Ιόνιο Πανεπιστήμιο

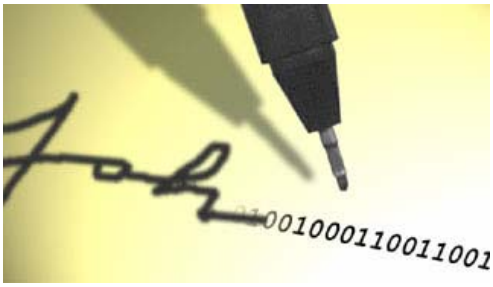
Τμήμα Αρχειονομίας – Βιβλιοθηκονομίας

Πρόγραμμα Μεταπτυχιακών Σπουδών στην Επιστήμη της Πληροφορίας

«Διοίκηση και Οργάνωση Βιβλιοθηκών με έμφαση στις Νέες Τεχνολογίες της Πληροφορίας»

Ψηφιακή Υπογραφή

Εργασία της φοιτήτριας
Αμαλίας Γιαννακά



Μάθημα
«Ψηφιακές Βιβλιοθήκες»

Υπεύθυνος Καθηγητής
Σαράντος Καπιδάκης

Ακαδημαϊκό έτος 2005-2006

Περιεχόμενα

Εισαγωγή

Η μετάδοση πληροφοριών χωρίς να γίνεται αντιληπτή από τρίτους, η εξασφάλιση της δυνατότητας να μην μπορεί να ερμηνευθεί το μήνυμα στην περίπτωση που η μετάδοση γίνει αντιληπτή καθώς και η απόδειξη της ιδιοκτησίας, κυριότητος ενός μηνύματος απασχόλησαν από το μακρινό παρελθόν και εξακολουθούν να απασχολούν έως σήμερα τον άνθρωπο. Τα προβλήματα αυτά, θα εξακολουθούν να υπάρχουν, όσο θα υπάρχουν άνθρωποι που θα προσπαθούν να προστατέψουν τα δικαιώματά τους και κάποιοι που θα προσπαθούν να τα παραβιάσουν. Στη σύγχρονη εποχή, η διαμάχη αυτή διεξάγεται στο χώρο των ψηφιακών δεδομένων. Σύγχρονες υπολογιστικές μηχανές, με υψηλές δυνατότητες επεξεργασίας και αποθήκευσης πληροφοριών, χρησιμοποιούνται τόσο για να εξασφαλίζουν τη νομιμότητα όσο και για να την παρακάμπτουν.

Ειδικότερα, η ανάπτυξη του διαδικτύου, το ηλεκτρονικό εμπόριο, οι συναλλαγές και η μετάδοση εμπιστευτικών δεδομένων, μέσω ανοιχτών δικτύων έχει γίνει κοινός τόπος σήμερα. Η σημερινή πραγματικότητα επιβάλλει μεταξύ των παραπάνω και την ύπαρξη μηχανισμών προστασίας του απαραβίαστου του προσωπικού και του επαγγελματικού απορρήτου των συναλλασσόμενων χρηστών. Επιβάλλει μηχανισμούς ασφάλειας στις συναλλαγές, ασφάλειας η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, την ταυτότητα δηλαδή των συναλλασσόμενων.

Λόγοι, οι οποίοι καθιστούν την ασφάλεια στην ηλεκτρονική επικοινωνία επιτακτική, είναι η ευκολία που παρέχεται μέσω ενός ανοικτού δικτύου, όπως είναι το Internet στην: α) παρακολούθηση της επικοινωνίας από τρίτους β) αλλοίωση του περιεχομένου του μεταφερόμενου μηνύματος γ) αδυναμία να εξακριβωθεί η ταυτότητα των επικοινωνούντων μερών (πλαστοπροσωπία με τη χρήση πλαστής ηλεκτρονικής διεύθυνσης).

Μια από τις μεθόδους που χρησιμοποιούνται για την ασφαλή διακίνηση των πληροφοριών στο σύγχρονο περιβάλλον, είναι η κρυπτογραφία. Η κρυπτογραφία αποτέλεσε πανάρχαια μέθοδο εξασφάλισης της εμπιστευτικότητας των συναλλαγών, όπως προκύπτει από την παρακάτω συνοπτική ιστορική διαδρομή. Εξακολουθεί επίσης, έως και σήμερα να συμβάλλει στον παραπάνω στόχο, καθώς η ίδια αποτελεί μια πολύ βασική τεχνολογία στον τομέα της ασφάλειας του Internet.

Ειδικότερα, με τη χρήση της τεχνολογίας της κρυπτογραφίας, δημιουργούνται οι προηγμένες ηλεκτρονικές υπογραφές ή αλλιώς λεγόμενες ψηφιακές υπογραφές, που θα μας απασχολήσουν στο πλαίσιο αυτής της εργασίας.

Κρυπτογραφία

Ιστορική αναδρομή κρυπτογραφίας

Η κρυπτογραφία είχε αρχικά την μορφή τέχνης που τα μυστικά της γνώριζαν λίγοι και εκλεκτοί. Η ιστορία της κρυπτογραφίας ξεκινά περίπου το 4000 π.Χ. στην αρχαία Αίγυπτο περνά στην αρχαία Ελλάδα που έχουμε αναφορές της στο ιστορικό Πολύβιο και συνεχίζεται στον Ιούλιο Καίσαρα. Ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί π.χ. 3. Δηλαδή, η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο. Θα μπορούσε το κλειδί να ήταν ο αριθμός 6, οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό. Έτσι, διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.
Ο πίνακας αντιστοίχισης των γραμμάτων, έχοντας ως κλειδί το 3, φαίνεται παρακάτω:

Το γράμμα	a	b	c	d	e	f	g	h	i	j	k	v	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Αντικαθίσταται από το γράμμα	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη secret, θα προκύψει το κρυπτογράφημα wigvix. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να

αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερότερά του στο αλφάβητο. Προφανώς, δεν αρκεί να ξέρει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά πρέπει να γνωρίζει και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει να γνωρίζει το κλειδί, που σε αυτήν την περίπτωση είναι ο αριθμός 3

Από την στιγμή που η κρυπτογραφία άρχισε να χρησιμοποιείται για στρατιωτικούς σκοπούς και για απόκρυψη ζωτικής σημασίας πληροφοριών, έπαψε να είναι απόκρυφη τέχνη και έτυχε της μελέτης τόσο αυτών που ήθελαν να αποκρύψουν τα μυστικά τους όσο και από αυτούς που ήθελαν να βρουν τρόπο να αποκαλύψουν τα μυστικά των αντιπάλων τους. Έτσι η κρυπτογραφία πέρασε στο πεδίο της επιστήμης. Κρυπτογράφοι και κρυπταναλυτές επιδόθηκαν σε έναν ανελέητο συναγωνισμό. Κάθε πρόοδος της κρυπτογραφίας συνοδευόταν από μια αντίστοιχη πρόοδο της κρυπτανάλυσης. Η κρυπτογραφία έγινε χρήσιμο εργαλείο στα χέρια του στρατού των διπλωματών και του κράτους με σκοπό την διαφύλαξη εθνικών μυστικών και στρατηγικών. Όσο πιο πολύτιμα τα μυστικά τόσο πιο μεγάλη αξία αποκτούσε η ασφαλής φύλαξή τους. Στον 20ό αιώνα τα παραδείγματα εκτεταμένης χρήσης κρυπτογραφικών τεχνικών είναι πολλά. Την περίοδο της ποτοαπαγόρευσης στην Αμερική (δεκαετία του 20-30) το νεοσύστατο τότε σώμα FBI χρησιμοποίησε τεχνικές κρυπτογραφίας για να αποκρύπτει από τη μαφία τους τόπους παράδοσης μεγάλων φορτίων ποτών.

