτικότητας της παραγωγής υπογραφής.

6. Αποδοτικότητα εύρους ζώνης (Bandwidth efficiency)

Η αποδοτικότητα εύρους ζώνης για ψηφιακές υπογραφές με ανάκτηση του μηνύματος αναφέρεται στο λόγο του δυαδικού λογαρίθμου του μεγέθους του χώρου υπογραφής M_s προς το δυαδικό λογάριθμο του μεγέθους της εικόνας M_R, (= Im (R)) της συνάρτησης πλεονάζουσας πληροφορίας. Για αυτό το λόγο, η αποδοτικότητα εύρους ζώνης καθορίζεται από τη συνάρτηση πλεονάζουσας πληροφορίας. Για παράδειγμα, για το RSA (και το σχήμα ψηφιακής υπογραφής Rabin), η συνάρτηση πλεονάζουσας πληροφορίας που καθορίζεται από τη διαδικασία ISO/IEC 9796 παίρνει μηνύματα k - bit και τα κωδικοποιεί σε 2k - bit στοιχεία του M_s από τα οποία σχηματίζεται μια υπογραφή 2k - bit. Σε αυτήν την περίπτωση η αποδοτικότητα εύρους ζώνης είναι $\frac{1}{2}$. Για παράδειγμα με ένα modulus μεγέθους 1024 bits το μέγιστο μέγεθος μηνύματος που μπορεί να υπογραφεί είναι 512 bits.

7. Γενικές παράμετροι (System-wide parameters)

Κάθε οντότητα πρέπει να έχει ένα διακεκριμένο RSA modulus.Δεν είναι ασφαλής η χρήση ενός γενικού modulus. Ο δημόσιος εκθέτης e μπορεί να είναι μια γενική παράμετρος και σε πολλές εφαρμογές είναι.

8. Μικρά μηνύματα εναντίον μεγάλων

Ας υποθέσουμε ότι n είναι ένα 2k-bit RSA modulus το οποίο χρησιμοποιείται στον αλγόριθμο 2.4 για την υπογραφή μηνυμάτων k - bit (δηλ., η αποδοτικότητα εύρους ζώνης είναι $\frac{1}{2}$). Έστω ότι η οντότητα A θέλει να υπογράψει ένα μήνυμα m kt - bit. Μια προσέγγιση είναι να χωριστεί το m σε πακέτα των k - bit έτσι ώστε $m = m_1 || m_2 || \ldots || m_t$ και να υπογραφεί το κάθε πακέτο ξεχωριστά (όμως βλ. σημείωση 2.4 γιατί αυτό δεν προτείνεται). Εναλλακτικά ο A μπορεί να κατακερματίσει το μήνυμα m σε μία ακολουθία bit μήκους $l \leq k$ και να υπογράψει την τιμή κατακερματισμού.

Η απαίτηση εύρους ζώνης για την υπογραφή αυτή είναι kt + 2k, όπου ο όρος kt προέρχεται από την αποστολή του μηνύματος m. Αφού kt + 2k ≤ 2kt όταν t ≥ 2, συνεπάγεται ότι η αποδοτικότερη, αναφορικά με το εύρος ζώνης, μέθοδος είναι η χρήση ψηφιακών υπογραφών RSA με παράρτημα. Για ένα μήνυμα μεγέθους το πολύ k - bits προτιμάται το σχήμα RSA με ανάκτηση του μηνύματος.

3.2 Το σχήμα υπογραφής δημοσίου κλειδιού Rabin

3.2.1 Το κρυπτοσύστημα Rabin

Μία επιθυμητή ιδιότητα οποιουδήποτε σχήματος κρυπτογράφησης είναι μία απόδειξη ότι το «σπάσιμο» του είναι τόσο δύσκολο όσο το να λυθεί ένα υπολογιστικό πρόβλημα το οποίο ευρέως θεωρείται ότι είναι δύσκολο, όπως η παραγοντοποίηση ακεραίων ή το πρόβλημα διακριτού λογαρίθμου. Ενώ πιστεύεται ότι το «σπάσιμο» του σχήματος κρυπτογράφησης RSA είναι τόσο δύσκολο όσο η παραγοντοποίηση του modulus n, καμία τέτοια ισοδυναμία δεν έχει αποδειχθεί. Το σχήμα κρυπτογράφησης δημοσίου κλειδιού Rabin ήταν το πρώτο παράδειγμα ενός αποδείξιμα ασφαλούς σχήματος κρυπτογράφησης δημοσίου κλειδιού. Το πρόβλημα της ανάκτησης του απλού κειμένου από κάποιο δοθέν κρυπτοκείμενο είναι υπολογιστικά ισοδύναμο με την παραγοντοποίηση.

Αλγόριθμος 3.5

Παραγωγή κλειδιού.

Συνοπτικά: Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί και ένα αντίστοιχο ιδιωτικό. Κάθε οντότητα Α ενεργεί ως ακολούθως:

1. *Παράγει δύο μεγάλους, τυχαίους, διακεκριμένους πρώτους p και q, περίπου ίδιου μεγέθους.*
2. *Υπολογίζει το n = p q.*
3. *Το δημόσιο κλειδί του Α είναι το n. Το ιδιωτικό του κλειδί είναι το ζεύγος (p,q).*

Αλγόριθμος 3.6

Κρυπτογράφηση δημοσίου κλειδιού Rabin.

Συνοπτικά: Ο Β κρυπτογραφεί ένα μήνυμα m για τον Α, το οποίο ο Α αποκρυπτογραφεί.

1. *Κρυπτογράφηση. Ο Β ενεργεί ως εξής:*
   - *1.1 Αποκτά το αυθεντικό δημόσιο κλειδί n του Α.*
   - *1.2 Αναπαριστά το μήνυμα ως έναν ακέραιο m στο σύνολο {0,1,...,n-1}.*

1.3 Υπολογίζει το $c = m^2 \bmod n$.

1.4 Στέλνει το κρυπτοκείμενο c στον Α.

2. *Αποκρυπτογράφηση. για να ανακτήσει το απλό κείμενο m από το c, ο Α ενεργεί ως εξής:*

2.1 Χρησιμοποιεί τον αλγόριθμο εύρεσης τετραγωνικών ριζών modulo n (βλ. [MOV96], κεφ.3) για να υπολογίσει τις 4 τετραγωνικές ρίζες m_1, m_2, m_3, m_4 του c modulo n[13].

2.2 Το μήνυμα που εστάλη ήταν κάποιο από τα m_1, m_2, m_3, m_4. Με κάποιο τρόπο ο Α (βλ. σημείωση 3.3) αποφασίζει ποιο από αυτά είναι το m.

Σημείωση 3.2 *(εύρεση των τετραγωνικών ριζών του c modulo n = pq όταν $p \equiv q \equiv 3 \pmod 4$) Αν οι p, q επιλέγονται και οι δύο να είναι $\equiv 3 \pmod 4$, τότε ο αλγόριθμος για τον υπολογισμό των τεσσάρων τετραγωνικών ριζών του c modulo n απλοποιείται ως ακολούθως:*

1. *Χρησιμοποιούμε τον επεκτεταμένο Ευκλείδιο αλγόριθμο για την εύρεση ακεραίων α και b τέτοιων ώστε $ap + bq = 1$.*
2. *Υπολογίζουμε το $r = c^{(p+1)/4} \bmod p$.*
3. *Υπολογίζουμε το $s = c^{(q+1)/4} \bmod q$.*
4. *Υπολογίζουμε το $x = (aps + bqr) \bmod n$.*
5. *Υπολογίζουμε το $y = (aps - bqr) \bmod n$.*
6. *Οι 4 τετραγωνικές ρίζες του c modulo n είναι x, -x mod n, y και -y mod n.*

Σημείωση 3.3 *(χρήση του πλεονασμού) Ένα μειονέκτημα του σχήματος κρυπτογράφησης δημοσίου κλειδιού Rabin είναι ότι ο παραλήπτης έρχεται αντιμέτωπος με το πρόβλημα της επιλογής του απλού κειμένου ανάμεσα σε 4 πιθανά απλά κείμενα. Αυτή η αμφιβολία στην αποκρυπτογράφηση μπορεί εύκολα να ξεπεραστεί στην πράξη με την πρόσθεση προκαθορισμένου πλεονασμού στο αρχικό απλό κείμενο πριν την κρυπτογράφηση (για παράδειγμα μπορούν να αντιγραφούν τα τελευταία 64 bits του μηνύματος) . Τότε, με υψηλή πιθανότητα,*

[13] Στην πολύ απίθανη περίπτωση όπου $(m.n) \neq 1$, το κρυπτοκείμενο c δεν έχει 4 διακεκριμένες τετραγωνικές ρίζες *modulo n*, αλλά αντιθέτως μόνο μία ή δύο.

ακριβώς μία από τις 4 τετραγωνικές ρίζες m_1,m_2,m_3,m_4 ενός γνήσιου κρυπτοκειμένου c θα έχει αυτόν τον πλεονασμό και ο παραλήπτης θα την επιλέγει ως το υποτιθέμενο απλό κείμενο. Αν καμία από τις τετραγωνικές ρίζες του c δεν θα έχει αυτόν τον πλεονασμό, τότε ο παραλήπτης θα απορρίπτει το c ως απατηλό.

3.2.2 Το σχήμα υπογραφής δημοσίου κλειδιού Rabin

Το σχήμα υπογραφής δημοσίου κλειδιού Rabin είναι όμοιο με το RSA, αλλά χρησιμοποιεί έναν άρτιο δημόσιο εκθέτη e[14]. Χάριν απλότητας υποθέτουμε ότι e=2. Ο χώρος υπογραφής Ms είναι το σύνολο Q_n (το σύνολο των τετραγωνικών υπολοίπων modulo n) (βλ. παράρτημα) και οι υπογραφές είναι τετραγωνικές ρίζες των στοιχείων του. Επίσης επιλέγεται μία συνάρτηση πλεονάζουσας πληροφορίας R από το χώρο των μηνυμάτων M στο Ms και είναι δημοσίως γνωστή.

Αλγόριθμος 3.7

Παραγωγή κλειδιού για το σχήμα υπογραφής δημοσίου κλειδιού Rabin.

Συνοπτικά: Κάθε οντότητα δημιουργεί ένα δημόσιο κλειδί και ένα αντίστοιχο ιδιωτικό. Κάθε οντότητα A ενεργεί ως ακολούθως:

1. *Παράγει δύο μεγάλους, τυχαίους, διακεκριμένους πρώτους p και q, περίπου ίδιου μεγέθους.*
2. *Υπολογίζει το $n = p \cdot q$.*
3. *Το δημόσιο κλειδί του A είναι το n. Το ιδιωτικό του κλειδί είναι το ζεύγος (p,q).*

Αλγόριθμος 3.8

Παραγωγή υπογραφής και επαλήθευση.

Συνοπτικά: Η οντότητα A υπογράφει ένα μήνυμα $m \in M$. Οποιαδήποτε οντότητα B μπορεί να επαληθεύσει την υπογραφή του A και να ανακτήσει το μήνυμα m από αυτήν.

1. *Παραγωγή υπογραφής. Ή. οντότητα A ενεργεί ως εξής:*
   - *1.1 Υπολογίζει το $\tilde{m} = R(m)$.*
   - *1.2 Υπολογίζει μια τετραγωνική ρίζα s του $\tilde{m}$ mod n.*
   - *1.3 Η υπογραφή του A για το m είναι s.*

[14] Αφού οι *p* και *q* είναι διακεκριμένοι πρώτοι στο *modulus* του RSA,τότε ο αριθμός $\varphi(n) = (p - 1)(q - 1)$ είναι άρτιος. Στο *RSA* ο δημόσιος εκθέτης e πρέπει να ικανοποιεί τη σχέση $(e, \varphi(n)) = 1$ και έτσι πρέπει να είναι περιττός.

2. *Επαλήθευση. Για να επαληθεύσει την υπογραφή s του Α και να ανακτήσει το μήνυμα m ο Β ενεργεί ως εξής:*

2.1 Αποκτά το αυθεντικό δημόσιο κλειδί m του Α.

2.2 Υπολογίζει το $\tilde{m} = s^2 \bmod n$.

2.3 Επαληθεύει ότι το $\tilde{m} \in M_R$. *Αν όχι απορρίπτει την υπογραφή.*

2.4 Ανακτά το $m = R^{-1}(\tilde{m})$.

Παράδειγμα 3.5 *(παραγωγή υπογραφής Rabin με τεχνητά μικρές παραμέτρους)*
Παραγωγή κλειδιού. Η οντότητα Α επιλέγει τους πρώτους p= 7, q = 11 και υπολογίζει το n = 77. Το δημόσιο κλειδί του Α είναι το n = 77 και το ιδιωτικό του το ζεύγος (p=7, q=11). Ο χώρος υπογραφής είναι $Ms=Q_{77}=\{1,4,9,15,16,23,25,36,37,53,58, 60,64,67,71\}$. *Τα τετραγωνικά υπόλοιπα mod 77.*
Για λόγους απλότητας θεωρούμε το M = Ms και τη συνάρτηση πλεονάζουσας πληροφορίας R να είναι η ταυτοτική απεικόνιση ($\tilde{m} = R(m) = m$*).*
Παραγωγή υπογραφής. Έστω m=23 0 Α υπολογίζει το $R(m) = \tilde{m} = 23$ *και στη συνέχεια υπολογίζει μία τετραγωνική ρίζα του* $\tilde{m}$ *modulo 77. Αν το s συμβολίζει μία τέτοια τετραγωνική ρίζα, τότε s =10,32,45 ή 67 (βλ. σημείωση 3.2, εδώ c =* $\tilde{m}$*). Ή. υπογραφή για το m επιλέγεται να είναι το s=45 (η υπογραφή θα μπορούσε να είναι οποιαδήποτε από τις 4 τετραγωνικές ρίζες).*
Επαλήθευση υπογραφής. Ο Β υπολογίζει το $\tilde{m} = s^2 \bmod 77 = 23$. *Αφού* $\tilde{m} = 23 \in M_R$, *ο Β αποδέχεται την υπογραφή και ανακτά το* $m = R^{-1}(\tilde{m}) = 23$.

Σημείωση 3.4 *(πλεονασμός)*

1 *Όπως και στο σχήμα υπογραφής RSA, έτσι και εδώ είναι κρίσιμη μία κατάλληλη επιλογή της συνάρτησης πλεονάζουσας πληροφορίας R για την ασφάλεια του σχήματος υπογραφής. Για παράδειγμα, έστω ότι* $M = M_s = Q_n$ *και* $R(m) = m$, $\forall m \in M$. *Αν ένας «αντίπαλος» επιλέξει οποιονδήποτε ακέραιο* $s \in \mathbb{Z}_n^*$ *και τον υψώσει στο τετράγωνο για να πάρει το* $\tilde{m} = s^2 \bmod n$, *τότε s είναι μία έγκυρη υπογραφή για το* $\tilde{m}$ *και αποκτάται χωρίς τη γνώση του ιδιωτικού κλειδιού (εδώ ο «αντίπαλος» έχει λίγο έλεγχο για το ποια θα είναι η μορφή του μηνύματος). Σε αυτή την περίπτωση η υπαρκτή πλαστογραφία είναι τετριμμένη.*

2. *Στις περισσότερες πρακτικές εφαρμογές σχημάτων ψηφιακής υπογραφής με*

ανάκτηση του μηνύματος, ο χώρος των μηνυμάτων M αποτελείται από ακολουθίες bit κάποιου σταθερού μήκους. Για το σχήμα υπογραφής Rabin,ο καθορισμός της συνάρτησης πλεονάζουσας πληροφορίας αποτελεί μια ενδιαφέρουσα υπόθεση ,αφού υπάρχει περίπτωση το $\tilde{m}$ = R(m) ∉ Q_n, δηλ. το $\tilde{m}$ να μην είναι τετραγωνικό υπόλοιπο modulo n και έτσι ο υπολογισμός μιας τετραγωνικής ρίζας να είναι αδύνατος. Κάποιος ίσως προσπαθήσει να προσαρτήσει ένα μικρό αριθμό τυχαίων bits στο m και να εφαρμόσει ξανά την R με την ελπίδα ότι R(m) ∈ Q_n .Κατά μέσο όρο, δύο τέτοιες απόπειρες θα επαρκούσαν, όμως μια προσδιοριστική (deterministic) μέθοδος θα ήταν προτιμότερη.

3.3 Το τροποποιημένο σχήμα υπογραφής Rabin

Για να ξεπεραστεί το πρόβλημα που αναφέρεται στη σημείωση 3.4(2), χρησιμοποιείται μια τροποποιημένη έκδοση του βασικού σχήματος υπογραφής Rabin. Το τροποποιημένο αυτό σχήμα παρέχει μια προσδιοριστική μέθοδο συσχέτισης των μηνυμάτων με στοιχεία του χώρου υπογραφής Ms, έτσι ώστε ο υπολογισμός μιας τετραγωνικής ρίζας να είναι πάντα εφικτός.

Πόρισμα 3.1 *Έστω p και q διακεκριμένοι πρώτοι καθένας≡(3 mod 4) και έστω $n = p \cdot q$.*

1. *Αν (x,n) = 1, τότε $x^{(p-1)(q-1)/2} \equiv 1 \pmod n$.*
2. *Αν x ∈ Q_n, τότε $x^{(n-p-q+5)/8} \bmod n$ είναι μια τετραγωνική ρίζα του x modulo n.*
3. *Έστω x ένας ακέραιος με σύμβολο Jacobi $(\frac{x}{n}) = 1$ (βλ. παράρτημα) και έστω d= (n-p-q+5)/8.Τότε*

$$x^{2d} \bmod n = \begin{cases} x, & \alpha\nu\ x \in Qn \\ n - x, & \alpha\nu\ x \notin Qn \end{cases} \qquad (2.4)$$

4. *Αν $p \not\equiv q \pmod 8$,τότε $(\frac{2}{n}) = -1$. Γι' αυτό το λόγο ο πολλαπλασιασμός ενός οποιουδήποτε ακεραίου x με 2 ή $2^{-1} \bmod n$ αντιστρέφει το σύμβολο Jacobi του x.*

0 αλγόριθμος 3.10 αποτελεί μια τροποποιημένη έκδοση του σχήματος υπογραφής Rabin. Τα μηνύματα που υπογράφονται προέρχονται από το σύνολο M_s = {m ∈ $\mathbb{Z}_n$: m ≡ 6 (mod 16)}. Η σημειογραφία δίνεται στον πίνακα 3.1. Στην πράξη η συνάρτηση

πλεονάζουσας πληροφορίας πρέπει να είναι πιο πολύπλοκη ώστε να προλαμβάνει τις επιθέσεις υπαρκτής πλαστογραφίας.

Σύμβολο	*Όρος*	*Περιγραφή*
M	*χώρος μηνυμάτων*	$\{ m \in \mathbb{Z}_n: m \leq \lfloor (n-6)/16 \rfloor \}$
Ms	*χώρος υπογραφής*	$\{ m \in \mathbb{Z}_n: m \equiv 6 \pmod{16} \}$
S	*χώρος υπογραφών*	$\{s \in \mathbb{Z}_n: (s^2 \bmod n) \in Ms\}$
R	*συνάρτηση πλεονάζουσας πληροφορίας*	$R(m) = 16m + 6, \forall m \in M$
M_R	*εικόνα της R*	$\{ m \in \mathbb{Z}_n: m \equiv 6 \pmod{16} \}$

***Πίνακας** 3.1 Ορισμός των συνόλων και των συναρτήσεων του αλγορίθμου 3.10.*

Αλγόριθμος 3.9

Παραγωγή κλειδιού για το τροποποιημένο σχήμα υπογραφής Rabin.

Συνοπτικά: Κάθε οντότητα παράγει ένα δημόσιο κλειδί και ένα αντίστοιχο ιδιωτικό. Κάθε οντότητα Α ενεργεί ως εξής:

1. *Επιλέγει τυχαίους πρώτους $p \equiv 3 \pmod 8$, $q \equiv 7 \pmod 8$ και υπολογίζει $n = p \cdot q$.*
2. *Το δημόσιο κλειδί του Α είναι το n, το ιδιωτικό του το $d = (n - p - q + 5)/8$.*

Αλγόριθμος 3.10

Παραγωγή υπογραφής και επαλήθευση.

Συνοπτικά: Η οντότητα Α υπογράφει ένα μήνυμα $m \in M$. Οποιαδήποτε οντότητα Β μπορεί να επαληθεύσει την υπογραφή του Α και να ανακτήσει το μήνυμα m από αυτήν.

