ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

ΣΥΣΤΗΜΑΤΑ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΜΑΡΙΝΑΚΗ ΙΩΑΝΝΗ ΝΙΚΟΛΑΟΥ

Εξεταστική Επιτροπή:

1. Χ. Κουκουβίνος, Καθηγητής ΕΜΠ
2. Α Παπαϊωάννου, Αναπληρωτής Καθηγητής ΕΜΠ (**Επιβλέπων)**
3. Π. Στεφανέας, Λέκτορας ΕΜΠ

Πρόλογος

Η παρούσα διπλωματική ασχολείται με τις Ψηφιακές Υπογραφές, μία από τις σημαντικότερες εφαρμογές της σύγχρονης Κρυπτογραφίας. Ψηφιακή Υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου.

Στο πρώτο κεφάλαιο εισάγουμε τις τον ορισμό και τις ιδιότητες των Ψηφιακών Υπογραφών. Στο δεύτερο κεφάλαιο παρουσιάζουμε κάποιες βασικές έννοιες από τα Διακριτά Μαθηματικά και την Άλγεβρα που θα φανούν χρήσιμα στην πορεία. Στο τρίτο και το τέταρτο κεφάλαιο αναφερόμαστε στις Hash Functions και στην Κρυπτογραφία Ασύμμετρου Κλειδιού, ενώ στο πέμπτο παρουσιάζουμε κάποιους από τους κινδύνους που μπορεί να συναντήσουμε όταν χρησιμοποιούμε τις Ψηφιακές Υπογραφές.

Στα υπόλοιπα κεφάλαια ασχολούμαστε με κάποια από τα σημαντικότερα Σχήματα Ψηφιακών Υπογραφών και τέλος κλείνουμε με μια σύντομη αναφορά στα Ψηφιακά Πιστοποιητικά.

Abstract

This thesis deals with Digital Signatures, one of the major applications of modern cryptography. A Digital Signature is a mathematical system used to prove the authenticity of a digital message or document.

In the first chapter we introduce the definition and properties of digital signatures. In the second chapter we present some basic concepts of Discrete Mathematics and Algebra. In the third and fourth chapter we take a look at Hash Functions and Asymmetric Key Cryptography, while the fifth chapter presents some of the attacks that may be encountered when using digital signatures.

The remaining chapters deal with some of the most important Digital Signature Schemes. We conclude with a brief reference to Digital Certificates.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον αναπληρωτή καθηγητή του Ε.Μ.Π. κ. Α. Παπαϊωάννου για την πολύτιμη καθοδήγησή του καθώς και τη βοήθεια που μου προσέφερε κατά την εκπόνηση αυτής της εργασίας. Θέλω επίσης να ευχαριστήσω τους καθηγητές της επιτροπής καθώς και τους υπόλοιπους καθηγητές της σχολής για τη συμβολή τους στην εκπαίδευση μου κατά τη διάρκεια της φοίτησής μου στη Σ.Ε.Μ.Φ.Ε. Μου έδωσαν εμπειρίες που θα μου μείνουν αξέχαστες και εφόδια που θα μου είναι χρήσιμα στο μέλλον.

ΠΕΡΙΕΧΟΜΕΝΑ

Αφιερωμένο στη μητέρα μου και στον πατέρα μου για την υπομονή τους
Στην αδερφή μου που είναι το πρότυπό μου
Και στη Σταλιάνα χωρίς την οποία αυτή η εργασία δε θα υπήρχε

1. Τί είναι οι ψηφιακές υπογραφές;

Η παρούσα εργασία θα ασχοληθεί με τις ψηφιακές υπογραφές. Η χρήση των ψηφιακών υπογραφών αποτελεί μια από τις σημαντικότερες εφαρμογές της σύγχρονης Κρυπτογραφίας. Τί είναι όμως η ψηφιακή υπογραφή;

Ψηφιακή υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου.

Το 1976 ο Whitfield Diffie και ο Martin Hellman για πρώτη φορά παρουσίασαν την ιδέα των ψηφιακών υπογραφών, αν και απλά έκαναν μια υπόθεση για την δυνατότητα ύπαρξης τέτοιων σχημάτων. Λίγο αργότερα ο Ronald Rivest, ο Adi Shamir και ο Len Adleman παρουσίασαν τον αλγόριθμο RSA (από τα αρχικά των ονομάτων τους) αποδεικνύοντας ότι η ιδέα των Diffie-Hellman ήταν υλοποιήσιμη. Οι πρώτες ψηφιακές υπογραφές με τον αλγόριθμο RSA όμως δεν ήταν ασφαλείς στην πράξη μέχρι την κυκλοφορία του Lotus Notes 1.0 από την IBM το 1989 όπου χρησιμοποιήθηκαν για πρώτη φορά σε ένα γνωστό στην αγορά λογισμικό.

Για να καλυφθούν οι ανάγκες ασφαλείας εισήχθη αργότερα η χρήση της συνάρτησης κατατεμαχισμού. Πλέον η ψηφιακή υπογραφή υπολογιζόταν πάνω στην σύνοψη του μηνύματος αντί για ολόκληρο το μήνυμα. Άλλοι αλγόριθμοι που αναπτύχθηκαν μετά το RSA ήταν οι ψηφιακές υπογραφές Lamport, οι ψηφιακές υπογραφές Merkle (γνωστές ως δένδρα Merkle ή απλούστερα "δένδρα συνόψεων/hash") και οι ψηφιακές υπογραφές Rabin.

Το 1988 ο Shafi Goldwasser, ο Silvio Micali και ο Ronald Rivest ήταν οι πρώτοι που δημοσίευσαν ολοκληρωμένη μελέτη για τις απαιτήσεις ασφάλειας των ψηφιακών υπογραφών. Παρουσίασαν με ποιους τρόπους κάποιος μπορεί να παραβιάσει τις υπάρχουσες υλοποιήσεις ψηφιακών υπογραφών καθώς και το μοντέλο ψηφιακών υπογραφών GMR.

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 και εφαρμόζονται σωστά (με χρήση ασφαλών κρυπτογραφικών αλγορίθμων), είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις αντίστοιχες

χειρόγραφες. Πολλοί οργανισμοί υιοθετούν την χρήση των ψηφιακών υπογραφών ώστε να αποφεύγεται η αποστολή τυπωμένων εγγράφων επικυρωμένα με χρήση σφραγίδων και υπογραφών, που είναι μια χρονοβόρα και δαπανηρή διαδικασία.

Για να κατανοήσουμε τη σπουδαιότητα των ψηφιακών υπογραφών στην εποχή μας αρκεί να αναλογιστούμε την ποσότητα των συναλλαγών ηλεκτρονικού εμπορίου που λαμβάνουν χώρα ημερησίως. Για παράδειγμα 5.5% των συνολικών χρηστών του διαδικτύου επισκέπτονται καθημερινά το amazon.com, ενώ 3% το ebay.com[1]. Το νούμερο δεν μοιάζει ίσως τόσο εντυπωσιακό μέχρι να αναφέρουμε ότι ο εκτιμώμενος αριθμός των χρηστών του Διαδικτύου για τον περασμένο χρόνο είναι μεγαλύτερος από 2 δισεκατομμύρια! Προφανώς κάθε επίσκεψη δεν αντιστοιχεί σε συναλλαγή αλλά από τα ετήσια έσοδα του Amazon τα οποία για το 2010 ανήλθαν σε 34.2 δισεκατομμύρια δολάρια[2], εύκολα μπορούμε να συνειδητοποιήσουμε ότι το ηλεκτρονικό εμπόριο αποτελεί ένα σημαντικό μέρος του σύγχρονου εμπορικού κόσμου.
Η χρήση των ψηφιακών υπογραφών όμως δεν περιορίζεται στο ηλεκτρονικό εμπόριο, Υπάρχει πληθώρα εφαρμογών στο e-banking, στη χρήση πιστωτικών καρτών, στα μηνύματα ηλεκτρονικού ταχυδρομείου (email) καθώς και σε κάθε άλλη ανθρώπινη δραστηριότητα όπου απαιτείται ασφαλής και γρήγορη ταυτοποίηση.

1.1 Ιδιότητες Ψηφιακών Υπογραφών

Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (π.χ. ένα μήνυμα ή ένα κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα γι αυτό άτομα (**εμπιστευτικότητα**). Το «κακόβουλο άτομο» που προσπαθεί να παραβιάσει τη συναλλαγή καλείται συνήθως **αντίπαλος**. Να σημειώσουμε ότι αυτή η εργασία υιοθετεί την κοινή

[1] Σύμφωνα με την ιστοσελίδα http://www.internetworldstats.com/ που συλλέγει δεδομένα για των αριθμό των επισκέψεων που δέχονται διάφοροι ιστότοποι
[2] UNITED STATES SECURITIES AND EXCHANGE COMMISSION - FORM 10-K - AMAZON.COM, INC. (AMZN)". Retrieved 2011-02-07.

σύμβαση τα δύο μέρη μια κρυπτογραφικής συναλλαγής Α, Β να ονομάζονται Alice και Bob, ενώ για τον αντίπαλο (opponent) δίνεται το όνομα Oscar.

Η υπηρεσία της εμπιστευτικότητας υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή δεδομένων. Μια αντιστοιχία με την καθημερινότητα είναι ένα αδιαφανές κουτί το οποίο είναι κλειδωμένο με ένα λουκέτο του οποίου το κλειδί κατέχει μόνο ο αποδέκτης. Το λουκέτο είναι πολύ δύσκολο να ανοιχθεί χωρίς το κλειδί αλλά ακόμα κι αν παραβιαστεί θα υπάρχουν ενδείξεις ότι έχει γίνει παραβίαση. Αυτό μας οδηγεί στην επόμενη ιδιότητα.

Τα δεδομένα, δεν θα πρέπει να είναι δυνατόν να αλλοιωθούν κατά την μετάδοσή τους. Ο παραλήπτης θα πρέπει να τα λάβει όπως ακριβώς ο αποστολέας τα έστειλε και να είναι σίγουρος ότι τα δεδομένα που λαμβάνει είναι αυτά που ο αποστολέας έχει στείλει (**ακεραιότητα**). Στο παράδειγμα μας το λουκέτο είναι σχεδιασμένο ώστε να φέρει ξεκάθαρες ενδείξεις ότι παραβιάστηκε σε περίπτωση που δεν ανοιχθεί με το κλειδί του.

Επιπλέον σε μία συναλλαγή, είναι απαραίτητο ο παραλήπτης να είναι σίγουρος για την ταυτότητα του αποστολέα (**αυθεντικοποίηση**). Δηλαδή, να γνωρίζει με σιγουριά ότι το μήνυμα που λαμβάνει και φαίνεται να το υπογράφει ο κ. Χ, είναι όντως από τον κ. Χ και όχι από κάποιον που παριστάνει τον Χ. Κάτι τέτοιο επιτυγχάνεται αν γνωρίζουμε για παράδειγμα ότι το μοναδικό άλλο κλειδί του λουκέτου βρίσκεται στην κατοχή του αποστολέα. Γενικά η αυθεντικοποίηση μπορεί να γίνει με διάφορους τρόπους:

1. Με κάποια πληροφορία που μας είναι γνωστή, όπως ένας κωδικός ή ένα PIN.
2. Με κάποιο αντικείμενο που βρίσκεται στην ιδιοκτησία μας, όπως το κλειδί που αναφέραμε ή κάποιου είδους ταυτότητα (π.χ. τραπεζική κάρτα)
3. Για ύψιστη ασφάλεια με κάποια γενετική ιδιότητα όπως είναι τα δακτυλικά αποτυπώματα ή η φωνή μας.

Η αυθεντικοποίηση είναι πολύ στενά συνδεδεμένη με την ακεραιότητα. Αν έχουμε αυθεντικοποίηση χωρίς ακεραιότητα ο αντίπαλος μπορεί να τροποποιήσει την πληροφορία της αυθεντικοποίησης και να αλλάξει την

ταυτότητα του αποστολέα. Στην αντίθετη περίπτωση (ακεραιότητα χωρίς αυθεντικοποίηση) ο αντίπαλος μπορεί ανεξέλεγκτα να τροποποιήσει το μήνυμα και να υπολογίσει με τέτοιο τρόπο τη κρυπτογραφικό άθροισμα ελέγχου ώστε το μήνυμα να φαίνεται ότι είναι ακέραιο.

Τέλος, συμμετέχοντας σε μία ηλεκτρονική συναλλαγή (π.χ. ηλεκτρονικό εμπόριο) θα πρέπει να μην είναι δυνατόν τα εμπλεκόμενα μέρη να αρνηθούν εκ των υστέρων την συμμετοχή τους στη συναλλαγή αυτή (**μη αποποίηση ευθύνης**). Η ασύμμετρη κρυπτογραφία παρέχει ψηφιακές υπογραφές που διαθέτουν αμφιμονοσήμαντη σχέση με τα μέλη της συναλλαγής, έτσι ώστε ο παραλήπτης να μπορεί να επιβεβαιώσει αν χρειαστεί την ταυτότητα του αποστολέα, ενώ αντίστοιχα ο παραλήπτης δε μπορεί να αρνηθεί ότι έλαβε το μήνυμα

Οι παραπάνω ιδιότητες, (**εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα, μη αποποίηση**) στον ηλεκτρονικό κόσμο, αποτελούν αντικείμενο της επιστήμης που ασχολείται με την ασφάλεια των πληροφοριών. Διάφοροι μηχανισμοί, τεχνικές και τεχνολογίες έχουν αναπτυχθεί αποσκοπώντας να διασφαλίσουν τις ιδιότητες αυτές σε μία ηλεκτρονική συναλλαγή. Σ'αυτές τις τεχνολογίες συμπεριλαμβάνονται και τα διάφορα σχήματα ψηφιακών υπογραφών που θα μελετήσουμε.

1.2 Ορισμός

Αφού εξηγήσαμε τι είναι η ψηφιακή υπογραφή, μπορούμε να προχωρήσουμε σε έναν μαθηματικά φορμαλιστικό ορισμό:

Ένα σχήμα υπογραφής είναι μια πεντάδα $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ που ικανοποιεί τα ακόλουθα:

1. $\mathcal{P}$ είναι ένα πεπερασμένο σύνολο δυνατών *μηνυμάτων* προς υπογραφή
2. $\mathcal{A}$ είναι ένα πεπερασμένο σύνολο δυνατών *υπογραφών*
3. $\mathcal{K}$ είναι ένα πεπερασμένο σύνολο όλων των δυνατών *κλειδιών*
4. Για κάθε $K \in \mathcal{K}$ υπάρχει μια *συνάρτηση υπογραφής*

$$sig_K \in \mathcal{S}, \qquad sig_K : \mathcal{P} \to \mathcal{A}$$

5. και μια αντίστοιχη *συνάρτηση επαλήθευσης*

$$ver_K \in \mathcal{V}, \qquad ver_K : \mathcal{P} \times \mathcal{A} \to \{true, false\}$$

για τις οποίες για κάθε μήνυμα $m \in \mathcal{P}$ και κάθε υπογραφή $y \in \mathcal{A}$ ισχύει η παρακάτω σχέση:

$$ver_K(m, y) = \begin{cases} true, & \text{αν } y = sig_K(m) \\ false, & \text{αν } y \neq sig_K(m) \end{cases}$$

Ένα ζεύγος (m, y) με $m \in \mathcal{P}$ και $y \in \mathcal{A}$ ονομάζεται *υπογεγραμένο μήνυμα*.

Θα πρέπει ακόμα να ικανοποιούνται οι ακόλουθες απαιτήσεις:

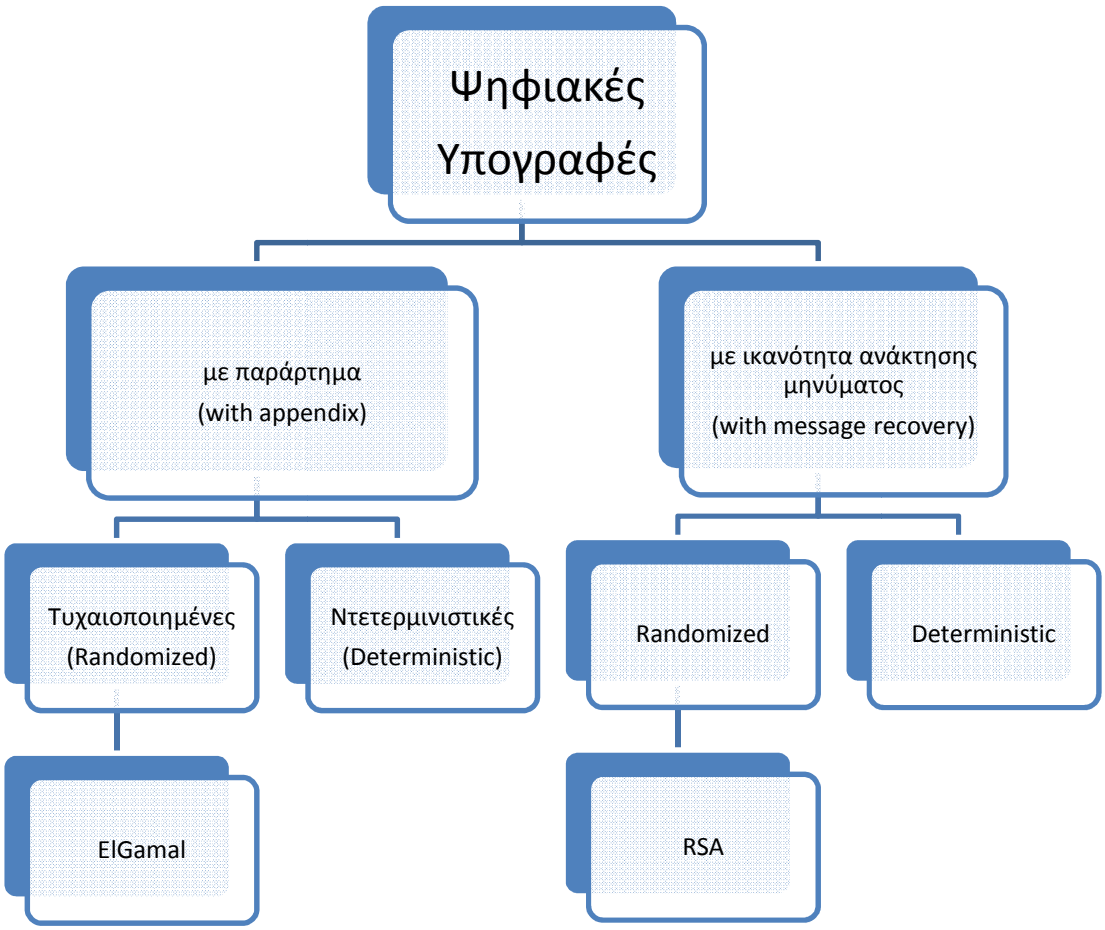
- Για κάθε $K \in \mathcal{K}$ οι συναρτήσεις sig_K και ver_K θα πρέπει να είναι πολυωνυμικού χρόνου.
- Η ver_K θα είναι δημόσια ενώ η sig_K ιδιωτική.
- Δεδομένου κάποιου μηνύματος m θα πρέπει να είναι υπολογιστικά ανέφικτο για οποιονδήποτε εκτός από τον υπογράφοντα να υπολογίσει υπογραφή τέτοια ώστε $ver_K(m, y) = true$. (Σημειώνουμε πως είναι δυνατόν να υπάρχουν περισσότερες από μία υπογραφές y για δεδομένο m, ανάλογα με τον τρόπο που ορίζεται η συνάρτηση επαλήθευσης.
- Θα πρέπει να είναι υπολογιστικά «εύκολο» για κάποιον να παράξει την υπογραφή του, όπως και για οποιονδήποτε άλλον να την επαληθεύσει.

- Επειδή η ψηφιακή υπογραφή δεν αποτελεί μέρος του μηνύματος θα πρέπει να περιέχει στοιχεία που να την την συνδέουν με το μήνυμα με κάποιο τρόπο.

Τέλος σημειώνουμε ότι οι ψηφιακές υπογραφές μπορούν να χωριστούν σε δύο μεγάλες κατηγορίες:

1. Σχήματα ψηφιακής υπογραφής με παράρτημα, στα οποία το αρχικό μήνυμα είναι απαραίτητο για την πιστοποίηση γνησιότητας της υπογραφής.
2. Σχήματα ψηφιακής υπογραφής με ικανότητα ανάκτησης του μηνύματος, στα οποία το αρχικό μήνυμα μπορεί να παραχθεί από την ίδια την υπογραφή.