Δεν θα ήταν υπερβολή να πούμε ότι η έκβαση του δευτέρου Παγκοσμίου Πολέμου κρίθηκε υπέρ των συμμάχων εξαιτίας της ικανότητας τους να αποκρυπτογραφούν τα γερμανικά μηνύματα και της ανικανότητας των Γερμανών να πράξουν κάτι ανάλογο με τα συμμαχικά μηνύματα. Είναι γνωστή άλλωστε η ιστορία της μηχανής ENIGMA που χρησιμοποίησαν οι Άγγλοι για να αποκρυπτογραφούν τα μηνύματα του Γερμανικού επιτελείου προς τις αγέλες των υποβρυχίων τους στη Μεσόγειο αλλά και τον Ατλαντικό ωκεανό.

Από την δεκαετία του 60 και μετά η κρυπτογραφία γνώρισε μεγάλη ανάπτυξη λόγω της ραγδαίας ανάπτυξης των υπολογιστών, αλλά και των τηλεπικοινωνιών. Έτσι λοιπόν, υπήρξε η ανάγκη για προστασία δεδομένων σε ψηφιακή μορφή. Αρχίζοντας με την εργασία του Feistel στην IBM στις

αρχές της δεκαετίας του '70 και καταλήγοντας το 1977 με την υιοθέτηση του Αμερικανικού ομοσπονδιακού προτύπου για την επεξεργασία των πληροφοριών την κρυπτογράφηση των μη-διαβαθμισμένων πληροφοριών, DES, το πρότυπο κρυπτογράφησης στοιχείων, είναι ο πιο γνωστός κρυπτογραφικός μηχανισμός της ιστορίας. Παραμένει μέχρι σήμερα το τυποποιημένο μέσο για την ασφάλεια του ηλεκτρονικού εμπορίου σε πολλά οικονομικά ιδρύματα σε όλο τον κόσμο.

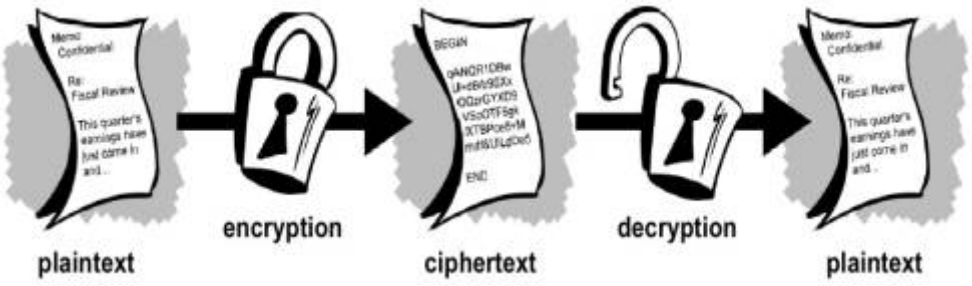
Η πιο εντυπωσιακή ανάπτυξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν ο Diffie και ο Hellman δημοσίευσαν το "New directions in cryptography". Αυτή η επιστημονική δημοσίευση εισήγαγε την επαναστατική έννοια τής κρυπτογραφίας δημοσίου κλειδιού. Παρόλο που οι συγγραφείς δεν έκαναν πρακτική εφαρμογή του σχήματος που πρότειναν, η αρχή είχε γίνει και το θέμα έτυχε μεγάλου ενδιαφέροντος από την κρυπτογραφική κοινότητα.

Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική εφαρμογή του προταθέντος σχήματος. Ήταν το λεγόμενο σχήμα RSA και βασιζόταν σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, αυτό της δυσκολίας παραγοντοποίησης μεγάλων ακεραίων. Όπως ήταν φυσικό οι κρυπταναλυτές σήκωσαν τα μανίκια και άρχισαν να ψάχνουν πιο αποτελεσματικούς τρόπους παραγοντοποίησης. Παρά τις μεγάλες προόδους τους κυρίως την δεκαετία του 80 το RSA παρέμεινε ακόμα ασφαλές! Μια από τις σημαντικότερες προσφορές της κρυπτογραφίας δημοσίου κλειδιού ήταν και η ψηφιακή υπογραφή.

Βασικές έννοιες της κρυπτογραφίας

Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών.

Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext) (Σχήμα 1).



Σχήμα 1: Κρυπτογράφηση απλού κειμένου

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτή μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος.

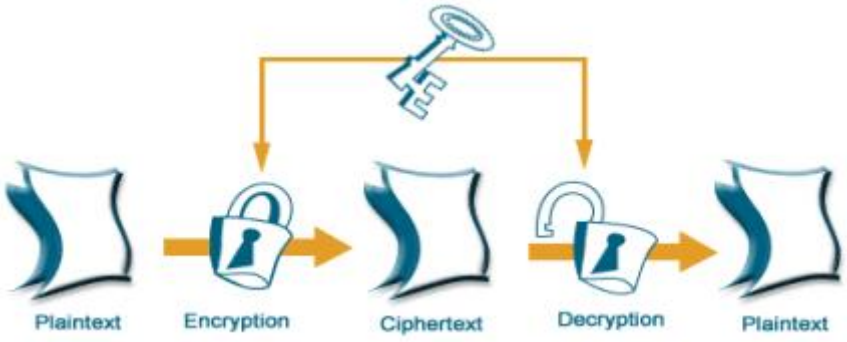
Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς την χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης.

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνει ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον διαβάλλει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key), για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

Συμμετρική και ασύμμετρη κρυπτογραφία

Συμμετρική κρυπτογραφία ή κρυπτογραφία συμμετρικού ή μυστικού κλειδιού

Στη συμμετρική κρυπτογραφία, χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση (Σχήμα 2). Επομένως, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.



Σχήμα 2: Συμμετρική Κρυπτογραφία

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με περισσότερο γνωστό το Data Encryption Standard (DES), ο οποίος όπως προαναφέρθηκε υιοθετήθηκε από την κυβέρνηση των Η.Π.Α., ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

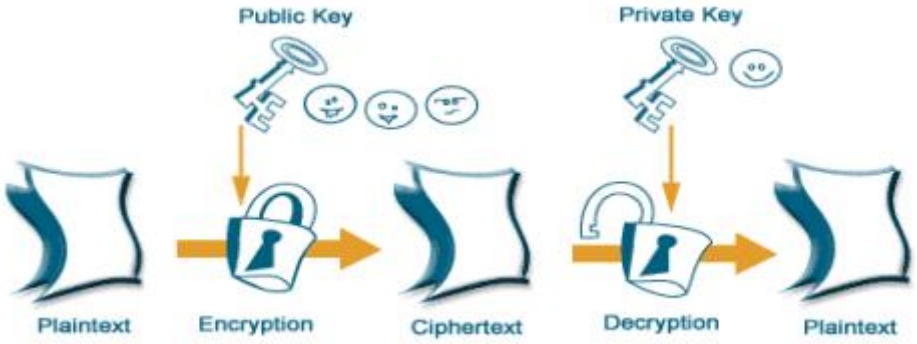
Το πρόβλημα που παρουσιάζει όμως αυτή η τεχνική είναι η διανομή των κλειδιών, η εξασφάλιση δηλαδή ότι τα κλειδιά που αποστέλλονται στους παραλήπτες που θα τα χρησιμοποιήσουν δεν θα πέσουν σε λάθος χέρια. Κατά αυτόν τον τρόπο τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα έχουν αναπτυχθεί και χρησιμοποιούνται, με περισσότερο διαδεδομένο το σύστημα Kerberos που έχει αναπτυχθεί στο MIT.

Ευνόητο επίσης είναι, ότι όσο ο αριθμός των χρηστών αυτού του συστήματος ασφαλείας μεγαλώνει, μεγαλώνουν και τα προβλήματα της δημιουργίας, της διανομής, της ασφάλειας αλλά και της καταγραφής και αντιστοιχίας των μυστικών κλειδιών. Άρα τα σχήματα αυτά δεν είναι εύκολο να επεκταθούν για την εξυπηρέτηση μεγάλων πληθυσμών και απαιτούν επίσης πρόσθετες διαδικασίες ασφάλειας, όπως την αποθήκευση των κλειδιών σε ένα κεντρικό ασφαλή εξυπηρετητή.