1. *Παραγωγή υπογραφής. Ή. οντότητα Α ενεργεί ως ακολούθως:*
   - 1.1 *Υπολογίζει το $\tilde{m} = R(m) = 16m + 6$._*
   - 1.2 *Υπολογίζει το σύμβολο Jacobi, $J = (\frac{\tilde{m}}{n})$ (βλ. παράρτημα).*
   - 1.3 *Αν $J = 1$ υπολογίζει $s = \tilde{m}^d \bmod n$.*
   - 1.4 *Αν $J = -1$ υπολογίζει $s = (\tilde{m}/2)^d \bmod n$[15].*
   - 1.5 *Η υπογραφή του Α για το m είναι s.*

[15] Αν $J \neq 1$ ή -1 τότε $J = 0$, που σημαίνει ότι $(\tilde{m}, n) \neq 1$. Αυτό οδηγεί σε μια παραγοντοποίηση του n. Στην πράξη, η πιθανότητα να συμβεί κάτι τέτοιο είναι αμελητέα.

2. *Επαλήθευση. Για να επαληθεύσει την υπογραφή s του Α και να ανακτήσει το μήνυμα m, ο Β ενεργεί ως εξής:*

2.1 Αποκτά το αυθεντικό δημόσιο κλειδί n του Α.

2.2 Υπολογίζει το $m' = s^2 \bmod n$.

2.3 Αν $m' \equiv 6 \pmod 8$, *παίρνει* $\tilde{m} = m'$.

2.4 Αν $m' \equiv 3 \pmod 8$, *παίρνει* $\tilde{m} — 2\ m'$.

2.5 Αν $m' \equiv 7 \pmod 8$, *παίρνει* $\tilde{m} = n - m'$.

2.6 Αν $m' \equiv 2 \pmod 8$, *παίρνει* $\tilde{m} = 2(n - m')$.

2.7 Επαληθεύει ότι $\tilde{m} \in M_R$ *(βλ. πίνακα 3.1).Αν όχι απορρίπτει την υπογραφή.*

2.8 Ανακτά το $m = R^{-1}(\tilde{m}) = (\tilde{m} - 6)/16$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί.

Κατά την παραγωγή της υπογραφής υπογράφεται είτε το $\upsilon = \tilde{m}$ *είτε το* $\upsilon = \tilde{m}/2$ *αναλόγως ποιο έχει σύμβολο Jacobi ίσο με 1. Από το πόρισμα 3.1(4) ακριβώς ένα από τα* $\tilde{m}, \tilde{m}/2$ *έχει σύμβολο Jacobi 1. Η τιμή υ που υπογράφεται είναι τέτοια ώστε* $\upsilon \equiv 3$ *ή* $6 \pmod 8$. *Από το πόρισμα 2.1(3),* $s^2 \bmod n = \upsilon$ *ή* $n - \upsilon$ *αναλόγως αν το v ανήκει ή όχι στο* Q_η. *Αφού* $n \equiv 5 \pmod 8$ *αυτές οι περιπτώσεις μπορούν να διακριθούν με μοναδικό τρόπο.*

Παράδειγμα 3.6 *(τροποποιημένο σχήμα υπογραφής Rabin με τεχνητά μικρές παραμέτρους)*

Παραγωγή κλειδιού. Ο Α επιλέγει p = 19, q = 31 και υπολογίζει n = pq = 589 και d = (n-p-q+5)/8 = 68. Το δημόσιο κλειδί του Α είναι n = 589 και το ιδιωτικό του κλειδί είναι d = 68. 0 χώρος υπογραφής M_s *δίνεται στον ακόλουθο πίνακα, μαζί με το σύμβολο Jacobi κάθε στοιχείου.*

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

Παραγωγή υπογραφής. Για να υπογράψει ένα μήνυμα m = 12, ο Α υπολογίζει $\tilde{m}$*= R(12) = 198,* $(\frac{\tilde{m}}{n})$ *=* $(\frac{198}{589})$ *= 1 και s =* 198^{68} *mod 589 = 102. Η υπογραφή του Α για το m= 12 είναι s = 102.*

Επαλήθευση υπογραφής .Ο Β υπολογίζει m' = s^2 *mod n =* 102^2 *mod 589 = 391.Αφού* $m' \equiv 7 \pmod 8$*, ο Β παίρνει* $\tilde{m} = n - m' = 589 — 391 = 198$*. Εν τέλει ο Β υπολογίζει m =* $R^{-1}(\tilde{m}) = (198 — 6)/16 = 12$ *και αποδέχεται την υπογραφή.*

Σημείωση 3.5 *(ασφάλεια του τροποποιημένου σχήματος υπογραφής Rabin)*

1. *Όταν κάποιος χρησιμοποιεί τον αλγόριθμο 3.10 δεν θα πρέπει ποτέ να υπογράφει μια τιμή* υ *με σύμβολο Jacobi -1, αφού αυτό οδηγεί σε μια παραγοντοποίηση του n. Για να το δούμε αυτό, παρατηρούμε ότι το* $y = \upsilon^{2d} = s^2$ *πρέπει να έχει σύμβολο Jacobi 1. Όμως* $y^2 \equiv (\upsilon^2)^{2d} \equiv \upsilon^2 \pmod n$ *από το πόρισμα 2.1(3). Επομένως* $(\upsilon - y)(\upsilon + y) \equiv 0 \pmod n$*. Αφού τα υ και y έχουν αντίθετα σύμβολα Jacobi,* $\upsilon \not\equiv y \bmod n$ *τότε* $(\upsilon - y, n) =$ *p ή q .*
2. *Η υπαρκτή πλαστογραφία μπορεί εύκολα να επιτευχθεί για το τροποποιημένο σχήμα υπογραφής Rabin, όπως και για το αρχικό σχήμα Rabin (βλ. σημείωση 3.4(1)). Κάποιος χρειάζεται μόνο να βρει ένα* $s, 1 \leq s \leq n-1$*, τέτοιο ώστε ή το* s^2 *ή το* $n - s^2$ *ή το* $2s^2$ *ή το* $2(n - s^2) \bmod n$ *να είναι* $\equiv 6 \bmod 16$*. Σε οποιαδήποτε από αυτές τις περιπτώσεις, το s είναι μια έγκυρη υπογραφή για το* $m' = s^2 \bmod n$*.*

Σημείωση 3.6 *(χαρακτηριστικά επίδοσης του σχήματος υπογραφής Rabin) Ο αλγόριθμος 3.8 απαιτεί μια συνάρτηση πλεονάζουσας πληροφορίας από το M στο* $M_s = Q_n$ *γεγονός που τυπικά περιλαμβάνει τον υπολογισμό ενός συμβόλου Jacobi. Η παραγωγή υπογραφής τότε περιλαμβάνει τον υπολογισμό τουλάχιστον ενός συμβόλου Jacobi και μιας τετραγωνικής ρίζας modulo n. Ο υπολογισμός της τετραγωνικής ρίζας είναι συγκρίσιμος με μια εκθετοποίηση modulo n. Αφού ο υπολογισμός του συμβόλου Jacobi είναι ισοδύναμος με ένα μικρό αριθμό modular πολλαπλασιασμών, η παραγωγή υπογραφής Rabin δεν είναι σημαντικά περισσότερο εντατική υπολογιστικά από μια παραγωγή υπογραφής RSA με το ίδιο μέγεθος modulus. Η επαλήθευση υπογραφών είναι πολύ γρήγορη αν e = 2 (απαιτεί μόνο έναν modular πολλαπλασιασμό).*

Σημείωση 3.7 *(αποδοτικότητα εύρους ζώνης) Το σχήμα ψηφιακής υπογραφής Rabin είναι όμοιο με το σχήμα RSA όσον αφορά την αποδοτικότητα εύρους ζώνης (βλ.§3.1.5 (6)).*

Κεφάλαιο 4

Σχήματα υπογραφής Fiat-Shamir

Τα σχήματα ψηφιακής υπογραφής που περιγράφονται σε αυτό το κεφάλαιο προκύπτουν από μετατροπές σχημάτων πιστοποίησης ταυτότητας (ή σχημάτων αναγνώρισης) (identification schemes), τα οποία είναι γνωστά ως σχήματα αναγνώρισης πρόκληση και ανταπόκριση (challenge-and-response identification schemes).

Οποιοδήποτε σχήμα αναγνώρισης πρόκληση και ανταπόκριση μπορεί να μετατραπεί σε σχήμα ψηφιακής υπογραφής αντικαθιστώντας την τυχαία πρόκληση (random challenge) της οντότητας που επαληθεύει με μια συνάρτηση κατακερματισμού μονής κατεύθυνσης. Το κεφάλαιο αυτό περιγράφει δύο μηχανισμούς υπογραφής που προκύπτουν με αυτόν τον τρόπο. Πρόκειται για τα σχήματα υπογραφής Feige-Fiat-Shamir και GQ (Guillou-Quisquater), τα οποία προκύπτουν από μετατροπές των ομώνυμων πρωτοκόλλων αναγνώρισης (βλ. παράρτημα).

4.1 Το σχήμα υπογραφής Feige-Fiat-Shamir

Το σχήμα υπογραφής Feige-Fiat-Shamir αποτελεί τροποποίηση ενός προηγούμενου σχήματος υπογραφής των Fiat και Shamir και απαιτεί μια συνάρτηση κατακερματισμού μονής κατεύθυνσης $h : \{0,1\}^* \rightarrow \{0, 1\}^k$ για κάποιο σταθερό θετικό ακέραιο k. Η μέθοδος παρέχει ένα σχήμα ψηφιακής υπογραφής με παράρτημα και αποτελεί έναν τυχαιοποιημένο μηχανισμό.

Αλγόριθμος 4.1

Παραγωγή κλειδιού για το σχήμα υπογραφής Feige-Fiat-Shamir.

Συνοπτικά: Κάθε οντότητα παράγει ένα δημόσιο κλειδί και ένα αντίστοιχο ιδιωτικό. Κάθε οντότητα Α ενεργεί ως εξής:

1. *Παράγει τυχαίους διακεκριμένους κρυφούς πρώτους p,q και υπολογίζει n=pq.*
2. *Επιλέγει έναν θετικό ακέραιο k και διακεκριμένους τυχαίους ακεραίους $s_1,s_2,\ldots,s_k \in \mathbb{Z}_n$.*
3. *Υπολογίζει $u_j = s_j^{-2} \bmod n, 1 \leq j \leq k$.*
4. *Το δημόσιο κλειδί του Α είναι η k-άδα $(u_1,u_2,\ldots,u_k)$ και το modulus n. Το*

ιδιωτικό του κλειδί είναι η k-άδα ($s_1,s_2,\ldots,s_k$).

Αλγόριθμος 4.2

Παραγωγή υπογραφής και επαλήθευση.

Συνοπτικά: Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m αυθαίρετου μήκους. Οποιαδήποτε οντότητα Β μπορεί να επαληθεύσει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Α.

1. *Παραγωγή υπογραφής . Ή οντότητα Α ενεργεί ως ακολούθως:*

   1.1 Επιλέγει έναν τυχαίο ακέραιο $r, 1 \leq r \leq n - 1$.

   1.2 Υπολογίζει $u = r^2 \bmod n$.

   1.3 Υπολογίζει $e = (e_1,e_2,\ldots,e_k) = h(m \,||\, u)$. Κάθε $e_i \in \{0,1\}$.

   1.4 Υπολογίζει $s = r \cdot \prod_{j=1}^{k} s_j^{ej} \bmod n$.

   1.5 Η υπογραφή του Α για το m είναι (e, s).

2. *Επαλήθευση. Για να επαληθεύσει την υπογραφή (e, s) του Α στο m, ο Β ενεργεί ως εξής:*

   2.1 Αποκτά το αυθεντικό δημόσιο κλειδί $(u_1,u_2,\ldots,u_k)$ και n του Α.

   2.2 Υπολογίζει $w = s^2 \cdot \prod_{j=1}^{k} u_j^{ej} \bmod n$.

   2.3 Υπολογίζει $e' = h(m \,||\, w)$.

   2.4 Αποδέχεται την υπογραφή αν και μόνον αν $e = e'$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί.

$$w \equiv s^2 \cdot \prod_{j=1}^{k} u_j^{ej} \bmod n \equiv r^2 \cdot \prod_{j=1}^{k} s_j^{2ej} \prod_{j=1}^{k} u_j^{ej} \equiv r^2 \cdot \prod_{j=1}^{k} (s^2_j\, u_j)^{ej} \equiv r^2 \equiv u \pmod n \qquad (3,1)$$

Επομένως $w = u$ και άρα $e = e'$.

Παράδειγμα 4.1 *(Παραγωγή υπογραφής Feige — Fiat — Shamir με τεχνητά μικρές παραμέτρους)*

Παραγωγή κλειδιού. Ή οντότητα Α παράγει τους πρώτους $p = 3571$, $q = 4523$ και υπολογίζει το $n = pq = 16151633$. Ο ακόλουθος πίνακας περιέχει τους ακεραίους s_j (ιδιωτικό κλειδί του Α) και u_j (δημόσιο κλειδί του Α) μαζί με τις ενδιάμεσες τιμές 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
$v_j = s_j^{-2} \bmod n$	503594	4879739	7104483	1409171	6965302

Παραγωγή υπογραφής. Έστω h : {0,1} → {0,1}^{5} μια συνάρτηση κατακερματισμού. Ο Α επιλέγει έναν τυχαίο ακέραιο r = 23181 και υπολογίζει u = r^2 mod n = 4354872. Για να υπογράψει το μήνυμα m, ο Α υπολογίζει e = h(m || u) = 10110 (για τις ανάγκες του παραδείγματος επινοήσαμε την τιμή κατακερματισμού). Ο Α υπολογίζει s = $rs_1s_3s_4$ mod n = (23181) (42) (85) (101) mod n = 7978909. Η υπογραφή για το m είναι το ζεύγος (e = 10110, s = 7978909).*

Επαλήθευση υπογραφής. Ο Β υπολογίζει s^2 mod n = 2926875 και $u_1u_3u_4$ mod n = (503594)(7104483)(1409171) mod n = 15668174. Ο Β έπειτα υπολογίζει w = s^2 $u_1u_3u_4$ mod n = 4354872. Αφού w = u, έπεται ότι e' = h(m || w) = h(m || u) = e και επομένως ο Β αποδέχεται την υπογραφή.

***Σημείωση 4.1** (ασφάλεια του σχήματος υπογραφής Feige-Fiat-Shamir)*

1. *Σε αντίθεση με το σχήμα υπογραφής RSA (αλγόριθμος 2.4), όλες οι οντότητες μπορούν να χρησιμοποιούν το ίδιο modulus.*
2. *Η ασφάλεια του σχήματος Feige - Fiat — Shamir βασίζεται στη δυσκολία του υπολογισμού τετραγωνικών ριζών modulo n. Το σχήμα έχει αποδειχθεί ασφαλές ενάντια σε προσαρμόσιμες επιθέσεις σε επιλεγμένο μήνυμα, εφόσον η παραγοντοποίηση είναι απρόσιτη, η h είναι τυχαία συνάρτηση και τα s_i είναι διακεκριμένα.*

***Σημείωση 4.2** (επιλογή παραμέτρων και απαιτήσεις για το χώρο αποθήκευσης των κλειδιών) Αν το n είναι ένας ακέραιος t-bit, τότε το ιδιωτικό κλειδί που κατασκευάζεται στον αλγόριθμο 4.1 έχει μέγεθος kt bits.Το μέγεθος αυτό μπορεί να μειωθεί επιλέγοντας τις τυχαίες τιμές s_j, $1 \leq j \leq k$, ως αριθμούς με μήκος bit $t' \leq t$. Το t', ωστόσο, δεν πρέπει να επιλεγεί τόσο μικρό ώστε το να μαντέψει κάποιος τα s_j να είναι εφικτό. Το δημόσιο κλειδί έχει μέγεθος (k + 1)t bits. Για παράδειγμα, αν t=768 και k=128, τότε το ιδιωτικό κλειδί απαιτεί 98304 bits και το δημόσιο 99072 bits.*

***Σημείωση 4.3** (χαρακτηριστικά επίδοσης των υπογραφών Feige-Fiat-Shamir) Με το σχήμα RSA και ένα modulus μήκους t =768, η παραγωγή υπογραφής, χρησιμοποιώντας απλοϊκές τεχνικές, απαιτεί, κατά μέσο όρο, 1152 modular*

πολλαπλασιασμούς. Η παραγωγή υπογραφής για το σχήμα Feige-Fiat-Shamir (αλγόριθμος 4.2) απαιτεί, κατά μέσο όρο, k/2 modular πολλαπλασιασμούς. Για την υπογραφή ενός μηνύματος με το σχήμα αυτό, ένα modulus μήκους t =768 και k =128 απαιτεί, κατά μέσο όρο 64 modular πολλαπλασιασμούς ή λιγότερο από το 6% της δουλειάς που απαιτείται για μια απλοϊκή υλοποίηση του RSA. Η επαλήθευση των υπογραφών απαιτεί μόνο έναν modular πολλαπλασιασμό για το RSA αν ο δημόσιος εκθέτης είναι e = 3 και 64 modular πολλαπλασιασμούς, κατά μέσο όρο, για το σχήμα Feige-Fiat-Shamir. Για εφαρμογές όπου η παραγωγή υπογραφών πρέπει να εκτελείται γρήγορα και ο χώρος αποθήκευσης των κλειδιών δεν είναι περιορισμένος, το σχήμα Feige-Fiat-Shamir ίσως είναι προτιμότερο από το RSA.

4.2 Το σχήμα υπογραφής GQ (Guillou-Quisquater)

Το πρωτόκολλο αναγνώρισης GQ μπορεί να μετατραπεί σε ένα μηχανισμό ψηφιακής υπογραφής (αλγόριθμος 4.4) αν χρησιμοποιηθεί μια συνάρτηση κατακερματισμού μονής κατεύθυνσης .Έστω $h : \{0,1\}^* \rightarrow \mathbb{Z}_n$ μια συνάρτηση κατακερματισμού, όπου n είναι ένας θετικός ακέραιος.

Αλγόριθμος 4.3

Παραγωγή κλειδιού για το σχήμα υπογραφής GQ.

Συνοπτικά: Κάθε οντότητα παράγει ένα δημόσιο κλειδί (n, e, J_A) και ένα αντίστοιχο ιδιωτικό κλειδί α. Η οντότητα Α ενεργεί ως εξής:

1. *Επιλέγει τυχαίους διακεκριμένους κρυφούς πρώτους p,q και υπολογίζει $n = pq$.*
2. *Επιλέγει έναν ακέραιο $e \in \{1,2, \ldots, n-1\}$ τέτοιον ώστε $(e, \varphi(n)) = 1$.*
3. *Επιλέγει έναν ακέραιο J_A, $1 < J_A < n$, το οποίο χρησιμεύει ως αναγνωριστικό του Α και είναι τέτοιο ώστε $(J_A, n) = 1$. (Η δυαδική αναπαράσταση του J_A θα μπορούσε να χρησιμοποιηθεί για τη μεταφορά πληροφοριών σχετικών με τον Α όπως όνομα, διεύθυνση, αριθμός άδειας οδήγησης, κτλ.)*
4. *Καθορίζει έναν ακέραιο $\alpha \in \mathbb{Z}_n$ τέτοιον ώστε $J_A a^e \equiv 1 \pmod n$ ως ακολούθως:*
   - *4.1 Υπολογίζει $J_A^{-1} \bmod n$.*
   - *4.2 Υπολογίζει $d_1 = e^{-1} \bmod (p - 1)$ και $d_2 = e^{-1} \bmod (q - 1)$.*

4.3 Υπολογίζει $\alpha_1 = (J_A^{-1})^{d1} \bmod p$ *και* $\alpha_2 = (J_A^{-1})^{d2} \bmod q$.

4.4 Υπολογίζει μια λύση α που ικανοποιεί ταυτοχρόνως τις ισοτιμίες $\alpha \equiv \alpha_1 \pmod p$, $\alpha \equiv \alpha_2 \pmod q$.

5. Το δημόσιο κλειδί του Α είναι (n, e, J_A). *Το ιδιωτικό του κλειδί είναι α.*

Αλγόριθμος 4.4

Παραγωγή υπογραφής GQ και επαλήθευση.

Συνοπτικά: Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m αυθαίρετου μήκους. Οποιαδήποτε οντότητα Β μπορεί να επαληθεύσει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Α.

