Κρυπτογραφία

εισαγωγικές έννοιες

*Από τον **Δημήτρη Εργαζάκη***
Σύμβουλο Ασφάλειας Πληροφοριών
ENCODE S.A.
e-mail: d.ergazakis@encode-sec.com

Η πληροφορία από τη φύση της είναι άμεσα συνυφασμένη με την έννοια του "απορρήτου". Ο βαθμός κρισιμότητας της πληροφορίας και η ανάγκη προστασίας του απορρήτού της αποτελούν μεγέθη ανάλογα. Όσο πιο κρίσιμη είναι μια πληροφορία τόσο πιο επιτακτική είναι η ανάγκη διασφάλισης του απορρήτου της. Το παραπάνω εντείνεται από το γεγονός ότι οι τρόποι (μέσα) μετάδοσης της πληροφορίας, τις περισσότερες φορές δεν είναι απόλυτα ασφαλείς. Μέσα σ' αυτό το πλαίσιο γεννήθηκε και εξελίχθηκε η κρυπτογραφία, τα πρώτα δείγματα της οποίας βρίσκονται χιλιάδες χρόνια πριν. Χαρακτηριστικό παράδειγμα αποτελεί η αποστολή κρυπτογραφημένων μηνυμάτων από τον Ιούλιο Καίσαρα προς τους στρατηγούς του λόγω της έλλειψης εμπιστοσύνης που είχε προς τους αγγελιοφόρους του.

Από εκείνη την εποχή πολλά έχουν αλλάξει, εκτός από την ανάγκη διασφάλισης του απορρήτου των προσωπικών πληροφοριών. Η αναγκαιότητα προστασίας κρίσιμων επιχειρηματικών πληροφοριών των οποίων η επεξεργασία και μετάδοση γίνονται ηλεκτρονικά έχει αυξηθεί σημαντικά τα τελευταία χρόνια. Ιδιαίτερα η χρήση του Internet ως μέσο μετάδοσης πληροφοριών τέτοιας φύσης, εντείνει την ανάγκη ασφαλών επικοινωνιών. Το ζήτημα προστασίας του απορρήτου αγγίζει πολλούς τομείς όπως η ηλεκτρονική αλληλογραφία (e-mail), η διεξαγωγή συναλλαγών (αριθμός πιστωτικής κάρτας, τραπεζικό απόρρητο), το ιατρικό απόρρητο. Σε οικονομικό επίπεδο, η προστασία των εμπορικών δεδομένων, όπως η εξασφάλιση της εγκυρότητας των συναλλαγών και η ασφάλεια των συναλλαγών είναι κρίσιμα ζητήματα τα οποία είναι άρρηκτα δεμένα με το υπόβαθρο της ψηφιακής παγκόσμιας αγοράς.

Βασικές Έννοιες της Κρυπτογραφίας

Βασικό μέλημα της κρυπτογραφίας είναι η ανταλλαγή μηνυμάτων μεταξύ δύο μερών κατά τρόπο τέτοιο που να καθιστά δυνατή την κατανόηση του περιεχομένου των μηνυμάτων αυτών αποκλειστικά και μόνο από τον αποστολέα και τον παραλήπτη. Το αρχικό μήνυμα ονομάζεται "καθαρό κείμενο" (plaintext ή cleartext), η διαδικασία παραμόρφωσης του αρχικού μηνύματος

ώστε να μην είναι κατανοητό ονομάζεται "κρυπτογράφηση" (encryption), το κρυπτογραφημένο μήνυμα ονομάζεται "κρυπτογράφημα" (ciphertext), ενώ η διαδικασία ανάκτησης του αρχικού μηνύματος από το κρυπτογράφημα ονομάζεται "αποκρυπτογράφηση" (decryption). Η κρυπτογράφηση και αποκρυπτογράφηση συνήθως κάνουν χρήση κάποιου κλειδιού (key). Η κωδικοποίηση του μηνύματος είναι τέτοια ώστε η αποκρυπτογράφηση να μπορεί να υλοποιηθεί μόνο εάν είναι γνωστό το κατάλληλο κλειδί. Η διαδικασία απεικονίζεται διαγραμματικά στο σχήμα 1.

Η κρυπτογραφία (cryptography) είναι η επιστήμη η οποία με τη χρήση μαθηματικών κωδικοποιεί και αποκωδικοποιεί δεδομένα προκειμένου να διατηρήσει τα μηνύματα ασφαλή. Κρυπτανάλυση (cryptanalysis) είναι η επιστήμη του σπασίματος κρυπτογραφικών αλγόριθμων (ciphers). Τέλος, κρυπτολογία (cryptology) είναι το γνωστικό αντικείμενο των μαθηματικών που μελετά τη μαθηματική θεμελίωση των κρυπτογραφικών μεθόδων, και συμπεριλαμβάνει την κρυπτογραφία και την κρυπτανάλυση. Η κρυπτογραφία με τη χρήση μαθηματικών τεχνικών προσπαθεί να διασφαλίσει: την εμπιστευτικότητα της πληροφορίας (confidentiality), την ακεραιότητα των δεδομένων (data integrity), την αυθεντικοποίηση (authentication), και την μηάρνηση ενεργειών των εμπλεκόμενων μερών (non-repudiation).