Το παρακάτω διάγραμμα μας δείχνει αυτό τον διαχωρισμό:



2. Βασικές Μαθηματικές Έννοιες

Για την καλύτερη κατανόηση της παρούσας εργασίας είναι απαραίτητες κάποιες έννοιες από τα Διακριτά Μαθηματικά και τη Θεωρία Αριθμών τις οποίες θα εισάγουμε στη συνέχεια. Παρακάτω δίνονται σημαντικοί ορισμοί καθώς και θεωρήματα. Οι αποδείξεις των θεωρημάτων κρίνεται ότι ξεφεύγουν από το σκοπό της παρούσης και ο αναγνώστης που ενδιαφέρεται μπορεί να ανατρέξει στη σχετική βιβλιογραφία για περαιτέρω πληροφορίες.

Ορισμός 1: Έστω α και β ακέραιοι. Ο α *διαιρεί* τον β $(\alpha|\beta)$ αν υπάρχει ακέραιος γ τέτοιος ώστε $\beta = \alpha \cdot \gamma$.

Θεώρημα 1: Για κάθε $\alpha, \beta, \gamma \in \mathbb{Z}$ ισχύουν τα παρακάτω
(α) $\alpha|\alpha$
(β) Αν $\alpha|\beta$ και $\beta|\gamma$ τότε $\alpha|\gamma$
(γ) Αν $\alpha|\beta$ και $\alpha|\gamma$ τότε $\alpha|(\beta \cdot x + \gamma \cdot y)$ για κάθε $x, y \in \mathbb{Z}$
(δ) Αν $\alpha|\beta$ και $\beta|\alpha$ τότε $\alpha = \pm\beta$

Ορισμός 2: Ένας ακέραιος γ είναι *κοινός διαιρέτης* των α, β αν $\gamma|\alpha$ και $\gamma|\beta$.

Ορισμός 3: Ένας μη αρνητικός ακέραιος δ είναι *μέγιστος κοινός διαιρέτης (greatest common divisor – gcd)* των ακεραίων α και β και συμβολίζεται $\delta = gcd(\alpha, \beta)$ αν:
(α) Ο δ είναι κοινός διαιρέτης των α και β.
(β) Για κάθε $\gamma \in \mathbb{Z}$ για τον οποίο ισχύουν $\gamma|\alpha$ και $\gamma|\beta$ έχουμε $\gamma|\delta$.

Ορισμός 4: Ένας μη αρνητικός ακέραιος δ είναι *ελάχιστο κοινό πολλαπλάσιο (lowest common denominator – lcd)* των ακεραίων α και β και συμβολίζεται $\delta = lcd(\alpha, \beta)$ αν:
(α) $\alpha|\delta$ και $\beta|\delta$
(β) Για κάθε $\gamma \in \mathbb{Z}$ για τον οποίο ισχύουν $\alpha|\gamma$ και $\beta|\gamma$ έχουμε $\delta|\gamma$.

Ορισμός 5: Αν α και β ακέραιοι με $\beta \geq 1$ τότε η διαίρεση του α με το β δίνει δύο (μοναδικούς) ακεραίους π (πηλίκο) και υ (υπόλοιπο) τέτοιους ώστε $\alpha = \beta \cdot \pi + \upsilon$, όπου $0 \leq \upsilon < \beta$. Συμβολίζουμε $\upsilon = \alpha \; mod \; \beta$.

Θεώρημα 2: Αν α και β θετικοί ακέραιοι τότε $lcd(\alpha, \beta) = \frac{\alpha \cdot \beta}{gcd(\alpha, \beta)}$.

Ορισμός 6: Ένας ακέραιος α είναι *πρώτος ως προς* ακέραιο β όταν $gcd(\alpha, \beta) = 1$.

Ορισμός 7: Ένας ακέραιος $\rho \geq 2$ είναι *πρώτος αριθμός* αν οι μοναδικοί θετικοί διαιρέτες του είναι η μονάδα και ο ίδιος ο ρ. Σε αντίθετη περίπτωση ο ρ είναι σύνθετος. Ο 1 δεν είναι ούτε πρώτος, ούτε σύνθετος.

Θεώρημα 3: Υπάρχουν άπειροι το πλήθος πρώτοι αριθμοί.

Θεώρημα 4: Αν ρ είναι πρώτος και $\rho | \alpha \cdot \beta$ τότε είτε $\rho | \alpha$ είτε $\rho | \beta$ (μπορεί να συμβαίνουν και τα δύο ταυτόχρονα).

Θεώρημα 5: Για κάθε ακέραιο $n \geq 2$ υπάρχουν $p_i, i = 1, 2, \dots, k$ μοναδικοί πρώτοι και $e_i, i = 1, 2, \dots, k$ θετικοί ακέραιοι έτσι ώστε: $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$
Με λίγα λόγια, κάθε ακέραιος $n \geq 2$ μπορεί να γραφτεί σαν γινόμενο δυνάμεων πρώτων παραγόντων με μοναδικό τρόπο. Το παραπάνω είναι γνωστό σαν **Θεμελιώδες Θεώρημα της Αριθμητικής (ΘΘΑ).**

Ορισμός 8: Έστω $n \geq 1$. Ορίζουμε τη *συνάρτηση Euler του n* την οποία συμβολίζουμε $\varphi(n)$ ως το πλήθος των ακεραίων που ανήκουν στο διάστημα $[1, \dots, n]$ οι οποίοι είναι πρώτοι ως προς τον n.

Θεώρημα 6: Η συνάρτηση Euler έχει τις ακόλουθες ιδιότητες:
(α) Αν p είναι πρώτος τότε $\varphi(p) = p - 1$
(β) Αν $gcd(\alpha, \beta) = 1$ τότε $\varphi(\alpha\beta) = \varphi(\alpha) \cdot \varphi(\beta)$
(γ) Αν $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$ τότε:
$\varphi(n) = n \cdot \left(1 - {}^{1}/_{p_1}\right) \cdot \left(1 - {}^{1}/_{p_2}\right) \cdot \dots \cdot \left(1 - {}^{1}/_{p_k}\right)$

Θεώρημα 7: Αν α και β θετικοί ακέραιοι με $\alpha > \beta$ τότε:
$gcd(\alpha, \beta) = gcd(\beta, \alpha \ mod \ \beta)$

Ορισμός 9: Αν n, α, β θετικοί ακέραιοι, λέμε ότι ο α είναι *ισότιμος* με τον $\beta \ mod \ n$ και γράφουμε $\alpha = \beta \ mod \ n$ αν ο n διαιρεί τον $(\alpha - \beta)$

Θεώρημα 8: Για κάθε $\alpha, \beta, \gamma, \alpha_1, \beta_1$ ακεραίους και n θετικό ακέραιο ισχύουν τα παρακάτω:
(α) $\alpha = \beta \ mod \ n$ αν και μόνο αν οι α, β έχουν το ίδιο υπόλοιπο όταν διαιρεθούν με n
(β) $\alpha = \alpha \ mod \ n$
(γ) Αν $\alpha = \beta \ mod \ n$ τότε $\beta = \alpha \ mod \ n$
(δ) Αν $\alpha = \beta \ mod \ n$ και $\beta = \gamma \ mod \ n$ τότε $\alpha = \gamma \ mod \ n$
(ε) Αν $\alpha = \alpha_1 \ mod \ n$ και $\beta = \beta_1 \ mod \ n$ τότε $\alpha + \beta = (\alpha_1 + \beta_1) mod \ n$ και $\alpha \cdot \beta = (\alpha_1 \cdot \beta_1) mod \ n$

Ορισμός 10: Ορίζουμε το σύνολο $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ που αποτελείται από τους ακέραιους $mod \ n$.

Ορισμός 11: Έστω $\alpha \in \mathbb{Z}_n$. Ορίζουμε τον *αντίστροφο* του $\alpha \ mod \ n$ και συμβολίζουμε $x = \alpha^{-1}$ έναν ακέραιο $x \in \mathbb{Z}_n$ τέτοιον ώστε $\alpha \cdot x = 1 \ mod \ n$. Αν υπάρχει τέτοιος x τότε είναι μοναδικός και ο α λέγεται *αντιστρέψιμος*.

Ορισμός 12: Έστω $\alpha, \beta \in \mathbb{Z}_n$ και $\beta \ modn$ αντιστρέψιμος. Ορίζουμε τη *διαίρεση* του α με β mod n ως το γινόμενο του α με το $\beta^{-1} mod \ n$.

Θεώρημα 9: Έστω $\alpha \in \mathbb{Z}_n$. Ο α είναι αντιστρέψιμος αν και μόνο αν $gcd(\alpha, n) = 1$.

Θεώρημα 10 (Κινέζικο Θεώρημα Υπολοίπων): Έστω οι ακέραιοι $n_1, n_2, \dots, n_k$ οι οποίοι είναι ανά δύο πρώτοι μεταξύ τους. Τότε το σύστημα εξισώσεων:

$$x = \alpha_1 \ mod \ n_1$$
$$x = \alpha_2 \ mod \ n_2$$

.

.

$$x = \alpha_k \; mod \; n_k$$

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

Θεώρημα 11: Έστω $gcd(n_1, n_2) = 1$. Τότε το ζευγάρι εξισώσεων $x = \alpha \; mod \; n_1$ και $x = \alpha \; mod \; n_2$ έχει μοναδική λύση $x = \alpha \; mod \; (n_1, n_2)$.

Ορισμός 13: Η πολλαπλασιαστική ομάδα του $\mathbb{Z}_n$ είναι $\mathbb{Z}_n{}^* = \{\alpha \in \mathbb{Z}_n | gcd(\alpha, n) = 1\}$. Στην ειδική περίπτωση όπου n είναι πρώτος τότε $\mathbb{Z}_n{}^* = \{\alpha \in \mathbb{Z}_n | 1 \leq \alpha \leq n - 1\}$.

Ορισμός 14: *Τάξη του* $\mathbb{Z}_n{}^*$ ονομάζεται το πλήθος των στοιχείων του και συμβολίζεται $|\mathbb{Z}_n{}^*|$.

Θεώρημα 12: Έστω $n \geq 2, n \in \mathbb{Z}$. Τότε:
(α) **(Θεώρημα Euler)** Αν $\alpha \in \mathbb{Z}_n{}^*$ τότε $\alpha^{\varphi(n)} = 1 \; mod \; n$.
(β) Αν n είναι γινόμενο διαφορετικών πρώτων αριθμών και αν $r = s \; mod \; \varphi(n)$ $τότε$ $\alpha^r = \alpha^s \; mod \; n$ για κάθε ακέραιο α.

Θεώρημα 13: Έστω p πρώτος αριθμός τότε:
(α) **(Θεώρημα Fermat)** Αν $gcd(\alpha, p) = 1$ τότε $\alpha^{p-1} = 1 \; mod \; p$.
(β) Αν $r = s \; mod \; (p - 1)$ τότε $\alpha^r = \alpha^s \; mod \; p$ για κάθε ακέραιο α.
(γ) $\alpha^p = \alpha \; mod \; p$ για κάθε ακέραιο α.

Ορισμός 15: Έστω $\alpha \in \mathbb{Z}_n{}^*$. Ορίζουμε *τάξη του* α και συμβολίζουμε $ord(\alpha)$ τον ελάχιστο θετικό ακέραιο t για τον οποίον $\alpha^t = 1 \; mod \; n$.

Θεώρημα 14: Έστω $\alpha \in \mathbb{Z}_n{}^*$. Αν $ord(\alpha) = t$ και $\alpha^s = 1 \; mod \; n$ τότε ο t διαιρεί τον s.

Ορισμός 16: Έστω $\alpha \in \mathbb{Z}_n{}^*$. Αν $ord(\alpha) = t$ τότε ο α είναι *πρωταρχική ρίζα* του $\mathbb{Z}_n{}^*$. Αν το σύνολο $\mathbb{Z}_n{}^*$ έχει πρωταρχική ρίζα ονομάζεται *κυκλικό*.

Θεώρημα 15:

(α) Το $\mathbb{Z}_n{}^*$ έχει πρωταρχική ρίζα αν και μόνο αν $n = 2, 4, p^k$ ή $2 \cdot p^k$ όπου p περιττός πρώτος αριθμός και $k \geq 1$.

(β) Αν α είναι πρωταρχική ρίζα του $\mathbb{Z}_n{}^*$ τότε $\mathbb{Z}_n{}^* = \{\alpha^i \ mod \ n | 0 \leq i \leq \varphi(n) - 1$.

(γ) Έστω α ένας πρωταρχική ρίζα του $\mathbb{Z}_n{}^*$. Τότε $\beta = \alpha^i$ είναι επίσης πρωταρχική ρίζα του αν και μονο αν $gcd\big(i, \varphi(n)\big) = 1$. Αν το $\mathbb{Z}_n{}^*$ είναι κυκλικό τότε το πλήθος των πρωταρχικών ριζών είναι $\varphi(\varphi(n))$.

(δ) Έστω $\alpha \in \mathbb{Z}_n{}^*$. Ο α είναι πρωταρχική ρίζα του $\mathbb{Z}_n{}^*$ αν και μόνο αν $\alpha^{\varphi(n)/p} \neq 1 \ mod n$ για κάθε πρώτο διαιρέτη p του $\varphi(n)$.

Ορισμός 17: Έστω g πρωταρχικό στοιχείο του πρώτου p.

(α) Έστω ακέραιος n. Τότε $g(n) \equiv 1 \ mod \ p$ αν και μόνο αν $n \equiv 0 \ mod \ (p - 1)$

(β) Έστω ακέραιοι j και k. Τότε $g^j \equiv g^k \ mod \ p$ αν και μόνο αν $j \equiv k \ mod \ (p - 1)$

Ορισμός 18: Έστω $\alpha \in \mathbb{Z}_n{}^*$. Το α ονομάζεται *τετραγωνικό υπόλοιπο του modulo* n (στο $\mathbb{Z}_n$) αν υπάρχει $x \in \mathbb{Z}_n{}^*$ τέτοιο ώστε $x^2 = \alpha \ mod \ n$. Σε αντίθετη περίπτωση ο α λέγεται μη τετραγωνικό υπόλοιπο του modulo n. Το σύνολο των τετραγωνικών υπολοίπων του modulo n συμβολίζεται Q_n.

Θεώρημα 16: Έστω p περιττός πρώτος αριθμός και α μια πρωταρχική ρίζα του $\mathbb{Z}_p{}^*$. Τότε $\beta \in \mathbb{Z}_p{}^*$ είναι τετραγωνικό υπόλοιπο του modulo n αν και μόνο αν $\beta = \alpha^i \ mod \ p$, όπου i είναι ένας άρτιος ακέραιος. Έπεται ότι $\big|Q_p\big| = \frac{p-1}{2}$, δηλαδή τα μισά στοιχεία στο $\mathbb{Z}_p{}^*$ είναι τετραγωνικά υπόλοιπα και τα άλλα μισά δεν είναι.

Θεώρημα 17: Έστω n είναι το γινόμενο δύο διαφορετικών περιττών πρώτων αριθμών p και q $(n = p \cdot q)$. Τότε $\alpha \in \mathbb{Z}_n{}^*$ είναι ένα τετραγωνικό υπόλοιπο του modulo n αν και μόνο αν $\alpha \in Q_p$ και $\alpha \in Q_q$.

Ορισμός 19: Έστω $\alpha \in Q_n$. Αν $x \in \mathbb{Z}_n{}^*$ ικανοποιεί την εξίσωση $x^2 = \alpha \ mod \ n$ τότε το x λέγεται *τετραγωνική ρίζα του* $\alpha \ mod \ n$.

Θεώρημα 18: Για το πλήθος των τετραγωνικών ριζών ισχύουν:

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

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

3. Δημιουργία Συναρτήσεων Κατακερματισμού και Υπογραφή (Hashing and Signing)

3.1 Συνάρτηση Κατακερματισμού (hash function)

Αν στα διάφορα σχήματα ψηφιακών υπογραφών χρησιμοποιήσουμε το αρχικό μήνυμα, τότε και η υπογραφή θα έχει μήκος μεγαλύτερο ή ίσο από το μήνυμα. Αυτό φυσικά είναι σημαντικό μειονέκτημα όταν το μήνυμα είναι μεγάλο, διότι αυξάνει την υπολογιστική ισχύ αλλά και τον χώρο που απαιτείται. Για να αποφύγουμε αυτά τα προβλήματα χρησιμοποιούμε μια Συνάρτηση Κατακερματισμού (hash function). Το σχήμα υπογραφής εφαρμόζεται στην σύνοψη που προκύπτει από τη συνάρτηση hash αντί σε ολόκληρο το μήνυμα.

Ορισμός

Η *συνάρτηση hash* είναι μια εύκολα υπολογίσιμη συνάρτηση $h(x) = y$ που αντιστοιχίζει δυαδικές συμβολοσειρές αυθαίρετου μήκους σε δυαδικές συμβολοσειρές σταθερού μήκους.

Όπως φαίνεται και από τον ορισμό, ζητάμε από τις hash functions να έχουν τις ακόλουθες ιδιότητες:

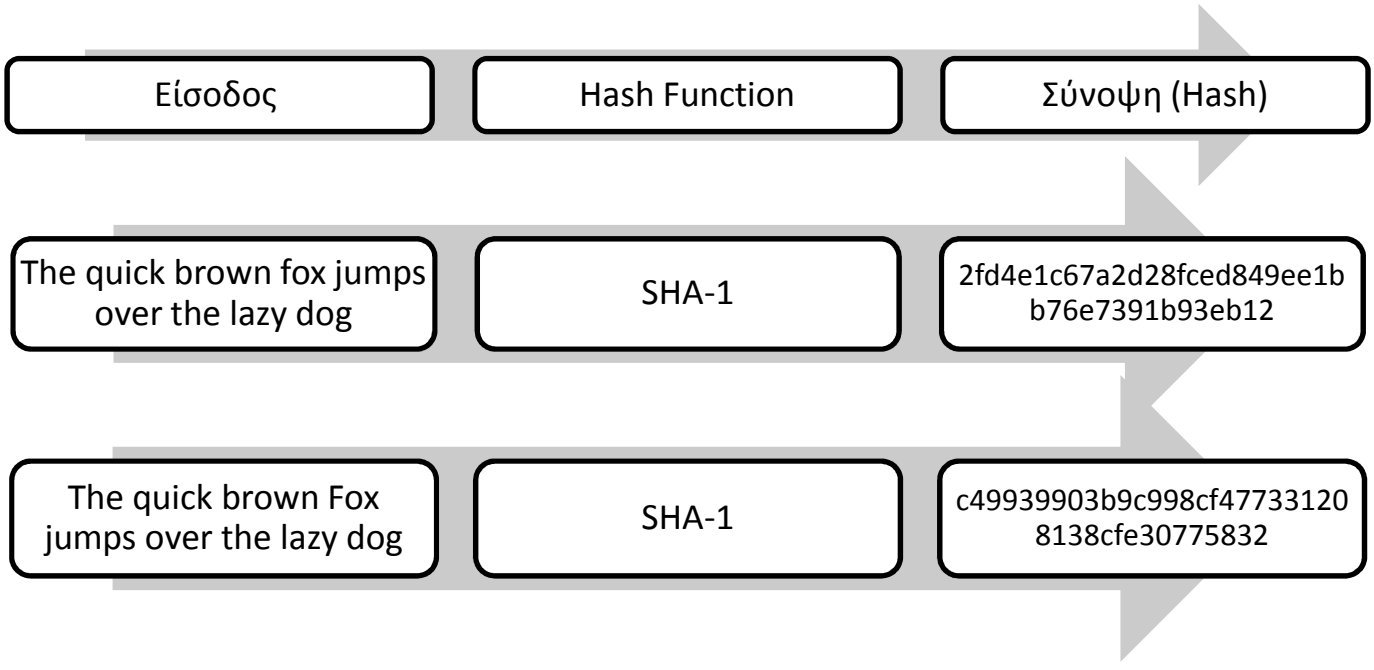
1. Μπορούν να δεχτούν είσοδο οποιουδήποτε μήκους
2. Έχουν έξοδο σταθερού μήκους
3. Δεδομένου του x είναι εύκολο να υπολογιστεί το y
4. Η $h(x)$ είναι μη αντιστρέψιμη (δηλαδή δοθέντος του y είναι σχεδόν αδύνατο να βρεθεί το x)
5. Η $h(x)$ είναι αμφιμονοσήμαντη (δηλαδή $x_1 \neq x_2 \Leftrightarrow h(x_1) \neq h(x_2)$)

Επιπλέον δίνουμε τους ακόλουθους ορισμούς:

Ορισμός

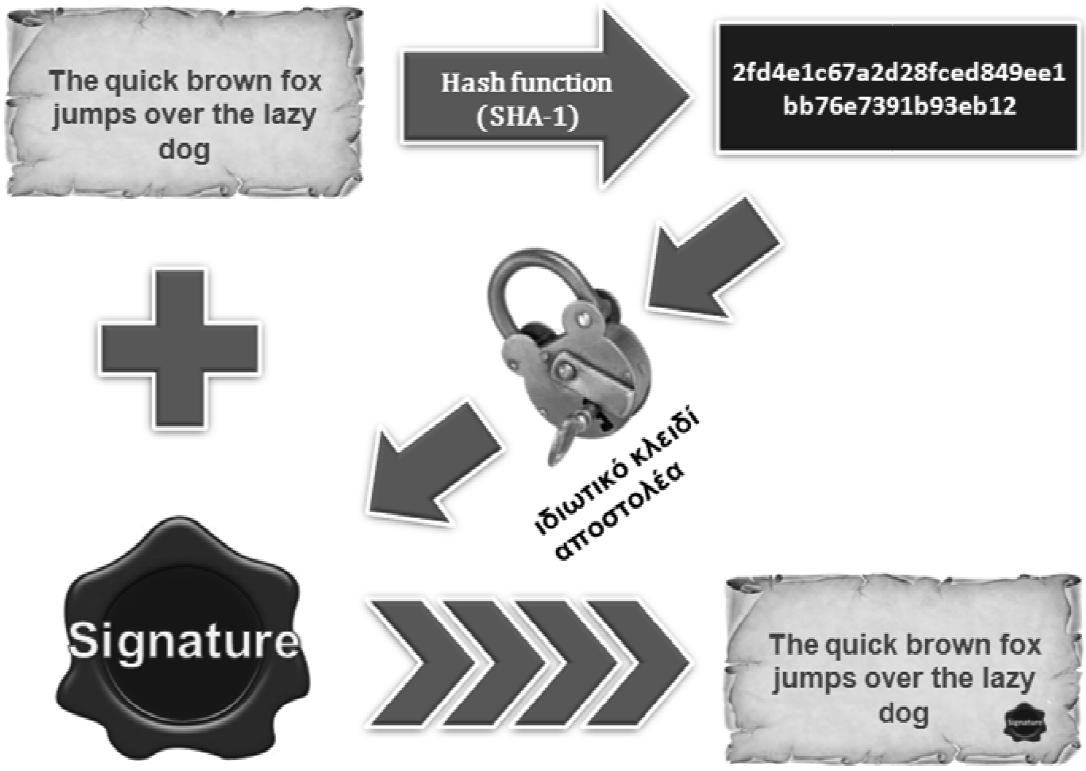
1. Μια hash function h είναι *weakly collision free (ασθενώς ελεύθερη συγκρούσεων)* για το μήνυμα x_1 αν είναι υπολογιστικά ανέφικτο να βρούμε ένα μήνυμα $x_2 \neq x_1$ τέτοιο ώστε $h(x_1) = h(x_2)$.
2. Μια hash function h είναι *strongly collision free (ισχυρά ελεύθερη συγκρούσεων)* αν είναι υπολογιστικά ανέφικτο να βρούμε μηνύματα $x_1 \neq x_2$ τέτοια ώστε $h(x_1) = h(x_2)$.
3. Μια hash function h είναι *one-way (μονόδρομη)* αν δοθέντος ενός μηνύματος x_1 είναι υπολογιστικά ανέφικτο να βρούμε μήνυμα $x_2 \neq x_1$ τέτοιο ώστε $h(x_2) = x_1$.

Η ιδιαιτερότητα των hash functions είναι ότι ακόμα και μια πολύ μικρή αλλαγή στο κείμενο (π.χ. κάνοντας ένα γράμμα κεφαλαίο ή αφήνοντας ένα παραπάνω κενό κάπου) παράγει τελείως διαφορετική σύνοψη. Ένα τέτοιο παράδειγμα βλέπουμε παρακάτω:

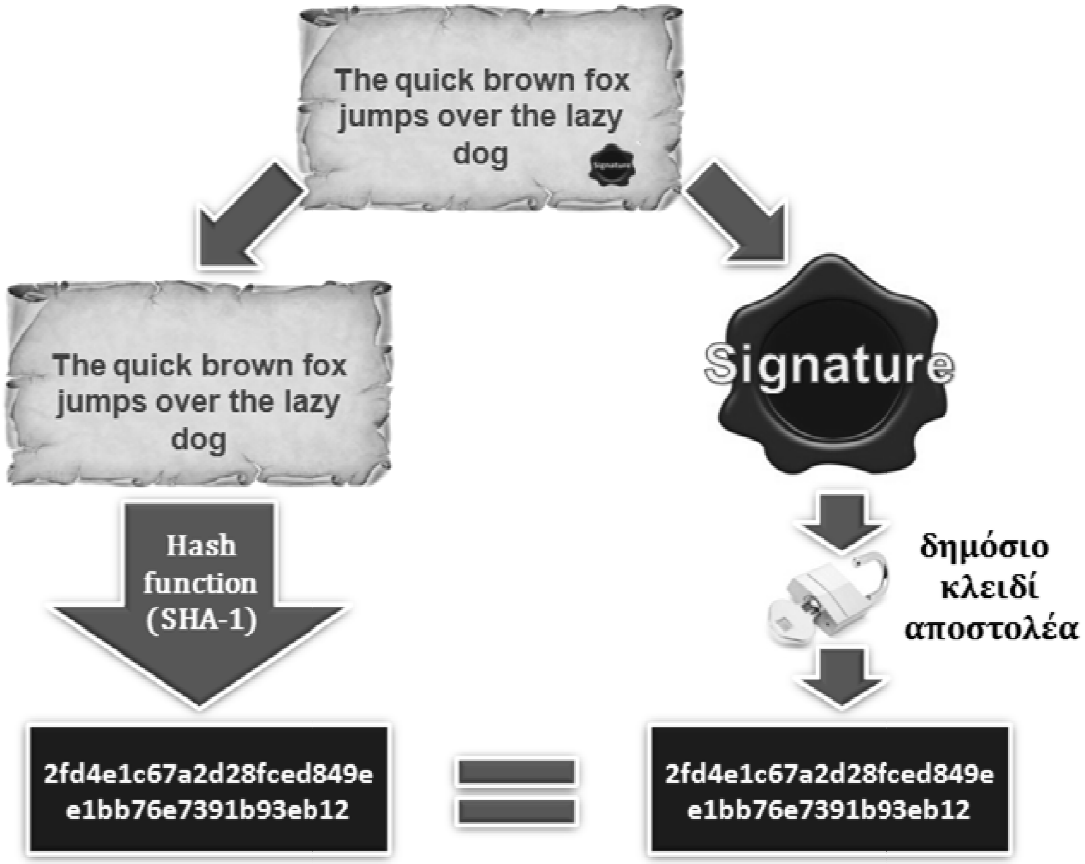


ΠΑΡΑΔΕΙΓΜΑ

Η hash function h αρχικά δημοσιοποιείται. Η Alice θέλει να υπογράψει το μήνυμα m οπότε υπολογίζει το $h(m)$. Το αποτέλεσμα είναι έχει πολύ μικρότερο μήκος από το αρχικό της μήνυμα και άρα μπορεί να υπογραφεί πιο γρήγορα. Στη συνέχεια λοιπόν υπολογίζει το $sig(h(m))$ και το χρησιμοποιεί σαν υπογραφή για το μήνυμα. Το ζεύγος $(m, sig(h(m))$ περιέχει την ίδια πληροφορία με το ζεύγος $(m, sig(m))$, απαιτεί λιγότερους πόρους για τη μετάδοση και αποθήκευση του μηνύματος και με την προϋπόθεση ότι η hash function είναι γρήγορη, κατασκευάζεται σε μικρότερο χρόνο.



Αντίστοιχα για να επαληθεύσει ο Bob ότι το υπογεγραμμένο μήνυμα είναι αυθεντικό θα χρησιμοποιήσει την hash function για να δημιουργήσει μια σύνοψη του μηνύματος και παράλληλα θα χρησιμοποιήσει το ιδιωτικό κλειδί του αποστολέα για να αποκωδικοποιήσει την ψηφιακή υπογραφή. Αν οι δύο hash στις οποίες καταλήξει είναι ίδιες τότε θα ξέρει ότι το μήνυμα είναι αυθεντικό.



Είναι όμως ασφαλής αυτή η μέθοδος; Ας υποθέσουμε ότι ο Oscar έχει στην κατοχή του το υπογεγραμμένο ζεύγος $(m, sig(h(m))$. Διαθέτει επίσης ένα μήνυμα m' στο οποίο θέλει να προσθέσει την υπογραφή της Alice. Πρέπει δηλαδή να ισχύει:

$$sig(h(m') = sig(h(m))$$

Επειδή όμως η $sig()$ είναι 1-1 θα πρέπει:

$$h(m') = h(m)$$

Αν η hash function είναι μονόδρομη, ο Oscar θα δυσκολευτεί πολύ να βρει κατάλληλο m', αφού η πιθανότητα κάποιο μήνυμα με νόημα (και όχι μια τυχαία σειρά από σύμβολα) να δουλέψει είναι μικρή. Επιπροσθέτως, αφού έχουμε απαιτήσει η hash function να είναι ισχυρά ανθεκτική σε συγκρούσεις είναι

απίθανο ο Oscar να καταφέρει να βρει οποιαδήποτε $m_1 \neq m_2$ που να παράγουν την ίδια σύνοψη.
Αν μπορούσε να το καταφέρει θα μπορούσε στη συνέχεια να βάλει την Alice να υπογράψει το m_1 και να μεταφέρει την υπογραφή της στο m_2. Η Alice όμως θα υποπτευόταν κάτι αφού το m_1 (και πιθανότατα και το m_2) θα ήταν κείμενα χωρίς νόημα. Θα εξετάσουμε όμως αργότερα ένα είδος επίθεσης το οποίο θα μπορούσε να δουλέψει αν το μέγεθος της σύνοψης είναι μικρό και η hash function δεν είναι ισχυρά ανθεκτική σε συγκρούσεις (birthday attack)

Οι γνωστότερες hash functions στην εποχή μας είναι η MD5, η SHA-1 και η SHA-2. Ξεκινώντας από το 2005 οι Rijmen και Oswald ανακοίνωσαν μια επίθεση σε μια μειωμένη έκδοση του SHA-1 (53 από 80 γύρους) η οποία μπορούσε να βρει συγκρούσεις σε μικρότερο από τις απαιτούμενες 2^{80} δοκιμές που απαιτεί μια brute-force επίθεση. Το Φεβρουάριο του ίδιου χρόνου οι Xiaoyun Wang, Yiqun Lisa Yin και Hongbo Yu (του Πανεπιστημίου Shandong στην Κίνα) εξέδωσαν μια εργασία όπου αποδείκνυαν ότι μπορούν να βρεθούν συγκρούσεις στην πλήρη SHA-1 σε 2^{69} δοκιμές που είναι μια σημαντική θεωρητική εξέλιξη. Μετά από αλλεπάλληλες μειώσεις του αριθμού αυτού, το 2008 ο Stéphane Manuel παρουσίασε μια μεθοδολογία επίθεσης που θεωρητικά μείωνε τις απαιτούμενες δοκιμές ανάμεσα σε 2^{51} και 2^{57}. Ο πρώτος που παρουσίασε μεθοδολογία που προσεγγίζει αυτά τα όρια είναι ο Marc Stevens στις 8 Νοεμβρίου 2010 με εκτιμώμενη πολυπλοκότητα $2^{57.5}$. Επίσης να σημειώσουμε ότι σε μειωμένες εκδόσεις της SHA-1 (73 από τους 80 γύρους) έχουν σημειωθεί επιθέσεις με πολυπλοκότητα 2^{35}. Συνεπώς η SHA-1 δε θεωρείται ασφαλής σήμερα.
Όσον αφορά την MD5, στις 30 Δεκεμβρίου 2008 οι Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik και Benne de Weger εξέδωσαν μια μελέτη με τίτλο "MD5 considered harmful today"[3] στην οποία απέδειξαν ότι το σύστημα MD5 μπορεί να χρησιμοποιηθεί για την παραγωγή ψευδών πιστοποιητικών ασφαλείας τα οποία θα γίνονται δεκτά από όλους τους σύγχρονους browsers. Η MD5 γρήγορα εγκαταλείφθηκε χωρίς

[3] http://www.win.tue.nl/hashclash/rogue-ca/

κάποιο μεγάλο κρούσμα πλαστογραφίας αφού οι hackers δεν είχαν προλάβει να μελετήσουν τη συγκεκριμένη μέθοδο.

Παρόλο που η SHA-2 δεν έχει παρουσιάσει αδυναμίες, επειδή αλγοριθμικά φέρει ομοιότητες με την SHA-1, η NIST ήδη έχει κηρύξει διαγωνισμό ανοιχτό στο κοινό για τη δημιουργία ενός προτύπου SHA-3 ώστε σε περίπτωση που υπάρξει κάποιο πρόβλημα στο μέλλον να υπάρχει ένας ασφαλής αλγόριθμος στον οποίο να μπορούν να βασιστούν οι χρήστες. Άλλωστε σύμφωνα με το νόμο του Moore για την αύξηση της υπολογιστικής δύναμης, ποτέ δεν πρόκειται κάποιο κρυπτογραφικό σύστημα να είναι απόλυτα ασφαλές.

4. Ασύμμετρη Μέθοδος Κρυπτογράφησης (Asymmetric Cryptography)

4.1 Κρυπτογράφηση Δημοσίου Κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρείχε ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Σε αντίθεση, οι αλγόριθμοι συμμετρικού κλειδιού, παραλλαγές των οποίων χρησιμοποιούνται εδώ και χιλιάδες χρόνια, χρησιμοποιούν ένα μυστικό κλειδί για κωδικοποίηση και αποκωδικοποίηση, το οποίο πρέπει να μοιράζονται και να διατηρούν κρυφό και τα δύο μέρη. Συνεπώς θα πρέπει να το έχουν ανταλλάξει εκ των προτέρων και οποιαδήποτε απροσεξία ενός θέτει σε κίνδυνο και τους δύο. Αυτό είναι ένα σημαντικό μειονέκτημα που δημιούργησε την ανάγκη για μια μέθοδο όπως η ασύμμετρη μέθοδος κρυπτογράφησης.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Key Server 0.9.6