1. Παραγωγή υπογραφής. Η οντότητα Α ενεργεί ως ακολούθως:

1.1 Επιλέγει έναν τυχαίο ακέραιο k και υπολογίζει $r = k^e \bmod n$.

1.2 Υπολογίζει $l = h(m \,||\, r)$.

1.3 Υπολογίζει $s = ka^l \bmod n$.

1.4 Η υπογραφή του Α για το m είναι το ζεύγος (s, l).

2. Επαλήθευση. Για. να επαληθεύσει την υπογραφή (s,l) του Α στο m, ο Β ενεργεί ως εξής:

2.1 Αποκτά το αυθεντικό δημόσιο κλειδί (n,e, J_A) *του Α.*

2.2 Υπολογίζει $u = s^e J_A \bmod n$ *και* $l' = h(m \,||\, u)$.

2.3 Αποδέχεται την υπογραφή αν και μόνον αν $l = l'$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί.

$$u \equiv s^e J_A^{\,l} \equiv (ka^l)^e J_A^{\,l} \equiv k^e (a^e J_A)^l \equiv k^e \equiv r (\mathrm{mod} n). \qquad (3.2)$$

Επομένως $u = r$ *και άρα* $l = l'$.

Παράδειγμα 4.2 *(Παραγωγή υπογραφής GQ με τεχνητά μικρές παραμέτρους) Παραγωγή κλειδιού. Η οντότητα Α επιλέγει τους πρώτους* $p = 20849$, $q = 27457$ *και υπολογίζει το* $n = pq = 572450993$. *Ο Α επιλέγει έναν ακέραιο* $e = 47$, *ένα αναγνωριστικό* $J_A = 1091522$ *και λύνει την ισοτιμία* $J_A a^e = 1 \pmod n$ *για να βρει το α =*

214611724. Το δημόσιο κλειδί του Α είναι η τριάδα (n = 572450993, e = 47, J_A = 1091522), ενώ το ιδιωτικό του κλειδί είναι a = 214611724.

Παραγωγή υπογραφής. Για να υπογράψει το μήνυμα m = 1101110001, ο Α επιλέγει έναν τυχαίο ακέραιο k = 42134 και υπολογίζει r = k^e mod n = 297543350. Στη συνέχεια ο Α υπολογίζει l = h(m || r) = 2713833 (η τιμή κατακερματισμού επινοήθηκε για τις ανάγκες του παραδείγματος) και s = ka^l mod n = (42134)$214611724^{2713833}$mod n = 252000854. Η υπογραφή του Α για το m είναι το ζεύγος (s = 252000854, l = 2713833). Επαλήθευση υπογραφής. Ο Β υπολογίζει s^e mod n= 252000854^{47}mod n = 398641962, J_A^l mod n = $1091522^{2713833}$ mod n = 110523867 και τελικά u = $s^e J_A^l$ mod n =297543350. Αφού u = r,l' = h(m || u) = h(m || r) = l ο Β αποδέχεται την υπογραφή.

Σημείωση 4.4 *(ασφάλεια του σχήματος υπογραφής GQ) Στον αλγόριθμο 4.3, το e πρέπει να είναι επαρκώς μεγάλο ώστε να αποκλείεται η πιθανότητα πλαστογράφησης που βασίζεται στο παράδοξο των γενεθλίων (βλ. [MOV96], κεφ.2). Η ενδεχόμενη επίθεση περιγράφεται ως εξής: ο «αντίπαλος» επιλέγει ένα μήνυμα m και υπολογίζει l = h(m || J_A^t) για επαρκώς πολλές τιμές του t μέχρι l ≡ t (mod e). Αυτό αναμένεται να συμβεί μέσα σε 0(√e) δοκιμές. Έχοντας καθορίσει ένα τέτοιο ζεύγος (l,t), ο «αντίπαλος» καθορίζει έναν ακέραιο x τέτοιον ώστε t = xe +l και υπολογίζει s = J_A^x mod n. Παρατηρούμε ότι $s^e J_A^l \equiv (J_A^x)^e J_A^l \equiv J_A^{xe+l} \equiv J_A^t$(mod n) και γι' αυτό h(m || J_A^t) = l. Έτσι το ζεύγος (s, l) είναι μια έγκυρη (πλαστογραφημένη) υπογραφή του μηνύματος m.*

Σημείωση 4.5 *(επιλογή παραμέτρων) Οι σύγχρονες μέθοδοι (από το 1996) για την παραγοντοποίηση των ακεραίων συνιστούν ότι είναι συνετή η χρήση ενός modulus με μέγεθος τουλάχιστον 768 bits. Το e πρέπει να έχει μέγεθος τουλάχιστον 128 bits.*

Τυπικές τιμές για το μέγεθος των τιμών κατακερματισμού είναι 128 ή 160 bits. Με ένα 768-bit modulus και ένα 128-bit e, το δημόσιο κλειδί για το σχήμα GQ έχει μέγεθος 896+u bits, όπου u είναι το πλήθος των bits που απαιτούνται για τη δυαδική αναπαράσταση του J_A. Το ιδιωτικό κλειδί α έχει μέγεθος 768 bits.

Σημείωση 4.6 *(χαρακτηριστικά επίδοσης των υπογραφών GQ) Η παραγωγή υπογραφής για το σχήμα GQ (αλγόριθμος 4.4) απαιτεί δυο modular εκθετοποιήσεις και έναν modular πολλαπλασιασμό. Χρησιμοποιώντας ένα 768-bit modulus n, μια 128-bit τιμή e και μια συνάρτηση κατακερματισμού με τιμές l μήκους 128-bit η*

παραγωγή υπογραφής (χρησιμοποιώντας απλοϊκές τεχνικές για την εκθετοποίηση) απαιτεί, κατά μέσο όρο, 384 modular πολλαπλασιασμούς. Η επαλήθευση των υπογραφών απαιτεί παρόμοιο μέγεθος δουλειάς. Το GQ είναι υπολογιστικά περισσότερο εντατικό από το Feige-Fiat-Shamir απαιτεί όμως σημαντικά μικρότερο χώρο αποθήκευσης για τα κλειδιά (βλ. σημείωση 4.5).

Σημείωση 4.7 *(το σχήμα GQ με ανάκτηση του μηνύματος) Ο αλγόριθμος 4.4 μπορεί να τροποποιηθεί ως ακολούθως ώστε να παρέχει ανάκτηση του μηνύματος. Έστω ότι ο χώρος υπογραφής M_s είναι το σύνολο $\mathbb{Z}_n$ και έστω ένα μήνυμα $m \in M_s$. Κατά την παραγωγή της υπογραφής επιλέγουμε ένα τυχαίο k τέτοιο ώστε (k,n) = 1 και υπολογίζουμε $r = k^e \bmod n$ και $l = mr \bmod n$. Η υπογραφή είναι $s = ka^l \bmod n$. Η επαλήθευση δίνει $s^e J A^l \equiv k^e a^{el} J_A{}^l \equiv k^e \equiv r \pmod n$. Το μήνυμα m ανακτάται από το $lr^{-1} \bmod n$. Όπως για όλα τα σχήματα ψηφιακής υπογραφής με ανάκτηση του μηνύματος, έτσι και εδώ απαιτείται μια κατάλληλη συνάρτηση πλεονάζουσας πληροφορίας για την αντιμετώπιση επιθέσεων υπαρκτής πλαστογραφίας.*

Κεφάλαιο 5

Το DSS και σχετικά σχήματα υπογραφής

*Στο κεφάλαιο αυτό παρουσιάζουμε το **Πρότυπο Ψηφιακής Υπογραφής** (Digital Signature Standard-DSS) και μερικά συγγενή σχήματα υπογραφής. Τα περισσότερα από αυτά παρουσιάζονται στο $\mathbb{Z}_p^*$ για κάποιο μεγάλο πρώτο p, αλλά όλοι αυτοί οι μηχανισμοί μπορούν να γενικευθούν σε οποιαδήποτε πεπερασμένη κυκλική ομάδα. Όλες οι μέθοδοι αυτού του κεφαλαίου είναι τυχαιοποιημένα σχήματα ψηφιακής υπογραφής. Όλα δίνουν ψηφιακές υπογραφές με παράρτημα και μπορούν να τροποποιηθούν ώστε να δώσουν ψηφιακές υπογραφές με ανάκτηση του μηνύματος (βλ. σημείωση 2.6) .Απαραίτητη προϋπόθεση για την ασφάλεια όλων των σχημάτων υπογραφής που περιγράφονται σε αυτό το κεφάλαιο είναι ότι ο υπολογισμός λογαρίθμων στο $\mathbb{Z}_p^*$ πρέπει να είναι υπολογιστικά ανέφικτος. Αυτή η προϋπόθεση, ωστόσο, δεν είναι απαραιτήτως επαρκής για την ασφάλεια αυτών των σχημάτων.*

5.1 Το σχήμα υπογραφής El Gamal

5.1.1 Το πρόβλημα διακριτού λογαρίθμου (Discrete Logarithm Problem-DLP)

Στο 3ο κεφάλαιο είδαμε ότι η ασφάλεια του κρυπτοσυστήματος RSA και κατ'επέκταση του σχήματος υπογραφής RSA βασίζεται στη δυσκολία του προβλήματος της παραγοντοποίηση ενός μεγάλου ακεραίου σε πρώτους παράγοντες.

*Με την εξέλιξη της κρυπτογραφίας επινοήθηκαν κρυπτοσυστήματα που στήριζαν την ασφάλεια τους σε δυσεπίλυτα προβλήματα της θεωρίας αριθμών, όπως το **Πρόβλημα Διακριτού Λογαρίθμου (Discrete Logarithm Problem-DLP)** και το **Πρόβλημα των Diffie-Hellman (Diffie-Hellman Problem-DHP).***

Η ασφάλεια πολλών κρυπτογραφικών τεχνικών βασίζεται στη δυσκολία επίλυσης των δύο παραπάνω προβλημάτων. Μια από αυτές είναι το κρυπτοσύστημα δημοσίου κλειδιού ElGamal και το ομώνυμο σχήμα υπογραφής.

5.2 Το σχήμα El Gamal

Υποθέτουμε ότι ο Α θέλει να στείλει στον Β το μήνυμα m υπογεγραμμένο ψηφιακά με το El Gamal χρησιμοποιώντας το κλειδί K=(p,q,g,α,β)

1. **Δημιουργία Υπογραφής :**
   i. Ο Α στέλνει έναν τυχαίο $k \in \mathbb{Z}_{p-1}^*$.
   ii. Ο Α υπολογίζει τα

$$\gamma = g^k \bmod p \qquad (1)$$

και

$$\delta = (m - \alpha\gamma)k^{-1} \pmod{p-1} \qquad (2)$$

   iii. Η ψηφιακή υπογραφή του Α για το μήνυμα m για το τυχαία επιλεγμένο k είναι η $sig_k(m,k) = (\gamma,\delta)$. Εδώ παρατηρούμε ότι η συνάρτηση sig_k παίρνει ένα επιπλέον όρισμα από τη γενική της μορφή, για να δουλέψει για το συγκεκριμένο κρυπτοσύστημα . Μπορεί λοιπόν κάνεις να την ορίσει εκ νέου σα συνάρτηση από το $M \times \mathbb{Z}_{p-1}^*$ στο S.
   iv. Ο Α στέλνει στον Β τριάδα (m,γ,δ), ήτοι το αρχικό του κείμενο με την ψηφιακή του υπογραφή (Εδώ φαίνετε ότι το El Gamal ανήκει στα Σχήματα Υπογραφής με ικανότητα ανάκτησης του μηνύματος) .

2. **Επαλήθευση Υπογραφής**

Ο Β υπολογίζει την τιμή της συνάρτησης:

$$ver_k(m,\gamma,\delta) = \begin{cases} αληθής, & αν\ \beta^{\gamma}\gamma^{\delta} \equiv g^m \bmod p \\ ψευδής, & αλλιώς. \end{cases}$$

Και πιστοποιεί ότι το μήνυμα m προέρχεται πράγματι από τον Α αν και μόνον αν $ver_k(m,\gamma,\delta) = αληθής$.

Λήμμα 5.2.1: Αν p πρώτος και g πρωταρχικό του $\mathbb{Z}_p^*$ (δηλ., $g^{p-1} \equiv 1 \pmod p$), *τότε για κάθε* $x, y \in \mathbb{Z}$ *ισχύει*

$g^x \equiv g^y \pmod p \Leftrightarrow x \equiv y \pmod{p-1}$

Απόδειξη: *Αν τα* $x, y < p-1$ *το λήμμα ισχύει κατά προφανή τρόπο.*

Θεωρώ τώρα ότι κάποιο x, y είναι μεγαλύτερο από p-1 (χωρίς βλάβη της γενικότητας έστω p-1 x>p-1). Προφανώς τότε θα υπάρχουν φυσικοί $\delta, \upsilon > 0, \upsilon < p-$

1 τέτοιοι που x=δ(p-1)+ υ (ήτοι το πηλίκο και το υπόλοιπο της ακεραίας διαίρεσης του x με τον p-1). Όμως τότε

$$g^x \equiv g^{\delta(p-1)+\upsilon} \equiv g^{\delta(p-1)}\, g^{\upsilon} \equiv g^{k\delta} \pmod p$$

Ανάλογα το αποδεικνύουμε και για τις περιπτώσεις y>p-1 και x,y>p-1.

Σημείωση 5.3 *(χαρακτηριστικά επίδοσης των υπογραφών ElGamal)*

1. *Η παραγωγή υπογραφής είναι σχετικά γρήγορη, αφού απαιτεί μια modular εκθετοποίηση (a^k mod p), εφαρμογή του επεκτεταμένου Ευκλείδιου αλγόριθμου (για τον υπολογισμό του k^{-1} mod (p - 1)) και δύο modular πολλαπλασιασμούς.*
2. *Η επαλήθευση των υπογραφών είναι περισσότερο δαπανηρή, αφού απαιτούνται τρείς modular εκθετοποιήσεις. Κάθε εκθετοποίηση (χρησιμοποιώντας απλοϊκές τεχνικές) απαιτεί, κατά μέσο όρο, $\frac{3}{2}\lceil lgp \rceil$ modular πολλαπλασιασμούς, για ένα συνολικό κόστος $\frac{9}{2}\lceil lgp \rceil$ πολλαπλασιασμών. Τα κόστη των υπολογισμών μπορούν να ελαττωθούν τροποποιώντας ελαφρώς την επαλήθευση. Υπολογίζουμε $u_1 = a^{-h(m)} y^r r^s$ mod p και δεχόμαστε την υπογραφή ως έγκυρη αν και μόνον αν $u_1 = 1$. Το u_1 τώρα μπορεί να υπολογιστεί αποδοτικότερα εκτελώντας συγχρόνως τις τρείς εκθετοποιήσεις. Το τελικό κόστος είναι τώρα περίπου $\frac{15}{8}\lceil lgp \rceil$ modular πολλαπλασιασμοί, σχεδόν 2.5 φορές αποδοτικότερα σε σχέση με πριν.*
3. *Οι υπολογισμοί για την επαλήθευση των υπογραφών εκτελούνται modulo p, ενώ οι υπολογισμοί για την παραγωγή των υπογραφών εκτελούνται modulo p και modulo (p-1).*

Σημείωση 5.4 *(προτεινόμενα μεγέθη των παραμέτρων) Σύμφωνα με την τελευταία πρόοδο σχετικά με το DLP στο $\mathbb{Z}_p$*, ένα 512-bit modulus p παρέχει μόνο οριακή ασφάλεια ενάντια σε μια συντονισμένη επίθεση. Από το 1996, προτείνεται ένα modulus p τουλάχιστον 768 bits. Για μακρόχρονη ασφάλεια πρέπει να χρησιμοποιούνται moduli 1024-bit ή μεγαλύτερα.*

Σημείωση 5.5 *(γενικές παράμετροι) Όλες οι οντότητες μπορούν να επιλέξουν τον ίδιο πρώτο αριθμό p και τον ίδιο γεννήτορα α. Σε αυτήν την περίπτωση οι p και α δεν χρειάζεται να αποτελούν μέρος του δημοσίου κλειδιού.*

Παραλλαγές του σχήματος υπογραφής ElGamal

Έχουν προταθεί πολλές παραλλαγές του σχήματος υπογραφής ElGamal. Οι περισσότερες από αυτές τροποποιούν αυτό που συνήθως αναφέρεται ως εξίσωση υπογραφής (δίνεται στο βήμα 2.4 του αλγορίθμου 5.3). Μετά από κατάλληλη επαναδιάταξη, αυτή η εξίσωση υπογραφής μπορεί να γραφεί ως u = α v + kw mod (p-1), όπου v = h(m), u = r και w = s (δηλ., h(m) = ar + ks mod (p - 1)). Άλλες εξισώσεις υπογραφής μπορούν να αποκτηθούν επιτρέποντας στα u,v και w να πάρουν τις τιμές s,r και h(m) με διαφορετική σειρά. Ο πίνακας 5.1 περιέχει τις 6 δυνατές περιπτώσεις.

	u	v	w	Εξίσωση υπογραφής	Επαλήθευση
1	$h(m)$	r	s	$h(m) = ar + ks$	$\alpha^{h(m)} = (\alpha^a)^r r^s$
2	$h(m)$	s	r	$h(m) = as + kr$	$\alpha^{h(m)} = (\alpha^a)^s r^r$
3	s	r	$h(m)$	$s = ar + kh(m)$	$\alpha^s = (\alpha^a)^r r^{h(m)}$
4	s	$h(m)$	r	$s = ah(m) + kr$	$\alpha^s = (\alpha^a)^{h(m)} r^r$
5	r	s	$h(m)$	$r = as + kh(m)$	$\alpha^r = (\alpha^a)^s r^{h(m)}$
6	r	$h(m)$	s	$r = ah(m) + ks$	$\alpha^r = (\alpha^a)^{h(m)} r^s$

Πίνακας 5.1 *Παραλλαγές της εξίσωσης υπογραφής ElGamal. Οι εξισώσεις υπογραφής υπολογίζονται modulo (p-1), ενώ η επαλήθευση modulo p.*

Σημείωση 5.6 *(σύγκριση των παραλλαγών του σχήματος υπογραφής ElGamal)*

1. *Κάποιες από τις εξισώσεις υπογραφής που περιέχονται στον πίνακα 5.1 είναι αποδοτικότερες ως προς τον υπολογισμό τους από ότι η αρχική εξίσωση ElGamal του αλγορίθμου 5.4. Για παράδειγμα, οι εξισώσεις (3) και (4) δεν απαιτούν τον υπολογισμό ενός αντιστρόφου για τον καθορισμό της υπογραφής s. Οι εξισώσεις (2) και (5) απαιτούν από τον υπογράφοντα τον υπολογισμό του $\alpha^{-1} \bmod (p-1)$, αλλά αυτή η σταθερή ποσότητα χρειάζεται να υπολογιστεί μόνο μια φορά.*
2. *Οι εξισώσεις επαλήθευσης (2) και (4) περιέχουν την έκφραση r^r. Μέρος της ασφάλειας σχημάτων υπογραφής που βασίζονται σε αυτές τις εξισώσεις υπογραφής είναι η δυσκολία εύρεσης λύσεων μιας έκφρασης της μορφής $x^x \equiv c \pmod p$ με c σταθερό. Το πρόβλημα αυτό φαίνεται απρόσιτο για μεγάλες*

τιμές του p, αλλά δεν έχει λάβει την ίδια προσοχή με το DLP.

Σημείωση 5.7 *(το γενικευμένο σχήμα υπογραφής ElGamal) Μέχρι τώρα περιγράψαμε το σχήμα ψηφιακής υπογραφής ElGamal πάνω στην πολλαπλασιαστική ομάδα $\mathbb{Z}_p^*$. Το σχήμα μπορεί να γενικευθεί με έναν άμεσο τρόπο ώστε να λειτουργεί πάνω σε οποιαδήποτε πεπερασμένη αβελιανή ομάδα G (βλ. [MOV96], κεφ. 11).*

5.3 Το Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard-DSS)

Τον Αύγουστο του 1991,το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Ηνωμένων Πολιτειών (U.S. National Institute of Standards and Technology-NIST) πρότεινε ένα Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard-DSS), βασισμένο στο σχήμα υπογραφής ElGamal .Το DSS είναι το πρώτο σχήμα ψηφιακής υπογραφής που αναγνωρίστηκε από οποιαδήποτε κυβέρνηση. Αποτελεί μια παραλλαγή του σχήματος ElGamal που προσπαθεί να μειώσει το μέγεθος της παραγόμενης υπογραφής και είναι ένα σχήμα ψηφιακής υπογραφής με παράρτημα.