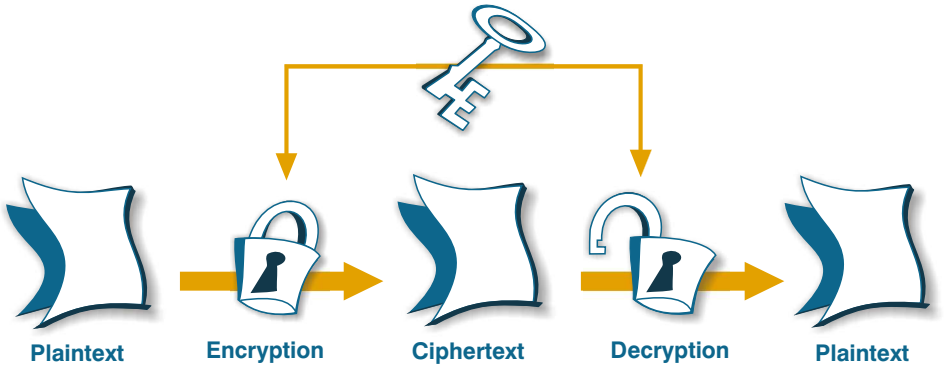
Είναι γεγονός ότι η κρυπτογραφία εξελίχθηκε μέσα στα πλαίσια επιχειρήσεων στρατιωτικής και διπλωματικής φύσης. Το "σπάσιμο" του τηλεγραφήματος του Zimmerman το 1917, ήταν καθοριστικό για την εμπλοκή των ΗΠΑ στον Α΄ παγκόσμιο πόλεμο, ενώ η πορεία του Β' παγκοσμίου πολέμου επηρεάστηκε σημαντικά από τους Άγγλους και Πολωνούς κρυπταναλυτές οι οποίοι "έσπασαν" κρυπταλγορίθμους των Γερμανών κατορθώνοντας να αποκομίσουν σημαντικές πληροφορίες.

Συμμετρική & Ασύμμετρη Κρυπτογραφία

Όλοι οι καθιερωμένοι κρυπτογραφικοί αλγόριθμοι στις ημέρες μας, χρησιμοποιούν ένα κλειδί για να παραμετροποιήσουν την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων[1]. Αυτό το κλειδί μπορεί να έχει μια τιμή, μέσα από ένα ευρύ φάσμα πιθανών τιμών. Το εύρος των πιθανών τιμών του κλειδιού ονομάζεται πεδίο τιμών (keyspace). Σε πολλούς αλγόριθμους το κλειδί που χρησιμοποιείται για αποκρυπτογράφηση είναι διαφορετικό από το κλειδί κρυπτογράφησης. Ουσιαστικά, τα κρυπτογραφικά συστήματα μπορούν διαχωριστούν σε δύο βασικές κατηγορίες: **συμμετρικά, συμβατικά** ή **μυστικού-κλειδιού** (symmetric, conventional, ή secret-key) στα οποία το κλειδί αποκρυπτογράφησης μπορεί να υπολογιστεί εάν γνωρίζουμε το κλειδί κρυπτογράφησης, και **ασυμμετρικά** ή **δημοσίου-κλειδιού**

Σχήμα 1: Διαδικασία Κρυπτογράφησης & Αποκρυπτογράφησης

1. Από τον 19ο αιώνα που θεμελιώθηκε μαθηματικά η κρυπτογραφία ήταν γνωστό ότι οι αλγόριθμοι κρυπτογράφησης δεν είναι αναγκαίο να είναι μυστικοί. Αρκούσε ο αλγόριθμος να μπορεί να παραμετροποιηθεί μέσω της χρήσης ενός κλειδιού και το κλειδί αυτό να παραμένει μυστικό. Έτσι η όλη ασφάλεια του συστήματος έγκειται στη μυστικότητα του κλειδιού αυτού.



Σχήμα 2: Συμμετρική Κρυπτογραφία

(asymmetric, ή public-key) στα οποία είναι υπολογιστικά ανέφικτο (αλλά όχι αδύνατο) να υπολογιστεί το κλειδί αποκρυπτογράφησης από το κλειδί κρυπτογράφησης.