mQGiBDmXx8cRBADd0Dko7J7Gb5G/FINwO48AgrlYE87wCT5dlqSXl2uoDmR0/dKp
pJmvDeLQw+Z02yGx7TKf7PC5dfh61tIHyeI0SfCZVA5DtRDk3keNXy2WLnLMg2yS
J44JG3I/o1QKXL8PKD2bkv/vUl7gtXe3qa57oC+2ZmxzptnLeBh08QrWXwCg/8A2
L7WHGKbhYKCApM+0FJStYrcD/1iTYhNsiZnW2tc86e/uHiX8rg7tD7VGm/Wg2E4V
Hadsb4wMLhlfi/vCSEZmlH3hFxvGk6YCWXkdFxzqhq2ZJRWQStqZqjSPWTI3Hv0K
NzjqSDbRMQY2O025g1FyWB62ZDrUWXqzyb14okoEdXT/lQA7Xe95T8uy1zfTUmBg
ieTtA/0RU3MYboVOyDgGvJ7fVyFNdk8+v6Hzcn6EZMWYJ1fE5hw/tSLnRAXb7ejh
wsLDDCGsjloUj4TnMHH0LUTZSWbgDZwCF6tig3mbhk7YH21zWrVQwPidSpS5O3Oh
85V3nJx5r0406nM4N1cp46yKUMekE6nhubCpVme6o+f9sUMXkLQhR2VydCBLYXNw
ZXJzZW4gPGdla2FzQHdtkGF0YS5jb20+iQBLBBARAgALBQI5l8fHBAsDAgEACgkQ
Ls3rBj/p+6oQGwCgv5ML3xAatvJtY1mKnwz1SH2YbJ8AoPeBkUY73P+QDc5aFdHC
rCkobzlYuQQNBDmXx8cQEAD5GKB+WgZhekOQldwFbIeG7GHszUUfDtjgo3nGydx6
C6zkP+NGlLYwSlPXfAIWSIC1FeUpmamfB3TT/+OhxZYgTphluNgN7hBdq7YXHFHY
UMoiV0MpvpXoVis4eFwL2/hMTdXjqkbM+84X6CqlFGHjhKlP0YOEqHm274+nQ0YI
xswdd1ck0ErixPDojhNnl06SE2H22+slDhf99pj3yHx5sHId0HX79sFzxIMRJitD
YMPj6NYK/aEoJguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4fdIRPyvHX86RA6dfSd7ZC
LQI2wSbLaF6dfJgkCo1+Le3kXXn11JJPmxiO/CqnS3wy9kJXtwh/CBdyorrWqULz
Bej5UxE5T7bxbrlLOCDaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DI09ZekX1KHT
UPj1WV/cdlJPPT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq
01uejaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O
9vPJI8BD8KVbGI2Ou1WMuF040zT9fBdXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcK
ctaGxAMZyAcpesqVDNmWn6vQClCbAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6z3W
FwACAhAAaumPF6HT301BhkfuMTVI2jFXUJ7prdWy4pwZArvdDVYQ35M8sG/ISJjwg
B2GdpK9i02B25Cen309snDSj/aJkz7PQgD8CyB1V0KiDFX+KxR8S0le2k1tdbiP3
wNYxw7MDiz757IY9/hmv6YDwSeS2sWnyjgfQXR5z2RBs4r+UZ8YWk8h4YQsLSL2B
Z/PImaiopMScDJy1m4AzasXNdyr1SywU4tlwOXZhZh6ccZB/z6nlZJgMnwfVw1fZ
8wyiTKGoyOp5eh9edDFwtcAVNHVoI0hj9kDfa5sfA9zcKfeLH7TouYLuMcdws9Uc
fNeJI6AgzUvGwzvG9HVuVGf7n5b1j9Kp+jcSjvWqpQX1/iDEN8KG6/yk5mtok4lv
JBieGM2SahP1cTk1P4kcrlwJ419EhKtC6xZS96J0+TmyLBTSrJHazWR+n/lQsXvz
g7wNUycZx+/v1QDGO3HyekqZR76BSMVrpNEYEWcBclTeJ6nBJCPTGxqvP4IQhzhJ
3znANVOsViJZ7rG3DrygE+8vQ32GjbBZzouN/gHxmSKOuvw6yjFdkiSMNNdlIeKm
05Z5aVSXPuE7+TfkbFGHy+GCxjsH6FNhU/8QKtr712NO9laDARGCVaOiVvBVevVO
PXajFSW19F7Rswmh7kD5jUEy9E7ANAa0YD5i07ee0wvmaGSwfKKIRgQYEQIABgUC
OZfHxwAKCRAuzesGP+n7qj2kAJ48xQqu8b8kzQHmmUvMFr8z+bfivQCgxXhBHUT1
LsvbbxbTJ/Da6n5YSYE=
=9v+B
-----END PGP PUBLIC KEY BLOCK-----
```

Στην ασύμμετρη μέθοδο κρυπτογράφησης, κάθε χρήστης διαθέτει ένα ζευγάρι από κρυπτογραφικά κλειδιά: ένα δημόσιο και ένα ιδιωτικό. Όπως φαίνεται από τα ονόματά τους, το δημόσιο κλειδί είναι εύκολα διαθέσιμο σε οποιονδήποτε, σε αντίθεση με το ιδιωτικό το οποίο είναι γνωστό μόνο στον παραλήπτη. Τα μηνύματα κωδικοποιούνται με το δημόσιο κλειδί του παραλήπτη και μπορούν να αποκωδικοποιηθούν μόνο με το αντίστοιχο ιδιωτικό κλειδί. Τα κλειδιά σχετίζονται μαθηματικά, αλλά οι παράμετροι επιλέγονται έτσι ώστε ο προσδιορισμός του ιδιωτικού κλειδιού από το δημόσιο να είναι απαγορευτικά ακριβός σε υπολογιστική δύναμη. Η ανακάλυψη αλγορίθμων που μπορούσαν να παράγουν ζεύγη δημοσίων/ιδιωτικών κλειδιών συνετέλεσε καθοριστικά στη διάδοση της κρυπτογραφίας στα μέσα της δεκαετίας του 1970.

Όταν αναφερόμαστε σε κρυπτοσύστημα δημόσιου κλειδιού, χρησιμοποιούμε τον όρο «ιδιωτικό κλειδί» (private key), για να αναφερθούμε στη μυστική ποσότητα που δεν είναι γνωστή στο ευρύτερο κοινό και ειδικότερα στον αντίπαλο. Αυτός ο όρος χρησιμοποιείται για λόγους διάκρισης από τα συμμετρικά κρυπτοσυστήματα, όπου η μυστική ποσότητα αναφέρεται ως «μυστικό κλειδί» (secret key).

Σε αντίθεση με τη συμμετρική κρυπτογραφία, σε ένα ασύμμετρο κρυπτοσύστημα ο αλγόριθμος κρυπτογράφησης είναι ίδιος με τον αλγόριθμο αποκρυπτογράφησης, με τη μόνη διαφορά ότι κατά την αποκρυπτογράφηση χρησιμοποιείται το αντίστροφο κλειδί. Έτσι, σε ένα ασύμμετρο κρυπτοσύστημα όπου το ζευγάρι του δημόσιου και ιδιωτικού κλειδιού είναι το (k_e, k_d), αν η κρυπτογράφηση ορίζεται από την πράξη e_{k_e} , τότε για την αποκρυπτογράφηση θα ισχύει:

$$d_{k_d}\ (x) = \ e_{k_d}\ (x)$$

Λόγω της συμμετρίας των πράξεων, αν η κρυπτογράφηση είναι η e_{k_d} , τότε η αποκρυπτογράφηση θα ορίζεται από την e_{k_e} .

ΠΑΡΑΔΕΙΓΜΑ

Μια καλή αναλογία για να κατανοήσουμε τον τρόπο με τον οποίο δουλεύει η ασύμμετρη μέθοδος κρυπτογράφησης είναι να φανταστούμε την Alice και τον Bob να στέλνουν ένα μυστικό μήνυμα μέσω του ταχυδρομείου. Ας υποθέσουμε ότι η Alice στέλνει πρώτη ένα κρυφό μήνυμα και περιμένει μια κρυφή απάντηση από τον Bob.

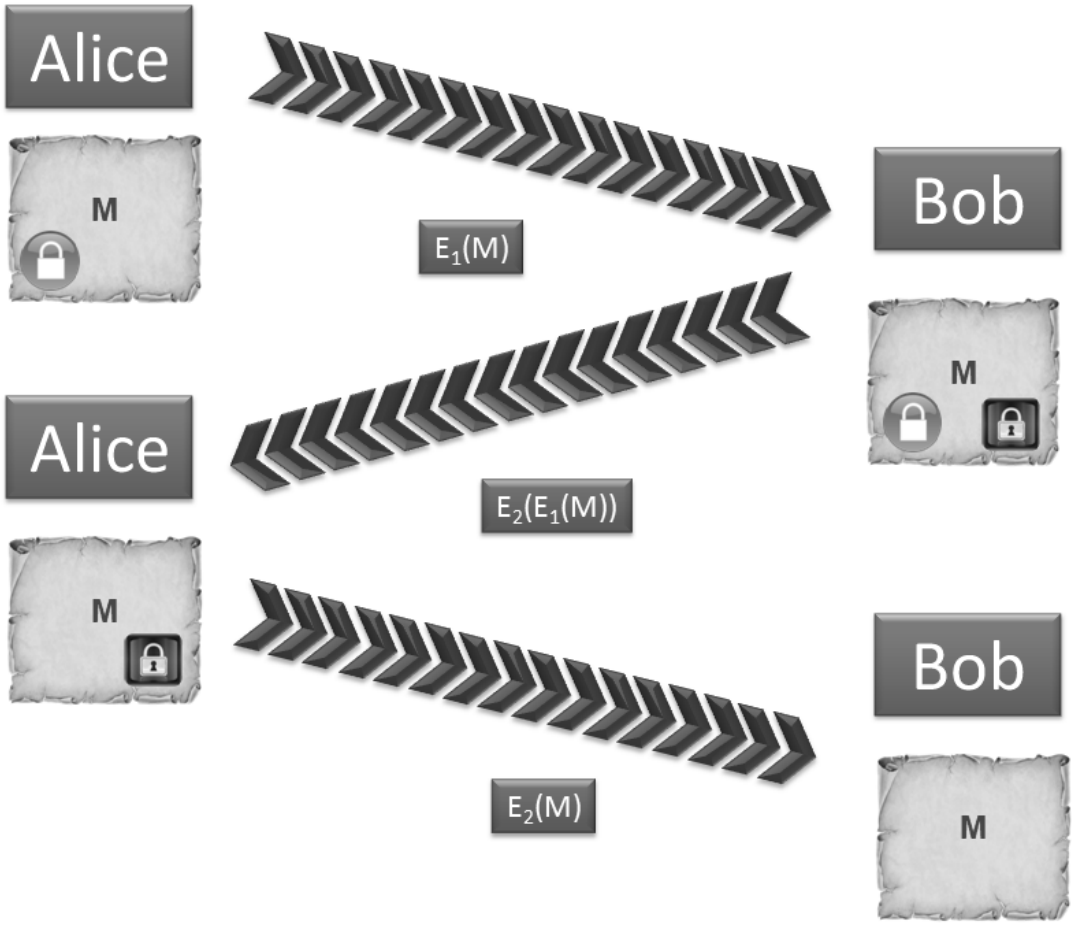
Στο συμμετρικό σύστημα η Alice βάζει το μήνυμά της μέσα σε ένα κουτί το οποίο κλειδώνει με ένα λουκέτο. Για το λουκέτο αυτό κατέχει ένα κλειδί η Alice καθώς και ένα ακριβές αντίγραφό του κλειδιού ο Bob, το οποίο του έχει παραδώσει η Alice με κάποιον ασφαλή τρόπο (π.χ. σε κάποια συνάντηση των δύο ή μέσω ταχυδρομείου). Η Alice στέλνει το κουτί μέσω του ταχυδρομείου, ο Bob το ξεκλειδώνει με το αντίγραφο του κλειδιού, διαβάζει το μήνυμα και μπορεί στη συνέχεια να στείλει την απάντηση του κλειδώνοντάς τη με το ίδιο λουκέτο.

Αντιθέτως στο ασύμμετρο κρυπτοσύστημα ο Bob και η Alice διαθέτουν δύο διαφορετικά λουκέτα. Αρχικά η Alice ζητάει από τον Bob να της στείλει ταχυδρομικά το λουκέτο του, αλλά ανοικτό, χωρίς να της στείλει το κλειδί του. Όταν λοιπόν θελήσει να στείλει το μήνυμά της θα το κλειδώσει με το λουκέτο του Bob ο οποίος μπορεί να το ξεκλειδώσει όταν το παραλάβει με το κλειδί του και να διαβάσει το μήνυμα. Για να απαντήσει θα χρησιμοποιήσει την ίδια διαδικασία, ζητώντας το λουκέτο της Alice και κλειδώνοντας το μήνυμά του με αυτό πριν την αποστολή.

Είναι προφανές ότι το μεγάλο πλεονέκτημα στη συγκεκριμένη μέθοδο είναι ότι δεν χρειάζεται να παρέχει το ένα μέρος στο άλλο ένα αντίγραφο του κλειδιού του το οποίο μπορεί να υποκλαπεί και να αντιγραφεί από τον Oscar ώστε να μπορεί στη συνέχεια να παρακολουθεί όλη την αλληλογραφία των δύο. Εδώ να σημειώσουμε ότι για να διαβάσει ο Oscar την αλληλογραφία θα πρέπει να έχει στην κατοχή του και τα δύο κλειδιά, ειδάλλως θα διαβάζει μόνο τη μισή. Επίσης, ακόμα κι αν καταφέρει να έχει στην κατοχή του το κλειδί της Alice, θα μπορεί να υποκλέπτει μόνο τις συζητήσεις της με τον Bob αφού σε κάθε συζήτηση με άλλα άτομα θα χρησιμοποιεί διαφορετικά λουκέτα.

Ένα διαφορετικό είδος ασύμμετρου κρυπτοσυστήματος περιγράφεται ως εξής: Η Alice και ο Bob έχουν δύο ξεχωριστά λουκέτα. Αυτή τη φορά η Alice

χρησιμοποιεί ένα κουτί που έχει δύο υποδοχές για λουκέτα. Βάζει το μήνυμα της μέσα, κλειδώνει το κουτί με το δικό της λουκέτο και το στέλνει στον Bob. Ο Bob προσθέτει το δικό του λουκέτο και στέλνει το κουτί πίσω στην Alice. Εκείνη αφαιρεί το λουκέτο της με το δικό της κλειδί και το στέλνει πίσω στον Bob, ο οποίος ξεκλειδώνει το δικό του λουκέτο και μπορεί να διαβάσει πλέον το μήνυμα. Παρατηρούμε ότι η σειρά με την οποία γίνεται η αποκρυπτογράφηση είναι η ίδια με αυτή της κρυπτογράφησης, κάτι το οποίο είναι δυνατόν μόνο στην περίπτωση όπου το κρυπτοσύστημα που χρησιμοποιείται είναι αντιμεταθετικό.



Έτσι έστω $E_1()$ και $E_2()$ δύο συναρτήσεις κρυπτογράφησης και M το μήνυμα. Η Alice κωδικοποιεί το μήνυμα μέσω της $E_1()$ και στέλνει το $E_1(M)$ στον Bob. Ο Bob κωδικοποιεί ξανά το μήνυμα με την $E_2()$ και στέλνει το $E_2(E_1(M))$ στην Alice. Η Alice αποκωδικοποιεί το $E_2(E_1(M))$ με την $E_1()$ και καταλήγει στο $E_2(M)$ το οποίο όταν πλέον παραλάβει ο Bob θα μπορεί να το αποκωδικοποιήσει με την $E_2()$ και να καταλήξει στο M.

Τα κλειδιά των δύο μελών δεν ανταλλάχθηκαν, θα μπορούσε όμως το ίδιο το Μ να είναι κάποιο κλειδί, π.χ. το δημόσιο κλειδί της Alice. Αυτό το πρωτόκολλο (three-pass protocol) χρησιμοποιείται συχνά για την ανταλλαγή κλειδιών. Επειδή οι αλγόριθμοι συμμετρικού κλειδιού έχουν σχεδόν πάντα πολύ μικρότερο υπολογιστικό κόστος δεν έχει σταματήσει η χρήση τους και είναι σύνηθες να ανταλλάσσεται ένα κλειδί με έναν αλγόριθμο ανταλλαγής κλειδιών και να διαβιβάζονται τα δεδομένα χρησιμοποιώντας το κλειδί και ένα αλγόριθμο συμμετρικού κλειδιού. Για παράδειγμα ο PGP καθώς και η οικογένεια SSL / TLS χρησιμοποιούν αυτή τη μέθοδο και γι'αυτό το λόγο ονομάζονται υβριδικά κρυπτοσυστήματα.

Ένα μειονέκτημα του three-pass protocol είναι ότι δεν παρέχει ταυτοποίηση. Συνεπώς είναι επιρρεπές σε επιθέσεις τύπου MITM (man-in-the-middle / άνθρωπος-στη-μέση) τις οποίες θα συζητήσουμε πιο αναλυτικά παρακάτω. Πρώτα όμως πρέπει να εξετάσουμε τους στόχους και τα διάφορα είδη επιθέσεων που μπορεί να δεχτεί ένα κρυπτογραφημένο μήνυμα.

5. Επιθέσεις στις Ψηφιακές Υπογραφές

5.1 Στόχοι επιθέσεων

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

Οι πιθανές επιθέσεις που μπορεί να δεχτεί ένα σύστημα είναι οι ακόλουθες:

5.2 Είδη επιθέσεων

Υπάρχουν δύο είδη επιθέσεων στα σχήματα υπογραφών δημοσίου κλειδιού:

1. **Επιθέσεις μόνο στο κλειδί (key-only attacks):** Ο αντίπαλος γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντα.
2. **Επιθέσεις στο μήνυμα (message attacks):** Ο αντίπαλος μπορεί να εξετάσει υπογραφές που αντιστοιχούν σε γνωστά ή σε επιλεγμένα μηνύματα και διακρίνονται σε :
    - **Επίθεση σε γνωστά μηνύματα (known-message attacks):** Ο αντίπαλος έχει υπογραφές για ένα σύνολο μηνυμάτων που είναι γνωστά σε αυτόν αλλά όχι επιλεγμένα από αυτόν.
    - **Επίθεση σε επιλεγμένο μήνυμα (chosen-message attack):** Ο αντίπαλος μπορεί να δημιουργήσει νόμιμες υπογραφές για ένα επιλεγμένο σύνολο μηνυμάτων πριν προσπαθήσει να πετύχει κατάρρεύση του συστήματος. Αυτή η επίθεση είναι μη

προσαρμόσιμη (non-adaptive) με την έννοια ότι τα μηνύματα επιλέγονται πριν από τις υπογραφές.

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

Η επίθεση προσαρμόσιμου επιλεγμένου μηνύματος είναι ο πιο δύσκολος τύπος επίθεσης. Αν ο αντίπαλος γνωρίζει αρκετά μηνύματα με τις αντίστοιχες υπογραφές τους μπορεί να εξάγει κάποιο τύπο για τον τρόπο υπογραφής και στη συνέχεια να μπορεί να πλαστογραφήσει ένα μήνυμα της επιλογής του. Άρα ένα καλά σχεδιασμένο σχήμα υπογραφής πρέπει να σχεδιαστεί με ισχυρές άμυνες ενάντια σε αυτού του είδους επίθεσης.
Το επίπεδο ασφάλειας που απαιτείται για κάθε σχήμα υπογραφής εξαρτάται από τις απαιτήσεις της εφαρμογής που χρησιμοποιείται. Σημαντικό ρόλο στην ασφάλεια του συστήματος έχει και η επιλογή της hash συνάρτησης όπου θα πρέπει να είναι τέτοια ώστε ο αντίπαλος να μη μπορεί να την αντικαταστήσει με κάποια άλλη, πιο αδύναμη συνάρτηση hash και να επιδιώξει να κάνει επίθεση επιλεκτικής πλαστογράφησης.

Υπάρχουν τέσσερα είδη πλαστογράφησης που μπορεί να αποφέρει μια επιτυχής επίθεση όπως φαίνεται παρακάτω:

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

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

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

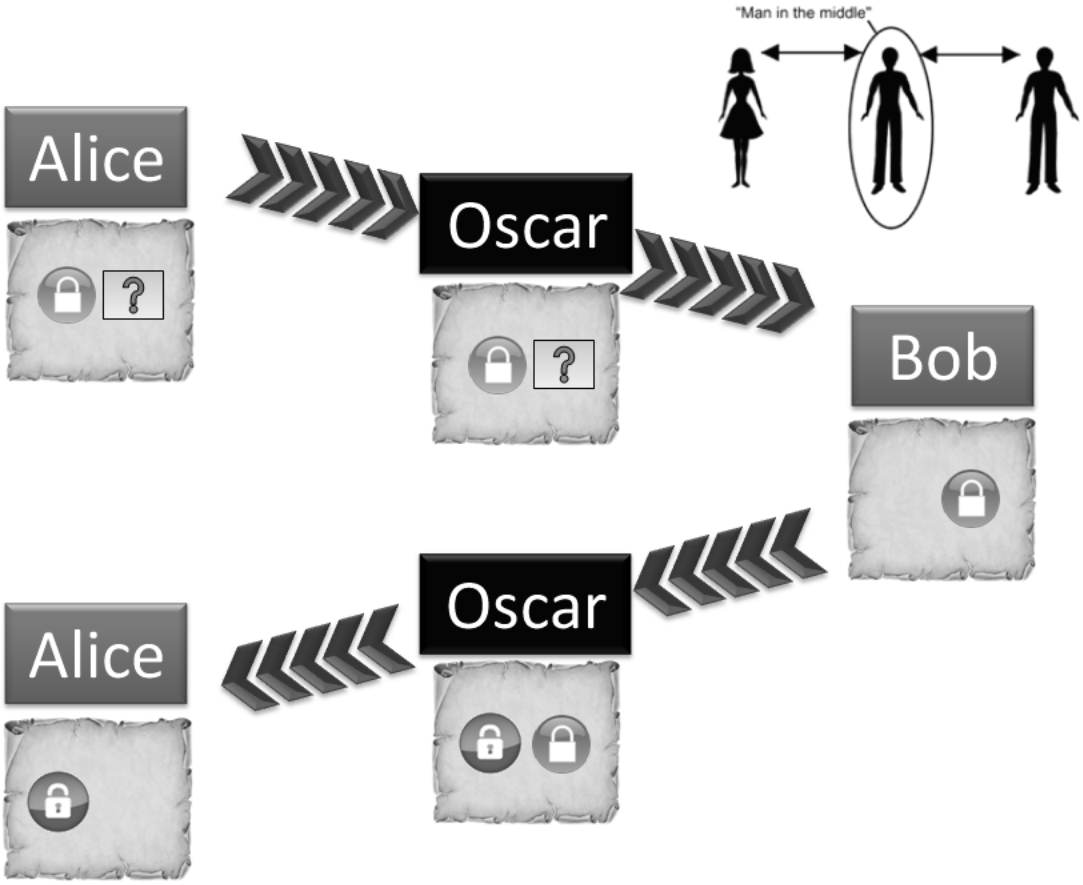
(δ) Υπαρξιακή πλαστογράφηση (existential forgery): Ο αντίπαλος είναι ικανός να πλαστογραφήσει τουλάχιστον ένα μήνυμα. Δύναται να έχει μικρό ή και καθόλου έλεγχο πάνω στο περιεχόμενο του μηνύματος που πλαστογράφησε και αυτό το μήνυμα μπορεί να μην έχει καν νόημα. Αρκεί να βρει ένα έγκυρο ζεύγος μηνύματος-υπογραφής. Καθώς αποτελεί την πιο αδύναμη επιτυχία του αντιπάλου τα πιο ανθεκτικά σχήματα υπογραφών είναι αυτά που δεν επιτρέπουν την υπαρξιακή πλαστογράφηση.

Προφανώς το πιο επικίνδυνο αποτέλεσμα είναι η ολική κατάρευση του συστήματος, όμως οποιαδήποτε επιτυχία του αντιπάλου μπορεί να προκαλέσει σοβαρό πρόβλημα.
Στη συνέχεια εξετάζουμε δυο είδη επιθέσεων που έχουμε ήδη αναφέρει, την MITM και την Birthday.

5.3 Επίθεση MITM (Άνθρωπος-Στη-Μέση / ManInTheMiddle)

Στην κρυπτογραφία έχουμε επίθεση MITM όταν μεταξύ των δύο μελών που ανταλλάζουν μηνύματα εισέρχεται ένας τρίτος ο οποίος «κρυφακούει» τη συζήτηση και πιθανόν να παρεμβαίνει σε αυτή. Ας δούμε ένα παράδειγμα:
Η Alice και ο Bob θέλουν να διεξάγουν μια μυστική συζήτηση, χωρίς να γνωρίζουν ότι ο Oscar έχει αποκτήσει πρόσβαση στον δίαυλο επικοινωνίας τους. Αρχικά ο Oscar δημιουργεί ανεξάρτητες συνδέσεις με τους συμβαλλομένους. Η Alice στέλνει το πρώτο της μήνυμα όπου ζητάει από τον Bob το δημόσιο κλειδί του, όμως ο Oscar αναχαιτίζει το συγκεκριμένο μήνυμα το οποίο αναμεταδίδει ο ίδιος στον Bob. Ο Bob, μη γνωρίζοντας ότι το μήνυμα δεν προέρχεται από την Alice, στέλνει το δημόσιο κλειδί του το οποίο αναχαιτίζει και πάλι ο Oscar. Σε αυτό το σημείο ο Oscar αλλάζει το κλειδί του Bob με το δικό του και προωθεί το μήνυμα στην Alice. Από εδώ και στο εξής η Alice κωδικοποιεί τα μηνύματα της με το κλειδί του Oscar (χωρίς να μπορεί να συμπεράνει ότι δεν είναι το κλειδί του Bob) και άρα ο υποκλοπέας μπορεί να διαβάζει και να τροποποιεί όλα τα ακόλουθα μηνύματα από τη μεριά της Alice. Ομοίως θα ξεγελάσει και τον Bob και θα αποκτήσει πρόσβαση στο δεύτερο μισό της συζήτησης. Πλέον ο Oscar μπορεί να τροποποιεί υπάρχοντα μηνύματα ή να στέλνει νέα χωρίς τα μέρη να αντιλαμβάνονται την απάτη.