Ο μηχανισμός υπογραφής απαιτεί μια συνάρτηση κατακερματισμού $h : \{0,1\}^* \rightarrow \mathbb{Z}_q$ για κάποιον ακέραιο q. Το DSS απαιτεί τη χρήση του αλγορίθμου κατακερματισμού SHA - 1 (Secure Hash Algorithm) ([MOV96], κεφ.9, αλγόριθμος 9.53).

Λήμμα 5.2 *Έστω p πρώτος και q τέτοιος ώστε $q|(p-1)$.Αν α_0 είναι πρωταρχικό στοιχείο του $\mathbb{Z}_p^*$, τότε το*

$$a = \alpha_0^{(p-1)/q}$$

είναι q-στη ρίζα της μονάδας modulo p, δηλαδή $a^q \equiv 1 \pmod p$.

Απόδειξη $a^q \equiv (\alpha_0^{(p-1)/q})^q \equiv \alpha_0^{p-1} \equiv 1 \pmod p$*,αφού το α_0 είναι πρωταρχικό στοιχείο του $\mathbb{Z}_p^*$.*

Αλγόριθμος 5.5

Παραγωγή κλειδιού για το DSS.

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

1. *Επιλέγει έναν πρώτο q τέτοιον ώστε $2^{159} < q < 2^{160}$*

2. *Επιλέγει ένα t τέτοιο ώστε $0 \leq t \leq 8$ και έναν πρώτο p όπου $2^{511+64t} < p < 2^{512+64t}$, με την ιδιότητα ότι $q \mid (p - 1)$.*

3. *(Επιλέγει ένα γεννήτορα α της μοναδικής κυκλικής ομάδας τάξεως q του $\mathbb{Z}_p^*$)*

3.1 Επιλέγει ένα στοιχείο $g_0 \in \mathbb{Z}_p^*$ και υπολογίζει $g = g_0^{(p-1)/q} \bmod p$.

3.2 Αν g = 1 τότε επιστρέφει στο βήμα 3.1.

4. *Επιλέγει έναν τυχαίο ακέραιο α τέτοιον ώστε $1 \leq \alpha \leq q - 1$. Αυτός θα είναι το ιδιωτικό κλειδί του Α.*

5. *Υπολογίζει το $y = g^a \bmod p$.*

6. *Το δημόσιο κλειδί του Α είναι (p,q,g,y). Το ιδιωτικό του κλειδί είναι α.*

Σημείωση 5.9 *(παραγωγή των πρώτων p και q) Στον αλγόριθμο 5.1 πρέπει κάποιος πρώτα να επιλέξει τον πρώτο q και στη συνέχεια να προσπαθήσει να βρει έναν πρώτο p τέτοιον ώστε $q \mid (p - 1)$ ([MOV96], κεφ.4, αλγόριθμος 4.56).*

Αλγόριθμος 5.6

Παραγωγή υπογραφής και επαλήθευση.

Συνοπτικά: Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m αυθαίρετου μήκους. Οποιαδήποτε οντότητα Β μπορεί να επαληθεύσει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Α.

1. Παραγωγή υπογραφής. Ή οντότητα Α ενεργεί ως εξής:

1.1 Επιλέγει έναν τυχαίο κρυφό ακέραιο $k, 0 < k < q$.

1.2 Υπολογίζει $r = (g^k \bmod p) \bmod q$ (βλ. παράρτημα).

1.3 Υπολογίζει $k^{-1} \bmod q$ (βλ. παράρτημα).

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

1.4 Η υπογραφή του Α για το m είναι το ζεύγος (r, s).

2. Επαλήθευση. Για να επαληθεύσει την υπογραφή (r, s) του Α στο m, ο Β ενεργεί ως εξής:

2.1 Αποκτά το αυθεντικό δημόσιο κλειδί του Α,(p,q,g,y).

2.2 Επαληθεύει ότι $0 < r < q$ και $0 < s < q$. Αν όχι, απορρίπτει την υπογραφή.

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

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

2.5 Υπολογίζει $\upsilon = (g^{u1} y^{u2} \bmod p) \bmod q$.

2.6 Αποδέχεται την υπογραφή αν και μόνον αν $\upsilon = r$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτούργει.

Αν (r, s) είναι μια νόμιμη υπογραφή της οντότητας Α για το μήνυμα m, τότε πρέπει να ισχύει $h(m) \equiv -gr + ks \pmod q$. Πολλαπλασιάζοντας και τα δυο μέλη αυτής της ισοτιμίας με w παίρνουμε $w \cdot h(m) + grw \equiv k \pmod q$,δηλαδή την ισοτιμία $u_1 + gu_2 \equiv k \pmod q$. Υψώνοντας το g και στα δυο μέλη της τελευταίας εξίσωσης παίρνουμε $(g^{u1} y^{u2} \bmod p) \bmod q = (g^k \bmod p) \bmod q$. Επομένως υ = r, όπως απαιτείται.

Παράδειγμα 5.4 *(παραγωγή υπογραφής DSS με τεχνητά μικρές παραμέτρους) Παραγωγή κλειδιού. Ο Α επιλέγει τους πρώτους p = 227 και q = 113 έτσι ώστε $q|(p-1)$. Εδώ $(p-1)/q = 2$. Ο Α επιλέγει ένα τυχαίο στοιχείο $g = 152 \in \mathbb{Z}_p^*$ και υπολογίζει $\alpha = g^2 \bmod p = 177$. Αφού $\alpha \neq 1$, το g είναι γεννήτορας της μοναδικής κυκλικής υποομάδας τάξεως q του $\mathbb{Z}_p^*$. Ο Α ύστερα επιλέγει έναν τυχαίο ακέραιο $\alpha = 53$ υπό την απαίτηση $1 \leq \alpha \leq q - 1$ και υπολογίζει το $y = g^a \bmod p = 177^{53} \bmod 227 = 84$. Το δημόσιο κλειδί του Α είναι η τετράδα (p = 227, q = 113, g = 177, y = 84),ενώ το ιδιωτικό του κλειδί είναι α = 53.*

Παραγωγή υπογραφής. Για να υπογράψει το μήνυμα m, ο Α επιλέγει έναν τυχαίο ακέραιο k = 91 και υπολογίζει το $r = (g^k \bmod p) \bmod q = (177^{91} \bmod 227) \bmod 113 = 167 \bmod 113 = 54$. Στη συνέχεια ο Α υπολογίζει $k^{-1} \bmod q = 77$, h(m)= 5246 (και πάλι η τιμή κατακερματισμού επινοήθηκε για τις ανάγκες του παραδείγματος) και τελικά $s = (77)\{5246 + (53)(54)\} \bmod q = 104$.Η υπογραφή του m είναι το ζεύγος (r = 54, s = 104).

Επαλήθευση υπογραφής. Ο Β υπολογίζει $w = s^{-1} \bmod q = 25$, $u_1 = w \cdot h(m) \bmod q = (25)(5246) \bmod 113 = 70$ και $u_2 = rw \bmod q = (54)(25) \bmod 113 = 107$. Έπειτα υπολογίζει $\upsilon = (g^{u1} y^{u2} \bmod p) \bmod q = (177^{70} \cdot 84^{107} \bmod 227) \bmod 113 = 167 \bmod 113 = 54$. Εφόσον υ= r, ο Β αποδέχεται την υπογραφή.

Σημείωση 5.10 *(ασφάλεια του DSS) Παρατηρώντας το DSS βλέπουμε ότι όλοι οι μετασχηματισμοί γίνονται μέσα σε μια υποομάδα του $\mathbb{Z}_p^*$ μεγέθους 2^{160}. Η ασφάλεια του σχήματος στηρίζεται στην εικασία ότι η επίλυση του DLP είναι «πολύ δύσκολη» σε μια τέτοια υποομάδα του $\mathbb{Z}_p^*$.*

Σημείωση 5.11 *(προτεινόμενα μεγέθη των παραμέτρων) Το μέγεθος του q καθορίζεται από τον αλγόριθμο 5.5 στα 160-bit, ενώ το μέγεθος του p μπορεί να είναι οποιοδήποτε πολλαπλάσιο του 64 μεταξύ των 512 και 1024 bits (συμπεριλαμβανομένων και των τιμών αυτών). Ένας 512-bit πρώτος p παρέχει οριακή ασφάλεια απέναντι σε μια συντονισμένη επίθεση. Από το 1996, προτείνεται ένα modulus τουλάχιστον 768 bits. Τέλος δεν επιτρέπεται ο πρώτος p να υπερβαίνει σε μέγεθος τα 1024 bits.*

Σημείωση 5.12 *(χαρακτηριστικά επίδοσης του DSS) Ας υποθέσουμε ότι ο p είναι ένας ακέραιος 768-bit. Η παραγωγή υπογραφής απαιτεί μια modular εκθετοποίηση η οποία, κατά μέσο όρο, χρειάζεται (χρησιμοποιώντας απλοϊκές τεχνικές) 240 modular πολλαπλασιασμούς, μια modular αντιστροφή με ένα 160-bit modulus, δύο 160-bit modular πολλαπλασιασμούς και μια πρόσθεση. Οι πράξεις που εκτελούνται με 160-bit modulus είναι σχετικά ασήμαντες συγκρινόμενες με την εκθετοποίηση.Το DSS έχει το πλεονέκτημα ότι η εκθετοποίηση μπορεί να προϋπολογιστεί και να μη χρειαστεί να εκτελεστεί κατά την παραγωγή της υπογραφής.*

Ο κύριος όγκος δουλειάς για την επαλήθευση των υπογραφών είναι δύο εκθετοποιήσεις modulo p, καθεμία σε εκθέτες μεγέθους 160-bit. Κατά μέσο όρο, κάθε εκθετοποίηση απαιτεί 240 modular πολλαπλασιασμούς άρα 480 συνολικά. Κάποια μείωση στο κόστος μπορεί να επιτευχθεί εκτελώντας συγχρόνως τις δύο εκθετοποιήσεις. Το κόστος είναι τότε, κατά μέσο όρο, 280 modular πολλαπλασιασμοί.

Σημείωση 5.13 *(γενικές παράμετροι) Δεν είναι απαραίτητο κάθε οντότητα να επιλέξει τους δικούς της πρώτους p και q. Το DSS επιτρέπει οι p,q και g να είναι γενικές παράμετροι σε ένα σύστημα που χρησιμοποιεί το DSS. Τότε όμως το σχήμα αποτελεί πιο ελκυστικό στόχο για έναν «αντίπαλο».*

Σημείωση 5.14 *(πιθανότητα αποτυχίας) Η επαλήθευση απαιτεί τον υπολογισμό του $s^{-1} \bmod q$.Αν $s = 0$, τότε το s^{-1} δεν υπάρχει. Για να αποφευχθεί αυτό, ο υπογράφων μπορεί να ελέγξει ότι $s \neq 0$. Αν όμως υποθέσουμε ότι το s είναι ένα τυχαίο στοιχείο του $\mathbb{Z}_q$, τότε η πιθανότητα το s να είναι 0 είναι $(\frac{1}{2})^{160}$. Στην πράξη, αυτό είναι εξαιρετικά απίθανο να συμβεί. Ο υπογράφων μπορεί επίσης να ελέγξει αν το r είναι*

$\neq 0$. *Αν κάποιο από τα r ή s προκύψει ίσο με 0, τότε πρέπει να παραχθεί μια νέα τιμή για το k.*

Παρατήρηση 5.2

1. *Παρατηρούμε ότι στις εξισώσεις υπογραφής για το ElGamal (βήμα 2.4, αλγόριθμος 5.4) και το DSS (βήμα 2.4, αλγόριθμος 5.6) υπάρχει μια διαφορά στο πρόσημο. Η διαφορά αυτή αποτελεί το λόγο για την αλλαγή της συνάρτησης επαλήθευσης.*
2. *Το γεγονός ότι όλοι οι υπολογισμοί για την παραγωγή μιας υπογραφής γίνονται modulo q, κάνει το μέγεθος της υπογραφής πολύ μικρότερο από την αντίστοιχη για το ElGamal. Για παράδειγμα, έστω ότι ο p είναι ένας πρώτος μεγέθους 768-bit. Τότε το ElGamal θα παράγει μια υπογραφή μεγέθους 1536-bit, ενώ το DSS μια υπογραφή μεγέθους 320-bit.*

5.4 Το σχήμα υπογραφής ElGamal με ανάκτηση του μηνύματος

Μέχρι τώρα είδαμε το σχήμα υπογραφής ElGamal και τις παραλλαγές του που όλα είναι τυχαιοποιημένα σχήματα ψηφιακής υπογραφής με παράρτημα (δηλ., ο αλγόριθμος επαλήθευσης απαιτεί ως όρισμα το αρχικό μήνυμα). Αντιθέτως, ο μηχανισμός υπογραφής του αλγορίθμου 5.8 έχει το χαρακτηριστικό ότι το μήνυμα μπορεί να ανακτηθεί από την ίδια την υπογραφή. Επομένως, αυτή η παραλλαγή του ElGamal παρέχει ένα τυχαιοποιημένο σχήμα υπογραφής με ανάκτηση του μηνύματος.

Για το σχήμα αυτό, ο χώρος υπογραφής είναι $M_s = \mathbb{Z}_p^*$ (p πρώτος) και ο χώρος υπογραφών είναι $S = \mathbb{Z}_p \times \mathbb{Z}_q$ (q πρώτος), όπου $q|(p-1)$. Έστω R μια συνάρτηση πλεονάζουσας πληροφορίας από το σύνολο των μηνυμάτων M στο M_s. Η παραγωγή κλειδιού για τον αλγόριθμο 5.8 είναι ίδια με αυτή για το DSS, με τη διαφορά ότι δεν υπάρχουν περιορισμοί για τα μεγέθη των p,q.

Αλγόριθμος 5.8

Παραγωγή υπογραφής Nyberg — Rueppel και επαλήθευση.

Συνοπτικά: Η οντότητα A υπογράφει ένα μήνυμα $m \in M$. Οποιαδήποτε οντότητα B μπορεί να επαληθεύσει την υπογραφή του A και να ανακτήσει το m από αυτήν.

1. Παραγωγή υπογραφής. Ή οντότητα A ενεργεί ως εξής:

1.1 Υπολογίζει το $\tilde{m} = R(m)$.

1.2 Επιλέγει έναν τυχαίο κρυφό ακέραιο k, $1 \leq k \leq q-1$ και υπολογίζει $r=g^{-k} \bmod p$.

1.3 Υπολογίζει $e = \tilde{m}r \bmod p$.

1.4 Υπολογίζει $s = ae + k \bmod q$. $a \neq g$

1.5 Η υπογραφή του Α για το m είναι το ζεύγος (e,s).

2. Επαλήθευση Για να επαληθεύσει την υπογραφή (e, s) του Α στο m, ο Β ενεργεί ως εξής:

2.1 Αποκτά το αυθεντικό δημόσιο κλειδί του Α, (p, q, g, y).

2.2 Επαληθεύει ότι $0 < e < p$. Αν αυτό δεν ισχύει απορρίπτει την υπογραφή.

2.3 Επαληθεύει ότι $0 \leq s < q$. Αν αυτό δεν ισχύει απορρίπτει την υπογραφή.

2.4 Υπολογίζει $u = g^s y^{-e} \bmod p$ και $\tilde{m} = ue \bmod p$.

2.5 Επαληθεύει ότι $\tilde{m} \in M_R$. Αν $\tilde{m} \notin M_R$ απορρίπτει την υπογραφή.

2.6 Ανακτά το $m = R^{-1}(\tilde{m})$.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί.

Αν ο Α δημιούργησε την υπογραφή, τότε $a \neq g$.

$$u \equiv g^s y^{-e} \equiv g^s g^{-ae} \equiv g^k \pmod p.$$

Έτσι $ue \equiv g^k \tilde{m} g^{-k} \equiv \tilde{m} \pmod p$, όπως απαιτείται.

Παράδειγμα 5.6 *(παραγωγή υπογραφής Nyberg - Rueppel με τεχνητά μικρές παραμέτρους)*

Παραγωγή κλειδιού. Η οντότητα Α επιλέγει τους πρώτους $p = 1256993$ και $q = 3571$, όπου $q|(p-1)$. Εδώ, $(p-1)/q = 352$. Ο Α στη συνέχεια επιλέγει έναν τυχαίο αριθμό $g_0 = 42077 \in \mathbb{Z}_p^*$ και υπολογίζει $g = 42077^{352} \bmod p = 441238$. Αφού $g \neq 1$, ο α παράγει τη μοναδική κυκλική υποομάδα του $\mathbb{Z}_p^*$ τάξεως 3571. Τελικά ο Α επιλέγει έναν τυχαίο ακέραιο $\alpha = 2774$ και υπολογίζει $y = g^a \bmod p = 1013657$.Το δημόσιο κλειδί του Α είναι ($p = 1256993$, $q = 3571$, $g = 441238$, $y = 1013657$), ενώ το ιδιωτικό του κλειδί είναι $\alpha = 2774$.

Παραγωγή υπογραφής. Για να υπογράψει ένα μήνυμα m, ο Α υπολογίζει το $\tilde{m} = R(m) = 1147892$ (η τιμή R(m) επινοήθηκε για τις ανάγκες του παραδείγματος). Ο Α κατόπιν επιλέγει το τυχαίο $k = 1001$ και υπολογίζει τα $r = g^{-k} \bmod p = 441238^{-1001} \bmod$

p = 1188935, e = $\tilde{m}r$ mod p = 138207 και s = (2774) (138207) + 1001 mod q = 1088. Η υπογραφή του m είναι (e = 138207, s = 1088).

Επαλήθευση της υπογραφής. Ο Β υπολογίζει υ = $441238^{1088} \cdot 1013657^{-138207}$ mod 1256993=504308 και $\tilde{m} = υ \cdot 138207$ mod 1256993=1147892. Ο Β επαληθεύει ότι $\tilde{m} \in M_R$ και ανακτά το $m = R^{-1}(\tilde{m})$.

Σημείωση 5.16 *(ασφάλεια του σχήματος υπογραφής Nyberg - Rueppel)*

1. *Αφού ο αλγόριθμος 4.8 είναι μια παραλλαγή του βασικού σχήματος ElGamal (αλγόριθμος 5.4), οι προσεγγίσεις σχετικά με την ασφάλεια, που περιέχονται στη σημείωση 5.3, εξακολουθούν να ισχύουν.*
2. *Εφόσον ο αλγόριθμος 5.8 παρέχει ανάκτηση του μηνύματος, απαιτείται μια κατάλληλη συνάρτηση πλεονάζουσας πληροφορίας για την αντιμετώπιση επιθέσεων υπαρκτής πλαστογραφίας. Ας δούμε την ακόλουθη δυνατή επίθεση. Έστω m ∈ M, $\tilde{m}$ = R(m) και (e, s) είναι μια υπογραφή του m. Τότε ισχύουν $e = \tilde{m}.g^{-k}$ mod p, για κάποιον ακέραιο k και s = ae + k mod q. Έστω $\tilde{m}^* = \tilde{m}.g^{l}$ mod p, για κάποιον ακέραιο l. Αν s* = s + l mod q και $\tilde{m}^* \in M_R$, τότε το ζεύγος (e, s*) είναι μια έγκυρη υπογραφή για το $m^* = R^{-1}(\tilde{m}^*)$. Για να το δούμε αυτό, ας θεωρήσουμε τον αλγόριθμο επαλήθευσης (αλγόριθμος 5.8, βήμα 2), $υ \equiv g^{s}*y^{-e} \equiv g^{s+l}g^{-ae} \equiv g^{k+l}$ (mod p). Εφόσον $\tilde{m}^* \in M_R$, η πλαστογραφημένη υπογραφή (e, s*) θα γίνει δεκτή ως έγκυρη υπογραφή του m*.*
3. *Η επαλήθευση του βήματος 3.2 του αλγορίθμου 5.8, δηλ. αν 0 < e < p, είναι πολύ σημαντική. Έστω (e, s) η υπογραφή του Α για το μήνυμα m. Τότε $e = \tilde{m}r$ mod p και s = ae + k mod q. Ένας αντίπαλος μπορεί να χρησιμοποιήσει αυτή την υπογραφή για να υπολογίσει μια υπογραφή σε ένα μήνυμα m* της επιλογής του. Καθορίζει ένα e* τέτοιο ώστε $e^* \equiv \tilde{m}^*r$ (mod p) και $e^* \equiv e$ (mod q) (αυτό είναι δυνατό από το Κινεζικό θεώρημα των υπολοίπων). Το ζεύγος (e*,s) θα γίνει δεκτό από τον αλγόριθμο επαλήθευσης αν δεν ελεγχθεί ότι το e* ικανοποιεί την ανισότητα 0 < e* < ρ.*

Σημείωση 5.17 *(μια γενίκευση των υπογραφών ElGamal με ανάκτηση τον μηνύματος) Η έκφραση $e = \tilde{m}r$ mod p του βήματος 2.3 του αλγορίθμου 5.8 παρέχει ένα σχετικά απλό τρόπο για την κρυπτογράφηση του $\tilde{m}$ με ένα κλειδί r και μπορεί να γενικευθεί σε οποιονδήποτε αλγόριθμο συμμετρικού κλειδιού. Έστω $E = \{E_r : r \in \mathbb{Z}_p\}$ ένα σύνολο μετασχηματισμών κρυπτογράφησης, όπου κάθε E_r έχει δείκτη ένα*

στοιχείο $r \in \mathbb{Z}_p^*$ και είναι μια 1-1 και επί συνάρτηση από το $M_s = \mathbb{Z}_p^*$ στο $\mathbb{Z}_p^*$. Αν για κάθε $m \in M$ επιλέξουμε έναν τυχαίο ακέραιο k με $1 \leq k \leq q - 1$ και υπολογίσουμε $r = g^k \bmod p$, $e = E_r(\tilde{m})$ και $s = ae + k \bmod q$, τότε το ζεύγος (e,s) είναι μια υπογραφή του m. Η βασική εξίσωση υπογραφής $s = ae + k \bmod q$ αποτελεί ένα μέσο για τη δέσμευση του ιδιωτικού κλειδιού της οντότητας A και του μηνύματος m με ένα συμμετρικό κλειδί, το οποίο μπορεί τότε να χρησιμοποιηθεί για την ανάκτηση του μηνύματος από οποιαδήποτε άλλη οντότητα σε κάποια μελλοντική στιγμή.