Ασύμμετρη Κρυπτογραφία ή κρυπτογραφία ασυμμετρικού ή δημόσιου κλειδιού

Στην ασύμμετρη κρυπτογραφία, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση, το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα (Σχήμα 3). Τα κλειδιά αυτά παράγονται έτσι ώστε να έχουν τις εξής ιδιότητες:

Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα. Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.



Σχήμα 3: Ασύμμετρη κρυπτογραφία

Όπως προαναφέρθηκε, η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού.

Για να αποκατασταθεί επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Αναλυτικότερα, ένα μήνυμα ή και ένα αρχείο που έχει κρυπτογραφηθεί με το δημόσιο κλειδί ενός κατόχου, μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί του ίδιου κατόχου, πράγμα που σημαίνει ότι μόνο ο κάτοχος ενός δημόσιου κλειδιού μπορεί να διαβάσει τα μηνύματα που έχουν κρυπτογραφηθεί με το κλειδί αυτό, καθώς μόνο αυτός γνωρίζει το αντίστοιχο ιδιωτικό κλειδί. Η διαδικασία αυτή εξασφαλίζει ότι το μήνυμα ή το αρχείο δεν μπορεί να παρακολουθείται ή και να αλλοιώνεται από κάποιον τρίτο που δεν κατέχει το αντίστοιχο ιδιωτικό κλειδί του δημοσίου κλειδιού με το οποίο κρυπτογραφήθηκε το μήνυμα ή το αρχείο. Στην περίπτωση αυτή λέμε ότι το μήνυμα είναι κρυπτογραφημένο

Συμπερασματικά, το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δε μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

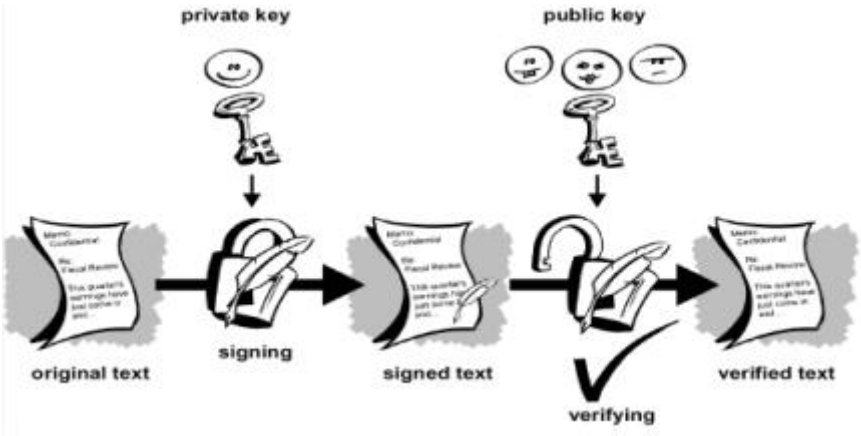
Η ασύμμετρη κρυπτογραφία προσφέρει μεγαλύτερη ασφάλεια από τη συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογράφησης.

Ασύμμετρη κρυπτογραφία και ψηφιακή υπογραφή

Η παραπάνω αναλυθείσα τεχνολογία της ασύμμετρης κρυπτογραφίας, χρησιμοποιείται για τη δημιουργία ψηφιακών υπογραφών. Ειδικότερα, παράγονται, βάσει συγκεκριμένων μαθηματικών αλγορίθμων (π.χ. RSA, DSA, κ.ά.), τυχαία ζεύγη κρυπτογραφικών κλειδιών (ψηφιακά δεδομένα) τα οποία χαρακτηρίζονται από δύο σημαντικές ιδιότητες: το καθένα κλειδί κρυπτογραφεί ψηφιακά δεδομένα τα οποία μπορούν να αποκρυπτογραφηθούν μόνο από το άλλο (συμπληρωματικό του) κλειδί, και δεν είναι δυνατό, με τις παρούσες δυνατότητες της τεχνολογίας, να συμπεράνει κανείς ή να αναδημιουργήσει το ένα κλειδί όταν γνωρίζει το άλλο.

Με την τεχνολογία της ασύμμετρης κρυπτογραφίας διατηρώντας μυστικό το ένα κλειδί ως «ιδιωτικό» (δεδομένα δημιουργίας υπογραφής) και διανέμοντας ελεύθερα το άλλο κλειδί ως «δημόσιο» (δεδομένα επαλήθευσης υπογραφής), εξασφαλίζουμε ότι όλοι όσοι γνωρίζουν ένα δημόσιο κλειδί μπορούν να επαληθεύσουν μια ψηφιακή υπογραφή που δημιουργείται από τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού.

Αξίζει να σημειωθεί ότι η διαφοροποίηση της κρυπτογράφησης και τη δημιουργίας ψηφιακής υπογραφής, έγκειται στο ότι για τη δημιουργία της υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Ειδικότερα, ένα μήνυμα ή και ένα αρχείο που έχει κρυπτογραφηθεί με το ιδιωτικό κλειδί ενός κατόχου, μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο δημόσιο κλειδί του ίδιου κατόχου, πράγμα που σημαίνει ότι ο οποιοσδήποτε μπορεί να το αποκρυπτογραφήσει και να το διαβάσει. Η διαδικασία αυτή εξασφαλίζει ότι το μήνυμα ή το αρχείο όντως προέρχεται από τον σωστό αποστολέα, εξακριβώνεται δηλαδή η ταυτότητα του αποστολέα. Στην περίπτωση αυτή λέμε ότι το μήνυμα είναι υπογεγραμμένο ψηφιακά.



Σχήμα 4: Ψηφιακές Υπογραφές

Συμπερασματικά, θα μπορούσαμε να αναφέρουμε ότι η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί τόσο για την ταυτόχρονη πιστοποίηση της ταυτότητας του αποστολέα, αλλά και για την κρυπτογράφηση του μηνύματος.

Ένα ακόμα πλεονέκτημα της ασύμμετρης κρυπτογράφησης είναι ότι τα μηνύματα που αποστέλλονται δεν είναι δυνατό να τροποποιηθούν κατά τη διάρκεια της μετάδοσής τους, καθώς η οποιαδήποτε αλλοίωσή τους τα καθιστά μη δυνάμενα να αποκρυπτογραφηθούν, κάτι που θα γίνει αμέσως αντιληπτό από τον παραλήπτη.

Ψηφιακή υπογραφή

Η «νομιμοποίηση» ενός εγγράφου ισοδυναμούσε ανέκαθεν με την υπογραφή που έφερε. Καθώς τα ηλεκτρονικά έγγραφα κάθε είδους τείνουν να αντικαταστήσουν τα «παραδοσιακά» χειρόγραφα, αντίστοιχα και η υπογραφή του συντάκτη γίνεται «εικονική», ηλεκτρονική.

Κρίνεται απαραίτητη η διευκρίνιση του όρου της «ψηφιακής υπογραφής», πριν την ανάλυση των εννοιών που σχετίζονται με τη δημιουργία, την επαλήθευσης της κλπ.

Ορισμοί

- Μια «κλειδωμένη» σύντμηση ενός ηλεκτρονικού κειμένου, η οποία παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσής του
- Είναι μια συμβολοσειρά από δεδομένα τα οποία σχετίζουν ένα μήνυμα (στην ψηφιακή του μορφή) με την οντότητα που το δημιούργησε.
- Οι ψηφιακές υπογραφές είναι δεδομένα που έχουν ενσωματωθεί σε άλλα δεδομένα για λόγους ταυτοποίησης και εξακρίβωσης στοιχείων.
- Οι ψηφιακές υπογραφές είναι ηλεκτρονικές υπογραφές που συνδέονται με τα υπογεγραμμένα δεδομένα με τέτοιο τρόπο ώστε οποιαδήποτε επέμβαση να μπορεί να γίνει αντιληπτή, αλλά και να μπορεί επίσης να αναγνωριστεί ο αποστολέας πέρα από κάθε αμφιβολία
- Η ψηφιακή υπογραφή είναι μία ακολουθία χαρακτήρων άμεσα συσχετισμένη με το περιεχόμενο του μηνύματος και την ταυτότητα αυτού που το υπογράφει. Αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί, ελέγχοντας την υπογραφή, να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι
- «Η ψηφιακής μορφής υπογραφή σε δεδομένα ή λογικά συνεχιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη υπογραφής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή α) συνδέεται μονοσήμαντα με τον υπογράφοντα, β) ταυτοποιεί τον υπογράφοντα, γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του και δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε αλλοίωση των εν λόγω δεδομένων» (Π.Δ. 150/2001 Προσαρμογή στην Οδηγία 99/93/ΕΚ)

Προκύπτει από τους παραπάνω ενδεικτικούς ορισμούς πως η ψηφιακή υπογραφή παρέχει εγγύηση της αυθεντικότητας και της μη αλλοίωσης του περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά. Επιπλέον, έχει επιβεβαιωτική λειτουργία, καθώς εξασφαλίζει ότι το μήνυμα που λαμβάνει ο παραλήπτης ανήκει όντως στον αποστολέα

και ότι είναι ακέραιο, αλλά και εμπιστευτική λειτουργία, καθώς μόνο ο παραλήπτης είναι σε θέση να διαβάσει το μήνυμα και κανένας άλλος.