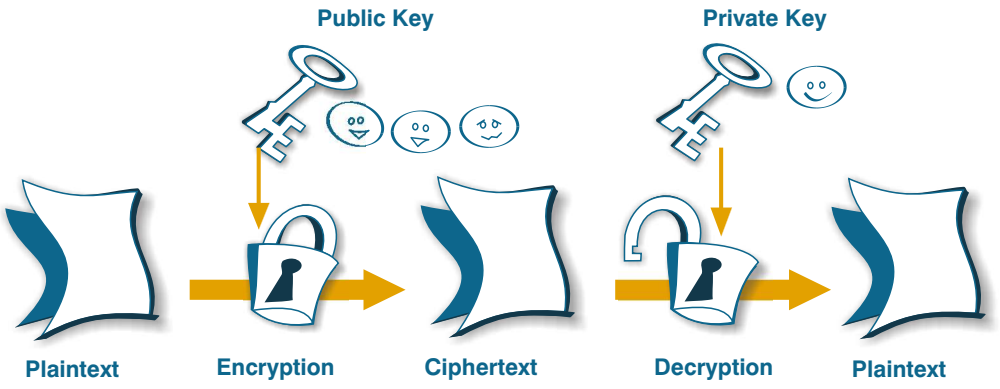
1. Συμμετρική κρυπτογραφία

Ένας κρυπτογραφικός αλγόριθμος είναι συμμετρικός όταν το κλειδί της κρυπτογράφησης είναι ίδιο με αυτό της αποκρυπτογράφησης. Κατά συνέπεια, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και άρα απαιτείται ασφαλές μέσο για τη μετάδοση του. Η εξασφάλιση της ασφαλούς ανταλλαγής του κλειδιού μεταξύ των δύο μερών αποτελεί προϋπόθεση για ένα τέτοιο κρυπτοσύστημα. Σε διαφορετική περίπτωση η συμμετρική κρυπτογραφία καθίσταται αναποτελεσματική.

Σημαντικό πλεονέκτημα των συμμετρικών κρυπτογραφικών αλγορίθμων αποτελεί η ταχύτητα τους. Για το λόγο αυτό χρησιμοποιούνται όταν ο όγκος των δεδομένων προς κρυπτογράφηση είναι μεγάλος. Οι συμμετρικοί αλγόριθμοι διαχωρίζονται σε δύο κατηγορίες: **stream ciphers**, και **block ciphers**. Οι stream ciphers κρυπτογραφούν ένα bit καθαρού κειμένου κάθε φορά, ενώ οι block ciphers κρυπτογραφούν ένα σύνολο από bits ταυτόχρονα (8, 64, 128 bits κλπ.).

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με περισσότερο γνωστό το Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Η.Π.Α. ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών. Στις μέρες μας χρησιμοποιείται ευρύτατα, ιδιαίτερα στον κλάδο των οικονομικών υπηρεσιών. Ο DES είναι ένα block cipher με μέγεθος block 64-bits, ενώ χρησιμοποιεί κλειδί μεγέθους 56-bits. Ο DES μπορεί να χρησιμοποιηθεί για να κρατήσει τα συστήματα ασφαλή από τους απλούς hackers αλλά σπάει εύκολα από ειδικό hardware που μπορούν να προμηθευτούν οι κυβερνήσεις ή οι οργανωμένοι εγκληματίες. Καθώς η υπολογιστική δύναμη των συμβατών συστημάτων αυξάνει με γρήγορο ρυθμό θα πρέπει να αποφεύγεται η χρήση του DES στον σχεδιασμό νέων συστημάτων. Μια παραλλαγή του DES με μεγαλύτερη κρυπτογραφική ισχύ είναι ο Triple-DES που βασίζεται στη χρήση του DES τρεις διαδοχικές φορές με δύο ή τρία διαφορετικά κλειδιά.

Με δεδομένη την ηλικία του DES και με την αύξηση της υπολογιστικής ισχύος των συστημάτων να φέρνει το σπάσιμό του ολοένα και πιο κοντά, το 1997 το National Institute for Standards & Technology (NIST) των ΗΠΑ προκήρυξε διεθνή διαγωνισμό για τη δημιουργία και υιοθέτηση νέου συμμετρικού αλγόριθμου κρυπτογράφησης. Από τους 15 υποψήφιους αλγόριθμους που αναλύθηκαν εξονυχιστικά τόσο από την αμερικανική κυβέρνηση όσο και από τη διεθνή ακαδημαϊκή κοινότητα, τελικά επιλέχθηκε ο αλγόριθμος Rijndael που μετονομάστηκε σε Advanced Encryption Standard (AES) και η υιοθέτησή του για χρήση από την αμερικανική ομοσπονδιακή κυβέρνηση ξεκίνησε στις 26 Μαΐου 2002 (FIPS 197). Ο AES είναι



Σχήμα 3: Ασύμμετρη κρυπτογραφία

ένας συμμετρικός αλγόριθμος κρυπτογράφησης (block cipher) με μήκος block 128 bits και μήκος κλειδιών 128, 192 ή 256 bits.

Όπως προαναφέρθηκε, 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 πανεπιστήμιο MIT και το πρωτόκολλο SSL που είναι ευρύτατα διαδεδομένο για ασφαλείς συναλλαγές στο Internet.

2. Ασύμμετρη Κρυπτογραφία

Τα ασύμμετρα κρυπτογραφικά συστήματα ή συστήματα δημοσίου-κλειδιού χρησιμοποιούν διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση, το δημόσιο (public key) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά παράγονται έτσι ώστε ένα μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί να μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί. Επίσης, το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο (Σχήμα 3). Τα συστήματα δημοσίου-κλειδιού είναι ιδιαίτερα σημαντικά γιατί εξαλείφουν το πρόβλημα της διανομής κλειδιών. Βασικό τους μειονέκτημα είναι η ταχύτητα, καθώς όλα τα γνωστά κρυπτογραφικά συστήματα δημοσίου κλειδιού είναι αρκετά αργά. Γι' αυτόν τον λόγο οι αλγόριθμοι δημοσίου-κλειδιού χρησιμοποιούνται συνήθως για να κρυπτογραφούν τα κλειδιά των συμμετρικών συστημάτων κατά την ανταλλαγή τους, και όχι τον κύριο όγκο των δεδομένων.