Κεφάλαιο 6

Σχήματα υπογραφής μιας χρήσης (One-time signature schemes)

Τα σχήματα ψηφιακής υπογραφής μιας χρήσης είναι μηχανισμοί οι οποίοι μπορούν να χρησιμοποιηθούν για την υπογραφή, το πολύ, ενός μηνύματος, διαφορετικά οι υπογραφές μπορούν να πλαστογραφηθούν. Για κάθε μήνυμα που υπογράφεται απαιτείται ένα νέο δημόσιο κλειδί. Οι δημόσιες πληροφορίες που χρειάζονται για την επαλήθευση υπογραφών μιας χρήσης συχνά αναφέρονται ως παράμετροι επιβεβαίωσης (validation parameters).

Τα περισσότερα, όχι όμως όλα, σχήματα υπογραφής μιας χρήσης έχουν το πλεονέκτημα ότι η παραγωγή των υπογραφών και η επαλήθευση τους είναι πολύ αποδοτικές διαδικασίες. Τα σχήματα υπογραφής μιας χρήσης είναι χρήσιμα σε εφαρμογές στις οποίες απαιτείται μικρή υπολογιστική ισχύ (π.χ. chipcards).

6.1 Το σχήμα υπογραφής μιας χρήσης Rabin

Το σχήμα υπογραφής μιας χρήσης Rabin ήταν μια από τις πρώτες προτάσεις για ένα σχήμα υπογραφής οποιουδήποτε είδους. Επιτρέπει την υπογραφή ενός μόνο μηνύματος, ενώ η επαλήθευση μιας υπογραφής απαιτεί αλληλεπίδραση μεταξύ του υπογράφοντος και της οντότητας που επαληθεύει. Σε αντίθεση με άλλα σχήματα υπογραφής, η επαλήθευση μπορεί να γίνει μόνο μια φορά. Παρ' όλο ότι δεν είναι πρακτικό, το παρουσιάζουμε για ιστορικούς λόγους.

Στον επόμενο πίνακα παρατίθεται η σημειογραφία που θα χρησιμοποιήσουμε σε αυτήν την παράγραφο.

Σύμβολο	Σημασία
M_0	0^l = όλες οι μηδενικές δυαδικές ακολουθίες μήκους $l-bit$.
$M_0(i)$	$0^{l-e}\|\|b_{e-1}...b_1b_0$, όπου $b_{e-1}...b_1b_0$ η δυαδική αναπαράσταση του i.
$\mathcal{K}$	ένα σύνολο δυαδικών ακολουθιών μήκους $l-bit$.
E	ένα σύνολο μετασχηματισμών κρυπτογράφησης με δείκτη ένα χώρο κλειδιών $\mathcal{K}$.
E_t	ένας μετασχηματισμός κρυπτογράφησης που ανήκει στο E με $t \in \mathcal{K}$. Κάθε E_t απεικονίζει ακολουθίες μήκους $l-bit$ σε ακολουθίες μήκους $l-bit$.
h	μια δημοσίως γνωστή συνάρτηση κατακερματισμού μονής κατεύθυνσης από το $\{0,1\}^*$ στο $\{0,1\}^l$.
n	ένας σταθερός θετικός ακέραιος ο οποίος εξυπηρετεί ως παράμετρος ασφαλείας.

Πίνακας 6.1 *Σημειογραφία για το σχήμα υπογραφής μιας χρήσης Rabin.*

Αλγόριθμος 6.1

Παραγωγή κλειδιού για το σχήμα υπογραφής μιας χρήσης Rabin.

Συνοπτικά: Κάθε οντότητα Α επιλέγει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού Ε, παράγει 2n τυχαίες δυαδικές ακολουθίες και δημιουργεί ένα σύνολο παραμέτρων επιβεβαίωσης. Κάθε οντότητα Α ενεργεί ως εξής:

1. Επιλέγει ένα σχήμα κρυπτογράφησης συμμετρικού κλειδιού Ε (π.χ. το DES).

2. Παράγει 2n τυχαίες κρυφές δυαδικές ακολουθίες $k_1,k_2,\ldots,k_{2n} \in K$, καθεμία μήκους l-bit.

3. Υπολογίζει τα $y_i = E_{ki}((M_o(i)), 1 \leq i \leq 2_n$.

4. Το δημόσιο κλειδί του Α είναι $(y_1,y_2,\ldots,y_{2n})$ και το ιδιωτικό του κλειδί είναι $(k_1,k_2,\ldots,k_{2n})$.

Αλγόριθμος 6.2

Παραγωγή υπογραφής μιας χρήσης Rabin και επαλήθευση.

Συνοπτικά: Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα πι αυθαίρετου μήκους. Η επαλήθευση της υπογραφής βρίσκεται σε αλληλεπίδραση με τον Α.

1. Παραγωγή υπογραφής. Ή οντότητα Α ενεργεί ως εξής:

1.1 Υπολογίζει το h(m).

1.2 Υπολογίζει τα $s_i = E_{ki}(h(m)), 1 \leq i \leq 2n$.

1.3 Η υπογραφή του Α για το m είναι $(s_1,s_2,\ldots,s_{2n})$.

2. Επαλήθευση. Για να επαληθεύσει την υπογραφή $(s_1,s_2,\ldots,s_{2n})$ του Α στο m, ο Β ενεργεί ως εξής:

2.1 Αποκτά το αυθεντικό δημόσιο κλειδί του Α, $(y_1,y_2,\ldots,y_{2n})$·

2.2 Υπολογίζει το h(m).

2.3 Επιλέγει n διακεκριμένους τυχαίους αριθμούς r_j, $1 \leq r_j \leq 2n$, $1 \leq j \leq n$.

2.4 Ζητά από τον Α τα κλειδιά k_{rj}, $1 \leq j \leq n$.

2.5 Επαληθεύει την αυθεντικότητα των κλειδιών που έλαβε υπολογίζοντας τα $z_j = E_{krj}(M_o(r_j))$ και ελέγχοντας ότι $z_j = y_{rj}$, για κάθε ένα j με $1 \leq j \leq n$.

2.6 Επαληθεύει ότι $s_{rj} = E_{krj}, (h(m)), 1 \leq j \leq n$.

Σημείωση 6.1 *(μεγέθη των κλειδιών για τις υπογραφές μιας χρήσης Rabin) Εφόσον ο E_t έχει ως εικόνες δυαδικές ακολουθίες μήκους l-bit, το δημόσιο και ιδιωτικό κλειδί*

στον αλγόριθμο 6.2 αποτελούνται από 2nl bits το καθένα. Για n = 80 και l = 64 κάθε κλειδί έχει μέγεθος 1280 bytes.

Σημείωση 6.2 *Ο Α μπορεί να υπογράψει το πολύ ένα μήνυμα με ένα δοθέν ιδιωτικό κλειδί, γιατί διαφορετικά ο Α θα αποκαλύψει (με υψηλή πιθανότητα) n+1 ή περισσότερες τιμές του ιδιωτικού κλειδιού και θα καταστήσει τον Β ικανό να πλαστογραφήσει υπογραφές σε νέα μηνύματα. Μια υπογραφή μπορεί να επαληθευθεί μόνο μια φορά χωρίς να αποκαλυφθούν (με υψηλή πιθανότητα) περισσότερες από n από τις 2n ιδιωτικές τιμές.*

6.2 Το σχήμα υπογραφής μιας χρήσης Merkle

Το σχήμα ψηφιακής υπογραφής μιας χρήσης Merkle (αλγόριθμος 6.4) διαφέρει ουσιωδώς από το αντίστοιχο Rabin (αλγόριθμος 6.2) στο ότι η επαλήθευση μιας υπογραφής δεν απαιτεί αλληλεπίδραση με τον υπογράφοντα. Μια έμπιστη αρχή (TTP) ή κάποιο άλλο έμπιστο μέσο απαιτείται για την πιστοποίηση των παραμέτρων επιβεβαίωσης που κατασκευάζονται στον αλγόριθμο 6.3.

Αλγόριθμος 6.3

Παραγωγή κλειδιού για το σχήμα υπογραφής μιας χρήσης Merkle.

Συνοπτικά: Για να υπογράψει μηνύματα μήκους n-bit, ο Α παράγει t=n+⌊lgn⌋+1 παραμέτρους επιβεβαίωσης. Κάθε οντότητα Α ενεργεί ως εξής:

1. *Επιλέγει t=n+⌊lgn⌋+1 τυχαίες κρυφές δυαδικές ακολουθίες $k_1, k_2, \ldots, k_t$ καθεμία μήκους l-bit.*
2. *Υπολογίζει $v_i = h(k_i)$, $1 \leq i \leq t$. Εδώ η h είναι μια συνάρτηση κατακερματισμού με αντίσταση 1ου-ορίσματος, $h : \{0,1\}^* \rightarrow \{0,1\}^l$ (βλ. §1.3).*
3. *Το δημόσιο κλειδί του Α είναι $(v_1, v_2, \ldots, v_t)$. Το ιδιωτικό του κλειδί είναι $(k_1, k_2, \ldots, k_t)$.*

Για την υπογραφή ενός n-bit μηνύματος m, σχηματίζεται μια ακολουθία w = m||c, όπου c είναι η δυαδική αναπαράσταση του αριθμού των μηδενικών στο m. Το c υποτίθεται ότι είναι μια ακολουθία bit μήκους ⌊lgn⌋+1 με τα bits υψηλής τάξεως να συμπληρώνονται με 0's, αν χρειάζεται. Γι' αυτό το w είναι μια ακολουθία bit μήκους t=n+⌊lgn⌋+1.

Αλγόριθμος 6.4

Παραγωγή υπογραφής μιας χρήσης Merkle και επαλήθευση.

Συνοπτικά: Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m μήκους n-bit. Οποιαδήποτε οντότητα Β μπορεί να επαληθεύσει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Α.

1. *Παραγωγή υπογραφής. Ή οντότητα Α ενεργεί ως εξής:*

   1.1 Υπολογίζει το c, τη δυαδική αναπαράσταση του πλήθους των μηδενικών στο m.

   1.2 Σχηματίζει το $w = m||c = (a_1\, a_2,\ldots a_t)$.

   1.3 Καθορίζει τις θέσεις συντεταγμένων $i_1<i_2<i_u$ *στο w έτσι ώστε* $a_{ij}=1, 1\leq j\leq u$.

   1.4 Θέτει $s_j = k_{ij}$, $1\leq j\leq u$.

   1.5 Η υπογραφή του Α για το m είναι $(s_1,s_2,\ldots,s_u)$.

2. *Επαλήθευση. Για να επαληθεύσει την υπογραφή* $(s_1,s_2,\ldots,s_u)$ *του Α στο m, ο Β ενεργεί ως εξής:*

   2.1 Αποκτά το αυθεντικό δημόσιο κλειδί του Α, $(\upsilon_1,\upsilon_2,\ldots,\upsilon_t)$.

   2.2 Υπολογίζει το c, τη δυαδική αναπαράσταση του πλήθους των μηδενικών στο m.

   2.3 Σχηματίζει το $w = m||c= (a_1\, a_2,\ldots a_t)$.

   2.4 Καθορίζει τις θέσεις συντεταγμένων $i_1<i_2<\ldots<i_u$ *στο w έτσι ώστε* $a_{ij}=1, 1\leq j\leq u$.

   2.5 Αποδέχεται την υπογραφή αν και μόνον αν $\upsilon_{ij} =h(s_j)$, *για όλα τα j με* $1\leq j\leq u$.

Σημείωση 6.3 *(ασφάλεια του σχήματος υπογραφής μιας χρήσης Merkle) Έστω ένα μήνυμα m,* $w = m||c$ *η δυαδική ακολουθία που σχηματίζεται στο βήμα 2.2 του αλγόριθμου 6.4 και* $(s_1,s_2,\ldots,s_u)$ *μια υπογραφή του m. Αν η h είναι μια συνάρτηση κατακερματισμού με αντίσταση 1ου-ορίσματος, τότε η ανάλυση που ακολουθεί δείχνει ότι δεν μπορεί να πλαστογραφηθεί μια υπογραφή για ένα μήνυμα* $m'\neq m$. *Έστω* $w' = m'||c'$ *όπου c' είναι η* $(\lfloor lgn\rfloor+1)$ *- bit ακολουθία, η οποία είναι η δυαδική αναπαράσταση του πλήθους των μηδενικών στο m'. Εφόσον ένας «αντίπαλος» έχει πρόσβαση μόνο στο τμήμα εκείνο του ιδιωτικού κλειδιού του υπογράφοντος που αποτελείται από την υπογραφή* $(s_1,s_2,\ldots,s_u)$, *το σύνολο των θέσεων συντεταγμένων του m' που έχουν μονάδα πρέπει να είναι υποσύνολο των θέσεων συντεταγμένων του m που επίσης έχουν μονάδα (διαφορετικά το m' θα έχει μια μονάδα σε κάποια*

θέση που το m έχει 0 και ο «αντίπαλος» θα χρειαστεί ένα στοιχείο του ιδιωτικού κλειδιού το οποίο ο υπογράφων δεν αποκαλύπτει). Αυτό όμως σημαίνει ότι το m' έχει περισσότερα 0 από το m και ότι c' > c (όταν οι c, c' θεωρούνται ακέραιοι). Σε αυτήν την περίπτωση το c' θα έχει μια μονάδα σε κάποια θέση που το c έχει 0. Ο αντίπαλος τότε θα χρειαστεί ένα στοιχείο του ιδιωτικού κλειδιού, αντίστοιχο της θέσης αυτής, το οποίο δεν αποκαλύφθηκε από τον υπογράφοντα.

6.3 Το σχήμα υπογραφής μιας χρήσης Lamport

Πριν αναφέρουμε τους αλγόριθμους παραγωγής κλειδιού, παραγωγής της υπογραφής και επαλήθευσης για το σχήμα υπογραφής μιας χρήσης Lamport, περιγράφουμε ανεπίσημα τη λειτουργία του.

Ο χώρος των μηνυμάτων M αποτελείται από δυαδικές ακολουθίες μήκους k-bit. Κάθε bit υπογράφεται ανεξάρτητα ως εξής: η τιμή z_{ij} αντιστοιχεί στο i-οστό bit του μηνύματος το οποίο έχει την τιμή j (j = 0,1). Κάθε z_{ij} είναι η εικόνα του y_{ij} μέσω της συνάρτησης μονής κατεύθυνσης $f(x) = a^x \bmod p$, όπου p πρώτος και α πρωταρχικό στοιχείο modulo p. Το i-οστό bit του μηνύματος m υπογράφεται χρησιμοποιώντας το όρισμα y_{ij} του z_{ij} που αντιστοιχεί στο i-οστό bit του m. Ή. διαδικασία της επαλήθευσης απλώς ελέγχει ότι κάθε στοιχείο της υπογραφής είναι όρισμα του κατάλληλου στοιχείου του δημοσίου κλειδιού.

Παραθέτουμε τώρα τους αλγορίθμους παραγωγής κλειδιού και παραγωγής της υπογραφής και επαλήθευσης για την καλύτερη κατανόηση του σχήματος.

Αλγόριθμος 6.5

Παραγωγή κλειδιού για το σχήμα υπογραφής μιας χρήσης Lamport.

Συνοπτικά: Για την υπογραφή ενός μηνύματος m μήκους k-bit, η οντότητα A επιλέγει τους 2k τυχαίους αριθμούς y_{i_j} και υπολογίζει τους $z_{i_j} = f(y_{i_j})$. Η οντότητα A ενεργεί ως εξής:

1. *Επιλέγει τους 2k τυχαίους αριθμούς y_{i_j}, $1 \leq i \leq k$, $j = 0,1$.*
2. *Υπολογίζει τα $z_{i_j} = 1 \leq i \leq k$, $j = 0,1$.*
3. *Το δημόσιο κλειδί του A είναι το (z_{1_j}, z_{2_j}, … , z_{k_j}), $j = 0,1$. Το ιδιωτικό του κλειδί είναι το { y_{1_j}, y_{2_j}, … , yz_{k_j}), $j = 0,1$.*

Το δημόσιο και ιδιωτικό κλειδί του Α μπορούν επίσης να γραφούν με τη μορφή των k x 2 πινάκων $[z_{i_j}]$ *και* $[y_{i_j}]$ *αντίστοιχα. Που η συνάρτηση* $f(y_{i_j})$ *είναι μια δημόσια γνωστή συνάρτηση μόνης κατεύθυνσης.*

Αλγόριθμος 6.6

Παραγωγή υπογραφής μιας χρήσης Lamport και επαλήθευση.

Συνοπτικά: Η οντότητα Α υπογράφει ένα δυαδικό μήνυμα m μήκους k-bit. Οποιαδήποτε οντότητα Β μπορεί να επαληθεύσει την υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Α. Έστω το μήνυμα $m = x_1x_2\ldots x_k$, *όπου* $x_i \in \{0,1\}$, $i = 1,2,\ldots, k$.

1. *Παραγωγή υπογραφής. Ή οντότητα Α ενεργεί ως εξής:*

   Η υπογραφή του Α για το μήνυμα m είναι

   $(s_1,s_2,\ldots,s_k)=(y_{1_{x_1}}, y_{2_{x_2}}, y_{k_{x_k}})=\vec{s}$

   Ο Α στέλνει στον Β το ζεύγος $(m, \vec{s})$

2. *Επαλήθευση. Η οντότητα Β ενεργεί ως εξής:*

   Αποδέχεται την υπογραφή αν και μόνον αν $f(s_i) = z_{i_{x_i}}$, $1 \leq i \leq k$.

Παράδειγμα 6.1 *(παραγωγή υπογραφής μιας χρήσης Lamport)*

Ο αριθμός p=7879 είναι πρώτος και ο α=3 είναι πρωταρχικό στοιχείο του $\mathbb{Z}^*_{7879}$. *Ορίζουμε τη συνάρτηση* $f(x) = 3^x \mod 7879$.