Ειδικότερα, οι βασικές λειτουργίες των ψηφιακών υπογραφών αποτελούν συνάμα και τους σημαντικότερους λόγους για την εφαρμογή τους στην ηλεκτρονική επικοινωνία. Οι λειτουργίες αυτές είναι:

- Εμπιστευτικότητα (Confidentiality): Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους.

- Ακεραιότητα (Integrity): Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους.

- Μη Άρνηση Αποδοχής (Non-Repudiation): Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας. Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. Η ασύμμετρη κρυπτογραφία παρέχει ηλεκτρονικές υπογραφές, κατά συνέπεια μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει τη συγκεκριμένη υπογραφή. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά ο παραλήπτης του μηνύματος, μπορεί να επιβεβαιώσει την ηλεκτρονική υπογραφή του αποστολέα.

- Πιστοποίηση (Authentication): Πρόκειται για την επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Κάθε χρήστης που επιθυμεί να επιβεβαιώσει την ταυτότητα ενός άλλου προσώπου με το οποίο επικοινωνεί, βασίζεται στην πιστοποίηση.

Σύγκριση ψηφιακών – χειρόγραφων υπογραφών

Η ψηφιακή υπογραφή υπηρετεί τους ίδιους σκοπούς ύπαρξης με αυτούς της ιδιόχειρης. Παρόλα αυτά, υπάρχουν μεταξύ τους διαφοροποιήσεις, οι οποίες επιγραμματικά συνοψίζονται στον παρακάτω πίνακα:

Ιδιόχειρη υπογραφή	Ψηφιακή υπογραφή
Ενσωματωμένη στο μήνυμα	Εξωτερικό «αντικείμενο» το οποίο συνδέεται με το μήνυμα
Για όλους τους σκοπούς χρησιμοποιείται η ίδια υπογραφή	Διαφορετικές υπογραφές για διαφορετικούς σκοπούς
Δυνατή η πλαστογράφηση	Σχεδόν αδύνατη η «πλαστογράφηση»
Πιστοποιεί την ταυτότητα του υπογράφοντος	Πιστοποιεί τη γνησιότητα του περιεχομένου της πληροφορίας και την ταυτότητα του υπογράφοντος
Απευθείας ορατή	Απαιτείται ειδικό λογισμικό για να δημιουργηθεί και κατά συνέπεια για να είναι ορατή
Ο «μηχανισμός» δημιουργίας της παραμένει ο ίδιος και δεν μπορεί να αποσυρθεί	Ο μηχανισμός δημιουργίας, επαλήθευσής της μπορεί να καταστραφεί (αποσυρθεί) και να υποκατασταθεί από κάποιον εντελώς διαφορετικό

Σε αντιδιαστολή λοιπόν, με την ιδιόχειρη υπογραφή, το ακριβές περιεχόμενο της ηλεκτρονικής υπογραφής διαφοροποιείται ανάλογα με τα προς υπογραφή δεδομένα αφού προκύπτει με βάση και αυτά. Η ψηφιακή υπογραφή σε ένα ηλεκτρονικό κείμενο δεν είναι παρά μια σειρά από bits, προσαρτημένη σε αυτό, τα οποία μπορούν να χρησιμοποιηθούν για την αναγνώριση του υπογράφοντος και την επαλήθευση της ακεραιότητας του μηνύματος.

Δημιουργία ψηφιακής υπογραφής

Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: α) τη δημιουργία της υπογραφής και β) την επαλήθευσή της. Κατά τη δημιουργία μιας ψηφιακής υπογραφής δεν κρυπτογραφούνται τα προς υπογραφήν δεδομένα, αλλά μία μικρή μαθηματική «σύνοψή» (message digest) τους, η οποία παράγεται από την χρήση μονόδρομων αλγορίθμων κατακερματισμού δεδομένων (one-way hashing algorithms). Για κάθε μήνυμα λοιπόν, και ανεξαρτήτως του μεγέθους του, δημιουργείται μια σύνοψή του, που είναι μια σειρά από bits με συγκεκριμένο πλήθος.

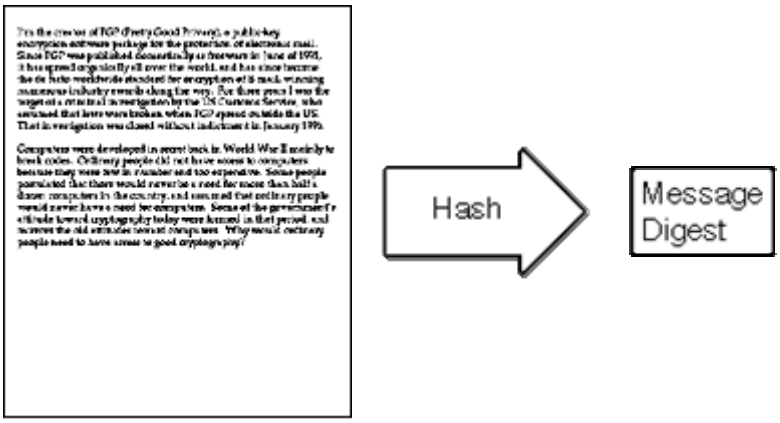
Σύνοψη Μηνύματος (Message digest)

Η σύνοψη του μηνύματος αποτελεί την ψηφιακή αναπαράστασή του μηνύματος και είναι μοναδική για το μήνυμα που αντιπροσωπεύει. Αν αλλάξουμε έστω και μια τελεία στο μήνυμα, θα αλλάξει και η σύνοψή του, ενώ είναι πρακτικά αδύνατο δύο διαφορετικά μηνύματα να δώσουν την ίδια σύνοψη. Η μεγάλη αυτή ευαισθησία στα δεδομένα εισόδου αποτελεί μια από τις πολυτιμότερες ιδιότητες (δυνατότητες) των συναρτήσεων hash. Είναι επίσης πρακτικά αδύνατο να ανακτήσουμε το αρχικό μήνυμα αν γνωρίζουμε τη σύνοψή του.

Αυτή η σύνοψη των δεδομένων, κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντα και επισυνάπτεται (πιθανώς μαζί και με άλλες χρήσιμες σχετικές πληροφορίες, π.χ. χρησιμοποιούμενοι αλγόριθμοι, εφαρμοζόμενη πολιτική υπογραφής, κ.ά.), στα αρχικά δεδομένα, αποτελώντας την προηγμένη ηλεκτρονική υπογραφή ή ψηφιακή υπογραφή.