Η βασική αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Whitfield Diffie και Martin Hellman. Χρησιμοποιείται συνήθως για ανταλλαγή κλειδιών και όχι για κρυπτογράφηση μηνυμάτων. Πολλά εμπορικά προϊόντα χρησιμοποιούν αυτό το σχήμα για ανταλλαγή κλειδιών. Ο αλγόριθμος θεωρείται ασφαλής[2] όταν το μέγεθος των κλειδιών είναι μεγάλο και οι γεννήτριες αριθμών που χρησιμοποιούνται είναι οι κατάλληλες.

Το 1977 οι Ron Rivest, Adi Shamir και Len Adleman βασισμένοι σε αρχές της θεωρίας των πεπερασμένων πεδίων δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού. Ο RSA μπορεί να χρησιμοποιηθεί για κρυπτογράφηση μηνυμάτων αλλά και για δημιουργία ψηφιακών υπογραφών (digital signatures), η λειτουργία των οποίων αναλύεται αργότερα. Ο συγκεκριμένος αλγόριθμος έχει υποστεί χρόνια εξαντλητικής κρυπτανάλυσης και παρ' ότι η ασφάλεια του δεν έχει αποδειχθεί αλλά ούτε δια-

2. Το πρωτόκολλο Diffie-Hellman προσφέρει μυστικότητα και ακεραιότητα αλλά όχι πιστοποίηση ταυτότητας των εμπλεκομένων μερών. Το αρχικό πρωτόκολλο έχει βελτιωθεί (authenticated Diffie-Hellman) για να προσφέρει και πιστοποίηση ταυτότητας.

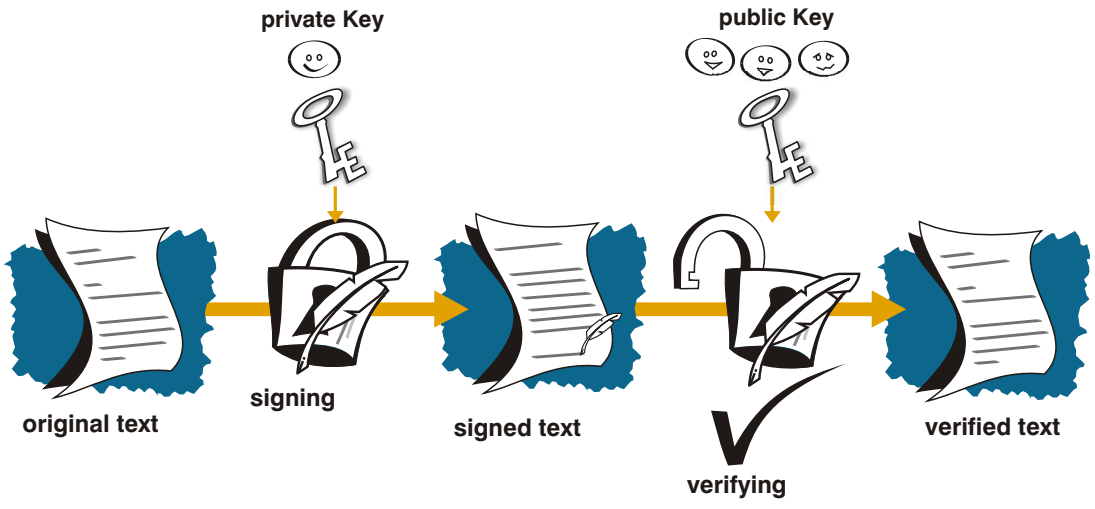
ψευσθεί, μπορεί υπό συνθήκες να παρέχει ένα υψηλό επίπεδο προστασίας. Προς το παρόν ο RSA είναι ο πιο σημαντικός αλγόριθμος δημοσίου-κλειδιού και θεωρείται ασφαλής όταν χρησιμοποιούνται κλειδιά μεγάλου μήκους (1024-bits key είναι αρκετό για τις περισσότερες εφαρμογές ενώ 2048-bits key πιθανόν να δώσει ασφάλεια για δεκαετίες). Η ασφάλεια του RSA βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων ακεραίων αριθμών που είναι γινόμενο μεγάλων πρώτων αριθμών. Εάν υπάρξουν κάποια στιγμή δραματικές εξελίξεις στον τρόπο παραγοντοποιήσης αυτών των αριθμών, τότε ο αλγόριθμος θα αποδειχθεί γρήγορα ευπαθής. Για να γίνει κατανοητή η διαφορά ταχύτητας μεταξύ συμμετρικών αλγορίθμων και αλγορίθμων δημοσίου κλειδιού, αρκεί να αναφερθεί ότι σε hardware εφαρμογές ο RSA είναι περίπου 1000 φορές πιο αργός από τον DES.

Εν κατακλείδι, η αδυναμία των συμμετρικών κρυπτοσυστημάτων να εξαρτώνται από ένα ασφαλές κανάλι επικοινωνίας εξαλείφεται στα ασύμμετρα κρυπτοσυστήματα δεδομένου ότι 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. Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. 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.