Παραγωγή κλειδιού. Έστω ότι ο Α επιθυμεί να υπογράψει ένα δυαδικό μήνυμα m μήκους k = 3 - bit. Επιλέγει τους τυχαίους 2k = 6 αριθμούς και κατασκευάζει τον ακόλουθο πίνακα, ο οποίος αποτελεί το ιδιωτικό του κλειδί.

$$\begin{pmatrix} y_{1_0} = 5831 & y_{1_1} = 735 \\ y_{2_0} = 803 & y_{2_1} = 2467 \\ y_{3_0} = 4285 & y_{3_1} = 6449 \end{pmatrix}$$

Στη συνέχεια υπολογίζει τα $z_{i_j}=f(y_{i_j})$, $i=1,2,3, i=0,1$ *και κατασκευάζει τον ακόλουθο πίνακα, ο οποίος αποτελεί το δημόσιο κλειδί του.*

$$\begin{pmatrix} z_{1_0} = 2009 & z_{1_1} = 3810 \\ z_{2_0} = 4672 & z_{2_1} = 4721 \\ z_{3_0} = 268 & z_{3_1} = 5731 \end{pmatrix}$$

Παραγωγή υπογραφής. Έστω ότι ο Α επιθυμεί να υπογράψει το μήνυμα m = (1,1,0). Η υπογραφή για το m είναι:

$(s_1,s_2,s_3) = (y_{1_1}, y_{2_1}, y_{3_0}) = (735, 2467, 4285)$.

Επαλήθευση υπογραφής. Για την επαλήθευση της υπογραφής ο Β υπολογίζει:

$f(s_1)= 3^{735} \bmod 7879 = 3810 (=z_{1_1})$.

$f(s_2)= 3^{2467} \bmod 7879 = 4721 (=z_{2_1})$.

$f(s_3)= 3^{4285} \bmod 7879 = 268 (=z_{3_0})$.

Αφού λοιπόν $f(s_i)= z_{i_{x_i}}$, i = 1,2,3, συνεπάγεται ότι η υπογραφή είναι έγκυρη.

Σημείωση 6.4 *(ασφάλεια του σχήματος υπογραφής μιας χρήσης Lamport) Ένας «αντίπαλος» δεν μπορεί να πλαστογραφήσει μια υπογραφή ενός μηνύματος m που έχει παραχθεί με το σχήμα υπογραφής μιας χρήσης Lamport, επειδή είναι ανέφικτη η αντιστροφή της συνάρτησης μονής κατεύθυνσης f. Επομένως ο «αντίπαλος» δεν μπορεί να αποκτήσει το ιδιωτικό κλειδί του υπογράφοντος $(y_1,y_2,\ldots,y_{k_j})$, j= 0,1. Ωστόσο το ιδιωτικό κλειδί $(y_1,y_2,\ldots,y_{kj})$ πρέπει να χρησιμοποιείται για την υπογραφή ενός μόνο μηνύματος, γιατί διαφορετικά είναι εύκολο για έναν «αντίπαλο» να πλαστογραφήσει την υπογραφή του Α υπογράφοντας μηνύματα της επιλογής του.*

Για να το καταλάβουμε αυτό ας υποθέσουμε ότι ο Α χρησιμοποιεί το ίδιο ιδιωτικό κλειδί $(y_1,y_2,\ldots, y_{k_j})$, j = 0,1 για την υπογραφή των μηνυμάτων m_1 = (0,1,1) και m_2 = (1,0,1). Οι υπογραφές για τα m_1,m_2 θα είναι αντίστοιχα $\vec{s}_1 = (y_{1_0}y_{2_1}, y_{3_1})$, $\vec{s}_2 = (y_{1_1}, y_{2_0}, y_{3_1})$. Δοθέντων αυτών των υπογραφών, ένας «αντίπαλος» μπορεί να κατασκευάσει υπογραφές για τα μηνύματα της επιλογής του m_3 = (1,1,1), m_4 = (0,0,1), οι οποίες θα είναι αντίστοιχα $\vec{s}_3 = (y_{1_1}, y_{2_1}, y_{3_1})$ και $\vec{s}_4 = (y_{1_0}, y_{2_0}, y_{3_1})$.

Κεφάλαιο 7

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

Οι μηχανισμοί υπογραφής που περιγράφονται σε αυτό το κεφάλαιο παρέχουν λειτουργικότητα πέραν της πιστοποίησης και της μη άρνησης μιας υπογραφής (βλ. §2.1). Στις περισσότερες περιπτώσεις συνδυάζουν ένα βασικό σχήμα ψηφιακής υπογραφής (π.χ το RSA) με ένα συγκεκριμένο πρωτόκολλο για την επίτευξη επιπρόσθετων χαρακτηριστικών, τα οποία η βασική μέθοδος δεν παρέχει.

7.1 Σχήματα τυφλής υπογραφής (Blind signature schemes)

Τα σχήματα τυφλής υπογραφής εξυπηρετούν γενικά ανάγκες ηλεκτρονικής επικοινωνίας στις οποίες η μια πλευρά επιθυμεί ανωνυμία απέναντι στην άλλη.

Σε αντίθεση με τα σχήματα υπογραφής που περιγράψαμε στο 2ο κεφάλαιο (§2.2,2.4 και 2.5), τα σχήματα τυφλής υπογραφής είναι πρωτόκολλα μεταξύ δύο οντοτήτων, ενός αποστολέα Α και ενός υπογράφοντος Β. Η βασική ιδέα είναι η ακόλουθη. Ο Α στέλνει μια πληροφορία στον Β την οποία ο Β υπογράφει και επιστρέφει στον Α. Από αυτήν την υπογραφή, ο Α μπορεί να υπολογίσει την υπογραφή του Β σε ένα μήνυμα m που εκ των προτέρων έχει επιλέξει. Με την ολοκλήρωση του πρωτοκόλλου, ο Β δεν ξέρει ούτε το μήνυμα m ούτε την υπογραφή που σχετίζεται με αυτό.

Ο σκοπός μιας τυφλής υπογραφής είναι να εμποδίσει τον υπογράφοντα Β να γνωρίσει το μήνυμα m και την υπογραφή. Επομένως, είναι αργότερα αδύνατη η συσχέτιση του υπογεγραμμένου μηνύματος με τον αποστολέα Α.

***Παράδειγμα 7.1** (εφαρμογές των τυφλών υπογραφών)*

Τα σχήματα τυφλής υπογραφής έχουν εφαρμογές κατά τις οποίες ο αποστολέας Α (πελάτης) δεν επιθυμεί ο υπογράφων Β (τράπεζα) να μπορεί να συσχετίσει εκ των υστέρων ένα μήνυμα m και μια υπογραφή S_B (m) σε ένα συγκεκριμένο βήμα του πρωτοκόλλου. Αυτό ίσως είναι σημαντικό σε εφαρμογές

ηλεκτρονικών μετρητών όπου ένα μήνυμα m μπορεί να αναπαριστά ένα χρηματικό ποσό το οποίο ο Α μπορεί να ξοδέψει. Όταν το m και η S_B (m) παρουσιάζονται στον Β για εξόφληση, ο Β δεν μπορεί να συμπεράνει σε ποια οντότητα δόθηκε αρχικά η υπογεγραμμένη τιμή. Αυτό επιτρέπει στον Α να παραμένει ανώνυμος έτσι ώστε ο τρόπος με τον οποίο ξοδεύει να μην μπορεί να παρακολουθηθεί.

Ένα πρωτόκολλο τυφλής υπογραφής χρειάζεται τις ακόλουθες συνιστώσες:

1. *Ένα σχήμα ψηφιακής υπογραφής για τον υπογράφοντα Β. Το S_B (m) συμβολίζει την υπογραφή του Β στο μήνυμα m.*
2. *Δύο συναρτήσεις f και g (γνωστές μόνο στον αποστολέα) τέτοιες ώστε*

$$g(S_B(f(m))) = S_B(m).$$

*Η f λέγεται **συνάρτηση τύφλωσης** (blinding function), η g **συνάρτηση αποτύφλωσης** (unblinding function) και το f(m) **τυφλωμένο μήνυμα** (blinded message).*

Παράδειγμα 7.2 *(συνάρτηση τύφλωσης βασισμένη στο RSA)*

Έστω $n = p \cdot q$ το γινόμενο δύο μεγάλων τυχαίων πρώτων αριθμών. Ο αλγόριθμος υπογραφής S_B για την οντότητα Β είναι το σχήμα υπογραφής RSA (αλγόριθμος 3.4) με δημόσιο κλειδί (n, e) και ιδιωτικό d. Έστω k κάποιος σταθερός ακέραιος με $0 \leq k \leq n-1$ και $(n,k) = 1$. Η συνάρτηση τύφλωσης $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ ορίζεται από τη σχέση $f(m) = m \cdot k^e \bmod n$ και η συνάρτηση αποτύφλωσης $g : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ από τη σχέση $g(m) = k^{-1} m \bmod n$. Για την επιλογή αυτή των f,g και S_B ισχύει ότι $g(S_B(f(m))) = g(S_B(mk^e \bmod n)) = g(m^d k \bmod n) = m^d \bmod n = S_B(m)$, όπως απαιτείται από τη δεύτερη ιδιότητα.

Το πρωτόκολλο 7.1 παρουσιάζει ένα σχήμα τυφλής υπογραφής το οποίο χρησιμοποιεί το σχήμα RSA και τις συναρτήσεις f και g που ορίστηκαν στο προηγούμενο παράδειγμα.

Πρωτόκολλο 7.1

Πρωτόκολλο τυφλής υπογραφής Chaum.

Συνοπτικά: Ο αποστολέας Α λαμβάνει μια υπογραφή του Β σε ένα τυφλωμένο μήνυμα. Από αυτήν ο Α υπολογίζει την υπογραφή του Β σε ένα μήνυμα m που έχει

επιλέξει εκ των προτέρων, $0 \leq m \leq n - 1$. Ο Β δεν έχει γνώση του μηνύματος m ούτε της υπογραφής που σχετίζεται με αυτό.

1. *Σημειογραφία. Το δημόσιο και ιδιωτικό κλειδί RSA του Β είναι αντίστοιχα (n, e) και d, ενώ k είναι ένας τυχαίος κρυφός ακέραιος που επιλέχθηκε από τον Α και ικανοποιεί τις σχέσεις $0 \leq k \leq n - 1$ και (n, k) = 1.*
2. *Ενέργειες του πρωτοκόλλου.*

   2.1 (τύφλωση) Ο Α υπολογίζει το $m^* = f(m) = mk^e \bmod n$ και το στέλνει στον Β.

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

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

7.2 Αδιαμφισβήτητα σχήματα υπογραφής
(Undeniable signature schemes)

Τα αδιαμφισβήτητα σχήματα υπογραφής διαφέρουν από τα συνήθη σχήματα υπογραφής (κεφάλαιο 2) με την έννοια ότι για την επαλήθευση της υπογραφής απαιτείται η συνεργασία του υπογράφοντος Α. Αυτό προστατεύει τον Α ενάντια στην πιθανότητα αντιγραφής των μηνυμάτων που υπογράφει και της ηλεκτρονικής διανομής τους χωρίς την έγκριση του. Η επαλήθευση επιτυγχάνεται με τη βοήθεια ενός πρωτοκόλλου πρόκληση και ανταπόκριση (challenge - and - response protocol).

Αν όμως για την επαλήθευση της υπογραφής απαιτείται η συνεργασία του Α, τότε τι μπορεί να τον εμποδίσει να αρνηθεί την αποδοχή μιας υπογραφής που δημιούργησε κάποια στιγμή στο παρελθόν; Ο Α ίσως ισχυριστεί ότι μια έγκυρη υπογραφή είναι πλαστογραφημένη και τότε μπορεί είτε να αρνηθεί να την επαληθεύσει, είτε να διεξάγει το πρωτόκολλο επαλήθευσης με τέτοιο τρόπο ώστε η υπογραφή να μην επαληθευθεί. Για να αποφευχθεί κάτι τέτοιο, ένα αδιαμφισβήτητο σχήμα υπογραφής ενσωματώνει ένα πρωτόκολλο αποκήρυξης (disavowal protocol) με το οποίο ο Α μπορεί να αποδείξει ότι μια υπογραφή είναι πλαστογραφημένη. Έτσι, ο Α μπορεί να αποδείξει ότι μια πλαστογραφημένη υπογραφή είναι όντως πλαστογραφημένη, ενώ αν ο Α αρνηθεί να συμμετάσχει στο

πρωτόκολλο αποκήρυξης, τότε αυτό αποτελεί ένδειξη ότι η υπογραφή είναι δεν γνήσια.

Επομένως ένα αδιαμφισβήτητο σχήμα υπογραφής αποτελείται από τρείς συνιστώσες: έναν αλγόριθμο υπογραφής, ένα πρωτόκολλο επαλήθευσης και ένα πρωτόκολλο αποκήρυξης.

Το ακόλουθο παράδειγμα περιγράφει δύο σενάρια στα οποία μπορεί να εφαρμοστεί ένα αδιαμφισβήτητο σχήμα υπογραφής.

***Παράδειγμα 7.3** (σενάρια αδιαμφισβήτητων υπογραφών)*

1. *Έστω ότι η οντότητα Α (πελάτης) επιθυμεί να αποκτήσει πρόσβαση σε μια περιοχή ασφαλείας που επιβλέπεται από την οντότητα Β (τράπεζα) .Η περιοχή ασφαλείας μπορεί να είναι ο χώρος της τράπεζας στον οποίο φυλάσσονται οι καταθέσεις των πελατών της. Η Β ζητάει από τον Α να υπογράψει ένα έγγραφο με ημερομηνία και ώρα πριν του δοθεί η άδεια πρόσβασης. Αν ο Α χρησιμοποιήσει μια αδιαμφισβήτητη υπογραφή, τότε η Β δεν θα μπορεί να αποδείξει ότι η υπογραφή δημιουργήθηκε από τον Α, χωρίς την άμεση ανάμειξη του Α στη διαδικασία επαλήθευσης.*
2. *Ας υποθέσουμε ότι μια μεγάλη εταιρεία Α δημιουργεί ένα νέο λογισμικό πακέτο. Η Α υπογράφει το πακέτο και το πουλάει στην οντότητα Β η οποία το αντιγράφει και το μεταπωλεί σε μια τρίτη οντότητα C. Η C δεν μπορεί να επαληθεύσει την αυθεντικότητα του λογισμικού χωρίς τη συνεργασία της Α. Βεβαίως, το σενάριο αυτό δεν εμποδίζει την Β να ξαναϋπογράψει το πακέτο με τη δική της υπογραφή. Αλλά τότε το πακέτο θα έχανε το αγοραστικό πλεονέκτημα της προέλευσης από τη γνωστή εταιρεία Α και επίσης θα ήταν εύκολο να ανιχνευθεί η απάτη της Β.*

***Λήμμα 7.1** Έστω οι πρώτοι p, q τέτοιοι ώστε p = 2q + 1. Τότε το σύνολο G των τετραγωνικών υπολοίπων modulo p των στοιχείων του $\mathbb{Z}_p^*$ αποτελεί πολλαπλασιαστική υποομάδα του $\mathbb{Z}_p^*$ τάξης q.*

***Παρατήρηση 7.1** Επίσης από το λήμμα 5.2 μπορούμε να υπολογίσουμε μια τέτοια υποομάδα του $\mathbb{Z}_p^*$ που θα αποτελείται από τις μέχρι τάξης q δυνάμεις του $g = g_0^{(p-1)/q}$, όπου g_0 πρωταρχικό στοιχείο του $\mathbb{Z}_p^*$.*

Αλγόριθμος 7.1

Παραγωγή κλειδιού για το αδιαμφισβήτητο σχήμα υπογραφής Chaum—van Antwerpen.

Συνοπτικά: Κάθε οντότητα επιλέγει ένα ιδιωτικό και ένα αντίστοιχο δημόσιο κλειδί. Κάθε οντότητα Α ενεργεί ως εξής:

1. *Επιλέγει έναν τυχαίο πρώτο p= 2q + 1, όπου q είναι επίσης πρώτος.*
2. *(Επιλέγει ένα γεννήτορα g της υποομάδας του $\mathbb{Z}_p$* τάξεως q.)*

   2.1 Επιλέγει ένα τυχαίο στοιχείο β ∈ $\mathbb{Z}_p$ και υπολογίζει το $g = g_0^{(p-1)/q} \bmod p$.*

   2.2 Αν g = 1 επιστρέφει στο βήμα 2.1.
3. *Επιλέγει έναν τυχαίο ακέραιο α ∈ {1, 2,..., q - 1} και υπολογίζει το $y = g^a \bmod p$.*
4. *Το δημόσιο κλειδί του Α είναι (p,g,y).Το ιδιωτικό του είναι α.*

Αλγόριθμος 7.2

Το αδιαμφισβήτητο σχήμα υπογραφής Chaum - van Antwerpen.

Συνοπτικά: Η οντότητα Α υπογράφει ένα μήνυμα m το οποίο ανήκει στην υποομάδα του $\mathbb{Z}_p$ τάξεως q. Οποιαδήποτε οντότητα μπορεί να επαληθεύσει την υπογραφή με τη συνεργασία του Α.*

1. Παραγωγή υπογραφής. Η οντότητα Α ενεργεί ως εξής:

1.1 Υπολογίζει το $s = m^a \bmod p$.

1.2 Η υπογραφή του Α για το m είναι s. Και στέλνει στο Β το (m,s).

2. Επαλήθευση. Το πρωτόκολλο για τον Β για την επαλήθευση της υπογραφής του Α στο m είναι το ακόλουθο:

2.1 Ο Β αποκτά το αυθεντικό δημόσιο κλειδί του Α, (p,g,y).

2.2 Ο Β επιλέγει τυχαίους κρυφούς ακεραίους $x_1, x_2 \in \{1, 2,..., p - 1\}$.

2.3 Ο Β υπολογίζει $z = s^{x_1} y^{x_2} \bmod p$ και στέλνει το z στον Α.

2.4 Ο Α υπολογίζει $w = (z)^{a^{-1}} \bmod p$ (όπου $\alpha\alpha^{-1} \equiv 1 \pmod q$) και στέλνει το w στον Β.

2.5 Ο Β υπολογίζει $w' = m^{x_1} g^{x_2} \bmod p$ και δέχεται την υπογραφή αν και μόνον αν w = w'.

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί.

$$w \equiv (z)^{a^{-1}} \equiv (s^{x_1} y^{x_2})^{a^{-1}} \equiv (m^{ax_1} g^{ax_2})^{a^{-1}} \equiv m^{x_1} g^{x_2} \equiv w' \bmod p,$$

όπως απαιτείται.

Παράδειγμα 7.4 (*παραγωγή αδιαμφισβήτητης υπογραφής Chaum-van Antwerpen) Παραγωγή κλειδιού. Η οντότητα Α επιλέγει τον τυχαίο πρώτο p= 467 = 2 · 233 + 1 (q = 233), όπου ο q = 233 είναι επίσης πρώτος. Κατόπιν επιλέγει το τυχαίο στοιχείο g_0 = 2 ∈ $\mathbb{Z}_p$* και υπολογίζει το g = $g_0^{(p-1)/q}$ mod p = 2^2 mod 467=4. Αφού g ≠ 1, τότε το g = 4 είναι γεννήτορας της υποομάδας του $\mathbb{Z}_p$* τάξης q^{16}. Ο Α τώρα επιλέγει τον τυχαίο ακέραιο α = 101 ∈ {1, 2,..., q - 1} και υπολογίζει το y = g^a mod p = 449. Το δημόσιο κλειδί του Α είναι η τριάδα (p = 467, g = 4, y = 449), ενώ το ιδιωτικό του κλειδί είναι α = 101.*

Παραγωγή υπογραφής. Έστω ότι ο Α επιθυμεί να υπογράψει το μήνυμα m = 119. Υπολογίζει το s = m^a mod p = 129.Η υπογραφή του Α στο μήνυμα m είναι s = 129. Ο Α στέλνει στον Β (119,129)

Επαλήθευση. Η οντότητα Β αποκτά το αυθεντικό δημόσιο κλειδί του Α, (p = 467, g = 4, y = 449) και κατόπιν επιλέγει τους τυχαίους κρυφούς ακέραιους x_1 = 38, x_2 = 397 ∈ {1, 2,..., q - 1}. Ο Β υπολογίζει το z = s^{x1} y^{x2} mod p = 13 και το στέλνει στον Α. Ο Α υπολογίζει το α^{-1} mod q=101^{-1} mod 233=30 και w=$c^{a^{-1}} mod\ q \cdot$ mod p = 13^{30} mod 467=9 (όπου $a\alpha^{-1} \equiv 1$ (mod q)) και στέλνει το w στον Β. Ο Β υπολογίζει το w' = $m^{x1}g^{x2}$ mod p = 9 και αποδέχεται την υπογραφή αφού w = w'.