Μια MITM επίθεση μπορεί να είναι επιτυχής μόνο αν ο Oscar μπορεί να υποδυθεί και τα δύο μέρη με αρκετά πειστικό τρόπο. Τα περισσότερα πρωτόκολλα περιλαμβάνουν κάποια μέθοδο ταυτοποίησης τελικού σημείου (endpoint authentication) για να αποτρέψουν τέτοιου είδους επιθέσεις. Για παράδειγμα, το SSL επαληθεύει την ταυτότητα του διακομιστή χρησιμοποιώντας μια αμοιβαία αξιόπιστη αρχή πιστοποίησης.



5.4 Επίθεση Γενεθλίων (Birthday Attack)

Η Alice θα υπογράψει ένα συμβόλαιο για την αγορά ενός οικοπέδου στην Εκάλη εφαρμόζοντας ένα από τα γνωστά σχήματα υπογραφών στη σύνοψη του ηλεκτρονικού εγγράφου. Ας υποθέσουμε ότι η hash function παράγει μια σύνοψη με μέγεθος 50 bits. Ανησυχεί ότι ο Oscar θα προσπαθήσει να την ξεγελάσει προσθέτοντας την υπογραφή της σε ένα επιπρόσθετο συμβόλαιο, πουλώντας της ένα διαμέρισμα στα Εξάρχεια. Παρόλαυτα αισθάνεται ασφαλής διότι γνωρίζει ότι η πιθανότητα ένα κείμενο να έχει την ίδια σύνοψη με το δικό της είναι 1 στις 2^{50}, δηλαδή περίπου 1 στις 10^{15}. Ο Oscar μπορεί να δοκιμάσει διάφορα πλαστά συμβόλαια, όμως είναι εξαιρετικά απίθανο να βρει ένα με τη σωστή σύνοψη.

Ο Oscar όμως έχει μελετήσει καλά το «πρόβλημα των γενεθλίων» και έχει σκεφτεί μια μέθοδο που μπορεί να δουλέψει:

Βρίσκει 30 σημεία μέσα στο κείμενο όπου μπορεί να κάνει κάποια μικρή αλλαγή, όπως να προσθέσει ένα επιπλέον κενό στο τέλος μιας σειράς, να αλλάξει μια λέξη κ.α. Σε κάθε σημείο έχει δύο επιλογές: Να κάνει την αλλαγή ή να κρατήσει το αρχικό κείμενο. Με αυτόν τον τρόπο μπορεί να δημιουργήσει 2^{30} διαφορετικές εκδόσεις του συμβολαίου οι οποίες όλες να μοιάζουν έγκυρες στα μάτια της Alice. Δημιουργεί επίσης 2^{30} εκδόσεις του πλαστού συμβολαίου και υπολογίζει όλες τις συνόψεις των αυθεντικών συμβολαίων καθώς και των πλαστών.

Το γενικευμένο «πρόβλημα των γενεθλίων» με $r = 2^{30}$ και $n = 2^{50}$ δίνει $r = \sqrt{\lambda n}$, όπου $\lambda = 2^{10} = 1024$. Σύνεπως η πιθανότητα μια έκδοση του αυθεντικού συμβολαίου να έχει ίδια σύνοψη με κάποιο πλαστό είναι $1 - e^{-1024} \approx 1$, δηλαδή είναι σίγουρο. Ο Oscar βρίσκει τα δύο συμβόλαια και βάζει την Alice να υπογράψει το αυθεντικό. Επειδή η σύνοψή τους είναι ίδια η υπογραφή θα είναι έγκυρη και για το πλαστό συμβόλαιο, οπότε ο Oscar μπορεί να ισχυριστεί ότι η Alice όντως αγόρασε το διαμέρισμα στα Εξάρχεια.

Πως θα μπορούσε η Alice να αποφύγει αυτή την παγίδα χωρίς να αλλάξουμε το μέγεθος της σύνοψης; Θα μπορούσε να ζητήσει από τον Oscar να αφαιρέσει ένα κόμμα σε κάποιο σημείο του κειμένου, δημιουργώντας έτσι μια τελείως διαφορετική σύνοψη. Ο Oscar αποτυγχάνει και μπορεί μόνο να ψάξει να βρει μια νέα έκδοση του πλαστού συμβόλου που να έχει την ίδια σύνοψη με το καινούριο, κάτι που όμως είναι πρακτικά αδύνατον. Αυτός είναι ο ενδεδειγμένος τρόπος να αποτρέψουμε μια τέτοιου είδους επίθεση, δηλαδή πριν την υπογραφή ενός ηλεκτρονικού εγγράφου να κάνουμε μια μικρή αλλαγή.

Η επίθεση αυτή ονομάζεται Birthday Attack ακριβώς επειδή βασίζεται στο «πρόβλημα των γενεθλίων». Το επακόλουθο είναι ότι θα πρέπει να χρησιμοποιούμε μια hash function που παράγει σύνοψη τουλάχιστον διπλάσια σε μήκος από αυτό που κρίνουμε απαραίτητο για την ασφάλειά μας, αφού η Birthday Attack μειώνει στο μισό τον δραστικό αριθμό των bits.

6. RSA

6.1 Το κρυπτοσύστημα RSA

Το κρυπτοσύστημα των Rivest, Shamir, Adleman είναι ένα από τα πιο παλιά και διαδεδομένα κρυπτοσυστήματα δημόσιου κλειδιού. Ιστορικά, η ιδέα του κρυπτοσυστήματος δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, αλλά το πρώτο πρακτικό κρυπτοσύστημα ανακαλύφθηκε το 1977 από τους Rivest, Shamir και Adleman.

Η ασφάλεια του κρυπτοσυστήματος βασίζεται στη δυσκολία του προβλήματος της παραγοντοποίησης ενός σύνθετου ακεραίου σε γινόμενο πρώτων παραγόντων.

Έστω $n = pq$ όπου p, q πρώτοι. Έστω ακόμη $\mathcal{P} = \mathcal{A} = \mathbb{Z}_n$ και ορίζουμε
$\mathcal{K} = \{(n, p, q, k_e, k_d)\colon\ n = pq,\ \ k_e \cdot k_d \equiv 1\ mod\ \varphi(n)\}$,
με $1 < k_e, k_d < (p-1)(q-1)$

Για $\mathcal{K} = (n, p, q, k_e, k_d)$ ορίζουμε πράξη κρυπτογράφησης:

$$c = e_k(m) \equiv m^{k_e}\ mod\ n$$

και πράξη αποκρυπτογράφησης:

$$d_k(c) \equiv c^{k_d}\ mod\ n, \text{ όπου } c \text{ το κρυπτομήνυμα}$$

Το δημόσιο κλειδί αποτελείται από τους ακεραίους (n, k_e), ενώ το ιδιωτικό κλειδί αποτελείται από τα (p, q, k_d).

Μπορούμε εύκολα να αποδείξουμε ότι η πράξη αποκρυπτογράφησης παράγει σωστά το αρχικό μήνυμα ως εξής:

$$d_k(c) \equiv c^{k_d}\ mod\ n \equiv (m^{k_e})^{k_d}\ mod\ n$$

Επειδή όμως:

$k_e \cdot k_d \equiv 1\ mod\ \varphi(n) \Rightarrow\ k_e \cdot k_d \equiv w\varphi(n) + 1$, όπου $w > 1$ τυχαία σταθερα.

Συνεπώς:

$$c^{k_d}\ mod\ n \equiv m^{w\varphi(n)+1} mod\ n\ \equiv m^{w\varphi(n)} m\ mod\ n$$

Λόγω του Θεωρήματος Euler ($m^{\varphi(n)} \equiv 1\ mod n$) προκύπτει τελικά:

$$c^{k_d}\ mod\ n \equiv 1^w\ m\ mod\ n \equiv m\ mod\ n$$

6.2 Ψηφιακή Υπογραφή RSA

ΚΑΤΑΣΚΕΥΗ ΥΠΟΓΡΑΦΗΣ

Ας υποθέσουμε ότι ο Bob έχει ένα μήνυμα m το οποίο η Alice συμφωνεί να υπογράψει. Η διαδικασία που θα ακολουθήσουν έχει ως εξής:

1. Η Alice διαλέγει δυο μεγάλους πρώτους p, q και υπολογίζει το γινόμενό τους $n = p \cdot q$. Στη συνέχεια επιλέγει e_A τέτοιο ώστε $1 \leq e_A \leq \varphi(n)$ με $gcd(e_A, \varphi(n)) = 1$ και υπολογίζει d_Aτέτοιο ώστε $e_A d_A \equiv 1 \, mod \, \varphi(n)$. Η Alice δημοσιοποιεί το ζεύγος (e_A, n) και κρατάει μυστικά τα (d_A, p, q).
2. Η υπογραφή της Alice είναι:
$$y \equiv m^{d_A} \, mod \, n$$
3. Το ζεύγος (m, y) επίσης δημοσιοποιείται.

ΕΠΑΛΗΘΕΥΣΗ ΥΠΟΓΡΑΦΗΣ

Ο Bob μπορεί τότε να επαληθεύσει ότι η Alice έχει υπογράψει το συγκεκριμένο μήνυμα ακολουθώντας την παρακάτω διαδικασία:

1. Ανακτά το δημοσιοποιημένο (e_A, n)
2. Υπολογίζει το $z \equiv y^{e_A} \, mod \, n$. Αν $z = m$ τότε ο Bob δέχεται την υπογραφή ως έγκυρη. Σε αντίθετη περίπτωση είναι μη έγκυρη.

Αν τώρα ο Oscar θέλει να προσάψει την υπογραφή της Alice σε κάποιο μήνυμα m_1 δε μπορεί απλά να χρησιμοποιήσει το ζεύγος (m_1, y) αφού $y^{e_A} \neq m_1 \, mod \, n$. Χρειάζεται συνεπώς κάποιο y_1τέτοιο ώστε ${y_1}^{e_A} \equiv m_1 \, mod \, n$. Αυτό το πρόβλημα ταυτίζεται με το πρόβλημα της αποκρυπτογράφησης του κρυπτοκειμένου m_1 για να ανακτήσει το κείμενο y_1 και είναι θεωρητικά δύσκολο να επιτευχθεί.
Μια άλλη πιθανότητα είναι ο Oscar να επιλέξει πρώτα το y_1 οπότε το μήνυμα θα είναι το $m_1 \equiv {y_1}^{e_A} \, mod \, n$. Η Alice δε μπορεί να αποδείξει ότι δεν έχει υπογράψει το συγκεκριμένο κείμενο. Επειδή όμως η πιθανότητα το m_1 να είναι ένα κείμενο με νόημα και όχι μια τυχαία αλληλουχία χαρακτήρων είναι ασύληπτα μικρή, η

Alice μπορεί εύκολα να επιχειρηματολογήσει ότι το μήνυμα είναι πλαστογραφημένο. Άλλωστε ο Oscar δεν έχει κάτι να κερδίσει προσθέτοντας την υπογραφή της Alice σε ένα τυχαίο κείμενο. Ιδανικά θα ήθελε να την προσαρτήσει σε ένα έγγραφο που υποχρεώνει την Alice να του δώσει μερικά εκατομύρια ευρώ.

ΠΑΡΑΔΕΙΓΜΑ

Έστω $p = 17$ και $q = 31$, $n = p \cdot q = 17 \cdot 31 = 527$ και $\varphi(n) = (p-1)(q-1) = 16 \cdot 30 = 480$.

Επιλέγουμε δημόσιο κλειδί $k_e = 167$ και υπολογίζουμε το ιδιωτικό κλειδί:

$$k_e \cdot k_d \equiv 1 \, mod \, 480 \Rightarrow k_d = 23$$

Στη συνέχεια θα κρυπτογραφήσουμε τη λέξη "knight" (ιππότης). Καταρχάς θα πρέπει να αντιστοιχίσουμε τα γράμματα του λατινικού αλφαβήτου σε στοιχεία του συνόλου $\mathbb{Z}_{527}$. Θεωρούμε μια αντιστοίχηση $a \to 18, b \to 19, c \to 20, \ldots$ Το μήνυμα τότε γράφεται [28 31 26 24 25 37]. Για ευκολία και εξοικονόμηση υπολογιστικής ισχύος ομαδοποιούμε τα ψηφία ζητώντας οι αριθμοί που προκύπτουν να είναι μικρότεροι από το δημόσιο modulo, δηλαδή 527. Κατόπιν εφαρμόζουμε την κρυπτογραφική πράξη σε κάθε αριθμό:

$$283^{167} \equiv 326 \, mod \, 527$$
$$126^{167} \equiv 97 \, mod \, 527$$
$$242^{167} \equiv 98 \, mod \, 527$$
$$53^{167} \equiv 43 \, mod \, 527$$
$$7^{167} \equiv 80 \, mod \, 527$$

Το κρυπτοκείμενο λοιπόν είναι $[326, 97, 98, 43, 80]$.

Αντίστοιχα για να το αποκωδικοποιήσω χρειάζεται απλά να κάνω την πράξη:

$$d_k(c) \equiv c^{k_d} \, mod \, n$$

Έχω:

$$326^{23} \equiv 283 \, mod \, 527$$
$$97^{23} \equiv 126 \, mod \, 527$$

$$98^{23} \equiv 242\ mod\ 527$$
$$43^{23} \equiv 53\ mod\ 527$$
$$80^{23} \equiv 7\ mod\ 527$$

Χωρίζουμε τους αριθμούς σε δυάδες και γνωρίζοντας ότι οι χαρακτήρας από a μέχρι z αντιστοιχούν στους αριθμούς 18 με 43 καταλήγουμε όπως ήταν αναμενόμενο στο αρχικό μήνυμα "knight".

Παρατηρούμε ότι θα μπορούσε κάποιος από τους αριθμούς μετά την κρυπτογράφηση να παραμένει ίδιος. Για παράδειγμα $154^{23} \equiv 154\ mod\ 527$. Για RSA με μεγάλες παραμέτρους, το φαινόμενο αυτό έχει μικρή πιθανότητα να συμβεί. Ωστόσο, ο αντίπαλος μπορεί να εντοπίσει σε ένα κρυπτογραφημένο μήνυμα ποια τμήματα δεν έχουν ουσιαστικά κρυπτογραφηθεί, αφού εφαρμόζοντας μόνο το δημόσιο κλειδί θα δίνουν την ίδια τιμή. Συνεπώς πρέπει να προσέχουμε να μην υπάρχουν πολλές τέτοιες περιπτώσεις.

6.2.1 Τυφλη Υπογραφή RSA

Υπάρχει τέλος μια παραλλαγή στη συγκεκριμένη διαδικασία που επιτρέπει στην Alice να υπογράψει ένα έγγραφο χωρίς να γνωρίζει τα το περιεχόμενο του. Για παράδειγμα ας υποθέσουμε ότι ο Bob έχει πραγματοποιήσει μια σημαντική ανακάλυψη. Θέλει να να καταγραφεί δημοσίως η ανακάλυψή του (σε περίπτωση που και κάποιος άλλος πραγματοποιήσει την ίδια ανακάλυψη θέλει να έχει προτεραιότητα για το βραβείο Nobel, καλώς εχόντων των πραγμάτων) αλλά θέλει να κρατήσει τις λεπτομέρειες κρυφές (επειδή οι πρακτικές εφαρμογές τις ανακάλυψής του είναι πολύ επικερδείς). Ο Bob και η Alice κάνουν τα ακόλουθα:

1. Η Alice διαλέγει ένα $n = p \cdot q$ (p, q μεγάλοι πρώτοι αριθμοί), έναν συντελεστή κωδικοποίησης e και έναν συντελεστή αποκωδικοποίησης d. Δημοσιοποιεί τα n, e και κρατάει μυστικά τα p, q, d. Αν είναι επιθυμητό

μπορεί και να σβήσει τα p, q, d από τη μνήμη του υπολογιστή της στο τέλος της διαδικασίας.

2. Ο Bob επιλέγει ένα τυχαίο ακέραιο k με $gcd(k, n) = 1$ και υπολογίζει το $t \equiv k^e m \; mod \; n$ το οποίο και στέλνει στην Alice.
3. Η Alice υπογράφει το t υπολογίζοντας το $s \equiv t^d \; mod \; n$. Επιστρέφει το s στον Bob.
4. Ο Bob υπολογίζει το ${}^{s}/_{k} \; mod \; n$. Αυτό είναι το υπογεγραμμένο μήνυμα m^d.

Ας δείξουμε ότι το ${}^{s}/_{k}$ είναι πράγματι το υπογεγραμμένο μήνυμα. Παρατηρούμε ότι $k^{ed} \equiv k^{e^d} \equiv k \; mod \; n$ αφού αυτή είναι απλά η κρυπτογράφηση και αποκρυπτογράφηση του k στο σχήμα RSA. Άρα:

$$\frac{s}{k} \equiv \frac{t^d}{k} \equiv \frac{k^{ed} m^d}{k} \equiv m^d \; mod \; n$$

το οποίο είναι το υπογεγραμμένο μήνυμα.

Η επιλογή του k είναι απολύτως τυχαία, συνεπώς το $k^e \; mod \; n$ είναι η κρυπτογράφηση στο RSA ενός τυχαίου αριθμού και αυτό με τη σειρά του τυχαίο. Οπότε το $k^e m$ δεν δίνει πρακτικά καθόλου πληροφορία για το περιεχόμενο του μηνύματος m (πλην της τετριμμένης περιπτώσεως όπου $m = 0$ το οποίο δε γίνεται να αποκρυφθεί). Έτσι η Alice δεν γνωρίζει τίποτα για το μήνυμα που υπογράφει.

Όταν η υπογραφή ολοκληρωθεί ο Bob έχει στα χέρια το ίδιο μήνυμα που θα είχε αν ακολουθούσε την κανονική διαδικασία.

Υπάρχουν διάφορα προβλήματα με τέτοιου είδους σχήματα ψηφιακών υπογραφών (οι οποίες ονομάζονται **τυφλές υπογραφές**), σημαντικότερο εκ των οποίων είναι ότι ο Bob θα μπορούσε να εξαπατήσει την Alice βάζοντάς την να υπογράψει κάποιο έγγραφο διαφορετικό από αυτό το οποίο της έχει ανακοινώσει (π.χ. να του παραχωρήσει ένα εκατομύριο ευρώ). Προφανώς χρειάζονται δικλείδες ασφαλείας για να αποφευχθούν τέτοιες περιπτώσεις. Περισσότερα για τις τυφλές υπογραφές θα δούμε σε επόμενο κεφάλαιο.

6.3 Ανάλυση του RSA

Η πρακτική αξία του RSA οφείλεται στο γεγονός ότι αφενός μεν δεν υπάρχει αλγόριθμος ο οποίος να εντοπίζει τους πρώτους παράγοντες ενός σύνθετου ακεραίου, αφετέρου δε ο υπολογισμός μεγάλης δύναμης ενός αριθμού σε modular αριθμητική μπορεί να γίνει σε επιτρεπτό (γραμμικό) χρόνο.
Όσον αφορά την ασφάλεια του κρυπταλγόριθμου, οι πρώτοι αριθμοί p και q θα πρέπει να είναι αρκετά μεγάλοι, ώστε ο καλύτερος γνωστός αλγόριθμος παραγοντοποίησης να απαιτεί χρόνο μεγαλύτερο από αυτόν με τον οποίο πρέπει να προστατευθούν τα δεδομένα. Στον Πίνακα παρουσιάζονται ενδεικτικά μεγέθη και αντίστοιχες περιπτώσεις στις οποίες θα πρέπει να εφαρμοσθούν τα μεγέθη αυτά.

p, q	***n***	**χρόνος προστασίας**	**τύπος δεδομένων**
256 bits	512 bits	μερικές εβδομάδες	πληροφορίες που επηρεάζουν βραχυπρόθεσμα το χρηματιστήριο (π.χ. απόφαση συγχώνευσης δύο εταιρειών)
512 bits	1024 bits	50-100 χρόνια	προσωπικά μυστικά
1024 bits	2048 bits	>100 χρόνια	εμπορικά μυστικά, προσωπικά δεδομένα
2048 bits	4096 bits	≈ ηλικία του Σύμπαντος	στρατιωτικά μυστικά

Μεγέθη παραμέτρων RSA και ενδεικτικοί τύποι δεδομένων προς προστασία

6.3.1 Ασφάλεια του RSA