Ψηφιακές Υπογραφές

Η ασύμμετρη κρυπτογραφία παρέχει τη δυνατότητα πιστοποίησης της αυθεντικότητας ενός μηνύματος, με την παραγωγή μιας μοναδικής ψηφιακής υπογραφής (digital signature). Η ψηφιακή υπογραφή είναι μία ακολουθία ψηφιακών χαρακτήρων που προσκολλάται στο τέλος ενός μηνύματος, 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.

Οι περισσότεροι αλγόριθμοι δημιουργίας ψηφιακών υπογραφών είναι δημοσίου κλειδιού. Σ' αυτήν την περίπτωση ο αποστολέας κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί για να δημιουργήσει την υπογραφή. Ο παραλήπτης



Σχήμα 4: Ψηφιακές Υπογραφές

αποκρυπτογραφεί την υπογραφή με το δημόσιο κλειδί του αποστολέα, για να επιβεβαιώσει την εγκυρότητα της υπογραφής (Σχήμα 4). Όπως προαναφέρθηκε, ο RSA είναι ένας αλγόριθμος που χρησιμοποιείται ευρύτατα για την δημιουργία ψηφιακών υπογραφών.

Ένα ιδιαίτερα σημαντικό σχήμα δημιουργίας ψηφιακών υπογραφών, εκτός του RSA, είναι το **DSS** (Digital Signature Standard), που εκδόθηκε από το NIST (National Institute of Standards and Technology) των Η.Π.Α. Αρχικά δημοσιεύθηκε το 1991, ενώ αναθεωρήθηκε το 1993. Το DSS χρησιμοποιεί μια νέα τεχνική ψηφιακών υπογραφών - τον αλγόριθμο δημοσίου-κλειδιού **DSA** (Digital Signature Algorithm). Ο DSA στηρίζεται στη δυσκολία υπολογισμού διακριτών λογαρίθμων. Ο σχεδιασμός του DSS δεν έχει δημοσιοποιηθεί, αλλά πιθανά προβλήματα έχουν προκύψει κατά περιόδους. Για παράδειγμα υπάρχει πιθανότητα αποκάλυψης του κρυφού κλειδιού, εάν συμβεί να υπογραφούν δύο διαφορετικά μηνύματα χρησιμοποιώντας τον ίδιο τυχαίο αριθμό.

Κρυπτογραφικές Υπηρεσίες

Οι κρυπτογραφικές υπηρεσίες είναι υπηρεσίες οι οποίες χρησιμοποιώντας κρυπτογραφία στοχεύουν στην αντιμετώπιση συγκεκριμένων απειλών. Οι υπηρεσίες αυτές είναι οι ακόλουθες:

- **Εμπιστευτικότητα (Confidentiality).** Είναι η προστασία της πληροφορίας από μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίηση της. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή δεδομένων.
- **Ακεραιότητα (Integrity).** Είναι η προστασία των δεδομένων από μη εξουσιοδοτημένη τροποποίηση ή αντικατάσταση τους. Η υπηρεσία αυτή παρέχεται από μηχανισμούς κρυπτογραφίας όπως είναι οι ψηφιακές υπογραφές.
- **Πιστοποίηση (Authentication).** Είναι η επιβεβαίωση της ταυτότητας ενός ατόμου ή η επιβεβαίωση της πηγής αποστολής των πληροφοριών. Η πιστοποίηση μπορεί να υλοποιηθεί με τρεις βασικές μεθόδους:

  1. Κάτι που γνωρίζουμε, π.χ. το PIN μιας τραπεζικής κάρτας ή το μυστικό κωδικό ενός λογαριασμού (password).

  2. Κάτι που έχουμε στην ιδιοκτησία μας, π.χ. το κλειδί μιας πόρτας ή μια τραπεζική κάρτα.

  3. Κάτι που έχουμε εκ γενετής, π.χ. δακτυλικά αποτυπώματα, φωνή κτλ.

- **Μη Άρνηση Αποδοχής (Non-Repudiation).** Είναι η υπηρεσία κατά την οποία ο παραλήπτης δεν μπορεί να απαρνηθεί ότι έλαβε το μήνυμα και ότι ο αποστολέας δεν μπορεί να απαρνηθεί ότι έστειλε το μήνυμα. Η μη άρνηση αποδοχής συνδυάζει τις υπηρεσίες της πιστοποίησης και της ακεραιότητας που παρέχονται σε μια τρίτη οντότητα. Έτσι, ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί τη δημιουργία και αποστολή του μηνύματος. Η ασύμμετρη κρυπτογραφία παρέχει ψηφιακές υπογραφές, τέτοιες ώστε μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει την συγκεκριμένη ψηφιακή υπογραφή, πρόκειται δηλαδή για μια αμφιμονοσήμαντη σχέση. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά και ο παραλήπτης του ψηφιακά υπογεγραμμένου μηνύματος μπορεί να επιβεβαιώσει την ψηφιακή υπογραφή του αποστολέα.

