8 ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

8.1. Εισαγωγή

Όπως είδαμε στο προηγούμενο κεφάλαιο, η ανταλλαγή κλειδιών πολλές φορές συνοδεύεται από αυθεντικοποίηση. Η αυθεντικοποίηση μπορεί να περιλαμβάνει ψηφιακές υπογραφές όπου ένα μέλος αποδεικνύει την ταυτότητά του έμμεσα δείχνοντας ότι γνωρίζει κάποια μυστική ποσότητα πληροφορίας, η οποία είναι συνδεδεμένη με την ταυτότητα του μέλους.

Είδαμε επίσης στο Κεφάλαιο 4 ότι η αυθεντικοποίηση είναι δυνατή και σε κάποιο μήνυμα. Η αυθεντικοποίηση μηνύματος αναφέρεται σε δύο επίπεδα, στην αυθεντικοποίηση του καναλιού επικοινωνίας και στην αυθεντικοποίηση της πηγής. Η αυθεντικοποίηση του καναλιού επικοινωνίας μεταξύ δύο μελών, σημαίνει ότι τα μέλη αυτά έχουν τη δυνατότητα να ελέγχουν ποια μηνύματα έχουν δημιουργηθεί και σταλεί από οποιονδήποτε από τους δύο, χωρίς να φαίνεται σε ποιον ανήκει το μήνυμα. Η αυθεντικοποίηση της πηγής αναφέρεται στη δυνατότητα διάκρισης του αποστολέα του μηνύματος.

Η αυθεντικοποίηση τόσο στην ταυτότητα ενός μέλους, όσο και σε ένα μήνυμα, μπορεί να πραγματοποιηθεί με μηχανισμούς ψηφιακών υπογραφών. Στο κεφάλαιο αυτό θα εξετάσουμε πιο συστηματικά τις ψηφιακές υπογραφές.

8.2. Απαιτήσεις – ορισμοί

Η κρυπτογραφία παρέχει τα εργαλεία ώστε να προστατευθούν δύο ή περισσότερα επικοινωνούντα μέλη από αντιπάλους. Οι τρόποι και ευκαιρίες επίθεσης του αντιπάλου καθορίζουν τις απαιτήσεις των μελών για προστασία. Η προστασία με τη σειρά της προσφέρεται στα μέλη με τη μορφή των κρυπτογραφικών υπηρεσιών.

Οι ψηφιακές υπογραφές απευθύνονται σε δύο κρυπτογραφικές υπηρεσίες, στην αυθεντικοποίηση και στη μη απάρνηση. Όπως αναφέραμε στην εισαγωγή του κεφαλαίου, η αυθεντικοποίηση μπορεί να αναφερθεί στην αυθεντικοποίηση της ταυτότητας ενός μέλους, ή στην αυθεντικοποίηση ενός μηνύματος. Η αυθεντικοποίηση παρέχει προστασία από ενεργητικές επιθέσεις, όπου ο αντίπαλος έχει τη δυνατότητα να τροποποιεί ή να επαναμεταδίδει μηνύματα, κατά τέτοιον τρόπο

ώστε τα μηνύματα να φαίνονται ότι προέρχονται από κάποια άλλη οντότητα. Η αυθεντικοποίηση παρέχει τη δυνατότητα ανίχνευσης των αυθαίρετων τροποποιήσεων ή επαναμεταδόσεων.

Κατά την ίδρυση μιας συνόδου επικοινωνίας όπου απαιτείται η αυθεντικοποίηση των ταυτοτήτων των επικοινωνούντων μελών, το κάθε μέλος αποδεικνύει την ταυτότητά του, προτού αρχίσει η ανταλλαγή πληροφοριών. Η ίδρυση της συνόδου επικοινωνίας συνοδεύεται και από την εδραίωση ενός κλειδιού συνόδου. Σε αυτό το στάδιο ο αντίπαλος επιχειρεί να προσποιηθεί την ταυτότητα ενός ή και των δύο μελών, ώστε να ελέγξει την επιλογή του κλειδιού συνόδου. Η αυθεντικοποίηση των ταυτοτήτων των μελών αποκλείει τον αντίπαλο από μια τέτοια επίθεση.

Μια τρίτη απαίτηση είναι η μη απάρνηση. Αυτή η απαίτηση θεωρεί ότι ο αντίπαλος είναι κάποιο από τα (νόμιμα) επικοινωνούντα μέλη. Έστω ότι η Αλίκη και ο Βύρων κλείνουν μια συμφωνία αγοραπωλησίας μετοχών. Η Αλίκη δεσμεύεται να πουλήσει στον Βύρωνα έναν αριθμό μετοχών σε μια ορισμένη τιμή. Αν πέσει η τιμή της μετοχής προτού πραγματοποιηθεί η συναλλαγή, ο Βύρων μπορεί να ισχυρισθεί ότι δε συμφώνησε στην αγορά της μετοχής αυτής. Αν ανέβει η τιμή της μετοχής, η Αλίκη μπορεί να ισχυρισθεί ότι ο Βύρων δε ζήτησε μετοχές, ή μπορεί να μεταβάλλει την ποσότητα και να ισχυρισθεί ότι ο Βύρων ζήτησε λιγότερες μετοχές. Η υπηρεσία της μη απάρνησης προσφέρει αποδείξεις αφενός μεν ότι η Αλίκη δέχεται να πουλήσει έναν ορισμένο αριθμό μετοχών σε μια ορισμένη τιμή στον Βύρωνα, αφετέρου δε ότι ο Βύρων δέχεται να αγοράσει τον αριθμό των μετοχών στην συμφωνηθείσα τιμή. Η ψηφιακή υπογραφή παρέχει τους μηχανισμούς επίλυσης της αμφισβήτησης της συναλλαγής και μπορεί να γίνει στο βαθμό που η ψηφιακή υπογραφή θα έχει νομική ισχύ.

Συνοψίζοντας, οι απαιτήσεις ασφάλειας της ψηφιακής υπογραφής είναι οι εξής:

- *Αυθεντικοποίηση της πηγής του μηνύματος.* Μεταξύ δύο επικοινωνούντων μελών, ο παραλήπτης ενός μηνύματος θα πρέπει να έχει τη δυνατότητα να επιβεβαιώσει την ταυτότητα του αποστολέα του μηνύματος.
- *Μη απάρνηση πηγής.* Σε περίπτωση που ο αποστολέας αρνηθεί ότι έστειλε το μήνυμα, θα πρέπει ο παραλήπτης του μηνύματος να είναι σε θέση να αποδείξει ότι το μήνυμα στάλθηκε από τον αποστολέα.
- *Μη απάρνηση προορισμού.* Σε περίπτωση που ο παραλήπτης αρνηθεί ότι παρέλαβε το μήνυμα, θα πρέπει να υπάρχει δυνατότητα απόδειξης ότι το μήνυμα παραλήφθηκε από τον παραλήπτη.

Η αυθεντικοποίηση της πηγής του μηνύματος προστατεύει τον αποστολέα ακόμα και σε περίπτωση που ο παραλήπτης τροποποιήσει το αρχικό μήνυμα του αποστολέα. Η ψηφιακή υπογραφή είναι επιθυμητή όταν δεν υπάρχει πλήρης εμπιστοσύνη μεταξύ του αποστολέα και του παραλήπτη, οπότε απαιτείται κάτι περισσότερο από αυθεντικοποίηση.

Η υπηρεσία της μη απάρνησης πηγής συναντάται συχνότερα από τη μη απάρ-

νηση προορισμού, καθώς οι ηλεκτρονικές συναλλαγές ξεκινούν πάντοτε από τον αποστολέα, και τις περισσότερες φορές οι ενέργειες του παραλήπτη γίνονται φανερές και αποδεικνύονται έτσι αυτόματα. Η μη απάρνηση της πηγής απαιτείται για να αποδειχθεί ότι ο παραλήπτης δεν ενήργησε αυθαίρετα χωρίς την αίτηση του αποστολέα. Έτσι η μη απάρνηση προορισμού δεν είναι υποχρεωτική.

Αυτές ήταν οι απαιτήσεις ασφάλειας των ψηφιακών υπογραφών. Προτού προχωρήσουμε στον ορισμό της ψηφιακής υπογραφής, θα συγκρίνουμε τις ψηφιακές υπογραφές με τις χειρόγραφες υπογραφές για να κατανοήσουμε και τις τεχνικές απαιτήσεις που μας οδηγούν στις ψηφιακές υπογραφές. Στον Πίνακα 8.1 φαίνονται οι αναλογίες μεταξύ χειρόγραφων και ψηφιακών υπογραφών.

Χειρόγραφες υπογραφές	Ψηφιακές υπογραφές
• Αναγνώριση της ταυτότητας του υπογεγραμμένου	• Αυθεντικοποίηση της ταυτότητας του υπογεγραμμένου: - Η ψηφιακή υπογραφή θα πρέπει να συνδέει την ταυτότητα ενός μέλους με κάποια πληροφορία με τέτοιον τρόπο ώστε να είναι αναμφισβήτητη η αναγνώριση του μέλους.
• Αναγνώριση της αυθεντικότητας του υπογεγραμμένου κειμένου	• Αυθεντικοποίηση του μηνύματος προορισμού - Η ψηφιακή υπογραφή θα πρέπει να αντιστοιχεί σε πληροφορία η οποία να εξαρτάται από το υπογεγραμμένο μήνυμα και τον υπογεγραμμένο.
• Δυνατότητα επαλήθευσης της υπογραφής από τρίτους	• Δυνατότητα επαλήθευσης της ψηφιακής υπογραφής από τρίτους: - Η επαλήθευση της ψηφιακής υπογραφής θα πρέπει να είναι εύκολη διαδικασία και θα πρέπει να μπορεί να εκτελεσθεί από οποιονδήποτε.

Πίνακας 8.1 Σύγκριση χειρόγραφης και ψηφιακής υπογραφής

Άλλα χαρακτηριστικά των χειρόγραφων υπογραφών είναι η δήλωση της ημερομηνίας που πραγματοποιείται η υπογραφή και πολλές φορές η δήλωση της τοποθεσίας. Το μειονέκτημα της χειρόγραφης υπογραφής είναι η επαλήθευσή της, δηλαδή ο έλεγχος γνησιότητας της υπογραφής. Στις ψηφιακές υπογραφές η διαδικασία ελέγχου είναι υποχρεωτική, ενώ στις χειρόγραφες υπογραφές η διαδικασία ελέγχου παραλείπεται και εκτελείται μόνον σε περίπτωση διαφωνίας.

ΟΡΙΣΜΟΣ 8.1 – Έστω ένα σύνολο μηνυμάτων $\boldsymbol{M}$, ένα σύνολο τιμών $\boldsymbol{S}$, και μια συνάρτηση μετασχηματισμού S_A: $\boldsymbol{M} \rightarrow \boldsymbol{S}$, μιας οντότητας με ταυτότητα A. Το σύνολο $\boldsymbol{S}$ αποτελεί σύνολο υπογραφών, όταν μόνον η οντότητα A για οποιοδήποτε $m \in \boldsymbol{M}$ μπορεί να υπολογίσει «με ευκολία» την $S_A(m) = s \in \boldsymbol{S}$. Η S_A ονομάζεται ***πράξη υπογραφής***.