Πόρισμα 7.1[17] *(ανιχνεύοντας πλαστογραφίες αδιαμφισβήτητων υπογραφών) Ας υποθέσουμε ότι s είναι μια πλαστογραφία της υπογραφής του Α σε ένα μήνυμα m, δηλαδή s ≠ m^a mod p. Τότε η πιθανότητα ο Β να αποδεχτεί την υπογραφή είναι μόνο $\frac{1}{q}$. Η πιθανότητα αυτή είναι ανεξάρτητη από τα υπολογιστικά μέσα του «αντιπάλου».*

---

[16] Ή υποομάδα αυτή του $\mathbb{Z}_p$* αποτελείται από τα τεραγωνικά υπόλοιπα *modulo p* των στοιχείων του $\mathbb{Z}_p$* (βλ. λήμμα 6.1).

[17] Η απόδειξη υπάρχει στο [Sti02], κεφ. 6.

Σημείωση 7.1 *(αποκηρύσσοντας υπογραφές) Ο υπογράφων Α θα μπορούσε να επιχειρήσει να αποκηρύξει μια (έγκυρη) υπογραφή, που κατασκευάστηκε με τον αλγόριθμο 7.2, με έναν από τους ακόλουθους τρείς τρόπους:*

1. *να αρνηθεί να συμμετάσχει στο πρωτόκολλο επαλήθευσης του αλγορίθμου 7.2·*
2. *να εκτελέσει το πρωτόκολλο επαλήθευσης λανθασμένα· ή*
3. *να ισχυριστεί ότι μια υπογραφή είναι πλαστή παρ' όλο που το πρωτόκολλο επαλήθευσης είναι επιτυχές.*

Η αποκήρυξη μιας υπογραφής σύμφωνα με την 1η περίπτωση θα θεωρηθεί φανερή απόπειρα (αδικαιολόγητης) άρνησης της υπογραφής και επομένως η υπογραφή δεν θα ληφθεί υπ' όψιν. Οι περιπτώσεις 2 και 3 αντιμετωπίζονται δυσκολότερα και για το λόγο αυτό απαιτείται ένα ***πρωτόκολλο αποκήρυξης.***

Το πρωτόκολλο 7.2 ουσιαστικά εφαρμόζει δυο φορές το πρωτόκολλο επαλήθευσης του αλγορίθμου 7.4 και στη συνέχεια εκτελεί έναν έλεγχο για να επαληθεύσει ότι η οντότητα Α εκτέλεσε σωστά το πρωτόκολλο.

Πρωτόκολλο 7.2

Πρωτόκολλο αποκήρυξης για το σχήμα αδιαμφισβήτητης υπογραφής Chaum - van Antwerpen.

Συνοπτικά: Το πρωτόκολλο αυτό καθορίζει αν ο υπογράφων Α επιχειρεί να αποκηρύξει μια έγκυρη υπογραφή s χρησιμοποιώντας τον αλγόριθμο 7.4 ή αν η υπογραφή είναι πλαστή.

1. *Ο Β αποκτά το αυθεντικό δημόσιο κλειδί του Α, (p, g, y).*
2. *Ο Β επιλέγει τυχαίους κρυφούς ακεραίους $x_1, x_2 \in \{1,2, \ldots, p-1\}$, $x_1, x_2 \in \mathbb{Z}_p^*$ υπολογίζει το $z = s^{x_1} y^{x_2} \bmod p$ και στέλνει το z στον Α.*
3. *Ο Α υπολογίζει το $w = (z)^{a^{-1}} \bmod p$ (όπου $aa^{-1} \equiv 1 \pmod q$) και στέλνει το w στον Β.*
4. *Αν $w = m^{x1} a^{x2} \bmod p$, τότε ο Β αποδέχεται την υπογραφή s και το πρωτόκολλο σταματά.*
5. *Ο Β επιλέγει τυχαίους κρυφούς ακεραίους $x'_1\, x'_2 \in \{1, 2, \ldots, p-1\}$, υπολογίζει το $z' = s^{x'1} y^{x'2} \bmod p$ και στέλνει το z' στον Α.*
6. *Ο Α υπολογίζει το $w' = (z')^{\alpha-1} \bmod p$ και στέλνει το w' στον Β.*
7. *Αν $w' = m^{x'1a} y^{x'2} \bmod p$, τότε ο Β αποδέχεται την υπογραφή s και το*

πρωτόκολλο σταματά.

8. *Ο Β υπολογίζει το* $c = (wg^{-x2})^{x'1} \bmod p$ *και* $c' = (w'g^{-x'2})^{x1} \bmod p$. *Αν* $c = c'$, *τότε ο Β συμπεραίνει ότι η s είναι πλαστή, διαφορετικά καταλήγει στο συμπέρασμα ότι η υπογραφή είναι έγκυρη και ο Α προσπαθεί να την αποκηρύξει.*

Παράδειγμα 7.5

Όπως και στο παράδειγμα 7.4 ας υποθέσουμε ότι p=467, g=4, α=101 και y=449. Έστω ότι υπογράφεται το μήνυμα m=286 με την (πλαστή) υπογραφή s=83 και ότι ο Α θέλει να πείσει τον Β ότι η υπογραφή δεν είναι έγκυρη.

Ας ξεκινήσουμε με την επιλογή από τον Β, των τυχαίων κρυφών ακεραίων $x_1=45$, $x_2= 237$. *Ο Β υπολογίζει το* $z = 83^{45}449^{237} \bmod 467 = 305$ *και το στέλνει στον Α. Ο Α υπολογίζει το* $w = 305^{30} \bmod 467 = 109$ *και το στέλνει στον Β. Ο Β υπολογίζει*

$$286^{45}\, 4^{237} \bmod 467 = 149$$

Αφού $w = 109 \neq 149$, *ο Β συνεχίζει στο 5ο βήμα του πρωτοκόλλου.*

Ας υποθέσουμε τώρα ότι ο Β επιλέγει τους ακεραίους $x'_1=125$, $x'_2=9$. *Ο Β υπολογίζει το* $z' = 83^{125}449^{9} \bmod 467 = 270$ *και το στέλνει στον Α. Ο Α υπολογίζει το* $w' = 270^{30} \bmod 467 = 68$ *και το στέλνει στον Β.Ο Β υπολογίζει*

$$286^{125}\, 4^{9} \bmod 467 = 25.$$

Αφού $w' = 68 \neq 25$, *ο Β συνεχίζει στο 8ο βήμα του πρωτοκόλλου και εκτελεί τον ακόλουθο έλεγχο: υπολογίζει*

$$c = (109 \cdot 4^{-237})^{125} \bmod 467 = 188$$

και

$$c' = (68 \cdot 4^{-9})^{45} \bmod 467 = 188.$$

Αφού $c= c'$ *ο Β καταλήγει στο συμπέρασμα ότι η s είναι πλαστή.*

Πόρισμα 7.2 *Έστω ένα μήνυμα m και έστω s η (φαινομενική) υπογραφή του Α στο m.*

1. *Αν η s είναι πλαστή, δηλ.* $s \neq m^a \bmod p$ *και οι Α,Β ακολουθήσουν σωστά το πρωτόκολλο 7.2, τότε w = w' (και επομένως το συμπέρασμα του Β ότι η s είναι πλαστή είναι σωστό).*
2. *Έστω ότι η s είναι όντως η υπογραφή του Α για το m, δηλ.* $s = m^a \bmod p$. *Ας υποθέσουμε ότι ο Β ακολουθεί σωστά το πρωτόκολλο 6.2, ενώ ο Α όχι. Τότε η*

πιθανότητα να ισχύει w = w' (δηλ. ο Α να επιτύχει στην αποκήρυξη της υπογραφής) είναι μόνο 1/q.

Τα ακόλουθα θεωρήματα παρατίθενται χωρίς απόδειξη. Για τις αποδείξεις ο αναγνώστης παραπέμπεται στο [Sti02], κεφ.6.

Θεώρημα 7.1 *Αν* $s \not\equiv m^a \pmod p$ *και οι Α,Β ακολουθήσουν το πρωτόκολλο αποκήρυξης, τότε*

$$(wa^{-x2})^{x'1} \equiv (w'a^{-x'2})^{x1} \pmod p.$$

Θεώρημα 7.2 *Έστω* $s \equiv m^a \pmod p$ *και ο Β ακολουθεί το πρωτόκολλο αποκήρυξης. Αν*

$$w \not\equiv m^{xl} a^{x2} \pmod p$$

και

$$w' \not\equiv m^{x'1}\, a^{x'2} \pmod p,$$

τότε η πιθανότητα να ισχύει

$$(wa^{-x2})^{x'1} \not\equiv (w'a^{-x'2})^{x1} \pmod p$$

είναι 1 - 1/g.

Σημείωση 7.2 *(ασφάλεια των αδιαμφισβήτητων υπογραφών)*

1. *Η ασφάλεια του αλγορίθμου 7.2 εξαρτάται από τη δυσκολία επίλυσης του DLP στην κυκλική υποομάδα του* $\mathbb{Z}_p^*$ *τάξεως q.*
2. *Ας υποθέσουμε ότι η οντότητα Β (που επαληθεύει) καταγράφει τα μηνύματα που ανταλλάσσονται στο βήμα 2 του αλγόριθμου 7.2 και τις τυχαίες τιμές* x_1, x_2 *που χρησιμοποιούνται στο πρωτόκολλο επαλήθευσης. Μια τρίτη οντότητα C δεν πρέπει σε καμία περίπτωση να δεχθεί αυτή την εγγραφή από τον Β ως επαλήθευση της υπογραφής s. Για να δούμε το γιατί, αρκεί να δείξουμε πώς ο Β μπορεί να επινοήσει μια επιτυχή εγγραφή του βήματος 2 του αλγόριθμου 7.2 χωρίς τη συμμετοχή του υπογράφοντος Α. Ο Β επιλέγει ένα μήνυμα m, τους ακεραίους* x_1, x_2 *και* l *στο διάστημα [1, q- 1] και υπολογίζει* $s=((m^{x_1}a^{x_2})^{l^{-1}}y^{-x_2})y^{-x_2})^{x_1{}^{-1}} \pmod p$. *Το μήνυμα του πρωτοκόλλου από τον Β στον Α θα είναι* $z = s^{x1}y^{x2} \pmod p$ *και από τον Α στον Β θα είναι* $w = z^l \pmod p$. *Ο αλγόριθμος 7.2 θα δεχθεί την s ως έγκυρη υπογραφή του Α στο μήνυμα m. Η ανάλυση αυτή καθιστά σαφές ότι οι υπογραφές μπορούν να επαληθευθούν μόνο με την άμεση αλληλεπίδραση μεταξύ του υπογράφοντος και της*

οντότητας που επαληθεύει.

7.3 Σχήματα υπογραφής fail-stop

Ένα σχήμα υπογραφής fail - stop παρέχει επιπλέον ασφάλεια ενάντια στην πιθανότητα ένας πολύ ισχυρός «αντίπαλος» να είναι ικανός να πλαστογραφήσει μια υπογραφή. Οι υπογραφές fail - stop έχουν λοιπόν το πλεονέκτημα ότι η πλαστογραφία μπορεί να ανιχνευθεί και τότε ο μηχανισμός υπογραφής παύει να χρησιμοποιείται.

Στην παράγραφο αυτή περιγράφουμε το σχήμα υπογραφής fail - stop που προτάθηκε το 1992 από τους van Heijst και Pedersen και που αποτελεί σχήμα μιας χρήσης (μόνο ένα μήνυμα μπορεί να υπογραφεί με κάποιο δοθέν κλειδί). Το σχήμα αποτελείται από τους αλγόριθμους υπογραφής και επαλήθευσης καθώς και από έναν αλγόριθμο απόδειξης της πλαστογράφησης. Τέλος το σχήμα διαφέρει στην ύπαρξη μιας έμπιστης αρχής (trusted third party - TTP).

Αλγόριθμος 7.3

Παραγωγή κλειδιού για το σχήμα υπογραφής fail—stop των van Heijst και Pedersen.

Συνοπτικά: Η παραγωγή κλειδιού διανέμεται ανάμεσα στην οντότητα A και σε μια TTP.

1. *Η TTP ενεργεί ως εξής:*

   1.1 Επιλέγει τους πρώτους p και q έτσι ώστε p=2q+1 και το DLP στο $\mathbb{Z}_p^*$ είναι απρόσιτο.

   1.2 (Επιλέγει ένα γεννήτορα α της κυκλικής υποομάδας G του $\mathbb{Z}_p^*$ τάξης q)

   1.3 Επιλέγει έναν τυχαίο ακέραιο α, $1 \leq \alpha \leq q - 1$ και υπολογίζει $\beta = g^{\alpha} \bmod p$. Ο ακέραιος α κρατείται κρυφός από την TTP.

   1.4 Στέλνει την τετράδα (p,q,g, β) στην οντότητα A.

2. *Η οντότητα A ενεργεί ως εξής:*

   2.1 Επιλέγει τυχαίους κρυφούς ακεραίους x_1,x_2,y_1,y_2 στο διάστημα [0,p - 1].

   2.2 Υπολογίζει $\beta_1 = g^{x1}\beta^{x2} \bmod p$ και $\beta_2 = g^{y1}\beta^{y2} \bmod p$.

2.3 Το δημόσιο κλειδί του Α είναι $(\beta_1,\beta_2,p,q,g,\beta)$*.Το ιδιωτικό του κλειδί είναι η τετράδα* $\bar{x} = (x_1,x_2,y_1,y_2)$*.*

Σημείωση 7.3 *(κρυφή πληροφορία της TTP) Υπό την υπόθεση ότι το DLP είναι απρόσιτο στην υποομάδα του* $\mathbb{Z}_p^*$ *τάξης q, η μόνη οντότητα που γνωρίζει το α, το διακριτό λογάριθμο του β στη βάση g, είναι η TTP.*

Αλγόριθμος 7.4

Το σχήμα υπογραφής fail — stop των van Heijst και Pedersen.

Συνοπτικά: Αυτό είναι σχήμα ψηφιακής υπογραφής μιας χρήσης του οποίου η ασφάλεια βασίζεται στο DLP στην υποομάδα του $\mathbb{Z}_p^*$*.*

1. *Παραγωγή υπογραφής. Για την υπογραφή ενός μηνύματος* $m \in [0, q-1]$*, η οντότητα Α ενεργεί ως εξής:*
   1.1 Υπολογίζει $s_{1,m} = x_1 + my_1 \bmod q$ *και* $s_{2,m} = x_2 + my_2 \bmod q$*.*
   1.2 Η υπογραφή του Α για το m είναι $s=(s_{1,m}, s_{2,m})$ *και ο Α στέλνει στον Β το* (m,s)
2. *Επαλήθευση. Για να επαληθεύσει την υπογραφή* $(s_{1,m}, s_{2,m})$ *του Α στο m, ο Β ενεργεί ως εξής:*
   2.1 Αποκτά το αυθεντικό δημόσιο κλειδί του Α, $(\beta_1,\beta_2,p,q,g,\beta)$*.*
   2.2 Υπολογίζει $\upsilon_1 = \beta_1\beta^{m}_2 \bmod p$ *και* $\upsilon_2 = g^{s1,m}\,\beta^{s2,m} \bmod p$*.*
   2.3 Αποδέχεται την υπογραφή αν και μόνον αν $\upsilon_1 = \upsilon_2$*.*

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί.

$$\upsilon_1 \equiv \beta_1\beta^{m}_2 \equiv (g^{x1}\,\beta^{x2})(g^{y1}\,\beta^{y2})^m \equiv g^{x1+my1}\,\beta^{x2+my2}$$
$$\equiv g^{s1,m}\,\beta^{s2,m} \equiv \upsilon_2 \pmod p.$$

Ο αλγόριθμος 7.4 είναι ένα σχήμα υπογραφής μιας χρήσης αφού το ιδιωτικό κλειδί του Α μπορεί να υπολογιστεί αν χρησιμοποιηθεί για την υπογραφή δύο μηνυμάτων. Πριν περιγράψουμε τον αλγόριθμο απόδειξης της πλαστογράφησης παραθέτουμε τα ακόλουθα πορίσματα.

Πόρισμα 7.3 *(πλήθος των διακεκριμένων τετράδων που αναπαριστούν ένα δημόσιο κλειδί και μια υπογραφή) Ας υποθέσουμε ότι το δημόσιο κλειδί του Α στον*

αλγόριθμο 7.4 είναι $(\beta_1,\beta_2,p,q,g,\beta)$ *και το ιδιωτικό του κλειδί είναι η τετράδα* $\bar{x} = (x_1,x_2,y_1,y_2)$.

1. *Υπάρχουν ακριβώς* q^2 *τετράδες* $\bar{x}' = (x'_1, x'_2, y'_1, y'_2)$ *με* $x'_1, x'_2, y'_1, y'_2 \in \mathbb{Z}_q$ *οι οποίες δίνουν το ίδιο τμήμα* (β_1,β_2) *του δημοσίου κλειδιού.*
2. *Έστω Τ το σύνολο των* q^2 *τετράδων οι οποίες δίνουν το ίδιο τμήμα του δημοσίου κλειδιού* (β_1,β_2). *Για κάθε* $m \in \mathbb{Z}_q$, *υπάρχουν ακριβώς q τετράδες στο Τ οι οποίες δίνουν την ίδια υπογραφή* $(s_{1,m}, s_{2,m})$ *για το m. Επομένως οι* q^2 *τετράδες στο Τ δίνουν ακριβώς q διαφορετικές υπογραφές για το m.*
3. *Έστω ένα μήνυμα* $m' \in \mathbb{Z}_q$ *διαφορετικό από το m.Τ ότε οι q τετράδες στο Τ οι οποίες δίνουν την υπογραφή* $(s_{1,m}, s_{2,m})$ *του Α για το m, δίνουν q διαφορετικές υπογραφές για το m'.*

Παράδειγμα 7.6 *(επεξήγηση του πορίσματος 7.3)*

Έστω p = 29 και q = 7. Ο g = 16 είναι γεννήτορας της υποομάδας του $\mathbb{Z}_p^*$ *τάξης q. Παίρνουμε* $\beta=g^5 \bmod 29=23$. *Υποθέτουμε ότι το ιδιωτικό κλειδί του Α είναι* $\bar{x} = (2,3,5,2)$. *Το δημόσιο κλειδί του Α είναι* $\beta_1 = g^2\beta^3 \bmod 29=7$, $\beta_2 = g^5\beta^2 \bmod 29=16$. *Ο ακόλουθος πίνακας περιέχει τις* $q^2 = 49$ *τετράδες οι οποίες δίνουν το ίδιο δημόσιο κλειδί.*

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

Αν οι 49 τετράδες του παραπάνω πίνακα χρησιμοποιηθούν για την υπογραφή του μηνύματος m = 1 θα προκύψουν ακριβώς q = 7 ζεύγη υπογραφής $(s_{1,m}, s_{2,m})$. *Ο ακόλουθος πίνακας περιέχει τα πιθανά ζεύγη υπογραφής καθώς και τις τετράδες που παράγουν το κάθε ζεύγος.*

ζεύγος υπογραφής	(26)	(33)	(40)	(54)	(61)	(05)	(12)
	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

Ο ακόλουθος πίνακας περιέχει, για κάθε μήνυμα $m' \in \mathbb{Z}_7$, όλα τα ζεύγη υπογραφής για τις 7 τετράδες οι οποίες δίνουν την υπογραφή (0,5) του Α για το m=1.