Πρωτόκολλο κρυπτογραφίας είναι η απόλυτα σαφής διαδικασία (ακολουθία βημάτων) που πρέπει να ακολουθήσουν τα μέρη που επικοινωνούν προκειμένου να επιτευχθεί μια συγκεκριμένη κρυπτογραφική υπηρεσία. Το κάθε μέλος πρέπει να γνωρίζει σε κάθε χρονική στιγμή ποιο βήμα και πως πρέπει να εκτελεστεί.

Ισχύς των Κρυπτογραφικών Αλγορίθμων

Θεωρητικά, κανένα κρυπτογραφικό σύστημα δεν είναι ασφαλές. Οποιοσδήποτε αλγόριθμος που χρησιμοποιεί κλειδί κρυπτογράφησης μπορεί να σπάσει δοκιμάζοντας όλα τα πιθανά κλειδιά (brute force attack). Αυτό που κάνει ασφαλές ένα κρυπτογραφικό σύστημα είναι ότι ο χρόνος που απαιτείται, χρησιμοποιώντας την υπάρχουσα τεχνολογία, για να δοκιμαστούν όλα τα κλειδιά είναι υπερβολικά μεγάλος. Όπως είναι ευνόητο το μέγεθος του κλειδιού καθορίζει σε μεγάλο ποσοστό τον βαθμό ασφάλειας που παρέχει το σύστημα (με δεδομένο ότι το κρυπτοσύστημα δεν έχει άλλες αδυναμίες η εκμετάλλευση των οποίων να οδηγεί στην αποκάλυψη των μηνυμάτων σε χρόνο μικρότερο από αυτόν που χρειάζεται για να δοκιμαστούν όλα τα πιθανά κλειδιά). Η απαιτούμενη υπολογιστική ισχύς για να σπάσει ένα σύστημα, αυξάνει εκθετικά με το μέγεθος του κλειδιού.

Από την άλλη πλευρά, η ταχύτατα αυξανόμενη υπολογιστική ισχύς των υπολογιστών αποτελεί σύμμαχο της κρυπτανάλυσης (του επιτιθέμενου). Υπολογίζεται ότι σε 50 χρόνια οι υπολογιστές θα είναι 10 δισεκατομμύρια φορές πιο γρήγοροι και αναμφισβήτητα προηγμένα κρυπταναλυτικά συστήματα θα έχουν αναπτυχθεί. Με δεδομένη την τρομακτική εξέλιξη της τεχνολογίας, ο καθορισμός του μεγέθους του κλειδιού ίσως να είναι η δυσκολότερη διαδικασία κατά την ανάπτυξη ενός κρυπτογραφικού συστήματος. Μόνο εάν τα κλειδιά είναι μεγαλύτερα από αυτό που θεωρείται απαραίτητο για τις ανάγκες μας, μπορούν να περιοριστούν στο ελάχιστο οι "δυσάρεστες" εκπλήξεις που μπορεί να επιφέρει η τεχνολογία.

Στα συμμετρικά συστήματα η μέθοδος σπασίματος που ακολουθείται συνήθως, είναι η brute force attack. Για ένα σύστημα με 56-bit κλειδί χρειάζεται να καταβληθεί αξιόλογη προσπάθεια για να σπαστεί (τα πιθανά κλειδιά είναι 2^{56}). Αλλά με χρήση εξειδικευμένου hardware (η αγορά του οποίου είναι εφικτή από μεγάλες εταιρείες, κυβερνήσεις κτλ.) , το σπάσιμο του είναι πολύ εύκολο. Κλειδιά μήκους 64-bits μπορούν πιθανότατα να σπαστούν από μεγάλες κυβερνήσεις, οργανωμένους εγκληματίες, πολύ μεγάλες εταιρείες και ακόμη περισσότερες κυβερνήσεις στο προσεχές μέλλον. Κλειδιά μήκους 80-bits πιθανότατα θα μπορούν να σπαστούν στο προσεχές μέλλον. Τέλος, κλειδιά μήκους 128-bits είναι επαρκή για τις περισσότερες εφαρμογές μιας και μπορούν να παραμείνουν ασφαλή για το πολλά χρόνια.

Τα κλειδιά που χρησιμοποιούνται στα κρυπτογραφικά συστήματα δημοσίου-κλειδιού είναι από την φύση τους πολύ μεγαλύτερα από αυτά των συμμετρικών συστημάτων. Εδώ το πρόβλημα δεν είναι πλέον να βρεθεί το σωστό κλειδί, αλλά να υπολογιστεί το κρυφό κλειδί γνωρίζοντας το δημόσιο. Όπως έχει ήδη αναφερθεί, στην περίπτωση του RSA αυτό ανάγεται στην παραγοντοποίηση ενός μεγάλου ακεραίου αριθμού, ενώ σε πολλά άλλα συστήματα ανάγεται στον υπολογισμό του διακριτού λογαρίθμου σε πεπερασμένο σύνολο τιμών. Και τα δύο προβλήματα θεωρούνται υπολογιστικά ισοδύναμα. Στα συστήματα που χρησιμοποιούν RSA, ένας αριθμός 256-bits μπορεί εύκολα να υπολογιστεί από απλούς ανθρώπους. Κλειδιά μήκους 384-bits μπορούν να σπαστούν από μέσες εταιρείες, ενώ με 512-bits από μεγάλες κυβερνήσεις. Στο κοντινό μέλλον τα κλειδιά μήκους 768-bits δεν θα είναι επαρκή. Τέλος, τα κλειδιά μήκους μεγαλυτέρου των 1024-bits είναι ασφαλή για τα σημερινά δεδομένα, ενώ κλειδιά 2048-bits θεωρείται ότι θα μείνουν ασφαλή για πολλές δεκαετίες.