Η ασφάλεια του RSA βασίζεται στη δυσκολία της παραγοντοποίησης ενός σύνθετου ακεραίου. Στην περίπτωση που ανακαλυφθεί αλγόριθμος ο οποίος μπορεί να παραγοντοποιεί σε πολυωνυμικό χρόνο έναν ακέραιο, το RSA δεν θα είναι πια ασφαλές. Παρόλαυτα θα πρέπει να αναφέρουμε πως δεν έχει αποδειχθεί ότι η ασφάλεια του RSA εξαρτάται αποκλειστικά από την

παραγοντοποίηση των ακεραίων. Υπάρχουν ορισμένες απειλές που οφείλονται κυρίως στην μη προσεκτική υλοποίηση και εκτέλεση του κρυπτοσυστήματος και για τις οποίες δεν απαιτείται γνώση των παραγόντων του n.

6.3.2 Επίθεση σε κοινό modulus

Η επίθεση σε κοινό modulus μπορεί να εφαρμοσθεί σε περιπτώσεις όπου οι επικοινωνούντες έχουν κλειδιά με ίδιο n. Έστω κείμενο m και δύο ζευγάρια κλειδιών (e_1, d_1) και (e_2, d_2) τα οποία έχουν κοινό modulus n. Η κρυπτογράφηση του απλού κειμένου με τα δύο δημόσια κλειδιά θα δώσει αντίστοιχα:

$$c_1 = m^{e_1} mod\ n, \qquad c_2 = m^{e_2} mod\ n$$

Αν $gcd(e_1, e_2) = 1$, τότε υπάρχουν ακέραιοι w και v, τέτοιοι ώστε:

$$we_1 + ve_2 = 1$$

Επειδή όμως είναι $e_1, e_2 > 0$, έπεται ότι κάποιο από τα w και v είναι αρνητικό και το άλλο είναι θετικό. Έστω ότι $w < 0$. Τότε ο Oscar έχοντας γνώση των κρυπτοκειμένων και των δημόσιων κλειδιών, μπορεί να ανακτήσει το μήνυμα υπολογίζοντας:

$$({c_1}^{-1})^{-w} c_2^v \equiv m^{we_1 + ve_2} \equiv m\ mod\ n$$

Η επίθεση αυτή συναντάται συνήθως όταν η παραγωγή των κλειδιών γίνεται από ένα κοινό κέντρο δημιουργίας κλειδιών το οποίο χρησιμοποιεί την ίδια διαδικασία για την δημιουργία των κλειδιών των μελών μιας ολόκληρης ομάδας. Η κρυπτογράφηση ενός μηνύματος με περισσότερα από ένα δημόσια κλειδιά εμφανίζεται σε περιπτώσεις εκπομπής (broadcast), όπου ένας πομπός στέλνει το μήνυμα σε πολλούς αποδέκτες.

6.3.3 Επίθεση επαναληπτικής κρυπτογράφησης

Σε αντίθεση με την επίθεση με κοινό modulus η οποία εκμεταλλεύεται συγκεκριμένη υλοποίηση του RSA η επίθεση της επαναληπτικής κρυπτογράφησης μπορεί να εφαρμοσθεί σε οποιαδήποτε περίπτωση.

Η επίθεση βασίζεται στην περιοδικότητα της συνάρτησης του κρυπτοσυστήματος RSA. Έστω (e, n) το δημόσιο κλειδί του Bob. Η Alice κρυπτογραφεί ένα μήνυμα m με την κρυπτογραφική πράξη του RSA:

$$c = m^e mod\ n$$

Αν c^0 είναι το κρυπτοκείμενο που προκύπτει από την κρυπτογράφηση του m με το δημόσιο κλειδί (e, n). Ο αντίπαλος έχοντας συλλάβει το c^0, εκτελεί διαδοχικά κρυπτογραφήσεις:

$$c^i \equiv (c^{i-1})^e\ mod\ n\ \text{για}\ i = 1,2,3,\ldots$$

Λόγω της περιοδικότητας, για κάποιο i = k, θα είναι:

$$c^k \equiv (c^{k-1})^e\ mod\ n \equiv m\ mod\ n$$

Ο Oscar δεν γνωρίζει ότι το μήνυμα της Alice είναι το c^k. Το ανακαλύπτει στην επόμενη επανάληψη:

$$c^{k-1} \equiv m^e \equiv c \bmod n$$

Η τιμή του k για την οποία καταλήγουμε στο αρχικό μήνυμα, ονομάζεται εκθέτης ανάκτησης (recovery exponent). Ένας τρόπος να κάνουμε την επίθεση επαναληπτικής κρυπτογράφησης πρακτικώς αδύνατη είναι ο εκθέτης ανάκτησης να είναι όσο το δυνατό μεγαλύτερος. Δυστυχώς λόγω της περιοδικότητας, ο εκθέτης ανάκτησης έχει ένα ανώτατο όριο. Χρησιμοποιώντας το θεώρημα του Carmichael, μπορούμε να υπολογίσουμε το άνω όριο του εκθέτη ανάκτησης, ως εξής:

$$c^{\mathrm{i}} \equiv m^{e^i}\ mod\ n \equiv m^{e^i mod\ \psi(n)}\ mod\ n \equiv m^{e^i mod\ \psi(\psi(n))}\ mod\ n$$

Για να καταλήξουμε στο m πρέπει ο εκθέτης του e να είναι ίσος με μηδέν, οπότε και $e^0 = 1$. Αυτό συμβαίνει για την τιμή όπου:

$$\mathrm{k} = \mathrm{i} = \psi(\psi(\mathrm{n}))$$

Επομένως, για να είναι η επίθεση επαναληπτικής κρυπτογράφησης πρακτικά αδύνατη, απαιτείται η τιμή του $\psi(\psi(n))$ να είναι όσο το δυνατόν μεγαλύτερη. Από τη σχέση:

$$\psi(n) = \psi(p \cdot q) = 2 \cdot lcm(\frac{p-1}{2}, \frac{q-1}{2})$$

μπορούμε να καταλήξουμε στις ακόλουθες απαιτήσεις, προκειμένου τουλάχιστον η $\psi(n)$ να είναι σχετικά μεγάλη:

1. οι ποσότητες $(p-1)/2$ και $(q-1)/2$ θα πρέπει να περιέχουν μεγάλους παράγοντες
2. ο μέγιστος κοινός διαιρέτης των $(p-1)/2$ και $(q-1)/2$ πρέπει να είναι μικρός

Η πρώτη σχέση απαιτείται λόγω της διπλής εφαρμογής της συνάρτησης $\psi(\,)$, οπότε κατά τη δεύτερη εφαρμογή της $\psi(\,)$ οι παράγοντες των δύο λόγων θα επηρεάσουν σημαντικά το μέγεθος του αποτελέσματος. Η δεύτερη σχέση απαιτείται λόγω της αντίστροφης σχέσης μεταξύ του μέγιστου κοινού διαιρέτη και του ελάχιστου κοινού πολλαπλασίου. Ιδανικά, οι παραπάνω τιμές είναι βέλτιστες όταν οι p και q είναι **ασφαλείς πρώτοι**, όταν δηλαδή οι ποσότητες $(p-1)/2$ και $(q-1)/2$ είναι επίσης πρώτοι.

Το Πρόβλημα Διακριτού Λογαρίθμου

Επειδή ένα πολύ βασικό θεμέλιο της ασφάλειας των σχημάτων ψηφιακής υπογραφής ElGamal και DSA που θα εξετάσουμε στη συνέχεια είναι η δυσκολία επίλυσης του DLP (Discrete Logarithm Problem - Πρόβλημα Διακριτού Λογαρίθμου) το οποίο ορίζουμε εδώ.

Ορισμός

Δίνονται ένας πρώτος αριθμός p, ένας γεννήτορας α του $\mathbb{Z}_p^*$ και ένα στοιχείο β του $\mathbb{Z}_p^*$. Ζητείται ακέραιος x , $0 \leq x \leq p-2$, τέτοιος ώστε:

$$\alpha^x \equiv \beta \ mod \ p$$

Έχουν γίνει πολλές προσπάθειες να αποδειχθεί ότι το DLP δε μπορεί να λυθεί γρήγορα, χωρίς αποτέλεσμα. Μέχρι τώρα πάντως δεν έχει δημιουργηθεί κανένας αλγόριθμος που να το λύνει σε αποδεκτό χρόνο για μεγάλα p και γι'αυτό το λόγο θεωρείται πολύ δύσκολο να λυθεί. Ένας απλός διπλασιασμός του μεγέθους του p αυξάνει εκθετικά το χρόνο επίλυσης κάτι που το κάνει ιδανικό για χρήση σε κρυπτογραφικούς αλγόριθμους.

7. Το Σχήμα Υπογραφής Elgamal

Το σχήμα υπογραφής ElGamal προτάθηκε για πρώτη φορά σε μια εργασία του Taher ElGamal το 1985. Το σχήμα όπως περιγράφεται στην εργασία του σπανίως χρησιμοποιείται, όμως μια παραλλαγή αυτού του σχήματος υιοθετήθηκε ως το Digital Signature Algorithm (DSA) από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), σχήμα το οποίο θα εξετάσουμε στο επόμενο κεφάλαιο. Αυτά τα σχήματα είναι σχεδιασμένα αποκλειστικά για χρήση σαν υπογραφές σε αντίθεση με το RSA το οποίο μπορεί να χρησιμοποιηθεί σαν κρυπτοσύστημα δημοσίου κλειδιού αλλά και σαν σχήμα υπογραφής. Μια άλλη σημαντική διαφορά είναι ότι με τη μέθοδο ElGamal περισσότερες από μία υπογραφές είναι έγκυρες για ένα δεδομένο μήνυμα.

Ορισμός

Έστω p πρώτος τέτοιος ώστε το πρόβλημα διακριτού λογαρίθμου στο $\mathbb{Z}_p$ να είναι δυσεπίλητο και $\alpha \in {\mathbb{Z}_p}^*$ γεννήτορας του $\mathbb{Z}_p$. Έστω επίσης $\mathcal{P} = {\mathbb{Z}_p}^*, \mathcal{A} = {\mathbb{Z}_p}^* \times \mathbb{Z}_{p-1}$, $1 \leq \lambda \leq p-2$ και ας ορίσουμε:

$$\mathcal{K} = \{(p, a, \lambda, \beta) : \beta \equiv \alpha^{\lambda} \, mod \, p\}$$

Οι τιμές των p, a, β αποτελούν το δημόσιο κλειδί ενώ το λ αποτελεί το ιδιωτικό κλειδί.

Για $\mathcal{K} = (p, a, \lambda, \beta)$ και για κάποιον (μυστικό) τυχαίο αριθμό $k \in {\mathbb{Z}_{p-1}}^*$ ορίζουμε:

$$sig_K(m, k) \equiv (r, s)$$

όπου

$$r \equiv \alpha^k \, mod \, p$$

και

$$s \equiv (m - \lambda r) k^{-1} mod \, (p-1)$$

Τέλος, για $m, r \in \mathbb{Z}_p{}^*$ και $s \in \mathbb{Z}_{p-1}$ ορίζουμε:

$$ver_K\big(m,(r,s)\big) = true \iff \beta^r r^s \equiv \alpha^m \, mod \, p$$

Το σχήμα υπογραφής ElGamal είναι μη-ντετερμινιστικό, όπως άλλωστε είναι και το αντίστοιχο κρυπτοσύστημα. Αυτό σημαίνει πως υπάρχουν περισσότερες από μία έγκυρες υπογραφές για οποιοδήποτε μήνυμα, συνεπώς ο αλγόριθμος επαλήθευσης θα πρέπει να μπορεί να δεχτεί οποιαδήποτε από αυτές σαν αυθεντική.
Υποθέτοντας ότι η υπογραφή έχει κατασκευαστεί σωστά, η επαλήθευση θα πετύχει αφού:

$$\beta^r r^s \equiv \alpha^{\lambda r} \alpha^{ks} \, mod \, p \equiv \alpha^m \, mod \, p$$

Όπου χρησιμοποιήσαμε ότι ισχύει:

$$\lambda r + ks \equiv m \, mod (p-1)$$

Η ύπαρξη του τυχαίου αριθμού r, έχει ως αποτέλεσμα τη δυνατότητα αντιστοίχισης του απλού κειμένου σε $p-1$ κρυπτοκείμενα. Η διαδικασία όπου το απλό κείμενο αναμειγνύεται με μια τυχαία μεταβλητή, ονομάζεται διαδικασία δημιουργίας συνθηκών τυχαιότητας (randomization process). Το βήμα αυτό το οποίο δεν υπάρχει στο RSA, καθιστά το κρυπτοσύστημα ElGamal ανθεκτικότερο σε επιθέσεις παρόμοιες με αυτές που παρουσιάστηκαν για το RSA. Βέβαια, η χρήση του τυχαίου αριθμού εισάγει έναν επιπλέον κίνδυνο που οδηγεί σε μια πρόσθετη απαίτηση. Για κάθε μήνυμα που κρυπτογραφείται, θα πρέπει να επιλέγεται διαφορετικός τυχαίος r. Στην περίπτωση που δύο μηνύματα m και m' κρυπτογραφηθούν με τον ίδιο r, τότε για τα αντίστοιχα κρυπτοκείμενα που θα προκύψουν (y_1, y_2) και (y_1', y_2'), η γνώση του ενός μηνύματος επιτρέπει την ανάκτηση του άλλου από τον λόγο:

$$\frac{y_2}{y_2'} = \frac{mb^r}{m'b^r} = \frac{m}{m'}$$

Τέλος, όσον αφορά το μέγεθος του p, το κατώτατο όριο που προτείνεται είναι 1024 bits. Γενικά, κατά την κρυπτογράφηση με το κρυπτοσύστημα ElGamal, το μέγεθος των παραμέτρων αποτελεί σημαντικό κριτήριο υλοποίησης, λόγω του αυξημένου χρόνου που απαιτείται για την κρυπτογράφηση (δύο πράξεις ύψωσης σε δύναμη έναντι της μιας στην περίπτωση του RSA), και λόγω της διαστολής του κρυπτοκειμένου. Τα μειονεκτήματα αυτά έχουν σαν αποτέλεσμα να προτιμάται μειωμένο μέγεθος του modulus.

ΠΑΡΑΓΩΓΗ ΥΠΟΓΡΑΦΗΣ

Για να υπογράψει το μήνυμα η Alice ακολουθεί την παρακάτω διαδικασία:

1. Επιλέγει ένα τυχαίο, κρυφό k τέτοιο ώστε $gcd(k, p-1) = 1$
2. Υπολογίζει το $r \equiv \alpha^k \ mod \ p$
3. Υπολογίζει το $s \equiv k^{-1}(m - \lambda r) \ mod \ (p-1)$

Το υπογεγραμμένο μήνυμα είναι η τριάδα (m, r, s).

ΕΠΑΛΗΘΕΥΣΗ ΥΠΟΓΡΑΦΗΣ

Ο Bob μπορεί να επαληθεύσει την υπογραφή ως εξής:

1. Κατεβάζει το δημόσιο κλειδί της Alice p, α, β
2. Υπολογίζει το $v_1 \equiv \beta^r r^s \ mod \ p$ και το $v_2 \equiv \alpha^m \ mod \ p$
3. Η υπογραφή θεωρείται έγκυρη αν και μόνο αν $v_1 \equiv v_2 \ mod \ p$

Θα δείξουμε τώρα πως δουλεύει η διαδικασία επαλήθευσης. Ας υποθέσουμε ότι η υπογραφή είναι έγκυρη.

Επειδή $s \equiv k^{-1}(m - \lambda r) mod \ (p-1)$ έχουμε $sk \equiv (m - \lambda r) mod \ (p-1)$, οπότε $m \equiv sk + \lambda r$. Άρα:

$$v_2 \equiv \alpha^m \equiv \alpha^{sk+\lambda r} \equiv \left(\alpha^{\lambda}\right)^r (\alpha^k)^s \equiv \beta^r r^s \equiv v_1 \ mod \ p$$

Μεγάλη προσοχή πρέπει να δοθεί στο να κρατηθεί η τιμή του λ μυστική. Σε περίπτωση που ο Oscar ανακαλύψει το λ μπορεί να υπογράψει οποιοδήποτε κείμενο επιθυμεί με την υπογραφή της Alice.

7.1 Ασφάλεια του ElGamal

Έστω ότι ο Oscar κατέχει ένα μήνυμα στο οποίο θέλει να προσαρτίσει την υπογραφή της Alice. Δε μπορεί όμως να υπολογίσει το s αφού δε γνωρίζει το λ. Προσπαθεί να προσπεράσει αυτό το πρόβλημα και να βρει απευθείας κάποιο s που να ικανοποιεί την εξίσωση επαλήθευσης, δηλαδή την:

$$\beta^r r^s \equiv \alpha^m \, mod \, p$$

Αυτή η εξίσωση μπορεί να γραφτεί:

$$r^s \equiv \beta^{-r} \alpha^m \, mod \, p$$

Το οποίο είναι ένα πρόβλημα διακριτού λογαρίθμου και συνεπώς είναι υπολογιστικά ανέφικτο για τον Oscar να βρει το s. Αν επιλέξει πρώτα το s τότε η εξίσωση που δίνει το r είναι παρόμοια με το DLP αλλά πιο σύνθετη και θεωρείται γενικά επίσης δύσκολη να λυθεί. Δεν έχει αποδειχθεί ότι δε γίνεται τα r, s να επιλεγούν ταυτόχρονα αλλά είναι απίθανο να γίνεται. Συνεπώς το συγκεκριμένο σχήμα είναι ασφαλές όσο τα διακριτά logs $mod \, p$ είναι δύσκολο να υπολογιστούν.

Τι θα γίνει αν η Alice επιλέξει το ίδιο k για να υπογράψει ένα δεύτερο μήνυμα; Είδαμε παραπάνω ότι αν ο Oscar γνωρίζει το ένα από τα δύο μηνύματα μπορεί τότε να διαβάσει και το άλλο. Υπάρχει όμως και μια πιο επικίνδυνη συνέπεια!
Έστω ότι η Alice χρησιμοποίησε το ίδιο k για να υπογράψει τα δύο μηνύματα m_1, m_2. Τότε το ίδιο r θα έχει χρησιμοποιηθεί και στις δύο υπογραφές, κάτι το οποίο ο Oscar θα ανακαλύψει. Το s δε θα είναι ίδιο οπότε ας υποθέσουμε ότι έχουμε τις τιμές s_1, s_2. Ο Oscar γνωρίζει ότι:

$$s_1 k - m_1 \equiv \lambda r \equiv s_2 k - m_2 \ mod\ (p-1) \Longrightarrow$$
$$(s_1 - s_2)k \equiv m_1 - m_2 \ mod\ (p-1)$$

Έστω $d = gcd(s_1 - s_2,\ p-1)$. Υπάρχουν d λύσεις για την αναλογία. Συνήθως το d είναι μικρό οπότε δεν υπάρχουν πολλές δυνατές τιμές για το k. Ο Oscar υπολογίζει τα α^k για τις πιθανές τιμές του k μέχρι να βρει το r. Έχοντας βρει το k λύνει τώρα την:

$$\lambda r \equiv m_1 - k s_1 \ mod\ (p-1)$$

ως προς α. Υπάρχουν $gcd(r,\ p-1)$ πιθανότητες. Ο Oscar υπολογίζει τα α^λ για την κάθε περίπτωση μέχρι να βρει το β και με βάση αυτό γνωρίζει και το α. Σ'αυτή τη φάση έχει σπάσει πλήρως το σύστημα και μπορεί να αναπαράγει κατά βούληση την υπογραφή της Alice.

8. Πρότυπο Ψηφιακής Υπογραφής (DSS)