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

Σημείωση 7.4 *(πιθανότητα επιτυχούς πλαστογραφίας στον αλγόριθμο 7.4) Ας υποθέσουμε ότι ένας «αντίπαλος» (ο πλαστογράφος) επιθυμεί να εξάγει την υπογραφή του Α σε κάποιο μήνυμα m'. Υπάρχουν δύο πιθανότητες που πρέπει να μελετήσουμε.*

1. *Ο πλαστογράφος έχει πρόσβαση μόνο στο δημόσιο κλειδί του υπογράφοντος (δηλ., ο πλαστογράφος δεν έχει στην κατοχή του ένα μήνυμα και μια έγκυρη υπογραφή γι' αυτό). Από το πόρισμα 7.3 (3), η πιθανότητα η υπογραφή που δημιουργήθηκε από τον «αντίπαλο» να είναι ίδια με την υπογραφή του Α για το m' είναι μόνο $q^2/q = 1/q$. Η πιθανότητα αυτή είναι ανεξάρτητη από τα υπολογιστικά μέσα του «αντιπάλου».*
2. *Ο πλαστογράφος έχει πρόσβαση σε ένα μήνυμα m και μια υπογραφή ($s_{1,m}$, $s_{2,m}$) που δημιούργησε ο υπογράφων. Από το πόρισμα 7.3 (3), η πιθανότητα η υπογραφή που δημιουργήθηκε από τον «αντίπαλο» να είναι ίδια με την υπογραφή του Α για το m' είναι μόνο 1/q. Ξανά, η πιθανότητα αυτή είναι ανεξάρτητη από τα υπολογιστικά μέσα του «αντιπάλου».*

   Ας υποθέσουμε τώρα ότι ένας «αντίπαλος» έχει πλαστογραφήσει την υπογραφή του Α σε ένα μήνυμα και η υπογραφή πέρασε το στάδιο

επαλήθευσης του αλγορίθμου 7.4. Στόχος είναι ο Α να μπορεί να αποδείξει ότι η υπογραφή αυτή είναι πλαστή. Ο ακόλουθος αλγόριθμος δείχνει πώς μπορεί ο Α, με υψηλή πιθανότητα, να χρησιμοποιήσει την πλαστογραφημένη υπογραφή ώστε να εξάγει τον κρυφό ακέραιο α. Αφού ο α υποτίθεται ότι είναι γνωστός μόνο στην ΤΤΡ, μπορεί να χρησιμεύσει ως αποδεικτικό της πλαστογράφησης.

Αλγόριθμος 7.5

Αλγόριθμος απόδειξης της πλαστογράφησης για τον αλγόριθμο 7.4.

Συνοπτικά: Για να αποδείξει ότι μια υπογραφή $s' = (s'_{1,m}, s'_{2,m})$ σε ένα μήνυμα m είναι πλαστή, ο υπογράφων εξάγει τον ακέραιο $\alpha = \log_g \beta$ ο οποίος χρησιμεύει ως αποδεικτικό της πλαστογράφησης. Ο υπογράφων (οντότητα Α) ενεργεί ως εξής:

1. *Υπολογίζει ένα ζεύγος υπογραφής $s = (s_{1,m}, s_{2,m})$ για το μήνυμα m χρησιμοποιώντας το ιδιωτικό του κλειδί $\bar{x}$ (βλ. αλγόριθμο 6.3).*
2. *Αν $s = s'$ επιστρέφει στο βήμα 1.*
3. *Υπολογίζει $\alpha = (s_{1,m}, s'_{1,m}) \cdot (s_{2,m}, s'_{2,m})^{-1} \bmod q$.*

Απόδειξη ότι ο αλγόριθμος 7.5 λειτουργεί.

Από το πόρισμα 7.3, η πιθανότητα να ισχύει $s = s'$ στο βήμα 1 του αλγορίθμου 7.5 είναι 1/q. Από τον αλγόριθμο επαλήθευσης (αλγόριθμος 7.4) έχουμε

$$a^{s1,m}\, \beta^{s2,m} \equiv a^{s'1,m}\, \beta^{s'2,m} \pmod{p}$$

ή

$$a^{s1,m - s'1,m} \equiv a^{a(s'2,m - s2,m)} \pmod{p}$$

ή

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

Επομένως

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

Κεφάλαιο 8

Αλλά σχήματα υπογραφής

Τα σχήματα υπογραφής που περιγράφονται σε αυτό το κεφάλαιο δεν ανήκουν σε καμία από τις κατηγορίες που περιγράφηκαν στα προηγούμενα κεφάλαια. Γι' αυτό το λόγο ο τίτλος του κεφαλαίου είναι απολύτως δικαιολογημένος.

8.1 Ψηφιακές υπογραφές εποπτείας (Arbitrated digital signatures)

Ορισμός 8.1 *Ένα σχήμα ψηφιακής υπογραφής εποπτείας είναι ένας μηχανισμός ψηφιακής υπογραφής ο οποίος απαιτεί τη συμμετοχή μιας ανεπιφύλακτα έμπιστης αρχής (TTP) για την παραγωγή της υπογραφής και την επαλήθευση.*

Ο αλγόριθμος 8.2 απαιτεί έναν αλγόριθμο κρυπτογράφησης συμμετρικού κλειδιού $E = \{E_k : k \in K,\}$, όπου K ο χώρος κλειδιών. Υποθέτουμε ότι τα ορίσματα και οι εικόνες κάθε E_k είναι ακολουθίες l - bit και έστω $h : \{0,1\}^* —^* \{0,1\}^l$ μια συνάρτηση κατακερματισμού μονής κατεύθυνσης. Η TTP επιλέγει ένα κλειδί $k_T \in K$ το οποίο κρατά κρυφό. Για την επαλήθευση μιας υπογραφής, μια οντότητα πρέπει να μοιραστεί ένα συμμετρικό κλειδί με την TTP.

Αλγόριθμος 8.1

Παραγωγή κλειδιού για υπογραφές εποπτείας.

Συνοπτικά: Κάθε οντότητα επιλέγει ένα κλειδί και το μεταδίδει κρυφά στην TTP. Κάθε οντότητα A ενεργεί ως εξής:

1. *Επιλέγει ένα τυχαίο κρυφό κλειδί $k_A \in K$.*
2. *Κρυφά και χρησιμοποιώντας κάποια μέσα πιστοποίησης, η οντότητα A θέτει το k_A στη διάθεση της TTP.*

Αλγόριθμος 8.2

Παραγωγή υπογραφής και επαλήθευση για υπογραφές εποπτείας.

Συνοπτικά: Η οντότητα A παράγει υπογραφές χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης συμμετρικού κλειδιού E_{k_A} .Οποιαδήποτε οντότητα B μπορεί να επαληθεύσει την υπογραφή του A με τη συνεργασία της TTP.

1. *Παραγωγή υπογραφής. Για την υπογραφή ενός μηνύματος m, η οντότητα A ενεργεί ως εξής:*

1.1 Υπολογίζει το H = h(m).

1.2 Κρυπτογραφεί το H με το E για να πάρει το u = E_{k_A}(H).

1.3 Στέλνει το u μαζί με κάποια ακολουθία αναγνώρισης I_A στην TTP.

1.4 Η TTP υπολογίζει το $E_{k_A}^{-1}$ (u) για να πάρει το H.

1.5 Η TTP υπολογίζει το s = E_{k_T} (H || I_A) και το στέλνει στον A.

1.6 Η υπογραφή του A για το m είναι s.

2. *Επαλήθευση. Οποιαδήποτε οντότητα B μπορεί να επαληθεύσει την υπογραφή s του A στο m ενεργώντας ως εξής:*

2.1 Υπολογίζει το υ = E_{k_B} (s).

2.2 Στέλνει το υ και κάποια ακολουθία αναγνώρισης I_B στην TTP.

2.3 Η TTP υπολογίζει το $E_{k_B}^{-1}$ (υ) για να πάρει το s.

2.4 Η TTP υπολογίζει το $E_{k_T}^{-1}$ (s) για να πάρει το H || I_A.

2.5 Η TTP υπολογίζει το w = E_{k_B} (H || I_A) και το στέλνει στον B.

2.6 Ο B υπολογίζει το $E_{k_B}^{-1}$ (w) για να πάρει το H || I_A.

2.7 Ο B υπολογίζει από το m το H' = h(m).

2.8 Ο B αποδέχεται την υπογραφή αν και μόνον αν H' = H.

Σημείωση 8.1 *(ασφάλεια των υπογραφών εποπτείας) Η ασφάλεια του αλγορίθμου 8.2 βασίζεται στο επιλεγμένο σχήμα κρυπτογράφησης συμμετρικού κλειδιού και στην ασφαλή διανομή των κλειδιών μεταξύ των συμμετεχόντων.*

Σημείωση 8.2 (*χαρακτηριστικά επίδοσης των υπογραφών εποπτείας) Εφόσον οι αλγόριθμοι συμμετρικού κλειδιού είναι τυπικά πολύ γρηγορότεροι από τις τεχνικές δημοσίου κλειδιού, η παραγωγή υπογραφής και η επαλήθευση, που περιγράφονται στον αλγόριθμο 8.2, είναι (σχετικά) πολύ αποδοτικές διαδικασίες. Ένα μειονέκτημα είναι ότι απαιτείται αλληλεπίδραση με την TTP, γεγονός που επιβαρύνει την TTP και απαιτεί επιπρόσθετη ανταλλαγή μηνυμάτων μεταξύ αυτής και των οντοτήτων που συμμετέχουν.*

8.2 Το σχήμα υπογραφής ESIGN

Το ESIGN (συντομογραφία του Efficient digital SIGNature) είναι άλλο ένα σχήμα ψηφιακής υπογραφής του οποίου η ασφάλεια βασίζεται στη δυσκολία του προβλήματος της παραγοντοποίησης ακεραίων. Είναι σχήμα υπογραφής με

παράρτημα και απαιτεί μια συνάρτηση κατακερματισμού μονής κατεύθυνσης h : {0,1} → $\mathbb{Z}_n$.*

Αλγόριθμος 8.3

Παραγωγή κλειδιού για το ESIGN.

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

1. *Επιλέγει τους περίπου ίδιου μήκους bit τυχαίους πρώτους p και q τέτοιους ώστε p≥q και p, q έχουν το ίδιο μήκος σε bit.*
2. *Υπολογίζει το n =$p^2 \cdot q$.*
3. *Επιλέγει ένα θετικό ακέραιο k ≥ 4.*
4. *Το δημόσιο κλειδί του Α είναι το ζεύγος (n, k), ενώ το ιδιωτικό του είναι το ζεύγος (p,q).*

Αλγόριθμος 8.4

Παραγωγή υπογραφής ESIGN και επαλήθευση.

Συνοπτικά: Ο αλγόριθμος υπογραφής υπολογίζει έναν ακέραιο s τέτοιον ώστε το s^k mod n να ανήκει σε ένα συγκεκριμένο διάστημα που καθορίζεται από το μήνυμα. Η διαδικασία της επαλήθευσης αποδεικνύει ότι το s^k mod n όντως ανήκει στο συγκεκριμένο διάστημα.

1. *Παραγωγή υπογραφής. Για να υπογράψει ένα μήνυμα m το οποίο είναι μια δυαδική ακολουθία αυθαίρετου μήκους, η οντότητα Α ενεργεί ως εξής:*

   1.1 Υπολογίζει το υ= h(m).

   1.2 Επιλέγει έναν τυχαίο κρυφό ακέραιο x, 0 ≤ x < p · q.

   1.3 Υπολογίζει w = $\lceil((\upsilon - x^k) mod\ n)/(p \cdot q)\rceil$ *και y= w · $(kx^{k-1})^{-1}$ mod p.*

   1.4 Υπολογίζει s = x + y · p · q mod n.

   1.5 Η υπογραφή του Α για το m είναι s.

2. *Επαλήθευση. Για να επαληθεύσει την υπογραφή s του Α στο m, ο Β ενεργεί ως εξής:*

   2.1 Αποκτά το αυθεντικό δημόσιο κλειδί του Α, (n,k).

   2.2 Υπολογίζει u = s^k mod n και z = h(m).

   2.3 Αν z ≤ u ≤ z + $2^{\lceil \frac{2}{3} lgn \rceil}$ *τότε αποδέχεται την υπογραφή, αλλιώς την απορρίπτει.*

Απόδειξη ότι η επαλήθευση της υπογραφής λειτουργεί.

Σημειώνουμε ότι

$$s^k \equiv (x + ypq)^k \equiv \sum_{i=0}^{k} \binom{k}{i} x^{k-i}(ypq)^i \equiv x^k + kypqx^{k-1} \pmod{n}.$$

Όμως $kx^{k-1}y \equiv w \pmod{p}$ *και επομένως* $kx^{k-1}y = w + lp$ *για κάποιο* $l \in \mathbb{Z}$ *.*

Αρα, $s^k \equiv x^k + pq(w + lp) \equiv x^k + pqw \equiv x^k + pq \left\lceil \frac{(h(m)-x^k) mod n}{pq} \right\rceil \equiv x^k +$

$pq \left(\frac{h(m)-x^k+jn+\epsilon}{pq}\right) \pmod{n}$*, όπου* $\epsilon = (x^k - h(m)) mod\ pq$*. Επομένως,* $s^k \equiv x^k +$

$h(m) - x^k + \epsilon = h(m) + \epsilon \pmod{n}$*. Αφού* $0 \leq \epsilon \leq p \cdot q$*, έπεται ότι* $h(m) \leq s^k \bmod n \leq$

$h(m) + pq \leq h(m) + 2^{\left\lceil \frac{2}{3} lgn \right\rceil}$ *όπως απαιτείται.*

Παράδειγμα 8.1 *(το σχήμα υπογραφής ESIGN με τεχνητά μικρές παραμέτρους) Για τις ανάγκες του παραδείγματος θεωρούμε τα μηνύματα ως ακεραίους* m *με* $0 \leq m \leq n$ *και τη συνάρτηση κατακερματισμού* h *τέτοια ώστε* $h(m) = m$*.*

Παραγωγή κλειδιού. Ο Α επιλέγει τους πρώτους $p = 17389$ *και* $q = 15401$*,το θετικό ακέραιο* $k = 4$ *και υπολογίζει το* $n = p^2q = 4656913120721$*. Το δημόσιο κλειδί του Α είναι* $(n = 4656913120721, k = 4)$*.Το ιδιωτικό του κλειδί είναι* $(p = 17389, q = 15401)$*.*

Παραγωγή υπογραφής. Για να υπογράψει το μήνυμα $m = 3111527988477$*, ο Α υπολογίζει* $υ=h(m) = 3111527988477$ *και επιλέγει τον τυχαίο κρυφό ακέραιο* $x = 14222$ *έτσι ώστε* $0 \leq x \leq p \cdot q$*. Ο Α στη συνέχεια υπολογίζει* $w = \lceil ((υ - x^k) mod n)/(pq) \rceil$ *=* $[2848181921806/267807989] = [10635.16414] = 10636$ *και* $y = w(kx^{k-1})^{-1} \bmod p = 10636(4 \times 14222^3)^{-1} \bmod 17389 = 9567$*. Τέλος ο Α υπολογίζει την υπογραφή* $s = x + ypq \bmod n = 2562119044985$*.*

Επαλήθευση υπογραφής. Ο Β αποκτά το δημόσιο κλειδί του Α $(n= 4656913120721, k=4)$ *και υπολογίζει* $u = s^k \bmod n = 3111751837675$*. Αφού* $3111527988477 \leq 3111751837\ 675 \leq 3111527988477 + 2^{29}$*, ο Β αποδέχεται την υπογραφή (εδώ* $\left\lceil \frac{2}{3} lgn \right\rceil = 29$*).*

Σημείωση 8.3 *(ασφάλεια του ESIGN)*

1. *Το modulus* $n = p^2q$ *που εμφανίζεται στον αλγόριθμο 8.4 διαφέρει από ένα RSA modulus στο ότι έχει έναν επαναλαμβανόμενο παράγοντα του* p*. Δεν είναι γνωστό αν η παραγοντοποίηση moduli αυτής της μορφής είναι ευκολότερη ή δυσκολότερη από την παραγοντοποίηση ακεραίων οι οποίοι είναι απλώς το γινόμενο δύο διακεκριμένων πρώτων.*

2. *Δοθείσης μιας έγκυρης υπογραφής s για ένα μήνυμα m, ένας «αντίπαλος» θα μπορούσε να πλαστογραφήσει μια υπογραφή για ένα μήνυμα m' αν το h(m') είναι τέτοιο ώστε* $h(m') \leq u \leq h(m') + 2^{\lceil \frac{2}{3} lgn \rceil}$ *(όπου* $u = s^k \bmod n$*). Αν βρεθεί ένα m' με αυτήν την ιδιότητα τότε η s θα είναι μια υπογραφή για αυτό. Αυτό θα συμβεί αν τα h(m) και h(m') συμφωνούν στα (lgn)/3 bits υψηλής τάξεως. Υποθέτοντας ότι η h συμπεριφέρεται ως μια τυχαία συνάρτηση, κάποιος θα περίμενε να δοκιμάσει* $2^{(lgn)/3}$ *διαφορετικές τιμές για το m' πριν παρατηρήσει την παραπάνω ομοιότητα μεταξύ h(m) και h(m').*
3. *Μια άλλη πιθανή προσέγγιση πλαστογραφίας είναι η εύρεση ενός ζεύγους μηνυμάτων m και m' έτσι ώστε τα h(m) και h(m') να συμφωνούν στα (lgn)/3 bits υψηλής τάξεως. Από το παράδοξο των γενεθλίων, ένα τέτοιο ζεύγος αναμένεται να βρεθεί σε* $O(2^{(lgn)/6})$ *δοκιμές. Αν ένας «αντίπαλος» μπορεί να κάνει το νόμιμο υπογράφοντα να υπογράψει ένα μήνυμα m, τότε η ίδια υπογραφή θα είναι υπογραφή και για το m'.*
4. *Αν το μέγεθος του ακεραίου n είναι τέτοιο ώστε η παραγοντοποίηση του να είναι ανέφικτη, τότε οι περιπτώσεις 2 και 3 είναι εξαιρετικά απίθανο να συμβούν.*

Σημείωση 8.4 *(χαρακτηριστικά επίδοσης των υπογραφών ESIGN) Η παραγωγή υπογραφής στον αλγόριθμο 8.4 είναι πολύ αποδοτική διαδικασία. Για μικρές τιμές του k (π.χ., k = 4), το πιο εντατικό υπολογιστικά τμήμα είναι η modular αντιστροφή που απαιτείται στο βήμα 2.3. Αναλόγως με την εφαρμογή, η αντιστροφή αυτή αντιστοιχεί σε ένα μικρό αριθμό modular πολλαπλασιασμών με modulus p. Για k = 4 και ένα 768-bit modulus n, η παραγωγή υπογραφής ESIGN είναι 10 με 100 φορές γρηγορότερη από την παραγωγή υπογραφής RSA με modulus ισοδύναμου μεγέθους. Η επαλήθευση των υπογραφών είναι επίσης πολύ αποδοτική διαδικασία και συγκρίνεται με το RSA στην περίπτωση που αυτό χρησιμοποιεί ένα μικρό δημόσιο εκθέτη.*

Παράρτημα

Βιβλιογραφία

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

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

Ε. Ζάχος. Αλγόριθμοι και Πολυπλοκότητα. Εκδόσεις Ε.Μ.Π., 2003.

Β. Ζήκας. Διπλωματική Εργασία: Αποδείξεις Μηδενικής Γνώσης.

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

Κ. Χαλάτσης. Η Παρούσα Κατάσταση σε Θέματα Κρυπτογραφίας. Τμήμα Πληροφορικής & Τηλεπικοινωνιών ΕΚΠΑ, Μάιος 2003.

Κ. Μπονίκος. Κρυπτογραφία. Άρθρο στο Περιοδικό Κυβερνογράφοι, Τεύχος 5ο.

Κ. Σταματίου. Νέες Εξελίξεις στην Κρυπτογραφία. Ειδικά Θέματα, 2004.

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

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

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

J. Tattersall. Elementary Number Theory in Nine Chapters. Cambridge U.P., 2001.

O. Goldreich. Modern Cryptography, Probabilistic Proofs and Pseudo-Randomness. Spring.

Richard G. Baldwin. Signing Messages using Redundancy Functions in Java. Java Programming: Notes # 731.

Federal Information: Processing Standards Publication 186 (FIPS PUB 186). Specifications for Digital Signature Standard (DSS). May, 1994.

Burt Kaliski. RSA Laboratories. RSA Digital Signature Standards. RSA Conference 2000.

Burt Kaliski. RSA Laboratories. Raising the Standard for RSA Signatures. Technical Notes and Reports, February 2003.

Mihir Bellare, Phillip Rogaway. The Exact Security of Digital Signatures. Advances in Ciyptology - EUROCRYPT 96, volume 1070 of Lecture Notes in Computer Science. Springer - Verlag, 1996.

Jean-Sebastien Coron. Optimal Security Proofs for PSS and Other Signature Schemes. Advances in Ciyptology - EUROCRYPT 2002, volume 2332 of Lecture Notes in Computer Science. Springer, 2002.

Σελίδες στο Διαδίκτυο:

www.itl.nist.gov, www.cryptogram.gr, www.axion.physics.ubc.ca/crypt.html, http://en.wikipedia.org/wiki/Digital_signature,