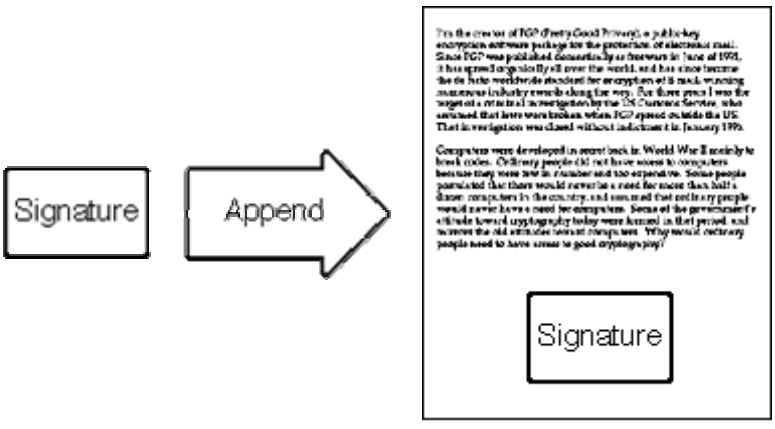
Συνοψίζοντας τα παραπάνω, τα βήματα που εντάσσονται στη δημιουργία της ψηφιακής υπογραφής είναι:

1. Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει.

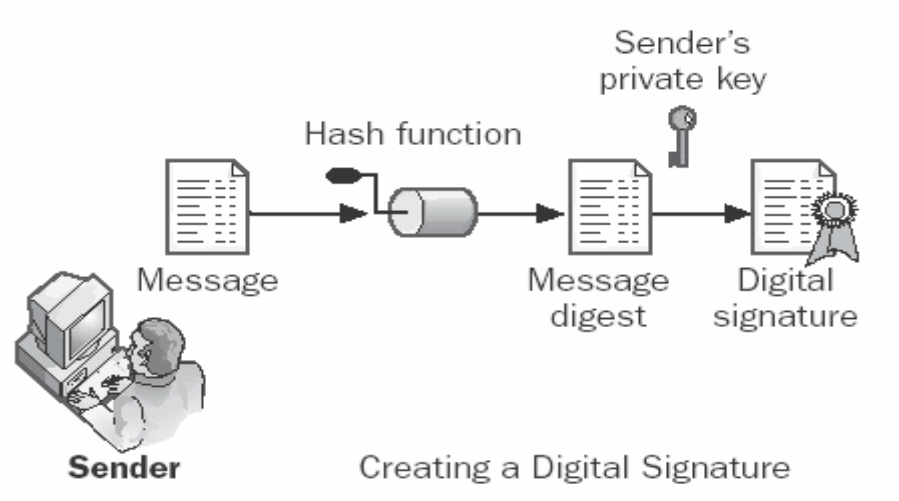


2. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη που έχει δημιουργηθεί. Αυτό που παράγεται είναι η ψηφιακή υπογραφή.

3. Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου

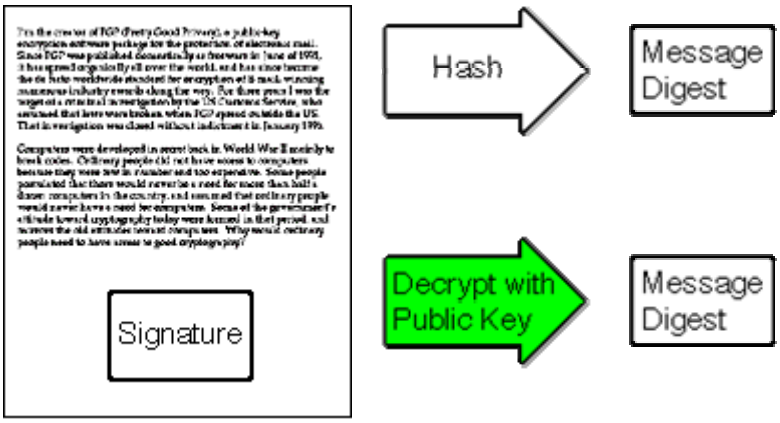


Γραφική αναπαράσταση της διαδικασίας δημιουργίας ψηφιακής υπογραφής αποτελεί η παρακάτω εικόνα:



Επαλήθευση ψηφιακής υπογραφής

Κατά τη διαδικασία της επαλήθευσης (verification) μιας ψηφιακής υπογραφής, εφαρμόζεται στο κανονικό κείμενο ο ίδιος αλγόριθμος κατακερματισμού που χρησιμοποιήθηκε κατά την υπογραφή του και δημιουργείται κατά αυτόν τον τρόπο μια νέα σύνοψη. Κατόπιν, αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα η κρυπτογραφημένη σύνοψη του μηνύματος. Έτσι, η νέα σύνοψη που παράγεται, συγκρίνεται με την αντίστοιχη σύνοψη που προέρχεται από την αποκρυπτογράφηση της ψηφιακής υπογραφής. Εάν ταυτίζονται οι δύο συνόψεις, τότε η υπογραφή επαληθεύεται και επιβεβαιώνεται αφενός μεν ότι τα δεδομένα υπογράφηκαν από τον κάτοχο του σχετικού ιδιωτικού κλειδιού, αφετέρου δε ότι τα αρχικά δεδομένα δεν έχουν αλλοιωθεί.



Συνοπτικά τα βήματα που περιλαμβάνονται στη διαδικασία επαλήθευσης της ψηφιακής υπογραφής είναι:

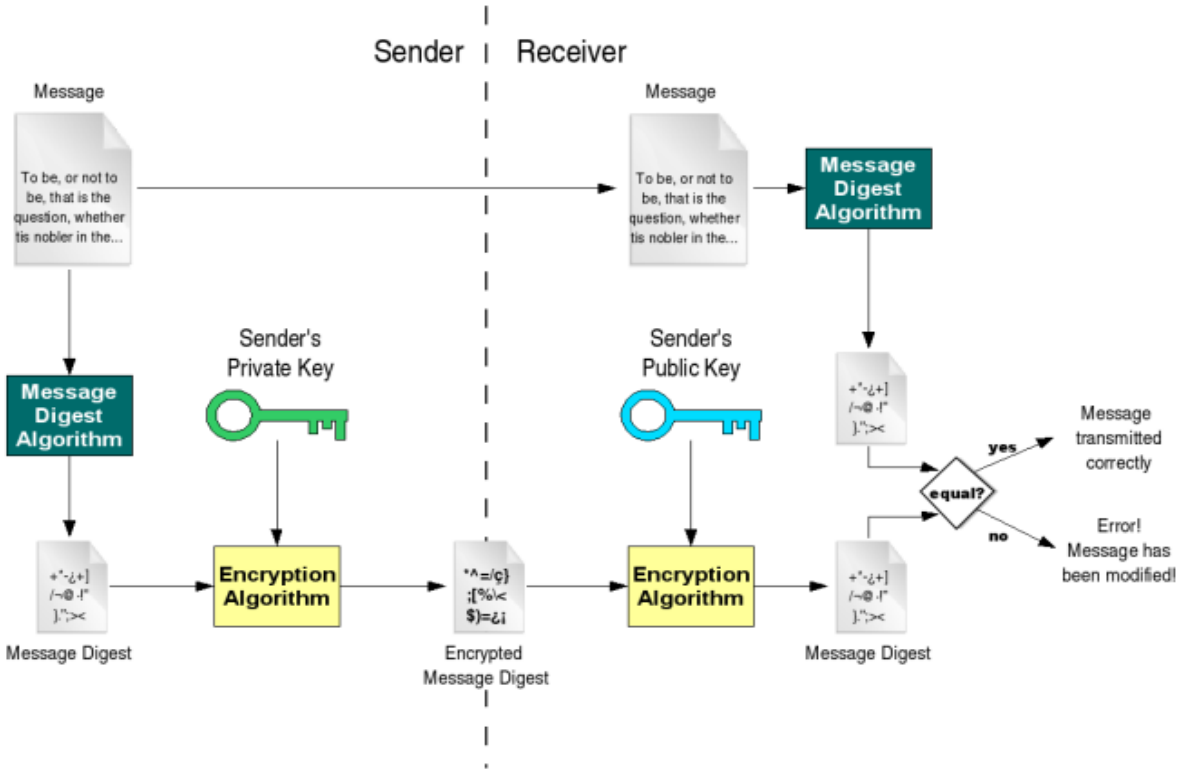
1. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή (κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη).

2. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, ο παραλήπτης δημιουργεί τη σύνοψη του μηνύματος.

3. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

4. Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.

Ο κύκλος από τη δημιουργία έως την επαλήθευση της ψηφιακής υπογραφής απεικονίζεται στην παρακάτω εικόνα:



Πιστοποίηση ψηφιακής υπογραφής

Με τη λήψη ενός μηνύματος με ψηφιακή υπογραφή, ο παραλήπτης επαληθεύοντας την βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης, όμως, πρέπει να είναι βέβαιος ότι ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Απαιτείται δηλαδή να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την 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 που κατέχει το δημόσιο κλειδί.

Ο Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) είναι ένας «οργανισμός», ο οποίος παρέχει μεταξύ άλλων την υπηρεσία εκείνη 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 (ηλεκτρονικό αρχείο), στο οποίο ο ΠΥΠ πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του. Η υποδομή με την οποία ένας ΠΥΠ εκδίδει, υπογράφει, δημοσιεύει και υποστηρίζει τυποποιημένες ηλεκτρονικές βεβαιώσεις (πιστοποιητικά) για τα κρυπτογραφικά κλειδιά των συνδρομητών του ονομάζεται Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure – PKI).

Ειδικότερα, το ψηφιακό αυτό πιστοποιητικό αναφέρει το δημόσιο κλειδί 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.

Σκοπός είναι:

- η ταυτοποίηση του υπογράφοντος, δηλαδή η σύνδεση της ηλεκτρονικής συναλλαγής με το φυσικό πρόσωπο που υπογράφει,
- η εγγύηση της γνησιότητας των ψηφιακών δεδομένων και
- η δέσμευση του υπογράφοντος ως προς την ηλεκτρονική συναλλαγή, δηλαδή ο υπογράφων δεν μπορεί να αρνηθεί την συμβολή του στην εν λόγω συναλλαγή.

Τα αναγνωρισμένα πιστοποιητικά πρέπει σύμφωνα με το Παράρτημα Ι του Π.Δ. 150/2001 να περιλαμβάνουν:

α) ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό,

β) τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος, στο οποίο είναι εγκατεστημένος,

γ) το όνομα του υπογράφοντος,

δ) πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό,

ε) δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος,

στ) ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού,

ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού,

η) την προηγμένη ηλεκτρονική υπογραφή του παρόχου των υπηρεσιών πιστοποίησης που το εκδίδει,

θ) τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού, και

ι) τυχόν όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

Επειδή τα πιστοποιητικά δημοσίων κλειδιών (public key certificates) που εκδίδει ένας ΠΥΠ προς τις ενδιαφερόμενους τελικούς χρήστες, είναι και αυτά μια μορφή ηλεκτρονικών εγγράφων, επιβάλλεται να φέρουν και αυτά την ψηφιακή υπογραφή του εκδότη τους. Αυτό προϋποθέτει ότι και ο ίδιος ο Εκδότης-ΠΥΠ διαθέτει το δικό του ζεύγος κρυπτογραφικών κλειδιών υπογραφής, το οποίο πρέπει εξίσου να υποστηρίζεται από σχετικό πιστοποιητικό δημοσίου κλειδιού -που κι αυτό, με την σειρά του, πρέπει να είναι υπογεγραμμένο ψηφιακά. Η σχηματιζόμενη αλληλουχία (αλυσίδα) πιστοποιητικών τερματίζεται με ένα τελικό και αξιόπιστα δημοσιευμένο αυτοϋπογραφόμενο πιστοποιητικό (self-signed certificate) που εκδίδεται από τον «Θεμελιώδη Εκδότη Πιστοποιητικών» (Root Certification Authority ή Root CA) του ΠΥΠ και το οποίο αποτελεί την κορυφή της πυραμίδας.

Λόγω της διαρκούς τεχνολογικής εξέλιξης, θεωρείται δεδομένη η εξασθένηση της ασφάλειας των χρησιμοποιούμενων κρυπτογραφικών κλειδιών στο πέρασμα του χρόνου. Έτσι, τα πιστοποιητικά δημοσίου κλειδιού, εκδίδονται με περιορισμένη διάρκεια ισχύος (συνήθως 1 έως 3 έτη). Εκτός όμως από την προγραμματισμένη λήξη, η ισχύς ενός πιστοποιητικού μπορεί οποτεδήποτε να ανακληθεί οριστικά (revocation) ή να ανασταλεί προσωρινά (suspension), ύστερα από αίτημα του ίδιου του τελικού χρήστη (π.χ. επειδή έχασε τον φορέα των κρυπτογραφικών κλειδιών του) ή/και από σχετική απόφαση του Εκδότη τους (π.χ. λόγω λάθους στην αναγραφή στοιχείων). Η ανάκληση και η αναστολή ενός πιστοποιητικού πραγματοποιείται με την εγγραφή του σειριακού αριθμού του πιστοποιητικού (certificate’s serial number) σε μια «Λίστα Ανακληθέντων Πιστοποιητικών» (Certificate Revocation List ή ‘CRL’) η οποία υπογράφεται και δημοσιεύεται σε τακτά χρονικά διαστήματα από τον ίδιο τον Εκδότη των πιστοποιητικών.

Τις εταιρείες που παρέχουν υπηρεσίες πιστοποίησης αλλά και βεβαιώσεις για την ασφάλεια της ψηφιακής υπογραφής ελέγχει στην Ελλάδα, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), η οποία διαπιστώνει εάν οι συγκεκριμένες εταιρείες είναι σε θέση να παρέχουν υπηρεσίες πιστοποίησης.

Υπηρεσίες Παροχών Πιστοποίησης

Όπως προαναφέρθηκε, οι Παροχείς Υπηρεσιών Πιστοποίησης εκδίδουν τα πιστοποιητικά με στόχο τη δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημόσιου κλειδιού και του δικαιούχου του, προβαίνοντας παράλληλα και στην οργάνωση μιας αξιόπιστης «Υποδομής Δημόσιου κλειδιού», (PKI Public Key Infrastructure) για την έκδοση, διάθεση και διαχείριση των σχετικών πιστοποιητικών.

Κατά συνέπεια, οι Παροχείς Υπηρεσιών Πιστοποίησης προσφέρουν μια σειρά από υπηρεσίες, που δεν περιορίζονται στην έκδοση του πιστοποιητικού, αλλά αφορούν στον «κύκλο ζωής» του. Οι υπηρεσίες αυτές είναι:

1) Υπηρεσία εγγραφής (Registration Authority). Παραλαμβάνει τις αιτήσεις και τα δικαιολογητικά για την έκδοση του πιστοποιητικού και είναι υπεύθυνη για τη συλλογή των πληροφοριών που αποτελούν το απαραίτητο περιεχόμενο του πιστοποιητικού. Τις πληροφορίες αυτές, που είναι απαραίτητες για την ταυτοποίηση του κατόχου των δεδομένων δημιουργίας με τον αιτούντα το πιστοποιητικό, τις μεταβιβάζει στη συνέχεια στην υπηρεσία έκδοσης των πιστοποιητικών.
2) Υπηρεσία έκδοσης πιστοποιητικών (Certification Authority). Εκδίδει το πιστοποιητικό σύμφωνα με τη «Δήλωση Πρακτικής Πιστοποίησης».
3) Υπηρεσία δημοσίευσης και διανομής (Dissemination Service). Δημοσιεύει τον κατάλογο με τα εκδοθέντα πιστοποιητικά, τους ιδιαίτερους όρους χρήσης του κάθε είδους πιστοποιητικού (Πολιτικές Πιστοποιητικών) καθώς και τη δήλωση Πρακτικής Πιστοποίησης, με τρόπο που να τις καθιστά προσβάσιμες σε κάθε ενδιαφερόμενο.

4) Υπηρεσία διαχείρισης και δημοσίευσης ανάκλησης (Revocation Management and Status Service). Διαχειρίζεται τον κατάλογο με τα υπό έκδοση ή εκδοθέντα πιστοποιητικά. Δέχεται και ελέγχει αιτήματα ανάκλησης ή παύσης των πιστοποιητικών και προβαίνει στην έγκαιρη ενημέρωση της «Λίστας Ανακληθέντων Πιστοποιητικών».