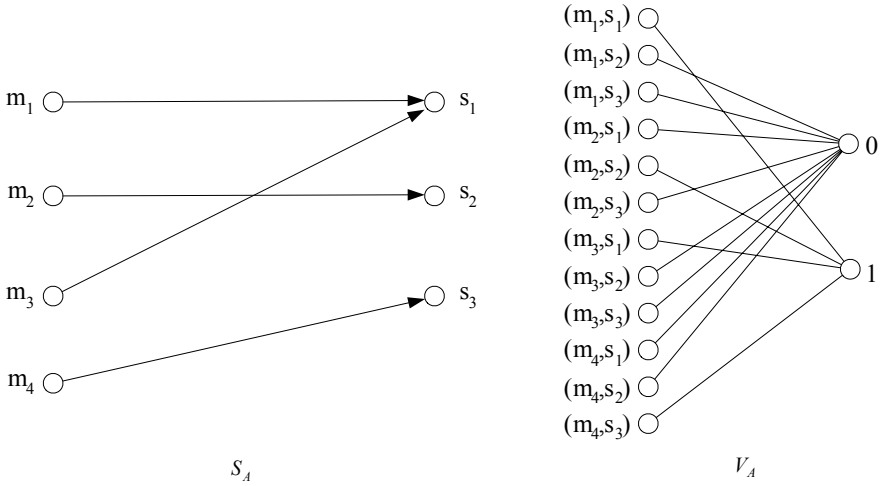
ΟΡΙΣΜΟΣ 8.2 – Έστω ένα σύνολο μηνυμάτων $\boldsymbol{M}$ και έστω η μπουλιανή συνάρτηση V_A: $\boldsymbol{S}\times\boldsymbol{M} \rightarrow \{0, 1\}$, όπου το **0** αντιστοιχεί στο «ψευδές» και το **1** αντιστοιχεί στο «αληθές». Η συνάρτηση V_A ορίζει την ***πράξη επαλήθευσης*** αν μπορεί να υπολογισθεί «με ευκολία» από οποιονδήποτε έτσι ώστε για δεδομένο $(s, m)\in \mathbf{S}\times\boldsymbol{M}$, είναι:

$$V_A(s,m) = \begin{cases} 1, & \text{αν } S_A(m) = s \\ 0, & \text{αν } S_A(m) \neq s \end{cases}$$

Ο όρος «ευκολία» που περιέχεται στους παραπάνω ορισμούς αναφέρεται στην πολυπλοκότητα που αντιμετωπίζει η οντότητα η οποία επιχειρεί να υπολογίσει την αντίστοιχη συνάρτηση. Έτσι από το σύνολο των μηνυμάτων στο σύνολο των υπογραφών, μόνο η οντότητα A είναι σε θέση να υπολογίσει s τέτοιο ώστε για δεδομένο $m\in\boldsymbol{M}$, να είναι $S_A(m)$, ενώ για κάποιον αντίπαλο είναι υπολογιστικά αδύνατο να εκτελέσει αυτόν τον υπολογισμό. Εφόσον η οντότητα A αποκαλύψει ένα ζεύγος (s, m) όπου $S_A(m) = s$, θα πρέπει να είναι υπολογιστικά δυνατή η επαλήθευση ότι όντως είναι $S_A(m) = s$, προκειμένου να θεωρηθεί έγκυρη η υπογραφή. Η πράξη επαλήθευσης γίνεται με τη βοήθεια της συνάρτησης επαλήθευσης V_A.

ΟΡΙΣΜΟΣ 8.3 – Η πράξη ψηφιακής υπογραφής S_A, μαζί με την πράξη επαλήθευσης V_A, αποτελούν ένα ***σύστημα ψηφιακής υπογραφής*** για την οντότητα A.

ΠΑΡΑΔΕΙΓΜΑ 8.1 – Σύστημα ψηφιακής υπογραφής. Έστω το σύνολο των μηνυμάτων $\mathbf{M}=\{m_1, m_2, m_3, m_4, m_5\}$ και το σύνολο υπογραφών $\mathbf{S}=\{s_1, s_2, s_3\}$. Στο Σχήμα 8.1 ορίζεται η πράξη υπογραφής και η πράξη επαλήθευσης.



Σχήμα 8.1 Παράδειγμα πράξεων υπογραφής και επαλήθευσης για τα σύνολα του Παραδείγματος 8.1.

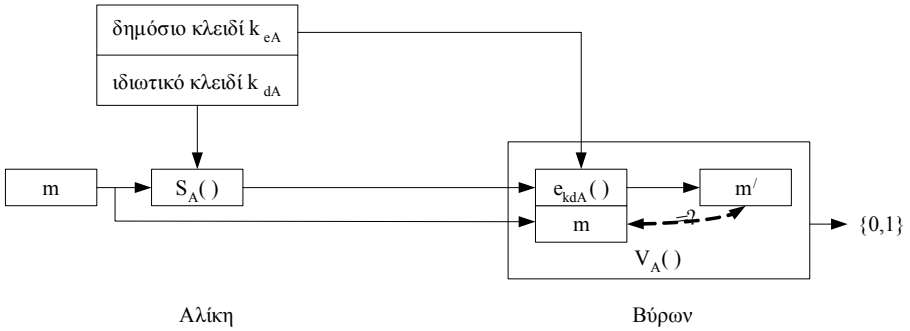
Στην πράξη, το σύνολο των μηνυμάτων είναι μεγαλύτερο από το σύνολο των υπογραφών. Μάλιστα, ο αριθμός των μηνυμάτων είναι κατά πολύ μεγαλύτερος από τον αριθμών των δυνατών υπογραφών. Το σύνολο των μηνυμάτων περιλαμβάνει μηνύματα με διαφορετικό μέγεθος, ενώ οι υπογραφές έχουν συνήθως ένα τυποποιημένο σταθερό μέγεθος. Έτσι, δεν μπορούμε να δεχθούμε ότι η πράξη υπογραφής είναι συνάρτηση 1 – 1. Αυτό έχει ως αποτέλεσμα στην ύπαρξη μιας επίθεσης η οποία εκφράζεται στην ακόλουθη επιπρόσθετη απαίτηση:

- *Αποτροπή πλαστογραφίας*. Θα πρέπει να είναι υπολογιστικά αδύνατον σε έναν αντίπαλο ο οποίος έχει στην κατοχή του μια έγκυρη υπογραφή s ενός μηνύματος m, να βρει ένα μήνυμα m', όπου $V_A(m', s) = 1$, με $m \neq m'$.

Η ασύμμετρη κρυπτογραφία είναι ένα αποτελεσματικό μέσο για να πληρούν οι ψηφιακές υπογραφές όλες τις απαιτήσεις. Έτσι, στις ψηφιακές υπογραφές χρησιμοποιείται κατά κόρον η ασύμμετρη κρυπτογραφία. Από την άλλη, έχουν προταθεί λύσεις συστημάτων ψηφιακής υπογραφής με τη χρήση συμμετρικής κρυπτογραφίας, αλλά όπως θα δούμε στη συνέχεια υπάρχουν αρκετοί περιορισμοί που αντιμετωπίζονται με μη κρυπτογραφικές μεθόδους. Για το λόγο αυτό θα ασχοληθούμε περισσότερο με τις ψηφιακές υπογραφές ασύμμετρης κρυπτογραφίας.

8.3. Ψηφιακές υπογραφές ασύμμετρης κρυπτογραφίας

Ένα απλό σύστημα ψηφιακής υπογραφής βασισμένο σε ασύμμετρη κρυπτογραφία παρουσιάζεται στο Σχήμα 8.2. Το μήνυμα απλά κρυπτογραφείται με το ιδιωτικό κλειδί της Αλίκης και το κρυπτοκείμενο που προκύπτει αποτελεί την ψηφιακή υπογραφή της Αλίκης στο m. Η Αλίκη στέλνει το μήνυμα συνοδευόμενο με την ψηφιακή υπογραφή στον Βύρωνα. Ο Βύρων, ο οποίος κατέχει το δημόσιο κλειδί της Αλίκης, έχει τη δυνατότητα να επαληθεύσει την ψηφιακή υπογραφή, εκτελώντας την αποκρυπτογράφηση του κρυπτοκειμένου με το δημόσιο κλειδί της Αλίκης και να ελέγξει αν τα δύο μηνύματα συμπίπτουν.



Σχήμα 8.2 Ένα απλό σύστημα ψηφιακής υπογραφής

Αυτό το απλό σύστημα έχει δύο μειονεκτήματα. Πρώτον, ο όγκος των μηνυμάτων που στέλνονται είναι διπλάσιος του μεγέθους του αρχικού μηνύματος m. Το μέγεθος της υπογραφής είναι μεταβλητό και εξαρτάται από το μέγεθος του μηνύματος. Σε δίκτυα όπου ανταλλάσσονται πολλά και μεγάλα μηνύματα, μπορεί να αυξηθεί απαγορευτικά η κίνηση και να μειωθεί η παραγωγή. Αν και το σύστημα της ψηφιακής υπογραφής ορίζει συνάρτηση υπογραφής η οποία είναι 1 – 1, δεν υπάρχει προστασία από επίθεση πλαστογραφίας, που είναι το δεύτερο μειονέκτημα του συστήματος. Η συνάρτηση της ψηφιακής υπογραφής είναι η αποκρυπτογράφηση του μηνύματος με το ιδιωτικό κλειδί. Αυτό σημαίνει ότι αν το μήνυμα έχει μεγαλύτερο μέγεθος από το μέγεθος που δέχεται η πράξη αποκρυπτογράφησης, τότε το μήνυμα θα διαιρεθεί σε μικρότερα τμήματα και θα κρυπτογραφηθεί το κάθε τμήμα χωριστά. Στην περίπτωση που ισχύει η ιδιότητα της αντιμετάθεσης στο ασύμμετρο κρυπτοσύστημα, τότε ο Βύρων μπορεί να κατασκευάσει μηνύματα επιλέγοντας και επαναλαμβάνοντας τμήματα του μηνύματος της αρεσκείας του και ταιριάζοντάς τα με τα αντίστοιχα τμήματα της ψηφιακής υπογραφής. Δηλαδή, σε αυτήν την επίθεση ο Βύρων μπορεί να κατασκευάσει έναν αριθμό από (m', s'), από το αρχικό (m, s), έτσι ώστε $V_A(m', s') = 1$.

Στην περίπτωση που ο Βύρων έχει κάποια γνώση του μηνύματος, μπορεί η Αλίκη να στείλει μόνο την υπογραφή. Έτσι αν για παράδειγμα το μήνυμα είναι γραμμένο στην Ελληνική, ο Βύρων εφαρμόζοντας την πράξη κρυπτογράφησης (που εδώ λειτουργεί ως αποκρυπτογράφηση) με το δημόσιο κλειδί της Αλίκης, μπορεί να εύκολα να διαπιστώσει αν το αποτέλεσμα που προκύπτει είναι Ελληνικά. Η Ελληνική γλώσσα όπως και κάθε φυσική γλώσσα έχει αρκετή περίσσεια, ώστε οποιαδήποτε τροποποίηση της υπογραφής θα έχει σαν αποτέλεσμα η κρυπτογράφησή του να οδηγήσει σε ασυνάρτητες για την Ελληνική γλώσσα λέξεις. Η γνώση του περιεχομένου του μηνύματος από τον παραλήπτη επιτρέπει μια άτυπη επαλήθευση της υπογραφής. Ένα τέτοιο σύστημα ψηφιακής υπογραφής έχει την ιδιότητα της ***αυτοανάκτησης*** (self recovery).