Το Πρότυπο Ψηφιακής Υπογραφής (Digital Signature Standard) δημοσιεύτηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) και καθορίζει ένα σύστημα ψηφιακών υπογραφών για γενική χρήση. Το DSS περιλαμβάνει έναν αλγόριθμο ψηφιακής υπογραφής (DSA - Digital Signature Algorithm) ο οποίος βασίζεται στην ασύμμετρη κρυπτογραφία. Σε αντίθεση με τα προηγούμενα σχήματα που μελετήσαμε, ο DSA δε μπορεί να χρησιμοποιηθεί σαν κρυπτοσύστημα, μπορεί να χρησιμοποιηθεί μόνο σαν σχήμα ψηφιακών υπογραφών. Το DSS προβλέπει χρήση της SHA-1 ως κρυπτογραφική μονόδρομη hash, η οποία συμμετέχει στη δημιουργία της ψηφιακής υπογραφής. Ο DSA αποτελεί ουσιαστικά μια πιο αποδοτική εκδοχή του El Gamal και κατά συνέπεια βασίζει την ασφάλεια του στη δυσκολία επίλυσης του προβλήματος διακριτού λογαρίθμου, η οποία είναι υπολογιστικά αδύνατη σε μια υποομάδα του $\mathbb{Z}_p^*$ μεγέθους 2^{160} (όπου γίνονται όλοι οι υπολογισμοί του συγκεκριμένου σχήματος).

ΚΑΤΑΣΚΕΥΗ ΚΛΕΙΔΙΟΥ

Για να κατασκευάσει ο Bob το κλειδί για τον DSA ακολουθεί την εξής διαδικασία (σύμφωνα με το πρότυπο FPS-186):

Επιλέγει πρώτο q τέτοιο ώστε $2^{159} < q < 2^{160}$. Άρα το μέγεθος του q θα είναι 160 bits όπως τονίσαμε προηγουμένως.

1. Επιλέγει πρώτο p μήκους L bits τέτοιον ώστε:
   - $p = qz + 1$ για κάποιον ακέραιο z (δηλαδή ο q διαιρεί τον $p - 1$)
   - $512 \leq L \leq 1024$, όπου L είναι πολλαπλάσιο του 64
2. Με βάση τους p και q επιλέγει γεννήτορα g μιας κυκλικής υποομάδας τάξης q της ομάδας $\mathbb{Z}_p^*$. Αυτό επιτυγχάνεται επιλέγοντας $h \in \mathbb{Z}_p^*$ τέτοιο ώστε:

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

   και θέτοντας:

   $$g = h^z \bmod p$$

όπου $z = (p-1)/q$

3. Επιλέγει τυχαίο αριθμό $x \in \{1, 2, \dots, q-1\}$ και υπολογίζει το

$$y = g^x \, mod \, p$$

Το δημόσιο κλειδί του Bob προκύπτει από τα παραπάνω και είναι το (p, q, g, y) και το ιδιωτικό είναι το x.

Σε αυτό το σημείο αξίζει να παρατηρήσουμε ότι σύμφωνα με την τελευταία έκδοση του DSA (FIPS-186-3) για να είναι ασφαλές το σχήμα πρέπει το q να έχει μέγεθος 224, 256 , 384 ή 512 bits (το οποίο εξακολουθεί να είναι μικρότερο από το ελάχιστο μέγεθος στο ElGamal), ενώ το L πρέπει να έχει μέγεθος 2048, 3072, 7680 ή 15360 bits.

ΠΑΡΑΓΩΓΗ ΥΠΟΓΡΑΦΗΣ

Έστω ότι ο Bob θέλει να στείλει ένα δυαδικό μήνυμα m υπογεγραμμένο ψηφιακά με DSS.

1. Χρησιμοποιεί μια μονόδρομη και ελεύθερη σύμπτωσης hash function $h: \{0,1\}^* \rightarrow \{0, 1, \dots, q-2\}$ για να εξασφαλίσει επιπρόσθετη ασφάλεια και έτσι παράγει το μήνυμα $h(m)$.
2. Στη συνέχεια επιλέγει τυχαίο αριθμό $k \in \{1, 2, \dots, q-1\}$ και υπολογίζει το $r = (g^k mod \, p) mod \, q$
3. Υπολογίζει το $s = \left(k^{-1}(h(m) + x \cdot r)\right) mod \, q$, όπου x το ιδιωτικό κλειδί του Bob
4. Στην περίπτωση όπου κάποιο από τα r ή s είναι ίσο με 0 επανυπολογίζει την υπογραφή.

Η υπογραφή του Bob είναι η δυάδα (r, s). Στέλνει λοιπόν στην Alice το μήνυμα μαζί με την υπογραφή, δηλαδή το $(h(m), r, s)$

ΕΠΑΛΗΘΕΥΣΗ ΥΠΟΓΡΑΦΗΣ

Η Alice από τη μεριά της λαμβάνει το μήνυμα μαζί με την υπογραφή και θέλει να τα επαληθεύσει.

1. Αρχικά ελέγχει αν $1 \leq r \leq q-1$ και $1 \leq s \leq q-1$. Αν κάτι εκ των δύο δεν ισχύει απορρίπτει την υπογραφή. Ειδάλλως
2. Υπολογίζει τα:
   - $w = s^{-1} mod\ q$
   - $u_1 = (h(m) \cdot w) mod\ q$
   - $u_2 = (r \cdot w) mod\ q$
   - $v = \big((g^{u_1} \cdot y^{u_2}) mod\ p\big) mod\ q$
3. Ελέγχει αν $v = r$. Αν ισχύει η ισότητα η υπογραφή είναι έγκυρη.

ΠΑΡΑΔΕΙΓΜΑ

Έστώ ότι η Alice θέλει να στείλει το μήνυμα m που έχει hash τιμή $h(m) = 38$ και επιλέγει $\mathrm{q} = 101$. Τότε $\mathrm{p} = 78\mathrm{q} + 1 = 7879$. Επιλέγει το 3 το οποίο είναι ένα πρωταρχικό στοιχείο του $\mathbb{Z}_{7879}^*$ και υπολογίζει το γεννήτορα:

$$\mathrm{g} \equiv \mathrm{h}^{\mathrm{z}} \bmod \mathrm{p} \equiv 3^{78} \bmod 7879 \equiv 170$$

Στη συνέχεια επιλέγει τυχαίο ακέραιο $\mathrm{x} \in \{1, 2, \dots, 100\}$, έστω $\mathrm{x} = 63$ και υπολογίζει το:

$$\mathrm{y} \equiv \mathrm{g}^{\mathrm{x}} \bmod \mathrm{p} \equiv 170^{63} \bmod 7879 \equiv 1803$$

Το δημόσιο κλειδί της Alice είναι (7879, 101, 170, 1803).

Για να υπογράψει η Alice το μήνυμα m επιλέγει τυχαίο ακέραιο $1 \leq k \leq 100$, έστω $k = 42$. Μετά υπολογίζει το:

$$k^{-1} mod\ 101 \equiv 42^{-1} mod\ 101 \equiv 89$$

το:

$$r \equiv (g^k mod\ p) mod\ q \equiv (170^{42} mod\ 7879) mod\ 101 \equiv 1934\ mod\ 101 \equiv 15$$

και το:

$$s \equiv \big(k^{-1}(h(m) + xr)\big)\ mod\ q \equiv \big(89(38 + 63 \cdot 15)\big) mod\ 101 \equiv 21$$

Η υπογραφή της Alice μαζί με το μήνυμα είναι $(m, r, s) = (38, 15, 21)$ το οποίο πακέτο αποστέλει στον Bob.

Ο Bob δέχεται την τριάδα και την επαληθεύει ως εξής:
Υπόλογίζει διαδοχικά τα

- $w \equiv s^{-1}\ mod\ q \equiv 21^{-1} mod\ 101 \equiv 77$
- $u_1 \equiv (h(m) \cdot w)\ mod\ q \equiv 38 \cdot 77\ mod\ 101 \equiv 98$
- $u_2 \equiv (r \cdot w)\ mod\ q \equiv 15 \cdot 77\ mod\ 101 \equiv 44$
- $v \equiv \big((g^{u_1} y^{u_2})\ mod\ p\big) mod\ q \equiv \big((170^{98} \cdot 1803^{44})\ mod\ 7879\big) mod\ 101 \equiv 1934\ mod\ 101 \equiv 15$

Αφού $v = r$ δέχεται την υπογραφή.

8.1 Ορθότητα του DSA

Από το μικρό θεώρημα του Fermat γνωρίζουμε ότι $g = h\ mod\ p$. Συνεπώς ισχύει ότι:

$$g^q \equiv h^q \equiv h^{p-1} \equiv 1\ mod\ p$$

Ο Bob υπολογίζει το:

$$s = \big(k^{-1}(h(m) + x \cdot r)\big) mod\ q$$

Λύνοντας ως προς q έχουμε:

$$k \equiv h(m)s^{-1} + xrs^{-1} (mod\ q) \Longrightarrow$$
$$k \equiv h(m)w + xrw\ (mod\ q)$$

Επειδή $g > 1$ και q πρώτος ισχύει ότι ο g είναι τάξης q, άρα:

$$g^q \equiv g^{h(m)w} g^{xrw} \equiv g^{h(m)w} y^{rw} \equiv g^{u_1} y^{u_2}\ (mod\ p)$$

Η ορθότητα του αλγορίθμου δίνεται τελικά από τη σχέση:

$$r = (g^k \bmod \text{p}) \bmod \text{q} \; = \; (g^{u_1} y^{u_2} \; mod \; p) \; mod \; q = v$$

8.2 Σύγκριση με ElGamal

Καταρχάς το μήκος υπογραφής του DSA είναι 320 bits ενώ στο ElGamal είναι τουλάχιστον 1536 bits, δηλαδή σχεδόν πενταπλάσιο. Επίσης τα δύο σχήματα διαφέρουν κατά πολύ στην παραγωγή της υπογραφής, με πλεονέκτημα να έχει ο DSA αφού οι εκθέτες είναι μικρότεροι του q, ενώ είναι ταχύτερος και στην επαλήθευση λόγω του ότι οι εκθέτες είναι σταθερά 160 bits σε αντίθεση με τον ElGamal όπου είναι όσα bits είναι και ο πρώτος p που επιλέγουμε, δηλαδή τουλάχιστον 768 bits. Τέλος στο σχήμα ElGamal χρειάζεται να υπολογίσουμε τρεις διαφορετικούς modulo n για την επαλήθευση της υπογραφής, ενώ στο DSA χρειάζονται μόνο δύο. Καθώς η εκθετοποίηση modulo n είναι ένα από τα πιο αργά τμήματα του υπολογισμού, αυτή η μετατροπή επιταχύνει τη διαδικασία της επαλήθευσης.

Όπως και στο σχήμα υπογραφών ElGamal, η ποσότητα g πρέπει να διατηρείται μυστική. Οποιοσδήποτε γνωρίζει τον p μπορεί να υπογράψει όποιοδήποτε επιθυμητό κείμενο. Επίσης αν η ίδια τιμή χρησιμοποιηθεί δύο φορές για τον k είναι εφικτό να βρεθεί ο p.

Σε αντίθεση όμως με το σχήμα ElGamal ο ακέραιος r δεν περιέχει πλήρη πληροφορία για τον k. Γνωρίζοντας τον r μπορούμε να βρούμε το $mod\, q$. Υπάρχουν περίπου $2^{512-160} = 2^{342}$ αριθμοί $mod\, p$ που καταλήγουν σε ένα συγκεκριμένο αριθμό $mod\, q$. Επίσης στο ElGamal ένας αντίπαλος μπορούσε να υπολογίσει το p $(mod 2^t)$, όπου 2^t είναι η μεγαλύτερη δύναμη του 2 που διαιρεί το $p-1$. Αυτό δε μας φέρνει ιδιαιτέρως κοντά στο να προσδιορίσουμε το p αλλά η γενικότερη φιλοσοφία της αποκρυπτογράφησης υποδεικνύει ότι πολλά μικρά τμήματα πληροφορίας μπορεί να είναι χρήσιμα αν συνδυαστούν. Το DSA αποφεύγει αυτό το πρόβλημα αφαιρώντας όλη την πληροφορία πλην του $mod\, q$ από το p.

Όταν το DSA προτάθηκε το 1991 υπήρξαν αντιδράσεις, κυρίως επειδή η διαδικασία επιλογής του NIST δεν ήταν δημόσια. Το πρότυπο κατασκευάστηκε από την NSA χωρίς τη συμβολή του κοινού και του ιδιωτικού τομέα. Ασχέτως των πλεονεκτημάτων του σχήματος που προέκυψε, το NIST δέχτηκε σκληρή κριτική για την διαδικασία που ακολούθησε.

Ως προς την τεχνική μεριά, ένα από τα πιο σημαντικά προβλήματα που παρατηρήθηκαν ήταν ότι το μέγεθος του p ήταν σταθερό και ίσο με 512 bits. Πολλοί ερευνητές πρότειναν το μέγεθος αυτό να είναι μεταβλητό ώστε να μπορούν να χρησιμοποιηθούν μεγαλύτερα μεγέθη αν κρινόνταν απαραίτητο. Σε απάντηση των σχολίων το NIST τροποποίησε το σχήμα ώστε να δέχεται μεταβλητό μήκος κλειδιού.

9. One-time

Το σχήμα ψηφιακής υπογραφής μιας χρήσης παρέχει ασφάλεια για την υπογραφή ενός μόνο μηνύματος. Ένα σημαντικό πλεονέκτημα αυτού του σχήματος είναι η ταχύτητα της παραγωγής καθώς και της επαλήθευσης της υπογραφής, γι'αυτό και χρησιμοποιείται συχνά σε εφαρμογές όπου απαιτείται μικρή υπολογιστική ισχύς. Υπάρχουν βέβαια και κάποια μειονεκτήματα, όπως για παράδειγμα ότι δε μπορεί να επαναχρησιμοποιηθούν το δημόσιο και το ιδιωτικό κλειδί. Από τη στιγμή που θα υπογραφεί ένα μήνυμα θα πρέπει να δημιουργηθούν από την αρχή νέα κλειδιά. Αυτό έχει σαν αποτέλεσμα την αύξηση του υπολογιστικού κόστους καθώς και του κόστους αποθήκευσης.

9.1 Lamport

Το σχήμα δουλεύει ώς εξής:
Ξεκινάμε με το μήνυμα σε δυαδική μορφή με μέγεθος k-bits, δηλαδή $m \in \{0,1\}^k$. Η αρχική μορφή του σχήματος χρησιμοποιεί κάποιον συμμετρικό κρυπταλγόριθμο, για παράδειγμα τον DES.

ΚΑΤΑΣΚΕΥΗ ΚΛΕΙΔΙΟΥ

Έστω η συνάρτηση μονής κατεύθυνσης $f(x) = \alpha^x \ mod \ p$, όπου p πρώτος και α πρωταρχικό στοιχείο modulo p. Ο Bob:

1. Επιλέγει $2k$ το πλήθος τυχαίους αριθμούς $y_{i,j}, 1 \leq i \leq k, j = 0,1$
2. Υπολογίζει τα $z_{i,j} = f(y_{i,j})$

Το κλειδί αποτελείται από τα $2k$ το πλήθος y και τα $2k$ το πλήθος z. Τα y αποτελούν το ιδιωτικό κλειδί ενώ τα z το δημόσιο.

ΠΑΡΑΓΩΓΗ ΥΠΟΓΡΑΦΗΣ

Έστω ότι ο Bob θέλει να στείλει στην Alice το μήνυμα $m = x_1 x_2 \dots x_k$, το οποίο όπως αναφέραμε βρίσκεται σε δυαδική μορφή και έχει μήκος k-bits. Η υπογραφή του Bob για το μήνυμα είναι:

$$(s_1, s_2, \dots, s_k) = (y_{1,x_1}, y_{2,x_2}, \dots, y_{k,x_k})$$

Στη συνέχεια στέλνει στην Alice το μήνυμα:

$$(m, s_1, s_2, \dots, s_k)$$

ΕΠΑΛΗΘΕΥΣΗ ΥΠΟΓΡΑΦΗΣ

Η Alice δέχεται το $(m, s_1, s_2, \dots, s_k)$. Αποδέχεται την υπογραφή ως έγκυρη αν και μόνο αν

$$f(s_i) = z_{i,x_i}$$

Παρατηρούμε ότι το κάθε bit του μηνύματος υπογράφεται ανεξάρτητα. Αν το bit στη θέση i ισούται με j, όπου $j \in \{0, 1\}$, τότε το στοιχείο i της υπογραφής αποτελεί την εικόνα του $y_{i,j}$ μέσω της f που είναι το $z_{i,j}$. Οπότε η διαδικασία της επαλήθευσης ελέγχει αν το στοιχείο i της υπογραφής είναι εικόνα του $z_{i,j}$ χρησιμοποιώντας τη δημοσιοποιημένη συνάρτηση f.

ΠΑΡΑΔΕΙΓΜΑ

Έστω ότι η Alice θέλει να στείλει το μήνυμα $(1, 1, 0)$ στον Bob και να το υπογράψει με το σχήμα Lamport. Επιλέγει συνάρτηση μονής κατεύθυνσης $f(x) = 3^x \ mod\ 7879$ και $2k \xrightarrow{k=3} 6$ το πλήθος τυχαίους αριθμούς $y_{i,j}$. Προκύπτει ο πίνακας:

$$(y_{i,j}) = \begin{pmatrix} 4815 & 108 \\ 1623 & 5055 \\ 42 & 713 \end{pmatrix}$$

Με βάση αυτόν υπολογίζουμε τις εικόνες των $y_{i,j}$ στην f και καταλήγουμε στον πίνακα:

$$(z_{i,j}) = \begin{pmatrix} 5259 & 1885 \\ 7853 & 3039 \\ 873 & 4400 \end{pmatrix}$$

Ο $(z_{i,j})$ αποτελεί το δημόσιο κλειδί της Alice.

Η υπογραφή για το μήνυμα είναι:

$$(s_1, s_2, \ldots, s_k) = \left(y_{1,1}, y_{2,1}, y_{3,0}\right) = (108, 5055, 42)$$

Για να επαληθεύσει το μήνυμα ο Bob υπολογίζει:

$$f(108) = 3^{108}\ mod\ 7879 = \ 1885 = z_{1,1}$$
$$f(5055) = 3^{5055}\ mod\ 7879 = 3039\ = z_{2,1}$$
$$f(42) = 3^{42}\ mod\ 7879 = 873\ = z_{3,0}$$

9.2 Ασφάλεια Lamport

Η ασφάλεια του συγκεκριμένου σχήματος βασίζεται στο γεγονός ότι ο Oscar δε μπορεί να αντιστρέψει τη συνάρτηση f ώστε να ανακαλύψει τα ιδιωτικά y. Θα πρέπει όμως να τονίσουμε ότι σε περίπτωση που χρησιμοποιηθεί ο ίδιος πίνακας $(y_{i,j})$ για την υπογραφή και κάποιου δεύτερου μηνύματος, τότε ο Oscar θα αποκτήσει την ικανότητα να υπογράφει άλλα μήνυματα, εκτός εαν τα δύο μηνύματα που έχει υποκλέψει διαφέρουν μόνο κατά ένα bit.
Για παράδειγμα, ας υποθέσουμε ότι ο Bob επιθυμεί να υπογράψει τα μηνύματα

$m_1 = (0, 1, 1)$ και $m_2 = (1, 0, 1)$

και λανθασμένα χρησιμοποιεί το ίδιο κλειδί..

Στο m_1 αντιστοιχεί η υπογραφή $(y_{1,0}, y_{2,1}, y_{3,1})$ και στο m_2 η $(y_{1,1}, y_{2,0}, y_{3,1})$

Ο Oscar μπορεί με βάση αυτές να κατασκευάσει υπογραφές για τα μηνύματα:

$$(1, 1, 1) \rightarrow\ (y_{1,1}, y_{2,1}, y_{3,1})$$
$$(0, 0, 1) \rightarrow\ (y_{1,0}, y_{2,0}, y_{3,1})$$

Παρά την κομψότητα του σχήματος υπογραφών Lamport, δεν έχει πρακτική εφαρμογή. Το σημαντικότερο πρόβλημα είναι το μέγεθος των υπογραφών που παράγει. Αν θέλουμε να υπογράψουμε ένα μήνυμα όπως στο παράδειγμά μας τότε για μια ασφαλή εκτέλεση θα έπρεπε το p να έχει μήκος τουλάχιστον 1024

bits, δηλαδή το κάθε bit του μηνύματος υπογράφεται χρησιμοποιώντας 1024 bits. Συνεπώς η υπογραφή θα είναι 1024 φορές μεγαλύτερη από το αρχικό μήνυμα! Πιθανόν να μπορούσαμε να χρησιμοποιήσουμε μια συνάρτηση που να βασίζεται στη δυσκολία του DLP αλλά και πάλι το σχήμα δε θα ήταν πολύ πρακτικο.

10. Σχήματα Ψηφιακών Υπογραφών με επιπρόσθετη λειτουργικότητα

10.1 Αδιαμφισβήτητα Σχήματα Υπογραφής (Undeniable Signature Schemes)

Τα συγκεκριμένα σχήματα υπογραφής παρουσιάστηκαν για πρώτη φορά σε μια εργασία των Chaum και van Antwerpen το 1989. Μια σημαντική διαφορά σε σχέση με άλλα σχήματα που έχουμε δει είναι ότι η επικύρωση της υπογραφής της Alice από τον Bob γίνεται με τη συμβολή της ίδιας. Έτσι το έγγραφο που έχει υπογράψει δε μπορεί να χρησιμοποιηθεί από τρίτους χωρίς την έγκρισή της. Για την επαλήθευση απαιτείται ένα πρωτόκολλο πρόκλησης-απόκρισης (challenge-and-response).