Ψηφιακή υπογραφή και νομικό πλαίσιο

Η νομική αναγνώριση των ψηφιακών υπογραφών σε διεθνές επίπεδο, ξεκίνησε από τα μέσα της προηγούμενης δεκαετίας με την θέσπιση σχετικών νόμων σε διάφορα κράτη.

Η Ευρωπαϊκή Ένωση, με την Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 «Σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές» (EEL 13/19.1.2000) αναγνωρίζει γενικά ως ηλεκτρονικές υπογραφές -οι οποίες μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε νομικές διαδικασίες (ά. 5§2 της Οδηγίας)-, όλα τα: «δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε, ή λογικά συσχετιζόμενα με, άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας» (ά. 2§1 της Οδηγίας).

Η ίδια οδηγία διακρίνει επίσης μία συγκεκριμένη κατηγορία ηλεκτρονικών υπογραφών, αποκαλούμενες ως αναγνωρισμένες ηλεκτρονικές υπογραφές, στην οποία κατηγορία αποδίδει πλήρη και άμεση νομική ισοδυναμία με τις ιδιόχειρες υπογραφές, σύμφωνα με το ισχύον δίκαιο του κάθε κράτους μέλους. Σε αυτήν την κατηγορία ανήκουν όλες οι: «προηγμένες ηλεκτρονικές υπογραφές που, επιπλέον, βασίζονται σε αναγνωρισμένο πιστοποιητικό και δημιουργούνται από ασφαλή διάταξη δημιουργίας υπογραφής» (ά. 5§1).

Στην Ελλάδα, η πρώτη νομοθετική πρόβλεψη για ψηφιακές υπογραφές (οι οποίες ταυτίζονται εννοιολογικά με τις προηγμένες ηλεκτρονικές υπογραφές της Οδηγίας) γίνεται ήδη από το άρθρο 14 του ν. 2672/98 όπου παρέχεται μια αρχική, αλλά περιορισμένη αναγνώρισή τους σε διαδικασίες του δημόσιου τομέα. Ειδικότερα, στις παραγράφους 19 και

22 του άρθρου 14 αναφέρονται τα εξής: Παράγραφος 19: «Με προεδρικό διάταγμα, που εκδίδεται με πρόταση των Υπουργών Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, Οικονομικών, Ανάπτυξης και Μεταφορών και Επικοινωνιών, καθορίζονται οι προϋπόθεσεις και η διαδικασία έκδοσης, διακίνησης, διαχείρισης και διασφάλισης της ψηφιακής υπογραφής, οι προϋπόθεσεις παροχής και το περιεχόμενο των υπηρεσιών πιστοποίησης, οι τεχνικοί κανόνες για την κατάρτιση, την αποστολή, τη διατήρηση, την αντιγραφή και την αναπαραγωγή των μηνυμάτων ηλεκτρονικού ταχυδρομείου, την εγγύηση ακεραιότητας, διάθεσης και διατήρησης των πληροφοριών που περιέχονται στο μήνυμα καθώς και κάθε άλλη αναγκαία λεπτομέρεια. Με το ίδιο προεδρικό διάταγμα μπορεί να καθορίζονται και οι κατηγόριες μηνυμάτων τα οποία έχουν ισχύ και χωρίς να φέρουν ψηφιακή υπογραφή. Παράγραφος 22: «Η ψηφιακή υπογραφή επιφέρει τα αποτελέσματα της ιδιόχειρης υπογραφής, και την κείμενη νομοθεσία. Το μήνυμα ηλεκτρονικού ταχυδρομείου που φέρει ψηφιακή υπογραφή σύμφωνα με το προεδρικό διάταγμα της παραγράφου 19 έχει τη αποδεικτική ισχύ εγγράφου κατά τους ορισμούς του Κώδικα Πολιτικής Δικονομίας και κάθε άλλης σχετικής διάταξης»

Ακολούθησε το π.δ. 150/2001 (ΦΕΚ Α'/125 25-6-2001) το οποίο εναρμόνισε το εθνικό μας δίκαιο με την Οδηγία 99/93/ΕΚ και καθόρισε την Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ) ως αρμόδια αρχή για την εποπτεία των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης ηλεκτρονικής υπογραφής. Σύμφωνα με το ίδιο Προεδρικό Διάταγμα, η ηλεκτρονική υπογραφή εξομοιώνεται με την ιδιόχειρη κάτω από αυστηρές προϋποθέσεις που θα εξασφαλίζουν την ταυτοπροσωπία αλλά και τη μοναδικότητα του φορέα της ηλεκτρονικής υπογραφής. Ο κάθε χρήστης θα μπορεί να εφοδιασθεί με τη δική του «ηλεκτρονική υπογραφή», μέσω διαπιστευμένων προς τον σκοπό αυτό εταιρειών, σε μορφή λογισμικού software, καθώς και μ' έναν μυστικό κωδικό αριθμό (PIN) για να είναι δυνατή η πρόσβαση στην ηλεκτρονική υπογραφή. Το software αυτό θα μπορεί να εγκατασταθεί στον προσωπικό υπολογιστή του χρήστη ώστε να βάζει την ψηφιακή υπογραφή του όταν χρειασθεί ή θα μπορεί να το έχει μαζί του αποθηκευμένο σε μια μνήμη USB flash ώστε να μπορεί να το χρησιμοποιεί και από άλλους υπολογιστές.

Τον Οκτώβριο του 2002, εκδόθηκε το π.δ. 342/02 το οποίο προσδιορίζει περαιτέρω κάποιους όρους για τη διακίνηση ψηφιακά υπογεγραμμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου στις επικοινωνίες του δημόσιου τομέα.

Τέλος, στο πλαίσιο άσκησης των σχετικών αρμοδιοτήτων της, η ΕΕΤΤ έχει εκδώσει έναν γενικό «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής», καθώς και τρεις Κανονισμούς σχετικά με την Εθελοντική Διαπίστευση των ΠΥΠ, την Διαπίστωση (της συμμόρφωσης με τις απαιτήσεις της Οδηγίας) βασικών προϊόντων ηλεκτρονικής υπογραφής και τον ορισμό των φορέων που θα προβαίνουν σε σχετικούς ελέγχους και διαπιστεύσεις για λογαριασμό της ΕΕΤΤ.

Ψηφιακές υπογραφές - υδατογραφημάτα (watermarks)

Όπως έχει αναφερθεί παραπάνω, η ραγδαία εξάπλωση και ευρύτατη διεισδύση του Διαδικτύου (Internet) σε ποικίλους χώρους της κοινωνικής δραστηριότητας είχε σαν αποτέλεσμα την ανάπτυξη συνόλου μηχανισμών προστασίας για τη διαφύλαξη της ασφάλειας των συναλλαγών, της κατοχύρωσης των πνευματικών δικαιώματων στα διακινούμενα ψηφιακά αντικείμενα. Εκτός από τις ψηφιακές υπογραφές και την κρυπτογραφία έννοιες όπως η στεγανογραφία, η υδατογράφηση αναφέρονται στη βιβλιογραφία ως μέθοδοι προστασίας των πνευματικών δικαιώματων στον ψηφιακό κόσμο. Κρίθηκε λοιπόν απαραίτητη, για την αποφυγή συγχύσεων η συνοπτική παράθεση των τεχνικών αυτών, και η αποσαφήνιση πιθανών μεταξύ τους διαφορών.

Η στεγανογραφία επιτρέπει την κρυφή επικοινωνία, συνήθως κρύβοντας τις πληροφορίες σε άλλα δεδομένα υπεράνω υποψίας. Βασίζεται στην υπόθεση ότι η ύπαρξη κρυφής επικοινωνίας είναι άγνωστη σε τρίτους και χρησιμοποιείται κυρίως στην κρυφή σημείο-προς-σημείο επικοινωνία ανάμεσα σε έμπιστα μέρη. Ως εκ τούτου, οι κρυφές πληροφορίες δε μπορούν να ανακτηθούν μετά από παραποίηση των δεδομένων.