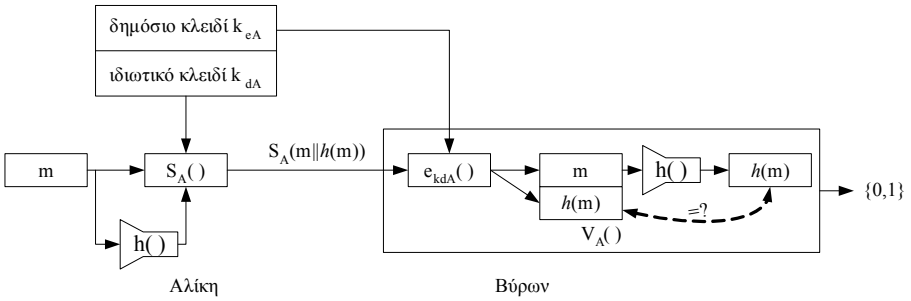
8.3.1. Σύστημα ψηφιακής υπογραφής με αυτοανάκτηση

Σε ένα σύστημα ψηφιακής υπογραφής με αυτοανάκτηση, η περίσσεια της γλώσσας του μηνύματος θα πρέπει να υπάρχει σε τέτοιο βαθμό, ώστε να είναι δυνατή η επαλήθευση της υπογραφής. Συνεπώς, όταν η γλώσσα του μηνύματος δεν έχει περίσσεια (ή όταν αυτή είναι μικρή), θα πρέπει με κάποιον τρόπο να προσθέσουμε περίσσεια. Αυτό θα έχει ως αποτέλεσμα την αύξηση του μεγέθους του μηνύματος. Η κωδικοποίηση των μηνυμάτων στα δίκτυα υπολογιστών συνήθως είναι τέτοια που η περίσσεια είναι ελάχιστη. Μάλιστα, οι αλγόριθμοι συμπίεσης δεδομένων αποβλέπουν στην εξάλειψη της περίσσειας έτσι ώστε το μήνυμα να καταλαμβάνει το μικρότερο δυνατό χώρο για την αποτελεσματική αποθήκευση και μεταφορά. Έτσι από τη μια ένας μηχανικός υπολογιστών επιδιώκει να μειώσει την περίσσεια, ενώ από την άλλη ένας κρυπτογράφος επιθυμεί να εισάγει περίσσεια. Συνεπώς η ισορροπία στην σύγκρουση των ενδιαφερόντων βρίσκεται στο να υπάρχει τόση

περίσσεια ώστε να είναι ασφαλές το σύστημα ψηφιακών υπογραφών, όσον αφορά την αξιοπιστία της διαδικασίας επαλήθευσης της υπογραφής.

Οι υποψήφιες κρυπτογραφικές συναρτήσεις που χρησιμοποιούνται για να εισάγουν περίσσεια στο σύστημα, δεν είναι άλλες από τις κρυπτογραφικές μονόδρομες hash. Οι ιδιότητες των κρυπτογραφικών μονόδρομων hash τις καθιστούν ιδανικές για να εισάγουν περίσσεια στο μήνυμα. Η περίσσεια εξαρτάται από όλα τα σύμβολα του μηνύματος, έχει σταθερό μέγεθος και είναι ανθεκτική σε συγκρούσεις (§4.3).

Στο Σχήμα 8.3 παρουσιάζεται ένα σύστημα ψηφιακής υπογραφής με αυτοανάκτηση.



Σχήμα 8.3 Σύστημα ψηφιακής υπογραφής με αυτοανάκτηση

Η Αλίκη υπογράφει το μήνυμα *m* ως εξής. Αρχικά δημιουργεί μια σύνοψη του μηνύματος με τη βοήθεια της κρυπτογραφικής μονόδρομης hash $h(\ )$. Στη συνέχεια προσθέτει στο τέλος του μηνύματος *m* τη σύνοψη $h(m)$ και τροφοδοτεί το συνδυασμό $m||h(m)$ στη συνάρτηση υπογραφής $S_A(\ )$. Η συνάρτηση υπογραφής αποτελείται από την κρυπτογραφική πράξη της αποκρυπτογράφησης με το ιδιωτικό κλειδί της Αλίκης k_{dA}. Εδώ η αποκρυπτογράφηση είναι στην πραγματικότητα πράξη κρυπτογράφησης, αλλά για λόγους τυποποίησης δεχόμαστε ότι η κρυπτογραφική πράξη με το ιδιωτικό κλειδί θεωρείται αποκρυπτογράφηση και μπορεί να γίνει μόνον από τον κάτοχο του ιδιωτικού κλειδιού, σε αντίθεση με την πράξη κρυπτογράφησης που μπορεί να γίνει από όλους που έχουν στην κατοχή τους το δημόσιο κλειδί.

Ο Βύρων, μόλις λάβει την υπογραφή, την κρυπτογραφεί εφαρμόζοντας το δημόσιο κλειδί της Αλίκης προκειμένου να ανακτήσει τα δύο τμήματα, το μήνυμα και τη σύνοψη. Στη συνέχεια, υπολογίζει τη σύνοψη του πρώτου τμήματος που αντιστοιχεί στο αρχικό μήνυμα και ελέγχει αν αυτή είναι ίση με τη σύνοψη που έστειλε η Αλίκη. Αν οι δύο συνόψεις είναι ίσες, τότε η υπογραφή είναι έγκυρη.

Ασφάλεια συστήματος ψηφιακής υπογραφής με αυτοανάκτηση

Η επιλογή της κρυπτογραφικής μονόδρομης hash είναι κρίσιμη όσον αφορά την ασφάλεια του συστήματος ψηφιακής υπογραφής με αυτοανάκτηση. Επειδή το μή-

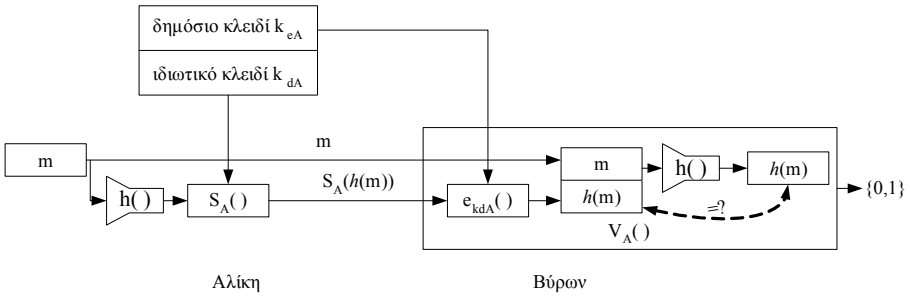
νυμα είναι μέρος της υπογραφής, η μονόδρομη hash θα πρέπει να έχει ασθενή αντίσταση σε συγκρούσεις.

Το σύστημα είναι ασφαλές σε επίθεση πλαστογραφίας, ακόμα και αν το ασύμμετρο κρυπτοσύστημα που χρησιμοποιείται διατηρεί την ιδιότητα της αντιμετάθεσης. Σε μια κρυπτογραφικά μονόδρομη hash η οποία έχει ασθενή αντίσταση σε συγκρούσεις, δεν ισχύει η αντιμεταθετικότητα, επομένως η σύνοψη ενός πλαστού μηνύματος το οποίο προκύπτει από την αντιμετάθεση των τμημάτων του αρχικού μηνύματος θα είναι διαφορετική από τη σύνοψη του αρχικού μηνύματος.

8.3.2. Σύστημα ψηφιακής υπογραφής με παράρτημα

Το παραπάνω σύστημα ψηφιακής υπογραφής με αυτοανάκτηση έχει το μειονέκτημα ότι το μέγεθος της ψηφιακής υπογραφής δεν είναι σταθερό και εξαρτάται από το μέγεθος του αρχικού μηνύματος. Αυτό έχει ως αποτέλεσμα την αύξηση της ανάγκης για επεξεργασία του μηνύματος. Είναι κοινή πρακτική οι πράξεις στις οποίες εμπλέκεται ασύμμετρη κρρυπτογραφία, να είναι όσο το δυνατόν περιορισμένες. Η ασύμμετρη κρυπτογραφία είναι αρκετές τάξεις μεγέθους πιο αργή από τη συμμετρική κρυπτογραφία. Η κρυπτογράφηση (ή αποκρυπτογράφηση) ενός μηνύματος με ασύμμετρη κρυπτογραφία θα πρέπει συστηματικά να αποφεύγεται για καθαρά πρακτικούς λόγους.

Με βάση τα παραπάνω, ορίζεται το σύστημα ψηφιακής υπογραφής με παράρτημα, όπως φαίνεται στο Σχήμα 8.4. Επειδή ο στόχος της ψηφιακής υπογραφής είναι η αυθεντικοποίηση και όχι η εμπιστευτικότητα, η ασύμμετρη κρυπτογραφία είναι προτιμότερο να αποδεσμευτεί από το μήνυμα. Έτσι, η αποκρυπτογράφηση κατά τη διαδικασία της δημιουργίας της ψηφιακής υπογραφής περιορίζεται στη σύνοψη του μηνύματος.



Σχήμα 8.4 Σύστημα ψηφιακής υπογραφής με παράρτημα

Ο ξεχωριστός χειρισμός της σύνοψης από το μήνυμα έχει σαν αποτέλεσμα να στέλνονται δύο ανεξάρτητα τμήματα, το αρχικό μήνυμα το οποίο δεν έχει υποστεί κανέναν μετασχηματισμό, και η ψηφιακή υπογραφή που συνήθως ακολουθεί το μήνυμα. Ο όρος «παράρτημα» οφείλεται στην προσκόλληση της ψηφιακής υπογραφής στο τέλος του μηνύματος, ως ανεξάρτητο αντικείμενο.

Ασφάλεια συστήματος ψηφιακής υπογραφής με παράρτημα

Η ασφάλεια του συστήματος ψηφιακής υπογραφής με παράρτημα είναι συγκρίσιμη με αυτήν του συστήματος ψηφιακής υπογραφής με αυτοανάκτηση. Επειδή όμως ο αντίπαλος έχει πρόσβαση σε περισσότερα μηνύματα, η κρυπτογραφική μονόδρομη hash θα πρέπει να παρουσιάζει ισχυρή αντίσταση σε συγκρούσεις. Στην περίπτωση του συστήματος της ψηφιακής υπογραφής με αυτοανάκτηση, ο αριθμός των μηνυμάτων που μπορεί να κατασκευάσει ο αντίπαλος καθορίζεται από το συνδυασμό των τμημάτων του αρχικού μηνύματος. Αντίθετα στην περίπτωση του συστήματος ψηφιακής υπογραφής με παράρτημα, ο αντίπαλος έχει ολόκληρο το σύνολο των μηνυμάτων στη διάθεσή του.

Στην περίπτωση που απαιτείται εμπιστευτικότητα, το μήνυμα m κρυπτογραφείται είτε με το ιδιωτικό κλειδί του Βύρωνα, είτε με συμμετρικό κλειδί συνόδου. Αν η επικοινωνία μεταξύ της Αλίκης και του Βύρωνα είναι συχνή ή περιλαμβάνει μεγάλα μηνύματα, τότε προτιμάται η χρήση συμμετρικής κρυπτογραφίας για να κρυπτογραφηθεί το μήνυμα, για λόγους ταχύτητας.

Υπάρχουν δύο συνδυασμοί για την κρυπτογράφηση και την εφαρμογή ψηφιακής υπογραφής:

- κρυπτογράφηση του μηνύματος με το συμμετρικό κλειδί συνόδου και στη συνέχεια υπογραφή του κρυπτοκειμένου,
- υπογραφή του (απλού κειμένου) μηνύματος και στη συνέχεια κρυπτογράφηση του μηνύματος.

Από τις δύο εναλλακτικές, η πρώτη δεν προτιμάται για δύο βασικούς λόγους. Η ψηφιακή υπογραφή του κρυπτοκειμένου εισάγει και τη μεταβλητή του μυστικού κλειδιού συνόδου. Έτσι, ο Βύρων θα μπορούσε να αποκρυπτογραφήσει το κρυπτοκείμενο με κάποιο άλλο κλειδί και να ισχυρισθεί ότι το απλό κείμενο που προκύπτει είναι το μήνυμα το οποίο έστειλε η Αλίκη. Με άλλα λόγια, η ψηφιακή υπογραφή της Αλίκης είναι έγκυρη για 2^n μηνύματα, όπου n το μέγεθος του μυστικού κλειδιού συνόδου σε bits. Έτσι, ο Βύρων έχει τη δυνατότητα να πραγματοποιήσει ***επιλεκτική πλαστογραφία***. Το πρόβλημα μπορεί να λυθεί αν η Αλίκη συμπεριλάβει στο μήνυμα και το μυστικό κλειδί και το υπογράψει. Όμως σε έναν τέτοιο διακανονισμό, ο κίνδυνος αποκάλυψης του κλειδιού σε τρίτους είναι μεγάλος και μπορεί να δημιουργήσει προβλήματα ασφάλειας, αν το κλειδί αυτό χρησιμοποιείται για περαιτέρω επικοινωνία μεταξύ της Αλίκης και του Βύρωνα.