Μπορεί σε αυτό το σημείο κάποιος να παρατηρήσει ένα πρόβλημα: Από τη στιγμή που είναι απαραίτητη η συμμετοχή της ιδίας για την επαλήθευση, τί εμποδίζει την Alice να αρνηθεί την εγκυρότητα κάποιας υπογραφής που έχει πραγματικά παράγει στο παρελθόν; Η Alice μπορεί να ισχυριστεί ότι μια υπογραφή της είναι άκυρη και να αρνηθεί να την επικυρώσει ή να μεταβάλλει τη διαδικασία επαλήθευσης με τέτοιον τρόπο ώστε η υπογραφή να μην επικυρωθεί. Για να αποφεχθούν τέτοιου είδους προβλήματα, το σχήμα περιέχει και ένα πρωτόκολλο αποκήρυξης (disavowal) με το οποίο η Alice μπορεί να αποδείξει ότι μια υπογραφή είναι πλαστογραφημένη. Έτσι η Alice μπορεί με ασφάλεια να αποκηρύξει μια πλαστή υπογραφή ενώ αν αρνηθεί να συμμετέχει στη διαδικασία επιβεβαίωσης είναι μια ένδειξη ότι η υπογραφή είναι έγκυρη.

Συμπεραίνουμε ότι τα απαραίτητα τμήματα ενός αδιαμφισβήτητου σχήματος υπογραφής είναι τρία:

1. Ένας αλγόριθμος υπογραφής
2. Ένα πρωτόκολλο επαλήθευσης
3. Ένα πρωτόκολλο αποκήρυξης

Το συγκεκριμένο σχήμα χρησιμοποιεί τον χώρο $\mathbb{Z}_p$, όμως οι υπολογισμοί μας γίνονται σε μια πολλαπλασιαστική υποομάδα G του $\mathbb{Z}_p^*$ πρώτης τάξης (διότι θέλουμε να μπορούμε να υπολογίσουμε αντιστρόφους modulo$|G|$, όποτε το $|G|$

πρέπει να είναι πρώτος). Είναι βολικό $p = 2q + 1$ όπου q πρώτος ώστε η υποομάδα G να είναι όσο το δυνατόν μεγαλύτερη. Αυτό είναι επιθυμητό αφού και τα μηνύματα και οι υπογραφές είναι στοιχεία της G.

ΚΑΤΑΣΚΕΥΗ ΚΛΕΙΔΙΟΥ

Η Alice επιθυμεί να στείλει ένα μήνυμα και να το υπογράψει με το αδιαμφισβήτητο σχήμα υπογραφής των Chaum και van Antwerpen. Επιλέγει ένα ιδιωτικό και ένα δημόσιο κλειδί ακολουθώντας την εξής διαδικασία:

1. Επιλέγει δύο τυχαίους πρώτους p, q με $p = 2q + 1$.
2. Υπολογίζει ένα πρωταρχικό στοιχείο α με τάξη q στην πολλαπλασιαστική υποομάδα G του $\mathbb{Z}_p^*$ ως εξής:
    - Επιλέγει τυχαίο στοιχείο z του $\mathbb{Z}_p^*$
    - Υπολογίζει το $\alpha = z^{(p-1)/q} mod\ p$
3. Επιλέγει τυχαίο s με $1 \leq s \leq q - 1$ και υπολογίζει το $\beta = \alpha^s mod\ p$

Το δημόσιο κλειδί της Alice είναι το (p, α, β) ενώ το ιδιωτικό της είναι το s.

ΠΑΡΑΓΩΓΗ ΥΠΟΓΡΑΦΗΣ

Για να υπογράψει το μήνυμα η Alice:

1. Υπολογίζει το $y = x^s\ mod\ p$

Στέλνει στον Bob το (x, y).

ΕΠΑΛΗΘΕΥΣΗ ΥΠΟΓΡΑΦΗΣ

Ο Bob τώρα θα συνεργαστεί με την Alice για να επαληθεύσει την υπογραφή. Θα εργαστούν ως εξής:

1. Ο Bob αποκτά το δημόσιο κλειδί της Alice.
2. Ο Bob επιλέγει δύο τυχαίους ακεραίους e_1, e_2 όπου $1 \leq e_1, e_2 \leq q - 1$ και τους κρατάει κρυφούς.
3. Ο Bob υπολογίζει το $c = y^{e_1}\beta^{e_2}\ mod\ p$ και το στέλνει στην Alice.
4. Η Alice από τη μεριά της υπολογίζει το $d = c^f\ mod\ p$, όπου $f = s^{-1}\ mod\ q$ το οποίο στέλνει πίσω στον Bob.
5. Ο Bob δέχεται την υπογραφή y ως έγκυρη αν και μόνο αν:

$$d \equiv x^{e_1}\alpha^{e_2}\ mod\ p.$$

Εύκολα δείχνουμε ότι η επαλήθευση λειτουργεί:

$$d \equiv c^f \ mod\ p \equiv y^{e_1}\beta^{e_2} \ mod\ p$$

Επειδή όμως:

$$\beta \equiv \alpha^s \ mod\ p \Longrightarrow$$

$$\beta^f \equiv \alpha \ mod\ p \quad (1)$$

Επίσης:

$$y \equiv x^s \ mod\ p \Longrightarrow$$

$$y^f \equiv x \ mod\ p \quad (2)$$

Άρα από τις (1), (2):

$$d \equiv x^{e_1}\alpha^{e_2} \ mod\ p$$

10.1.1 Πρωτοκολλο Αποκηρυξης

Το πρωτόκολλο αποκήρυξης εφαρμόζει δύο φορές το πρωτόκολλο επαλήθευσης και στη συνέχεια εκτελεί έναν έλεγχο για να επαληθεύσει ότι η Alice εκτέλεσε σωστά το πρωτόκολλο. Η διαδικασία είναι η ακόλουθη:

1. Ο Bob αποκτά το δημόσιο κλειδί της Alice.
2. Ο Bob επιλέγει δύο τυχαίους ακεραίους e_1, e_2 όπου $1 \leq e_1, e_2 \leq q-1$ και τους κρατάει κρυφούς.
3. Ο Bob υπολογίζει το $c = y^{e_1}\beta^{e_2} \ mod\ p$ και το στέλνει στην Alice.
4. Η Alice από τη μεριά της υπολογίζει το $d = c^f \ mod\ p$, όπου $f = s^{-1} \ mod\ q$ το οποίο στέλνει πίσω στον Bob.

5. Ο Bob επαληθεύει ότι $d \neq x^{e_1}\alpha^{e_2} \; mod \; p$.
6. Ο Bob επιλέγει δύο τυχαίους ακεραίους w_1, w_2 όπου $1 \leq w_1, w_2 \leq q-1$ και τους κρατάει κρυφούς.
7. Ο Bob υπολογίζει το $c' = y^{w_1}\beta^{w_2} \; mod \; p$ και το στέλνει στην Alice.
8. Η Alice από τη μεριά της υπολογίζει το $d' = c'^{f} \; mod \; p$ το οποίο στέλνει πίσω στον Bob.
9. Ο Bob επαληθεύει ότι $d' \neq x^{w_1}\alpha^{w_2} \; mod \; p$.
10. Ο Bob συμπεραίνει ότι η υπογραφή είναι πλαστή αν και μόνο αν:

$$(d\alpha^{-e_2})^{w_1} \equiv (d'\alpha^{-w_2})^{e_1}$$

10.2 Τυφλά Σχήματα Υπογραφών (Blind Signature Schemes)

Υπάρχουν μερικές περιπτώσεις όπου επιθυμούμε να υπογραφεί ένα κείμενο χωρίς ο υπογράφων να γνωρίζει το περιεχόμενό του. Σε προηγούμενο κεφάλαιο αναφέραμε την επιθυμία του Bob να μπορέσει να κερδίσει το βραβείο Nobel και παράλληλα να συγκεντρώνει μια αμύθητη περιουσία από την πατέντα για την ανακάλυψή του. Αυτό το παράδειγμα προφανώς αποτελεί μια ακραία περίπτωση που όμως βασίζεται σε μια πραγματική ανάγκη για την κατωχείρωση των πνευματικών δικαιωμάτων. Ένα άλλο καλό παράδειγμα είναι το ηλεκτρονικό χρήμα.

Ένα από τα βασικά πλεονεκτήματα του ηλεκτρονικού χρήματος είναι η ανωνυμία που παρέχει. Πως όμως θα μπορέσει μια τράπεζα να εγγυηθεί τη γνησιότητα του ηλεκτρονικού χρήματος χωρίς να είναι «παρούσα» στη διάρκεια της συναλλαγής; Αυτό το ρόλο έρχονται να παίξουν τα Τυφλά Σχήματα Υπογραφών (Blind Signature Schemes).

Ένα σχήμα τυφλής υπογραφής πρέπει να διαθέτει τα εξής:

1. Ένα μηχανισμό υπογραφής για την Alice. Το $S_A(x)$ ορίζει ακριβώς αυτή την υπογραφή στο x.
2. Συναρτήσεις f, g (γνωστές μόνο στον αποστολέα) τέτοιες ώστε $g\left(S_A(f(m))\right) = S_A(m)$. Η f καλείται *συνάρτηση τύφλωσης (blinding function)*, η g *συνάρτηση επαναφοράς (unblinding function)* και το $f(m)$ *τυφλό μήνυμα (blinded message).*

Έχουμε μελετήσει ένα είδος τυφλής υπογραφής στο κεφάλαιο του RSA. Ένα εναλλακτικό πρωτόκολλο πρότεινε ο David Chaum.

10.2.1 Τυφλό Σχήμα Υπογραφής Chaum

Η Alice ζητάει από τον Bob να της υπογράψει ένα μήνυμα m χωρίς να το διαβάσει. Ο Bob χρησιμοποιεί τον RSA με δημόσιο κλειδί (n, e) και ιδιωτικό κλειδί d. Το k είναι μυστικό και το επιλέγει η Alice, όπου:

$$0 \leq k \leq n-1 \text{ και } gcd(n,k) = 1$$

- Η Alice υπολογίζει το $m^* = m \cdot k^e \, mod \, n$ και το στέλνει στον Bob(τύφλωση)
- Ο Bob υπολογίζει το $s^* = (m^*)^d \, mod \, n$ και το στέλνει στην Alice(υπογραφή)
- Η Alice υπολογίζει το $s = k^{-1} \, s^* \, mod \, n$ που αποτελεί την υπογραφή του Bob για το μήνυμα m (αποτύφλωση)

10.3 Fail-Stop

Ένα σχήμα υπογραφής fail-stop προτάθηκε από τους van Heyst και Pedersen το 1992 και στόχος του ήταν να παρέχει αυξημένη ασφάλεια σε περίπτωση που κάποιος ισχυρός αντίπαλος έχει την ευκαιρία να πλαστογραφήσει μια υπογραφή. Εκτός από της διαδικασίες κατασκευής κλειδιού, παραγωγής και επαλήθευσης υπογραφής διαθέτει επιπλέον έναν αλγόριθμο απόδειξης πλαστογραφίας, ο οποίος όμως απαιτεί την ύπαρξη μιας Έμπιστης Αρχής (TTP).

ΚΑΤΑΣΚΕΥΗ ΚΛΕΙΔΙΟΥ

Στην κατασκευή του κλειδιού εμπλέκεται και η TTP. Ας υποθέσουμε ότι η Alice θέλει να υπογράψει το μήνυμα m. Τότε αρχικά η TTP:

1. Επιλέγει πρώτο q και υπολογίζει τον $p = 2q + 1$ τέτοιον ώστε $q|(p-1)$
2. Επιλέγει ένα τυχαίο στοιχείο z του $\mathbb{Z}_p^*$ και υπολογίζει το $\alpha = z^{(p-1)/q} \, mod \, p$ το οποίο είναι από τον τρόπο υπολογισμού γεννήτορας τάξεως q κυκλικής υποομάδας του $\mathbb{Z}_p^*$.
3. Επιλέγει έναν τυχαίο ακέραιο s, $1 \leq s \leq q-1$ και υπολογίζει το $\beta = \alpha^s mod \, p$

Τα (p, q, α, β) αποτελούν το δημόσιο κλειδί της TTP, ενώ το s το ιδιωτικό **(το οποίο παραμένει κρυφό ακόμα και από την Alice).**

Η Alice με τη σειρά της:

1. Επιλέγει τυχαίους ακεραίους $1 \leq \alpha_1, \alpha_2, \beta_1, \beta_2 \leq q-1$
2. Υπολογίζει τα $\gamma_1 = \alpha^{\alpha_1}\beta^{\alpha_2} \, mod \, p$ και $\gamma_2 = \alpha^{\beta_1}\beta^{\beta_2} \, mod \, p$

Το δημόσιο κλειδί της Alice είναι το $(\gamma_1, \gamma_2, p, q, \alpha, \beta)$ και το ιδιωτικό το $(\alpha_1, \alpha_2, \beta_1, \beta_2)$.

ΠΑΡΑΓΩΓΗ ΥΠΟΓΡΑΦΗΣ
Η Alice:

1. Υπολογίζει τα $y_1 = \alpha_1 + m\beta_1 \; mod \; q$ και $y_2 = \alpha_2 + m\beta_2 \; mod \; q$

Η υπογραφή της για το μήνυμα m είναι η δυάδα (y_1, y_2) και θα στείλει στον Bob το (m, y_1, y_2).

ΕΠΑΛΗΘΕΥΣΗ ΥΠΟΓΡΑΦΗΣ
Ο Bob τώρα για να επαληθεύσει την υπογραφή ανακτά το δημόσιο κλειδί της Alice και στη συνέχεια:

1. Υπολογίζει τα $u_1 = \gamma_1 {\gamma_2}^m \; mod \; p$ και $u_2 = \alpha^{y_1}\beta^{y_2} \; mod \; p$
2. Δέχεται την υπογραφή ως έγκυρη αν και μόνο αν $u_1 = u_2$

ΑΠΟΔΕΙΞΗ ΠΛΑΣΤΟΓΡΑΦΙΑΣ
Έστω ότι ο Oscar έχει παράγει την υπογραφή $y'' = sig_K(m')$ η οποία πέρασε επιτυχώς το στάδιο της επαλήθευσης. Τότε ισχύει:

$$\gamma_1 {\gamma_2}^{m'} \; mod \; p = a^{{y_1}''}\beta^{{y_2}''} \; mod \; p \quad (1)$$

Η υπογραφή της Alice για το μήνυμα m' είναι η y', όπότε:

$$\gamma_1 {\gamma_2}^{m'} \; mod \; p = a^{{y_1}'}\beta^{{y_2}'} \; mod \; p \quad (2)$$

Από τις (1),(2): $a^{{y_1}'}\beta^{{y_2}'} \; mod \; p = a^{{y_1}''}\beta^{{y_2}''} \; mod \; p$

$$\xRightarrow{\beta = \alpha^s mod \; p} a^{{y_1}' + s{y_2}'} \; mod \; p = a^{{y_1}'' + s{y_2}''} \; mod \; p$$

$$\Rightarrow {y_1}' + s{y_2}' = {y_1}'' + s{y_2}''$$

$$\Rightarrow {y_1}'' - {y_1}' = s({y_2}' - {y_2}'')$$

Επειδή όμως η y'' είναι πλαστογραφημένη θα έχουμε ${y_2}' \neq {y_2}''$, άρα υπάρχει ο $({y_2}' - {y_2}'')^{-1} \; mod \; q$ οπότε:

$$s = log_\alpha \beta = ({y_1}'' - {y_1}')({y_2}' - {y_2}'')^{-1} mod \; q$$

11. Ψηφιακά πιστοποιητικά

Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι (και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί) ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε (μη αποποίηση).

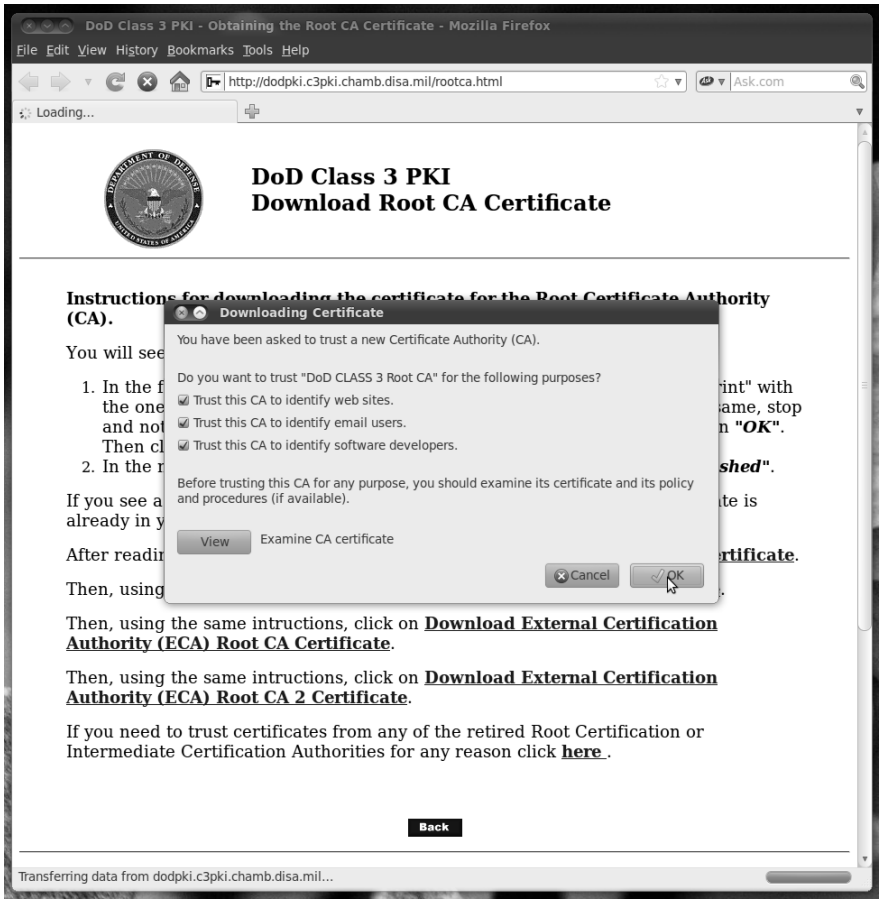
Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί.

Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι μια οντότητα που παρέχει την υπηρεσία με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ένα ηλεκτρονικό αρχείο) στο οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών είναι το πιστοποιητικό δημοσίου κλειδιού (public key certificate). Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το

πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει.

Το ψηφιακό πιστοποιητικό, είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Παρόχου Υπηρεσιών Πιστοποίησης, όπου ο Πάροχος με την ψηφιακή του υπογραφή, υπογράφει το πιστοποιητικό του δικαιούχου. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο Πάροχος εκδίδει.



Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο

χρήστης δεν γνωρίζει έναν Πάροχο (π.χ. τον πάροχο Death Metal) και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει, και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο (Classical Music For The Masses) που ο χρήστης εμπιστεύεται, τότε ο χρήστης μπορεί να εμπιστευθεί τον πρώτο Πάροχο. Ο χρήστης, μπορεί να επαληθεύσει τη ψηφιακή υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που έχει εκδώσει ένα ψηφιακό πιστοποιητικό, χρησιμοποιώντας το δημόσιο κλειδί του Death Metal, για το οποίο (δημόσιο κλειδί) ο Classical Music For The Masses μπορεί να έχει εκδώσει πιστοποιητικό κ.λπ.

Ένα πιστοποιητικό εφόσον διαπιστωθεί ή υπάρχει υπόνοια ότι για κάποιους λόγους δεν είναι έγκυρο (π.χ. αν το ιδιωτικό κλειδί του δικαιούχου έχει γίνει γνωστό σε τρίτους ή το πρόσωπο εξαπάτησε τον Πάροχο Υπηρεσιών Πιστοποίησης ως προς τα στοιχεία της ταυτότητάς του κ.λπ), τότε ο Πάροχος Υπηρεσιών Πιστοποίησης προβαίνει στην ανάκλησή του, όπως ρυθμίζεται από τη νομοθεσία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Χ. Κουκουβίνος, Α. Παπαϊωάννου. *Εισαγωγή στην Κρυπτογραφία*. Εκδόσεις Ε.Μ.Π., 2004
2. Α. Παπαϊωάννου. *Διακριτά Μαθηματικά*. Εκδόσεις Ε.Μ.Π., 2003
3. Douglas R. Stinson. *Cryptography: Theory and Practice, Third Edition*. Chapman & Hall / CRC, 2006
4. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997
5. Δημήτριος Μ. Πουλάκης. *Κρυπτογραφία: Η Επιστήμη της Ασφαλούς Επικοινωνίας*. Εκδόσεις Ζήτη, 2006
6. Wade Trappe, Lawrence Washington. *Introduction to Cryptography with Coding Theory, Second Edition*
7. Διπλωματική Εργασία του Γρηγορίου Κόλλια. *Σχήματα Ψηφιακών Υπογραφών*. Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών, Τομέας Μαθηματικών. Ε.Μ.Π. , 2006
8. Διπλωματική Εργασία του Γεωργίου Χ. Κρανία. *Σχήματα Ψηφιακής Υπογραφής*. Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών, Τομέας Μαθηματικών. Ε.Μ.Π. , 2005
9. Βασίλειος Α. Κάτος, Γιώργος Στεφανίδης. *Τεχνικές κρυπτογραφίας και κρυπτανάλυσης*. Εκδόσεις Ζυγός, 2003

Ιστοσελίδες

www.rsa.com

www.wikipedia.org

http://www.wolframalpha.com

http://www.eett.gr

http://www.cryptosys.net