Σε αντίθεση με την κρυπτογράφηση, όπου επιτρέπεται στον "εχθρό" να ανιχνεύσει και να παρεμβληθεί ή να αιχμαλωτίσει την πληροφορία, ο στόχος της στεγανογραφίας είναι να κρύψει την πληροφορία μέσα σε άλλη

"αθώα" πληροφορία με τέτοιο τρόπο που δεν αφήνει περιθώρια στον "εχθρό" ούτε να ανιχνεύσει την ύπαρξή της.

Συμπερασματικά, θα μπορούσαμε να αναφέρουμε ότι η στεγανογραφία επιδιώκει την απόκρυψη της πληροφορίας χωρίς να λαμβάνει υπόψη το ενδεχόμενο επίθεσης σε αυτήν, προφυλάσσοντάς την μέσα σε κάποιο "στεγανό". Η κρυπτογραφία εξασφαλίζει ότι η πληροφορία που θα διαβαστεί από μη εξουσιοδοτημένους χρήστες θα είναι άχρηστη και ακατανόητη ή παραπλανητική. Η κρυπτογραφία επίσης, προστατεύει ένα προϊόν υπό μεταφορά, αλλά μόλις αποκρυπτογραφηθεί, το περιεχόμενο είναι ευάλωτο.

Η υδατογράφηση (watermarking) έχει την ιδιότητα προστασίας του περιεχομένου και μετά την αποκρυπτογράφηση του, τοποθετώντας την πληροφορία μέσα στο περιεχόμενο, απ’ όπου δεν αφαιρείται ποτέ κατά την κανονική χρήση. Ακόμα κι αν η ύπαρξη κρυφών πληροφοριών είναι γνωστή, είναι δύσκολο -ιδανικά αδύνατο- να καταστραφεί το ένθετο υδατογράφημα.

Συμπεράσματα

Η ευρύτατη διείσδυση της τεχνολογίας σε όλους τους τομείς του κοινωνικού γίγνεσθαι, κάνει επιτακτική περισσότερο από ποτέ την ανάπτυξη μηχανισμών και μεθόδων προστασίας για την ασφαλή διακίνηση των ψηφιακών «αντικειμένων». Η ανάγκη προστασίας του απαραβίαστου του απορρήτου, στο σύγχρονο ψηφιακό περιβάλλον προκύπτει περισσότερο καθοριστική από ποτέ. Ειδικότερα, καθώς το Διαδίκτυο αποτελεί σήμερα το σημαντικότερο εκφραστικό μέσο της ελευθερίας στην επικοινωνία των ανθρώπων, θα πρέπει να αναπτυχθούν μηχανισμοί προστασίας και ασφάλειας, από εκείνους που επιβουλεύονται την ελευθερία αυτή.

Η δημιουργία των ψηφιακών υπογραφών, βασιζόμενη στη τεχνολογία της κρυπτογραφίας, αποτελεί μια διαδεδομένη μέθοδο, προστασίας και ασφαλείας στη διακίνηση των ηλεκτρονικών εγγράφων. Συμπερασματικά, κρίνεται σκόπιμο να αναφερθεί ότι η ψηφιακή υπογραφή, παρέχει εγγύηση της αυθεντικότητας, της ακεραιότητας, της μη αλλοίωσης

του περιεχομένου των μηνυμάτων που διακινούνται ηλεκτρονικά. Ωστόσο, όπως προαναφέρθηκε, η ψηφιακή υπογραφή προστατεύει ένα προϊόν υπό μεταφορά, αλλά μόλις αποκρυπτογραφηθεί, το περιεχόμενο είναι ευάλωτο. Κατά συνέπεια, προκύπτει πως η ιδανικότερη λύση για την ασφαλή διακίνηση αλλά και χρήση των ψηφιακών αντικειμένων είναι ο συνδυασμός των αναπτυγμένων μεθόδων προστασίας. Η προσθήκη δηλαδή ψηφιακής υπογραφής και υδατογραφήματος στα διακινούμενα ηλεκτρονικά έγγραφα, αποτελούν ενδεδειγμένο τρόπο, για την προστασία του εγγράφου τόσο κατά την μεταφορά του, όσο και κατά τη χρήση του.

Βιβλιογραφία

1. Wikipedia, The Free Encyclopedia, *History of Cryptography* http://en.wikipedia.org/wiki/History_of_cryptography, Ημερ. Πρόσβασης 05/02/2006

2. *Εισαγωγή στην κβαντική κρυπτογραφία: Ιστορική αναδρομή*, http://www.geocities.com/kzerzel/history.htm Ημερ. Πρόσβασης 05/02/2006

3. Cypher Research Laboratories, *A brief history of cryptography* http://www.cypher.com.au/crypto_history.htm Ημερ. Πρόσβασης 05/02/2006

4. Wikipedia, The Free Encyclopedia, *Digital Signature*, http://en.wikipedia.org/wiki/Digital_signature Ημερ. Πρόσβασης 05/02/2006

5. Η-επιχειρείν, *Ψηφιακή υδατογράφηση*, http://www.go-online.gr/ebusiness/specials/article.html?article_id=618, Ημερ. Πρόσβασης 05/02/2006

6. Εθνική Συνομοσπονδία Ελληνικού Εμπορίου, *Προεδρικό Διάταγμα υπ' αριθ. 150*, Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές http://www.esee.gr/el/Emporio/DedomenaProsopikouXaraktira/Proedriko-Diatagma-150.shtml, Ημερ. Πρόσβασης 05/02/2006

7. David Youd, *What is a Digital Signature?* http://www.youdzone.com/signature.html, Ημερ. Πρόσβασης 05/02/2006

8. The Official Website of the State of Utah, Utah Department of Commerce, *Digital Signature Tutorial*, http://www.commerce.state.ut.us/digsig/tutorl.htm Ημερ. Πρόσβασης 05/02/2006

9. American Bar Association, Section of Science and Technology Information Security Committee, *Digital Signature Guidelines Tutorial,* http://www.abanet.org/scitech/ec/isc/dsg.pdf, Ημερ. Πρόσβασης 05/02/2006

10. Sandy Shaw, Computing Services, The University of Edinburgh, *JISC Technology Applications Programme (JTAP) — Overview of Watermarks, Fingerprints, and Digital Signatures* http://www.jisc.ac.uk/uploaded_documents/jtap-034.doc, Ημερ. Πρόσβασης 05/02/2006

11. *Public key cryptography, Fundamental Security Concepts* http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html Ημερ. Πρόσβασης 05/02/2006

12. Ricky M. Magalhaes, *Digital Signatures*, http://www.windowsecurity.com/articles/Digital_Signatures.html Ημερ. Πρόσβασης 05/02/2006

13. Η-επιχειρείν, *Η υποδομή δημοσίου κλειδιού και η κρυπτογράφηση στην πράξη*, http://www.go-online.gr/ebusiness/specials/article.html?article_id=714 Ημερ. Πρόσβασης 05/02/2006

14. *Η ηλεκτρονική υπογραφή στις online συναλλαγές* http://www.eone.gr/4dcgi/_w_articles_technoextrat_2_28/01/2006_83439 Ημερ. Πρόσβασης 05/02/2006

15. Κέντρο ΠΛΗ.ΝΕ.Τ Ν. Φλώρινας, *Κρυπτογραφία και ψηφιακή υπογραφή*, http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Cryptography-DigitalSignature.html Ημερ. Πρόσβασης 05/02/2006

16. Υπουργείο Ανάπτυξης, Ε.Π. Κοινωνία της Πληροφορίας, EBusinessForum, *Ηλεκτρονικές Υπογραφές και Ηλεκτρονικά Πιστοποιητικά Ταυτοποίησης (Τεχνική & Νομική προσέγγιση),* http://www.ebusinessforum.gr/index.php?op=modload&modname=Teams&action=teamsviewnewall&pageid=32 Ημερ. Πρόσβασης 05/02/2006

17. ΦΕΚ 290 - ΤΕΥΧΟΣ Α. Διακίνηση εγγράφων με ηλεκτρονικά μέσα