Ο δεύτερος λόγος είναι καθαρά δεοντολογικός. Η ενέργεια της υπογραφής υποδεικνύει γνώση του περιεχομένου που υπογράφεται. Η ψηφιακή υπογραφή σε κάποιο κρυπτοκείμενο δε στηρίζει την έννοια της υπογραφής, αφού η Αλίκη δε γνωρίζει άμεσα τι υπογράφει.

8.3.3. Ψηφιακές υπογραφές με το κρυπτοσύστημα RSA

Το κρυπτοσύστημα RSA μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός συστήματος ψηφιακών υπογραφών. Το σύστημα ψηφιακών υπογραφών RSA απαιτεί

ότι όλες οι οντότητες έχουν στην κατοχή τους αντίστοιχα ζεύγη δημόσιου και ιδιωτικού κλειδιού.

ΟΡΙΣΜΟΣ 8.4 – Έστω p και q δύο πρώτοι αριθμοί και $n = pq$. Το σύστημα ψηφιακών υπογραφών RSA ορίζεται με $\mathcal{M} = \mathcal{S} = \mathbf{Z}_n$, πράξη υπογραφής:

$$S_A(m) = m^{k_{dA}} \bmod n$$

και πράξη επαλήθευσης:

$$V_A(s) = s^{k_{eA}} \bmod n,$$

όπου $k_{eA}k_{dA} \equiv 1 \pmod{\varphi(n)}$, με k_{eA} το δημόσιο κλειδί και k_{dA} το ιδιωτικό κλειδί της οντότητας A.

Επειδή η ψηφιακή υπογραφή αποτελείται από το μήνυμα αποκρυπτογραφημένο με το ιδιωτικό κλειδί του αποστολέα, το παραπάνω σύστημα ψηφιακών υπογραφών RSA μπορεί να λειτουργήσει ως σύστημα ψηφιακής υπογραφής με αυτοανάκτηση, αν σταλεί μόνον η ψηφιακή υπογραφή χωρίς το μήνυμα.

ΠΑΡΑΔΕΙΓΜΑ 8.2 – Σύστημα ψηφιακής υπογραφής RSA. Έστω το κρυπτοσύστημα RSA με τις εξής παραμέτρους:

$p = 29$, $q = 17$, $n = 29 \cdot 17 = 493$, $k_{dA} = 319$, $k_{eA} = 191$.

Αρχικά επαληθεύουμε την ορθότητα του ζεύγους των κλειδιών:

$k_{dA} \cdot k_{eA} = 319 \cdot 191 = 60929 \equiv 1 \pmod{448}$.

Το προς υπογραφή μήνυμα είναι το: [τεχνη], το οποίο αντιστοιχίζεται στο αριθμητικό ισοδύναμο: [28 14 31 22 16]. Για το παράδειγμά μας, επιλέξαμε την αντιστοίχιση $\mathrm{A} \mapsto 10$, $\mathrm{B} \mapsto 11$, …, ώστε όλα τα γράμματα να έχουν ίδιο μέγεθος, ίσο με δύο ψηφία. Στη συνέχεια ομαδοποιούμε τα ψηφία του μηνύματος, ώστε να σχηματίζουν αριθμούς μικρότερους του δημόσιου modulus, 493: (281, 431,221, 6). Εφαρμόζοντας τέσσερις φορές το ιδιωτικό κλειδί, παίρνουμε την ψηφιακή υπογραφή:

$281^{319} \equiv 36 \bmod (493)$
$431^{319} \equiv 343 \bmod (493)$
$221^{319} \equiv 425 \bmod (493)$
$6^{319} \equiv 241 \bmod (493)$

και η υπογραφή που προκύπτει είναι η τετράδα (36, 343, 425, 241)

Ασφάλεια συστήματος ψηφιακών υπογραφών RSA

Το κρυπτοσύστημα RSA διατηρεί την αντιμεταθετική ιδιότητα που σημαίνει ότι ένας αντίπαλος μπορεί να εκτελέσει ενεργητική επίθεση και να αναδιατάξει το μήνυμα και την υπογραφή του κατά τη μεταφορά τους από τον αποστολέα στον

παραλήπτη. Οι αναδιατάξεις πραγματοποιούνται σε τμήματα των $\lfloor \log_2(n) \rfloor$ bits, όπου n το δημόσιο modulus του αποστολέα. Επίσης, ο αντίπαλος έχει τη δυνατότητα να επαναλάβει ορισμένα τμήματα του μηνύματος, σε θέσεις της επιλογής του, κατοπτρίζοντας τις επαναλήψεις και στα αντίστοιχα τμήματα της ψηφιακής υπογραφής.

Μια λύση είναι να κρυπτογραφηθεί η ψηφιακή υπογραφή με το δημόσιο κλειδί του παραλήπτη, εκμεταλλευόμενοι το γεγονός ότι όλα τα επικοινωνούντα μέλη που συμμετέχουν στην υποδομή του RSA θα έχουν δημόσια και ιδιωτικά κλειδιά. Έστω ότι η Αλίκη επιθυμεί να στείλει εμπιστευτικά στον Βύρωνα ένα μήνυμα m το οποίο να είναι συγχρόνως υπογεγραμμένο από την ίδια. Τα στοιχεία τα οποία απαιτούνται για τις κρυπτογραφικές πράξεις είναι οι παράμετροι RSA (k_{eA}, k_{dA}, n_A) της Αλίκης, καθώς και οι παράμετροι RSA (k_{eB}, k_{dB}, n_B) του Βύρωνα. Αρχικά η Αλίκη υπογράφει ψηφιακά το μήνυμα m:

$$s = S_A(m) = m^{k_{dA}} \bmod n_A .$$

Στη συνέχεια κρυπτογραφεί την υπογραφή με το δημόσιο κλειδί του Βύρωνα:

$$c = s^{k_{eB}} \bmod n_B .$$

Έτσι, ο αντίπαλος θα έχει πρόσβαση μόνο στο μήνυμα και δε θα έχει τη δυνατότητα να πραγματοποιήσει τις αλλαγές του μηνύματος στην ψηφιακή υπογραφή.

Ωστόσο, η εξάρτηση του μεγέθους των δεδομένων που κρυπτογραφούνται από τις RSA παραμέτρους των μελών, έχει επιπτώσεις στην αντιστρεψιμότητα της πράξης της κρυπτογράφησης. Πιο συγκεκριμένα, αν τα modulus των δύο μελών είναι διαφορετικά με $n_A > n_B$, τότε υπάρχει πιθανότητα η κρυπτογραφημένη υπογραφή να μην μπορεί να αποκρυπτογραφηθεί σωστά από τον Βύρωνα. Για την αποφυγή αυτού του ενδεχόμενου υπάρχουν οι εξής τακτικές:

- να προηγηθεί η κρυπτογράφηση του μηνύματος με το δημόσιο κλειδί του Βύρωνα της ψηφιακής υπογραφής, στην περίπτωση που $n_A > n_B$. Η τακτική αυτή δεν συστήνεται για τους λόγους που αναφέραμε στην προηγούμενη ενότητα.
- να τμηματοποιηθεί η υπογραφή προκειμένου να είναι συμβατή με το n_B. Η τακτική αυτή δημιουργεί προβλήματα υλοποίησης, αυξάνοντας την πολυπλοκότητα και τις απαιτήσεις επεξεργασίας του συστήματος ψηφιακών υπογραφών.
- το κάθε μέλος να έχει δύο διαφορετικά ζεύγη κλειδιών, το ένα για ψηφιακή υπογραφή και το άλλο για κρυπτογράφηση, έτσι ώστε το modulus για την κρυπτογράφηση να είναι μεγαλύτερο από όλα τα moduli που χρησιμοποιούνται στις ψηφιακές υπογραφές.
- να μειωθεί η πιθανότητα μη αντιστρεψιμότητας της κρυπτογράφησης σε πρακτικώς ανεκτά επίπεδα. Έχει δειχθεί ότι αυτό μπορεί να γίνει αν η δυαδική αναπαράσταση του n έχει τη μορφή:

$$n = (1\underbrace{00...0}_{k}1...)_2$$

δηλαδή το σημαντικότερο bit θα πρέπει να είναι άσσος και στη συνέχεια να ακολουθήσουν k μηδενικά, όπου k αριθμός επιλογής μας. Επειδή το n είναι γινόμενο δύο αριθμών, υπάρχει τρόπος επιλογής των p και q έτσι ώστε το γινόμενο που προκύπτει να έχει την επιθυμητή μορφή. Έτσι η ψηφιακή υπογραφή θα είναι μικρότερη του n και θα έχει **0** στη θέση του σημαντικότερου bit.

Στην περίπτωση του συστήματος ψηφιακής υπογραφής RSA με παράρτημα, το κατώτατο μέγεθος της κρυπτογραφικής μονόδρομης hash θα πρέπει να είναι ίσο με 128 bit. Στη βιβλιογραφία το μέγεθος αυτό προτείνεται για τη μονόδρομη MD5, η οποία έχει αναλυθεί και θεωρείται ασφαλής. Στην περίπτωση που χρησιμοποιηθεί hash άλλη από την MD5, προτείνεται η hash να είναι ανθεκτική σε συγκρούσεις, με ελάχιστο μέγεθος σύνοψης ίσο με 160 bit.

Τέλος, όσον αφορά το μέγεθος των RSA παραμέτρων, αν το κρυπτοσύστημα RSA χρησιμοποιείται μόνο για ψηφιακές υπογραφές και όχι για εμπιστευτικότητα, τότε ο δημόσιος εκθέτης k_e μπορεί να έχει οποιαδήποτε τιμή, καθώς δεν έχουν αναφερθεί αδυναμίες για μικρές τιμές του k_e. Ο αριθμός n θα πρέπει να έχει μέγεθος το λιγότερο ίσο με 1024 bits, ενώ σε περιπτώσεις όπου απαιτείται μεγάλη διάρκεια ζωής των κλειδιών, προτείνεται το μέγεθος των 2048 bits.

8.3.4. Το σύστημα ψηφιακών υπογραφών Fiege-Fiat-Shamir

Η υπεροχή του συστήματος ψηφιακών υπογραφών Fiege-Fiat-Shamir (FFS) έναντι των ψηφιακών υπογραφών με RSA είναι ο κατά πολύ μικρότερος χρόνος υπολογισμών. Το σύστημα ψηφιακών υπογραφών FFS απαιτεί περίπου το 4 τοις εκατό των modular πολλαπλασιασμών που απαιτεί το σύστημα RSA.

Το σύστημα περιλαμβάνει μια διαδικασία δημιουργίας των κλειδιών, ένα πρωτόκολλο δημιουργίας ψηφιακής υπογραφής και ένα πρωτόκολλο επαλήθευσης.

Θεωρούμε ότι η Αλίκη επιθυμεί να στείλει ένα υπογεγραμμένο μήνυμα m στον Βύρωνα. Η διαδικασία δημιουργίας των κλειδιών έχει ως εξής. Η Αλίκη επιλέγει δύο πρώτους αριθμούς p, q και υπολογίζει το γινόμενό τους $n = pq$, όπως και στο κρυπτοσύστημα RSA. Στη συνέχεια, επιλέγει μια ακολουθία k ακεραίων:

$$s_i \in Z_n^*, \text{ για } 1 \le i \le k .$$

Το διάνυσμα $(s_1, s_2, \ldots, s_k)$ αποτελεί το ιδιωτικό κλειδί της Αλίκης. Από την ακολουθία δημιουργεί το δημόσιο κλειδί το οποίο είναι το διάνυσμα $(v_1, v_2, \ldots, v_k)$, όπου:

$$v_i \equiv s_i^{-2} \pmod{n}, \text{ για } 1 \le i \le k .$$

Η δημιουργία της ψηφιακής υπογραφής υλοποιείται με το ακόλουθο πρωτόκολλο:

Αλίκη:

1. Επιλογή τυχαίου ακεραίου r, όπου $0 < r < n$.
2. Υπολογισμός του $u \equiv r^2 \pmod{n}$.
3. Υπολογισμός της σύνοψης $h(m \,||\, u) = (e_1 e_2 \ldots e_k)_2 = e$.
4. Υπολογισμός του $s \equiv r \cdot \prod_{i=1}^{k} s_i^{e_i} \pmod{n}$. Η ψηφιακή υπογραφή είναι το (e, s).

Αλίκη → Βύρων: $m||(e, s)$.

Ο Βύρων μπορεί να πραγματοποιήσει επαλήθευση της ψηφιακής υπογραφής εφόσον γνωρίζει το δημόσιο κλειδί της Αλίκης, εκτελώντας τον ακόλουθο πρωτόκολλο:

Βύρων:

1. Υπολογισμός του $w \equiv s^2 \cdot \prod_{i=1}^{k} v_i^{e_i} \pmod{n}$.
2. Υπολογισμός της σύνοψης $e' = h(m \,||\, w)$.
3. Η υπογραφή θεωρείται έγκυρη αν και μόνο αν $e = e'$.

Αν η υπογραφή είναι έγκυρη, τότε οι δύο συνόψεις θα πρέπει να είναι ίσες, που σημαίνει ότι $u = w$. Όντως, μπορούμε να επαληθεύσουμε ότι:

$$w \equiv s^2 \cdot \prod_{i=1}^{k} v_i^{e_i} \equiv \left(r^2 \cdot \prod_{i=1}^{k} s_i^{2e_i} \right) \cdot \prod_{i=1}^{k} v_i^{e_i} \equiv r^2 \cdot \prod_{i=1}^{k} (s_i^2 v_i)^{e_i}$$

$$\equiv r^2 \cdot \prod_{i=1}^{k} 1^{e_i} \equiv r^2 \equiv u \pmod{n}$$

Ασφάλεια του συστήματος ψηφιακών υπογραφών FFS

Η ασφάλεια του συστήματος ψηφιακών υπογραφών FFS βασίζεται στη δυσκολία υπολογισμού της τετραγωνικής ρίζας ενός ακεραίου, modulo n. Ο αντίπαλος (που μπορεί να είναι και ο Βύρων) γνωρίζει το s_i^{-2} και για να επιτύχει σε επίθεση πλαστογραφίας καλείται να ανακαλύψει το s_i.

Επειδή η Αλίκη δεν απαιτείται να γνωρίζει τους παράγοντες του n προκειμένου να δημιουργήσει το ιδιωτικό και το δημόσιο κλειδί συνιστάται, όπου είναι δυνατόν, οι παράγοντες του n να είναι κρυφοί από όλα τα μέλη που συμμετέχουν στο σύστημα των ψηφιακών υπογραφών FFS και να αναλάβει μια έμπιστη οντότητα να κατασκευάσει και να διαθέσει το n στα μέλη.

8.3.5. Το σύστημα ψηφιακών υπογραφών ElGamal

Σε αναλογία με το ασύμμετρο κρυπτοσύστημα ElGamal που παρουσιάσαμε στο Κεφάλαιο 6, η ασφάλεια του συστήματος των ψηφιακών υπογραφών ElGamal βασίζεται στη δυσκολία του υπολογισμού του διακριτού λογάριθμου από τον αντίπαλο. Για την υλοποίηση του συστήματος ψηφιακών υπογραφών ElGamal απαιτείται κρυπτογραφική μονόδρομη hash, της οποίας η σύνοψη είναι στοιχείο του συνόλου $\boldsymbol{Z}_p^*$, όπου p πρώτος αριθμός.

Η υποδομή ενός συστήματος ψηφιακών υπογραφών ElGamal απαιτεί την ακόλουθη διαδικασία δημιουργίας ζεύγους κλειδιών από τα μέλη. Αρχικά επιλέγεται ένας μεγάλος πρώτος αριθμός p και ένας ακέραιος a ο οποίος είναι γεννήτορας του συνόλου $\boldsymbol{Z}_p^*$. Στη συνέχεια επιλέγεται ένας ακέραιος b τέτοιος ώστε $0 < b < p–1$, και υπολογίζεται το:

$$y \equiv a^b \pmod{p}.$$

Το δημόσιο κλειδί αποτελείται από τους τρεις ακέραιους (p, a, y) ενώ το ιδιωτικό κλειδί είναι ο εκθέτης b. Η παραπάνω διαδικασία εκτελείται από κάθε μέλος.

Κατά τη διαδικασία υπογραφής, εκτελείται το ακόλουθο πρωτόκολλο:

1. Επιλογή μυστικού ακεραίου k, με $0 < k < p–1$, και $\gcd(k, p–1) = 1$.
2. Υπολογισμός του $r \equiv a^k \pmod{p}$.
3. Υπολογισμός του $k^{-1} \bmod p$.
4. Υπολογισμός του $s \equiv k^{-1}(h(m) – br) \pmod{p–1}$.
5. Η υπογραφή για το μήνυμα m είναι το ζεύγος (r, s), το οποίο αποστέλλεται μαζί με το μήνυμα στον παραλήπτη.

Η διαδικασία επαλήθευσης πραγματοποιείται με το ακόλουθο πρωτόκολλο:

1. Έλεγχος ότι $0 < r < p–1$. Στην περίπτωση που το r δε βρίσκεται μεταξύ των ενδεδειγμένων ορίων, απορρίπτεται η ψηφιακή υπογραφή.
2. Υπολογισμός του $v \equiv y^r r^s \pmod{p}$.
3. Υπολογισμός της σύνοψης $h(m)$ και υπολογισμός του $v' \equiv a^{h(m)} \pmod{p}$.
4. Η υπογραφή θεωρείται έγκυρη αν και μόνο αν $v = v'$.

Μπορούμε να επαληθεύσουμε την εγκυρότητα της υπογραφής με την ισοδυναμία του τελευταίου βήματος του πρωτοκόλλου επαλήθευσης ως εξής:

$$\begin{aligned}
&s \equiv k^{-1}(h(m) - br) \pmod{p-1} \Rightarrow \\
&ks \equiv h(m) - br \pmod{p-1} \Rightarrow \\
&h(m) \equiv ks + br \pmod{p-1} \Rightarrow \\
&a^{h(m)} \equiv a^{ks+br} \pmod{p} \Rightarrow \\
&a^{h(m)} \equiv (a^b)^r (a^k)^s \pmod{p} \Rightarrow \\
&a^{h(m)} \equiv y^r r^s \pmod{p}
\end{aligned}$$

ή ισοδύναμα $v' = v$.

Ασφάλεια του συστήματος ψηφιακών υπογραφών ElGamal

Όπως αναφέραμε στην προηγούμενη ενότητα, η ασφάλεια του συστήματος ψηφιακών υπογραφών ElGamal βασίζεται στη δυσκολία υπολογισμού του διακριτού λογάριθμου. Ο αντίπαλος έχει στην κατοχή του το δημόσιο κλειδί (p, a, y) του υπογεγραμμένου και καλείται να ανακαλύψει το ιδιωτικό κλειδί b, το οποίο ικανοποιεί τη σχέση:

$$y \equiv a^b \pmod{p}.$$

Αν θεωρήσουμε ότι το πρόβλημα του διακριτού λογάριθμου είναι υπολογιστικά αδύνατο, τότε αν ο αντίπαλος επιλέξει στην τύχη έναν ακέραιο για υποψήφιο ιδιωτικό κλειδί, η πιθανότητα να επιλέξει το σωστό κλειδί είναι ίση με $1/(p-1)$, εφόσον οι επιτρεπτές τιμές του ιδιωτικού κλειδιού βρίσκονται στο διάστημα $0 < b < p-1$. Επομένως, το p θα πρέπει να είναι αρκετά μεγάλο ώστε η πιθανότητα εύρεσης του ιδιωτικού κλειδιού να είναι μικρή.

Ένα άλλο σημείο το οποίο θέτει σε κίνδυνο το σύστημα δίνοντας πλεονέκτημα για επιτυχή πλαστογραφία, είναι η επιλογή του τυχαίου ακέραιου k, κατά τη διαδικασία δημιουργίας της ψηφιακής υπογραφής. Πιο συγκεκριμένα, ο υπογεγραμμένος θα πρέπει να διατηρεί ιστορικό όλων των τυχαίων αριθμών που έχει επιλέξει, ώστε σε κάθε υπογραφή να χρησιμοποιείται διαφορετικός ακέραιος k.

ΠΑΡΑΔΕΙΓΜΑ 8.3 – Επίθεση πλαστογραφίας λόγω κοινού τυχαίου ακεραίου. Έστω ότι η Αλίκη έχει υπογράψει δύο μηνύματα m_1 και m_2, χρησιμοποιώντας τον ίδιο τυχαίο ακέραιο k. Τότε για τις δύο υπογραφές (r_1, s_1) και (r_2, s_2), θα είναι $r_1 = r_2 = r$ ενώ για τα s_1 και s_2 θα είναι:

$$s_1 \equiv k^{-1}(h(m_1) - br) \pmod{p-1} \quad \text{και}$$

$$s_2 \equiv k^{-1}(h(m_2) - br) \pmod{p-1}$$

Αφαιρώντας τις δύο σχέσεις μεταξύ τους προκύπτει:

$$s_1 - s_2 \equiv k^{-1}((h(m_1) - br) - (h(m_2) - br) \pmod{p-1}$$

ή ισοδύναμα:

$$(s_1 - s_2)k \equiv h(m_1) - h(m_2) \pmod{p-1}$$

Αν

$$s_1 - s_2 \not\equiv 0 \pmod{p-1},$$

τότε μπορεί να υπολογιστεί ο k από την

$$k \equiv (s_1 - s_2)^{-1}(h(m_1) - h(m_2)) \pmod{p-1}.$$

Όλες οι μεταβλητές που βρίσκονται στο δεξί μέλος της παραπάνω ισοδυναμίας είναι γνωστές στον αντίπαλο. Η εύρεση του k αποκαλύπτει την ποσότητα ($h(m_1) - br$) που υπάρχει στην s_1, από όπου ο αντίπαλος μπορεί να εξάγει το ιδιωτικό κλειδί b.

Τέλος, αν ο αρχικός έλεγχος στο πρωτόκολλο επαλήθευσης δεν πραγματοποιηθεί, τότε ο αντίπαλος είναι σε θέση να εκτελέσει πλαστογραφία δημιουργώντας ψηφιακή υπογραφή για οποιοδήποτε μήνυμα της επιλογής του. Αυτό οφείλεται στο γεγονός ότι στο σύνολο των ακεραίων ορίζονται άπειρες ισοδυναμίες, αν επιτρέψουμε το r να πάρει ανεξέλεγκτη τιμή, εκτός των ορίων $0 < r < p-1$. Αν και ο έλεγχος είναι φαινομενικά ένα ασήμαντο βήμα, η παράλειψη αυτού καθιστά όλο το σύστημα ευάλωτο σε επίθεση πλαστογραφίας.

ΠΑΡΑΔΕΙΓΜΑ 8.4 – Επίθεση πλαστογραφίας λόγω παράλειψης του αρχικού ελέγχου $0 < r < p-1$. Έστω ότι ο αντίπαλος έχει στην κατοχή του ένα μήνυμα m και την αντίστοιχη υπογραφή (r, s) στο μήνυμα αυτό. Αν $h(m) \not\equiv 0 \pmod{p-1}$, τότε ο αντίπαλος μπορεί να επιλέξει ένα δικό του μήνυμα m' και στη συνέχεια να υπολογίσει την ποσότητα:

$$w \equiv h(m')h(m)^{-1} \pmod{p-1}$$

Στη συνέχεια ο αντίπαλος υπολογίζει την υπογραφή έτσι ώστε:

$$s' \equiv sw \pmod{p-1}$$

και r' τέτοιο ώστε:

$$r' \equiv rw \pmod{p-1} \quad \text{και}$$
$$r' \equiv r \pmod{p}$$

το οποίο υπολογίζεται με τη βοήθεια του Κινέζικου θεωρήματος υπολοίπων. Είναι φανερό ότι η πλαστογραφημένη υπογραφή (r', s') περνάει με επιτυχία το πρωτόκολλο επαλήθευσης, αν παραληφθεί το πρώτο βήμα.

8.3.6. Το Πρότυπο Ψηφιακής Υπογραφής (DSS)

Το Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard, DSS), δημοσιεύθηκε από το Εθνικό Ινστιτούτο Τυποποίησης και Τεχνολογίας (NIST) το οποίο καθορίζει ένα σύστημα ψηφιακών υπογραφών, για γενική χρήση. Το DSS περιγράφει έναν αλγόριθμο ψηφιακής υπογραφής, τον DSA (Digital Signature Algorithm), οποίος βασίζεται σε ασύμμετρη κρυπτογραφία. Σε αντίθεση με τα συστήματα ψηφιακών υπογραφών που περιγράψαμε, ο DSA αναφέρεται αποκλειστικά σε σύστημα ψηφιακών υπογραφών και δεν μπορεί να χρησιμοποιηθεί ως κρυπτοσύστημα. Επίσης, το DSS προβλέπει τη χρήση της SHA-1 (Κεφάλαιο 4) ως κρυπτογραφική μονόδρομη hash, η οποία συμμετέχει στη δημιουργία της ψηφιακής υπογραφής.

Ο DSA είναι μια τροποποίηση του συστήματος ψηφιακής υπογραφής ElGamal. Επομένως, η ασφάλειά του βασίζεται στο πρόβλημα του υπολογισμού του διακριτού λογάριθμου.

Όπως όλα τα συστήματα ψηφιακών υπογραφών που εξετάσαμε παραπάνω, έτσι και ο DSA αποτελείται από τον καθορισμό των ασύμμετρων παραμέτρων (των κλειδιών), το πρωτόκολλο ψηφιακής υπογραφής και το πρωτόκολλο επαλήθευσης της υπογραφής.

Κατά τη δημιουργία των κλειδιών, το κάθε μέλος θα πρέπει να εκτελέσει τα ακόλουθα βήματα. Αρχικά, επιλέγεται ένας πρώτος αριθμός q τέτοιος ώστε $2^{159} < q < 2^{160}$. Από τα όρια αυτά φαίνεται ότι το μέγεθος του αριθμού q θα είναι ίσο με 160 bits. Στη συνέχεια επιλέγεται πρώτος αριθμός p τέτοιος ώστε $2^{t-1} < p < 2^t$, με $512 \le t \le 1024$, και ο t να είναι ακέραιο πολλαπλάσιο του 64. Επίσης ο q θα πρέπει να διαιρεί τον $(p-1)$.

Με βάση τους πρώτους αριθμούς p και q, επιλέγεται γεννήτορας a μιας κυκλικής υποομάδας τάξης q της ομάδας $\boldsymbol{Z}_p^*$. Αυτό επιτυγχάνεται επιλέγοντας $g \in \boldsymbol{Z}_p^*$ τέτοιο ώστε:

$$g^{(p-1)/q} \bmod p > 1$$

και θέτουμε

$$a \equiv g^{(p-1)/q} \pmod{p}.$$

Στη συνέχεια, επιλέγεται τυχαίος ακέραιος τέτοιος ώστε $0 < b < q$, και υπολογίζεται ο:

$$y \equiv a^b \pmod{p}.$$

Η τετράδα (p, q, a, y) αποτελεί το δημόσιο κλειδί, ενώ ο b αποτελεί το ιδιωτικό κλειδί.

Το πρωτόκολλο υπογραφής ενός μηνύματος m αποτελείται από τα ακόλουθα βήματα:

1. Επιλογή τυχαίου μυστικού ακέραιου k τέτοιου ώστε $0 < k < q$.
2. Υπολογισμός του $r \equiv (a^k \bmod p) \pmod q$.
3. Υπολογισμός του $k^{-1} \bmod q$.
4. Υπολογισμός του $s \equiv k^{-1}(h(m) + br) \pmod q$.

Η ψηφιακή υπογραφή του μηνύματος m είναι το ζεύγος (s, r). Κατά την επαλήθευση της ψηφιακής υπογραφής εκτελείται το ακόλουθο πρωτόκολλο:

1. Έλεγχος ότι $0<r,s<q$. Σε περίπτωση που κάποιο από τα r,s δεν είναι εντός των καθορισμένων ορίων, η υπογραφή απορρίπτεται.
2. Υπολογισμός του $w=s^{-1} \bmod q$.
3. Υπολογισμός των:

$$u_1 \equiv wh(m) \pmod q$$
$$u_2 = rw \pmod q$$

4. Υπολογισμός του $r' \equiv a^{u_1} y^{u_2} \pmod q$.
5. Η υπογραφή θεωρείται έγκυρη αν και μόνο αν $r = r'$.

Το παράδοξο της επαλήθευσης της υπογραφής του τελευταίου βήματος είναι ότι η ποσότητα r δεν εξαρτάται από το μήνυμα, οπότε δεν είναι ευθέως φανερό πως μπορεί να πραγματοποιηθεί η επαλήθευση χωρίς την άμεση συμβολή του μηνύματος που υπογράφηκε. Ωστόσο, μπορούμε να επαληθεύσουμε την εγκυρότητα της υπογραφής με την ισοδυναμία του τελευταίου βήματος του πρωτοκόλλου επαλήθευσης ως εξής:

$$s \equiv k^{-1}(h(m) + br) \pmod q \Rightarrow$$
$$ks \equiv h(m) + br \pmod q \Rightarrow$$
$$wks \equiv wh(m) + wbr \pmod q \Rightarrow$$
$$(ws) \cdot k \equiv u_1 + u_2 b \pmod q \Rightarrow$$
$$k \equiv u_1 + u_2 b \pmod q \Rightarrow$$
$$(a^k \bmod p) \bmod q = (a^{u_1} y^{u_2} \bmod p) \bmod q$$

ή ισοδύναμα, $r' = r$.

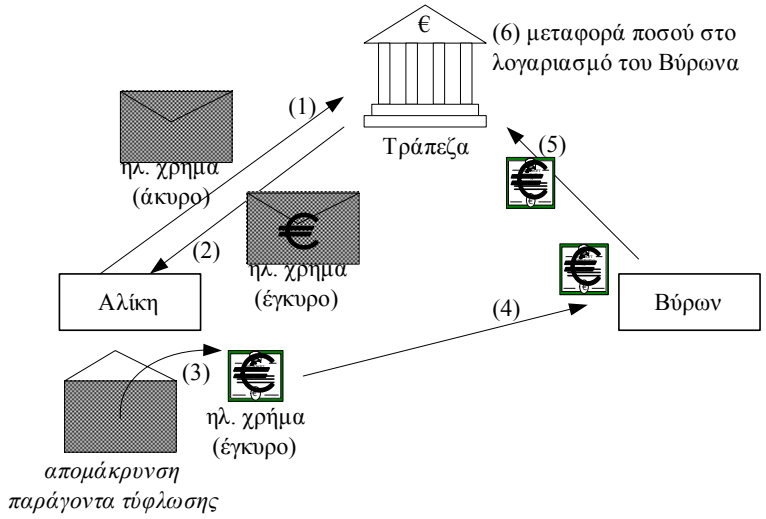
8.3.7. Συστήματα τυφλών ψηφιακών υπογραφών

Οι τυφλές ψηφιακές υπογραφές παρουσιάζουν πρακτικό ενδιαφέρον σε πολλές εφαρμογές, όπως στο ηλεκτρονικό χρήμα και στις ηλεκτρονικές εκλογές. Η χαρακτηριστική ιδιότητα που καθιστά μια υπογραφή τυφλή είναι το γεγονός ότι ο υπογράφων δε γνωρίζει το περιεχόμενο του μηνύματος που υπογράφει.

Η αναλογία της τυφλής υπογραφής παριστάνεται στο ακόλουθο παράδειγμα. Έστω ότι απαιτείται να υπογραφεί ένα έγγραφο χωρίς να γνωρίζει ο υπογράφων το περιεχόμενο του. Το έγγραφο μπορεί να μπει σε φάκελο, μαζί με ένα φύλλο καρμπόν και να σφραγισθεί. Στη συνέχεια, ο υπογράφων βάζει την υπογραφή του επάνω στο φάκελο και λόγω της παρεμβολής του καρμπόν, η υπογραφή μεταφέρεται στο κλειστό έγγραφο. Στη συνέχεια, ο παραλήπτης του εγγράφου μπορεί να ανοίξει το φάκελο και να παραλάβει το υπογεγραμμένο έγγραφο.

Η παραπάνω αναλογία είναι χρήσιμη στο ηλεκτρονικό χρήμα ως εξής. Ο πελάτης της ηλεκτρονικής τράπεζας ετοιμάζει ηλεκτρονικά χρήματα, τα οποία επικυρώνονται από την ηλεκτρονική τράπεζα. Η επικύρωση πραγματοποιείται όταν η ηλεκτρονική τράπεζα υπογράφει τα ηλεκτρονικά χρήματα του πελάτη, τα οποία αυτόματα μετατρέπονται σε ηλεκτρονικό χρήμα. Μια βασική ιδιότητα του φυσικού χρήματος είναι η ανωνυμία ξοδέματος (anonymity of spending). Η τράπεζα δεν μπορεί να ανιχνεύσει που ξοδεύονται τα φυσικά χρήματα τα οποία έχει διανέμει στους πολίτες. Αυτή η ιδιότητα είναι επιθυμητή και στον ηλεκτρονικό κόσμο.

Αν η ηλεκτρονική τράπεζα ήταν σε θέση να γνωρίζει τα χρήματα που υπογράφει, τότε θα είχε τη δυνατότητα να αναγνωρίσει τον αγοραστή σε μια συναλλαγή. Ο κύκλος του ηλεκτρονικού χρήματος παριστάνεται στο Σχήμα 8.5.



Σχήμα 8.5 Ο κύκλος του ηλεκτρονικού χρήματος

Η Αλίκη αποφασίζει να αγοράσει ένα σαξόφωνο από τον μουσικό οίκο του Βύρωνα. Αρχικά, δημιουργεί ένα ηλεκτρονικό «χαρτονόμισμα» που αναγράφει την αξία του σαξόφωνου (ας χρησιμοποιήσουμε καταχρηστικά τον όρο «χαρτονόμισμα» προς χάριν της παραστατικής περιγραφής). Στη συνέχεια, το τοποθετεί σε ηλεκτρονικό φάκελο, εφαρμόζοντας έναν μυστικό παράγοντα τύφλωσης (blinding factor) και στέλνει τον ηλεκτρονικό φάκελο στην Τράπεζα (1). Η Τράπεζα με τη σειρά της υπογράφει ψηφιακά τον φάκελο, καθιστώντας έγκυρο το περιεχόμενό του και στέλνει το αποτέλεσμα πίσω στην Αλίκη (2). Η Αλίκη απομακρύνει τον παράγοντα τύφλωσης, το οποίο ισοδυναμεί με την εξαγωγή του έγκυρου πλέον χαρτονομίσματος από τον φάκελο (3) και το μεταβιβάζει στον Βύρωνα (4). Ο Βύρων ελέγχει την εγκυρότητα της υπογραφής, εφόσον γνωρίζει το αντίστοιχο δημόσιο κλειδί της Τράπεζας και παραδίδει το προϊόν στην Αλίκη. Τέλος, ο Βύρων στέλνει το χαρτονόμισμα στην Τράπεζα η οποία ενημερώνει το λογαριασμό του Βύρωνα με το αναγραφόμενο ποσό.

Η παραπάνω περιγραφή του κύκλου του ηλεκτρονικού χρήματος δίνει μόνον την αρχή λειτουργίας μιας υποδομής ηλεκτρονικού χρήματος. Στην πράξη εφαρμόζονται ποικίλα πρωτόκολλα τα οποία ανταλλάσσονται μεταξύ των επικοινωνούντων μελών, για την προστασία αυτών. Τα πρωτόκολλα απαιτούνται για να μειωθούν ή και να εξαλειφθούν σοβαρές απειλές του συστήματος. Ίσως η σημαντικότερη από αυτές είναι η απειλή του διπλού ξοδέματος (double spending). Καθώς το ηλεκτρονικό χρήμα δεν είναι τίποτε άλλο από μια σειρά δυαδικών ψηφίων, η Αλί-

κη θα μπορούσε να κρατήσει ένα αντίγραφο του χαρτονομίσματος και να το παρουσιάσει σε κάποιο άλλο κατάστημα για να πραγματοποιήσει αγορά με το ίδιο χαρτονόμισμα. Παρόμοια και ο Βύρων θα μπορούσε να χρησιμοποιήσει το χαρτονόμισμα της Αλίκης για να πραγματοποιήσει δική του αγορά. Για λεπτομέρειες σχετικά με τα πρωτόκολλα ηλεκτρονικού χρήματος παραπέμπουμε τον αναγνώστη στη βιβλιογραφία, καθώς στο σημείο αυτό θα ασχοληθούμε αποκλειστικά με τα συστήματα τυφλών υπογραφών.

Σύστημα τυφλών ψηφιακών υπογραφών RSA

Η ανακάλυψη των τυφλών υπογραφών αποδίδεται στον Chaum ο οποίος είναι και ο βασικός ερευνητής στο συγκεκριμένο χώρο. Το πρώτο και απλούστερο σύστημα ψηφιακών υπογραφών που κατασκευάσθηκε βασίζεται στις κρυπτογραφικές πράξεις του ασύμμετρου κρυπτοσυστήματος RSA.

Έστω ότι η Αλίκη επιθυμεί να παραλάβει υπογεγραμμένο το μήνυμα m από τον Βύρωνα, χωρίς αυτός να γνωρίζει το περιεχόμενο του μηνύματος. Θεωρούμε ότι το δημόσιο κλειδί του Βύρωνα είναι (e, n) και το ιδιωτικό του κλειδί είναι το d. Επίσης, για το μήνυμα ισχύει $m < n$.

Αρχικά η Αλίκη επιλέγει τον παράγοντα τύφλωσης ο οποίος είναι ένας μυστικός ακέραιος k, τέτοιος ώστε $0 < k < n$ και $\gcd(k, n) = 1$. Ένα σύστημα τυφλών ψηφιακών υπογραφών αποτελείται από τρεις διαδικασίες: την τύφλωση, την υπογραφή και την απομάκρυνση του παράγοντα τύφλωσης. Στο σύστημά μας, οι τρεις διαδικασίες ορίζονται ως εξής:

- (*τύφλωση*). Υπολογισμός του $m' \equiv mk^e \pmod{n}$ από την Αλίκη.
  Αλίκη $\rightarrow$ Βύρων: m'
- (*υπογραφή*). Υπολογισμός του $s \equiv (m')^d \pmod{n}$ από τον Βύρωνα.
  Βύρων $\rightarrow$ Αλίκη: s
- (*απομάκρυνση του παράγοντα τύφλωσης*). Υπολογισμός του $sk^{-1} \bmod n$. Το αποτέλεσμα του υπολογισμού θα είναι η υπογραφή του Βύρωνα στο μήνυμα m.

ΠΑΡΑΔΕΙΓΜΑ 8.5 – Σύστημα τυφλής υπογραφής RSA. Έστω το σύστημα RSA του Παραδείγματος 8.2:

$$p = 29,\ q = 17,\ n = 29 \cdot 17 = 493,\ k_{dA} = 319,\ k_{eA} = 191$$

και έστω ότι το μήνυμα που επιθυμούμε να υπογραφεί τυφλά είναι το $m = 351$. Αρχικά επιλέγουμε παράγοντα τύφλωσης, έστω $k = 31$. Στη συνέχεια υπολογίζουμε το μήνυμα

$$m' = 351 \cdot 31^{191} \equiv 351 \cdot 300 \equiv 291 \pmod{493}.$$

το οποίο αποτελεί και το μήνυμα προς υπογραφή. Η πράξη της υπογραφής στο m' δίνει:

$s = 291^{319} \equiv 349 \pmod{493}$.

Τέλος, υπολογίζουμε τον αντίστροφο του παράγοντα τύφλωσης, ο οποίος είναι:

$k^{-1} = 31^{-1} \equiv 334 \pmod{493}$.

Έτσι, το υπογεγραμμένο μήνυμα «351» είναι το:

$349 \cdot 334 \equiv 218 \pmod{493}$,

από όπου μπορούμε να επαληθεύσουμε ότι:

$218^{191} \equiv 351 \pmod{493}$.

8.4. Ψηφιακές υπογραφές συμμετρικής κρυπτογραφίας

Αν και οι ψηφιακές υπογραφές είναι κατεξοχήν θέμα ασύμμετρης κρυπτογραφίας, έχουν προταθεί εναλλακτικά συστήματα ψηφιακών υπογραφών που βασίζονται σε συμμετρική κρυπτογραφία.

Τα συστήματα ψηφιακών υπογραφών συμμετρικής κρυπτογραφίας χωρίζονται σε συστήματα ψηφιακών υπογραφών με τη συμμετοχή τρίτης έμπιστης οντότητας και σε συστήματα ψηφιακών υπογραφών χωρίς τη συμμετοχή της έμπιστης οντότητας. Επειδή η τρίτη έμπιστη οντότητα χρησιμοποιείται στην ασύμμετρη κρυπτογραφία, στα συστήματα ψηφιακών υπογραφών χρησιμοποιείται ο όρος ***διαιτητής*** (arbitrator), ο οποίος περιγράφει με ικανοποιητική ακρίβεια το ρόλο της έμπιστης οντότητας σε ένα σύστημα ψηφιακών υπογραφών.

8.4.1. Σύστημα ψηφιακής υπογραφής χωρίς τη συμμετοχή διαιτητή

Θα παρουσιάσουμε το σύστημα ψηφιακής υπογραφής του Lamport. Το σύστημα ψηφιακής υπογραφής εφαρμόζει την ψηφιακή υπογραφή σε μήνυμα του ενός bit, δηλαδή $m \in \{0, 1\}$. Η αρχική πρόταση του συστήματος χρησιμοποιεί τον συμμετρικό κρυπταλγόριθμο DES, αλλά μπορεί να χρησιμοποιηθεί οποιοσδήποτε συμμετρικός κρυπταλγόριθμος.

Όπως και στα συστήματα ψηφιακών υπογραφών ασύμμετρης κρυπτογραφίας, υπάρχει το στάδιο δημιουργίας των κλειδιών. Εφόσον στη συμμετρική κρυπτογραφία δεν ορίζεται η έννοια του δημόσιου και ιδιωτικού κλειδιού, θα ονομάσουμε τις απαιτούμενες αντίστοιχες ποσότητες ως «ισοδύναμο ιδιωτικό» και «ισοδύναμο δημόσιο» κλειδί, των οποίων οι ρόλοι θα είναι ίδιοι με τα ασύμμετρα κλειδιά των συστημάτων ψηφιακής υπογραφής που εξετάσαμε.

Έστω $e_k(\cdot)$ η πράξη κρυπτογράφησης ενός συμμετρικού κρυπτοσυστήματος. Ο υπογράφων επιλέγει δύο κλειδιά k_0 και k_1, καθώς και δύο απλά κείμενα, p_0 και p_1. Από τα δύο απλά κείμενα, το p_0 αντιστοιχεί στο **0** ενώ το p_1 αντιστοιχεί στο **1**. Ας σημειωθεί ότι τα μεγέθη των δύο κρυπτοκειμένων είναι προκαθορισμένα όπως απαιτεί ο συμμετρικός κρυπταλγόριθμος, τα οποία θα είναι ασφαλώς μεγαλύτερα του ενός bit. Έχουμε δηλαδή μεγάλη αύξηση της περίσσειας, αφού απαιτούνται n

bits προκειμένου να περιγράψουμε πληροφορία ενός bit (όπου n το μέγεθος του τμήματος του απλού κειμένου που απαιτεί ο συμμετρικός κρυπταλγόριθμος).

Στη συνέχεια, ο υπογράφων κρυπτογραφεί με το συμμετρικό κρυπταλγόριθμο τα δύο απλά κείμενα, όπου στο κάθε απλό κείμενο εφαρμόζει διαφορετικό κλειδί:

$c_0 = e_{k_0}(p_0)$, και

$c_1 = e_{k_1}(p_1)$.

Η παραπάνω κρυπτογράφηση ολοκληρώνει τη διαδικασία δημιουργίας των κλειδιών. Το ισοδύναμο δημόσιο κλειδί αποτελείται από τα (p_0, p_1, c_0, c_1), ενώ το ισοδύναμο ιδιωτικό κλειδί αποτελείται από τα μυστικά κλειδιά (k_0, k_1).

Η δημοσίευση του ισοδύναμου δημόσιου κλειδιού περικλείει και τη διαδικασία υπογραφής του μηνύματος. Με αυτόν τον τρόπο δεν υπάρχει ξεχωριστή διαδικασία υπογραφής. Πιο συγκεκριμένα, η εκτέλεση της ψηφιακής υπογραφής είναι η κρυπτογράφηση των δύο απλών κειμένων.

Κατά τη διαδικασία της επαλήθευσης, ο υπογράφων αποκαλύπτει ένα από τα κλειδιά. Αν το μήνυμα είναι το $m = \mathbf{0}$, τότε ο υπογράφων αποκαλύπτει το κλειδί k_0, ενώ αν το μήνυμα είναι το $m = \mathbf{1}$, τότε ο υπογράφων αποκαλύπτει το κλειδί k_1. Έτσι ο παραλήπτης του υπογεγραμμένου bit μπορεί να εκτελέσει την ίδια συμμετρική κρυπτογράφηση με τον υπογράφοντα και να ελέγξει αν το κλειδί είναι αυτό που αντιστοιχίζει το απλό κείμενο στο κρυπτοκείμενο, όπως περιγράφονται στο ισοδύναμο δημόσιο κλειδί.

Ασφάλεια και μειονεκτήματα του συστήματος ψηφιακής υπογραφής του Lamport

Η ασφάλεια του συστήματος ψηφιακής υπογραφής που παρουσιάσαμε είναι ισοδύναμη με την ασφάλεια του συμμετρικού κρυπταλγόριθμου, που χρησιμοποιείται. Η επίθεση της πλαστογραφίας σε αυτήν την περίπτωση είναι η πρόκληση του αντιπάλου να ανακαλύψει το κλειδί το οποίο δεν έχει αποκαλυφθεί από τον υπογράφοντα. Ο αντίπαλος γνωρίζει ένα ζεύγος απλού κειμένου και του αντίστοιχου κρυπτοκειμένου, επομένως θα επιχειρήσει επίθεση γνωστού απλού κειμένου. Έτσι, η ασφάλεια του συστήματος ψηφιακών υπογραφών εξαρτάται από την κρυπτογραφική δύναμη του συμμετρικού κρυπταλγόριθμου. Επιπλέον, η φύλαξη των μυστικών κλειδιών είναι προφανής απαίτηση ασφάλειας του συστήματος ψηφιακής υπογραφής.

Η εξάρτηση της ασφάλειας του συστήματος ψηφιακής υπογραφής από την κρυπτογραφική δύναμη του συμμετρικού κρυπταλγόριθμου είναι το κριτήριο επιλογής ενός συστήματος ψηφιακής υπογραφής συμμετρικής κρυπτογραφίας, έναντι ενός συστήματος ασύμμετρης κρυπτογραφίας. Το μακρύ ιστορικό των τεχνικών σχεδιασμού, καθώς και της αξιολόγησης της ασφάλειας και των κρυπτογραφικών ιδιοτήτων των κρυπτογραφικών συναρτήσεων που αφορά τη συμμετρική κρυπτογραφία προτιμάται από πολλούς έναντι της ασύμμετρης κρυπτογραφίας, η οποία βασίζεται σε «δύσκολα» προβλήματα.

Ωστόσο, ένα σύστημα ψηφιακής υπογραφής συμμετρικού κρυπτοσυστήματος όπως αυτό του Lamport που παρουσιάσαμε, έχει σοβαρά πρακτικά μειονεκτήματα. Αν υπολογίσουμε τον αριθμό των συνολικών bits που απαιτούνται προκειμένου να υπογραφεί ένα bit, θα διαπιστώσουμε ότι το υπολογιστικό κόστος καθώς και το κόστος αποθήκευσης είναι μεγάλα. Αν υποθέσουμε ότι ο κρυπταλγόριθμος είναι ο DES (όπως ήταν και στην αρχική πρόταση του συστήματος), για την υπογραφή ενός bit, το ισοδύναμο δημόσιο κλειδί θα έχει μέγεθος ίσο με 256 bits ενώ η υπογραφή (το ισοδύναμο ιδιωτικό κλειδί) θα έχει μήκος ίσο με 52 bits.

Ένα άλλο μειονέκτημα είναι ότι δεν μπορούν να επαναχρησιμοποιηθούν το ισοδύναμο δημόσιο και ιδιωτικό κλειδί. Από τη στιγμή που υπογραφεί ένα bit, θα πρέπει να δημιουργηθούν από την αρχή νέα ισοδύναμα κλειδιά. Αυτό σημαίνει ότι αν χρησιμοποιηθεί (για οικονομία!) μια κρυπτογραφική μονόδρομη hash για να υπογραφούν τα bits αυτής, τότε με βάση το παράδειγμα του DES, ο όγκος των δημόσιων κλειδιών θα είναι ίσος με $\nu \cdot 256$ bits, όπου ν το μέγεθος της σύνοψης σε bits.

ΠΑΡΑΔΕΙΓΜΑ 8.6 – Υπολογισμός ασφαλούς συστήματος ψηφιακής υπογραφής με σημερινά δεδομένα. Έστω ότι επιθυμούμε να κατασκευάσουμε το σύστημα ψηφιακών υπογραφών Lamport ώστε να είναι ασφαλές με τα σημερινά δεδομένα υπολογιστικής ισχύος. Θα χρησιμοποιήσουμε τον κρυπταλγόριθμο AES με μεγέθη απλού κειμένου, κρυπτοκειμένου και κλειδιού ίσα με 128 bits. Επίσης, μπορούμε να χρησιμοποιήσουμε την κρυπτογραφική hash MD5, η οποία θεωρείται ανθεκτική σε συγκρούσεις.

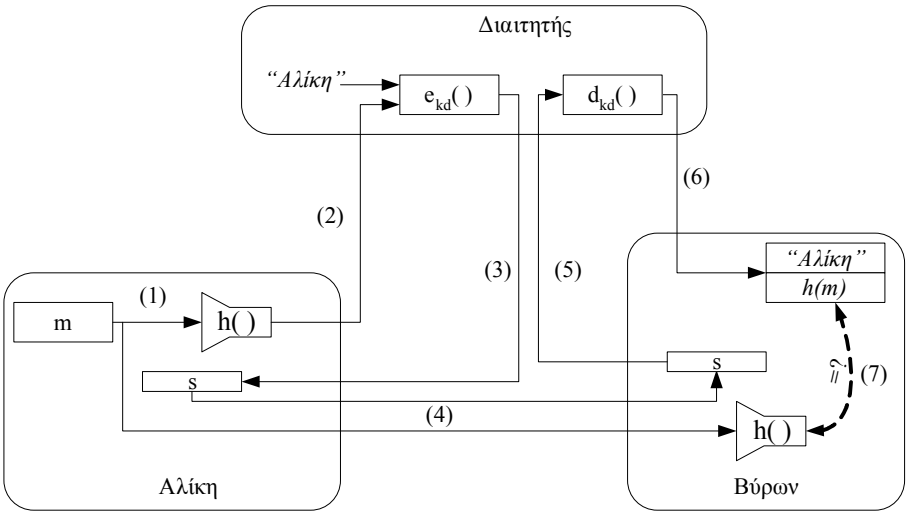
- Δεδομένης της σημερινής υπολογιστικής ισχύος, προκειμένου να είναι υπολογιστικά αδύνατο να βρεθούν συγκρούσεις στην hash, επιλέγουμε το μέγεθος της σύνοψης να είναι 160 bits.
- Για κάθε bit της σύνοψης που θα υπογράφεται, απαιτείται διαφορετικό ισοδύναμο δημόσιο και ιδιωτικό κλειδί. Το μέγεθος του ισοδύναμου δημόσιου κλειδιού θα είναι ίσο με: $4 \cdot 128 = 512$ bits. Το ιδιωτικό κλειδί θα έχει μέγεθος ίσο με 256 bits (για τα δύο κλειδιά), ενώ η ψηφιακή υπογραφή του για το συγκεκριμένο bit θα έχει μέγεθος 128 bits.
- Συνολικά, για τα 160 bits της σύνοψης, ο όγκος των ισοδύναμων δημόσιων κλειδιών ανέρχεται στα $512 \cdot 160 = 81920$ bits, ενώ η ψηφιακή υπογραφή θα έχει μέγεθος ίσο με $128 \cdot 160 = 20480$ bits.

8.4.2. Σύστημα ψηφιακής υπογραφής με διαιτητή

Τα μειονεκτήματα του συστήματος ψηφιακής υπογραφής συμμετρικής κρυπτογραφίας άνευ διαιτητού που περιγράψαμε, καθιστούν πρακτικά άχρηστο ένα τέτοιο σύστημα, σε πολλές εφαρμογές. Η εισαγωγή του διαιτητή στο σύστημα έχει στόχο να ξεπεράσει τα μειονεκτήματα. Βέβαια, η ανάγκη εμπιστοσύνης μιας τρίτης οντότητας μειώνει την ασφάλεια του συστήματος, αφού στην περίπτωση που η οντότητα δεν αποδώσει την επιθυμητή εμπιστοσύνη, τότε υπάρχει κίνδυνος κα-

τάρρευσης του συστήματος. Για μια ακόμη φορά είμαστε αναγκασμένοι να εντοπίσουμε τη χρυσή τομή μεταξύ του πρακτικού και της ασφάλειας· για μια ακόμη φορά η κρυπτογραφία δε δίνει λύσεις αλλά δίνει τα εργαλεία για να μετασχηματίσουμε ένα πρόβλημα σε μορφή που η διαχείρισή του θα είναι ευκολότερη.

Το σύστημα ψηφιακής υπογραφής συμμετρικής κρυπτογραφίας με τη συμμετοχή διαιτητή που θα παρουσιάσουμε στη συνέχεια είναι των Needham και Schroeder. Περιλαμβάνει μια κρυπτογραφική μονόδρομη hash και έναν συμμετρικό κρυπταλγόριθμο. Η hash εκτελείται από τα επικοινωνούντα μέλη, ενώ η κρυπτογράφηση και αποκρυπτογράφηση εκτελούνται από το διαιτητή. Έστω ότι η Αλίκη υπογράφει ένα μήνυμα *m* για να το στείλει στον Βύρωνα. Η διαδικασία παρουσιάζεται στο Σχήμα 8.6.



Σχήμα 8.6 Σύστημα ψηφιακής υπογραφής με διαιτητή

Υποθέτουμε ότι όλα τα κανάλια επικοινωνίας μεταξύ των τριών συμμετασχόντων του μοντέλου του σχήματος προσφέρουν αυθεντικοποίηση και ακεραιότητα των μηνυμάτων. Αυτό μπορεί να γίνει με τη βοήθεια κάποιου κέντρου διανομής κλειδιών. Τα κλειδιά αυτά μπορούν να χρησιμοποιηθούν σε μονόδρομη MAC. Οι διαδικασίες αυθεντικοποίησης και ακεραιότητας δεν φαίνονται στο παραπάνω σχήμα. Το σύστημα ψηφιακών υπογραφών αποτελείται από τα εξής βήματα:

1. Η Αλίκη υπολογίζει τη σύνοψη του μηνύματος *m* και στη συνέχεια στέλνει το αποτέλεσμα στον διαιτητή, μαζί με την ταυτότητά της. Ο διαιτητής θα πρέπει να είναι σε θέση να γνωρίζει την ταυτότητα της υπογράφουσας για να την συμπεριλάβει στην ψηφιακή υπογραφή, όπως θα δούμε στη συνέχεια.

2. Ο διαιτητής δημιουργεί ένα νέο μήνυμα το οποίο αποτελείται από την ταυτότητα της Αλίκης και τη σύνοψη που παρέλαβε. Στη συνέχεια, κρυπτογραφεί το μήνυμα με το μυστικό του κλειδί *kd*:

$$s = e_{kd}(\text{"Αλίκη"} \| h(m))$$

3. Το αποτέλεσμα της παραπάνω συμμετρικής κρυπτογράφησης είναι η ψηφιακή υπογραφή, την οποία στέλνει ο διαιτητής πίσω στην Αλίκη.
4. Όταν η Αλίκη αποφασίσει να στείλει το υπογεγραμμένο μήνυμα στον Βύρωνα, προσκολλά την υπογραφή *s* στο μήνυμα *m* και τα στέλνει στον Βύρωνα.
5. Μόλις ο Βύρων λάβει το μήνυμα και την υπογραφή αυτού ($m||s$), στέλνει την υπογραφή *s* στον διαιτητή.
6. Ο διαιτητής αποκρυπτογραφεί την υπογραφή με το μυστικό του κλειδί και το αποτέλεσμα που προκύπτει στέλνεται ως απάντηση στον Βύρωνα. Το αποτέλεσμα είναι η ταυτότητα της Αλίκης και η σύνοψη υπό μορφή απλού κειμένου.
7. Τέλος, ο Βύρων εξακριβώνει την ταυτότητα της Αλίκης στο πρώτο τμήμα της αποκρυπτογραφημένης υπογραφής και στη συνέχεια υπολογίζει τη σύνοψη του μηνύματος ($h(m)$) και τη συγκρίνει με αυτήν που παρέλαβε από τον διαιτητή. Αν οι δύο συνόψεις συμπίπτουν, τότε δέχεται την ψηφιακή υπογραφή.

Από την παραπάνω περιγραφή είναι φανερό ότι οι ψηφιακές υπογραφές κατασκευάζονται από τον διαιτητή. Στην πραγματικότητα, η ψηφιακή υπογραφή μοιράζεται μεταξύ της Αλίκης και του διαιτητή, καθώς ο διαιτητής δε γνωρίζει το μήνυμα το οποίο υπογράφεται. Η Αλίκη βασίζεται στον διαιτητή για να ολοκληρώσει τη διαδικασία της ψηφιακής υπογραφής, αλλά αντίθετα, ο διαιτητής έχει τη δυνατότητα να πλαστογραφήσει μήνυμα της Αλίκης, εφόσον γνωρίζει τη κρυπτογραφική μονόδρομη hash που χρησιμοποιείται. Έτσι, η ασφάλεια του συστήματος εξαρτάται από την εμπιστοσύνη του διαιτητή, την κρυπτογραφική δύναμη του συμμετρικού κρυπταλγόριθμου που χρησιμοποιεί ο διαιτητής και από τη μυστικότητα και σωστή φύλαξη του συμμετρικού κλειδιού του διαιτητή.

Όροι-κλειδιά του κεφαλαίου

- αυθεντικοποίηση ταυτότητας και αυθεντικοποίηση μηνύματος
- πράξη υπογραφής και πράξη επαλήθευσης
- σύστημα ψηφιακής υπογραφής
- ψηφιακή υπογραφή με ανάκτηση μηνύματος
- ψηφιακή υπογραφή με παράρτημα
- πλαστογραφία ψηφιακής υπογραφής
- επίθεση επιλεκτικής πλαστογραφίας

- σύστημα τυφλής ψηφιακής υπογραφής και ηλεκτρονικό χρήμα