Κάποιος θα μπορούσε να υποστηρίξει: "γιατί να μην χρησιμοποιήσουμε ακόμη μεγαλύτερα κλειδιά, εάν αυτό μας δίνει πιο ασφαλή συστήματα;". Σίγουρα η χρήση μεγαλύτερων κλειδιών είναι δυνατή, αλλά θα πρέπει να λάβουμε επίσης υπ' όψη μας ότι η ισχυρή κρυπτογραφία απαιτεί κόστος σε υπολογιστική ισχύ και χρόνο. Πάντα θα πρέπει να βρίσκεται η χρυσή τομή μεταξύ ασφάλειας και κόστους εφαρμογής της.

Το μέγεθος του κλειδιού δεν είναι το μοναδικό

ζήτημα από το οποίο εξαρτάται η ισχύς ενός κρυπτογραφικού συστήματος. Πολλά συστήματα έχουν σπάσει χωρίς να γίνει καμιά προσπάθεια να υπολογιστεί το κλειδί. Στην πραγματικότητα, τα πιο δυνατά κρυπτογραφικά συστήματα έχουν σπάσει λόγω ασθενούς **σχήματος διαχείρισης κλειδιών** (key management). Ένα σχήμα διαχείρισης κλειδιών περιλαμβάνει:

- *Δημιουργία Κλειδιών (key generation).* Πόσο τυχαίοι ή προβλέψιμοι είναι οι αριθμοί που χρησιμοποιούμε για την δημιουργία κλειδιών;
- *Αποθήκευση Κλειδιών (key storage).* Τα κλειδιά φυλάσσονται σε tamper-resistant hardware, σε smart cards ή σε κάποιο άλλο token, ή κρυπτογραφούνται με κάποιο άλλο κλειδί και φυλάσσονται σε μια βάση δεδομένων;
- *Αλλαγή Κλειδιών (key change).* Πόσο συχνά αλλάζονται τα βασικά κλειδιά κρυπτογράφησης, ποιο σχήμα αντικατάστασης κλειδιών είναι διαθέσιμο εάν κάποιο από τα κλειδιά διαρρεύσει;
- *Καταστροφή Κλειδιών (key destruction).* Με ποιον τρόπο καταστρέφονται τα κλειδιά πού δεν χρησιμοποιούνται πια, υπάρχει κίνδυνος ανάκτησης τους;
- *Χρήση και Διαχωρισμός Κλειδιών (key usage and separation).* Υπάρχει διαχωρισμός των κλειδιών αναλόγως την χρήση τους (κλειδί αποθήκευσης δεδομένων, κλειδί διανομής άλλων κλειδιών κτλ.);

Πρέπει να τονιστεί ιδιαίτερα ότι η ισχύς ενός κρυπτογραφικού συστήματος είναι ισοδύναμη με το ασθενέστερο του σημείο. Καμία παράμετρος σχεδιασμού του συστήματος δεν πρέπει να υποτιμάται, από την επιλογή του αλγορίθμου έως την δικαιοδοσία των χρηστών ως προς την χρήση των κλειδιών.

Εφαρμογές της Κρυπτογραφίας

Η κρυπτογραφία σήμερα χρησιμοποιείται σε ένα μεγάλο εύρος εφαρμογών. Η σημαντικότητα της κρυπτογραφίας θα αυξάνεται όσο θα αυξάνεται και ο όγκος των πληροφοριών που θα αποθηκεύονται και θα μεταδίδονται ηλεκτρονικά. Μερικές εφαρμογές στις οποίες χρησιμοποιείται η κρυπτογραφία είναι οι ακόλουθες:

- **Ηλεκτρονικό ταχυδρομείο.** Τα δεδομένα ενός μηνύματος ηλεκτρονικού ταχυδρομείου στέλνονται συνήθως μέσω μη ασφαλών καναλιών επικοινωνίας όπως το Internet. Η χρήση, αλλά και η κατάχρηση, του Internet έχει καταστήσει απαραίτητη την κρυπτογράφηση των μηνυμάτων που αποστέλλονται μέσω της υπηρεσίας του ηλεκτρονικού ταχυδρομείου δεδομένου ότι η εξάπλωσή της έχει ως αποτέλεσμα την αποστολή κρίσιμων πληροφοριών.
- **Ασφαλείς συναλλαγές στο Internet - Ψηφιακές Συναλλαγές (Digital transactions)**. Από τη στιγμή που οικονομικές συναλλαγές λαμβάνουν χώρα και μέσω δικτύων (γενικότερα μέσα σε ένα ηλεκτρονικό επιχειρηματικό περιβάλλον), η αυθεντικοποίηση των συναλλαγών είναι ζωτικής σημασίας για την αποφυγή εξαπάτησης κάποιου από τους συναλλασσομένους. Το πρωτόκολλο SSL αποτελεί το πιο επιτυχημένο πρότυπο κρυπτογραφημένης επικοινωνίας. Έρευνες αποδεικνύουν ότι συνεχώς αυξανόμενο είναι το ποσοστό των δικτυακών τόπων που προσφέρουν κρυπτογράφηση SSL. Επίσης, σημαντικά έχει αυξηθεί και ο αριθμός των Αρχών Πιστοποίησης (Certification Authorities) οι οποίες προσφέρουν πιστοποιητικά SSL τόσο για servers όσο και για clients. Το SSL χρησιμοποιείται κυρίως για την παροχή ενός ασφαλούς καναλιού επικοινωνίας μεταξύ servers και clients για τη μετάδοση πληροφοριών όπως passwords, αριθμοί πιστωτικών καρτών.
- **Εθνική Ασφάλεια.** Όπως προαναφέρθηκε η κρυπτογραφία και η κρυπτανάλυση έχουν διαδραματίσει, και συνεχίζουν να διαδραματίζουν, καθοριστικό ρόλο σε σημαντικό

αριθμό στρατιωτικών υποθέσεων. Οι πρεσβείες των κρατών μεταδίδουν και δέχονται διαρκώς κρίσιμες πληροφορίες των οποίων η εμπιστευτικότητα πρέπει να εξασφαλίζεται.

- **"Έξυπνες κάρτες" (Smart Cards).** Η κρυπτογραφία χρησιμοποιείται στις έξυπνες κάρτες λόγω της αυξανόμενης χρήσης της ως μηχανισμού ελέγχου λογικής και φυσικής πρόσβασης σε ευαίσθητες πληροφορίες και χώρους.
- **Πρόσβαση σε ασφαλείς δικτυακούς τόπους.** Η αποδοχή της Αρχής Πιστοποίησης συνεπάγεται την προσθήκη ψηφιακών πιστοποιητικών στον browser του χρήστη του Internet. Με βάση τα ιδιαίτερα χαρακτηριστικά του πιστοποιητικού αυτού, ο χρήστης έχει τη δυνατότητα να επισκεφτεί ασφαλείς δικτυακούς τόπους και να προσπελάσει δεδομένα, χωρίς αυτά να είναι δημοσιευμένα σε κοινή θέα.
- **Εικονικά Ιδιωτικά Δίκτυα (VPNs).** Οι routers και οι firewalls χρησιμοποιούν κρυπτογραφία για την ασφαλή σύνδεση ενός υπολογιστή με ένα εταιρικό δίκτυο.
- **Κρυπτογράφηση αρχείων και αποθηκευτικών μέσων.**

Συμπέρασμα

Αυτό που πρέπει να τονισθεί ιδιαίτερα, είναι **ότι η κρυπτογραφία δεν μπορεί να θεωρηθεί πανάκεια** στο συνολικότερο πρόβλημα της ασφάλειας πληροφοριών. Το μήκος του κλειδιού δεν αποτελεί από μόνο του, εχέγγυο "απόλυτης" ασφάλειας. Η μονομερής επικέντρωση στη δημιουργία προηγμένου κρυπτογραφικού αλγορίθμου χωρίς την απαραίτητη προσοχή σε άλλες διαστάσεις της ασφάλειας (όπως αδυναμίες στην υλοποίηση των συστημάτων ή -ακόμη περισσότερο- στις διαδικασίες χρήσης τους) δε θα έχει τα επιθυμητά αποτελέσματα. Πολλοί κρυπταναλυτές δεν προσπαθούν να σπάσουν τον αλγόριθμο κρυπτογράφησης αλλά επικεντρώνονται στην αναζήτηση αδυναμιών στον σχεδιασμό και την υλοποίηση των κρυπτοσυστημάτων.

Με δεδομένο ότι κάθε κρυπτοσύστημα αργά ή γρήγορα θα καταστεί τρωτό από κάποια μορφή κρυπταναλυτικής επίθεσης, το ζητούμενο για τα κρυπτοσυστήματα είναι να μπορούν να παρέχουν ασφάλεια ενάντια σε επιθέσεις οι οποίες θα επιχειρηθούν στο μέλλον.

Λίγα λόγια για τον αρθρογράφο

Ο **Δημήτρης Εργαζάκης** είναι απόφοιτος του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας. Κατέχει επίσης μεταπτυχιακό τίτλο του London School of Economics (MSc in Analysis, Design & Management of Information Systems). Διαθέτει τριετή εμπειρία στον τομέα του Information Security και εργάζεται στην ENCODE S.A. Έχει εργαστεί στο παρελθόν στην LogicDIS ως Senior ERP Implementation Consultant και στην Deloitte & Touche ως Enterprise Risk Services Consultant. Από το 2000 είναι μέλος του ISACA (Information Systems Audit and Control Association, USA). Οι κύριοι τομείς εξειδίκευσης του είναι οι :

Information Risk Assessment & Management, Enterprise Security Policy development, ISO/IEC: 17799 (BS 7799) Implementation/Compliance, Security Organization Design, Business Continuity Planning, Enterprise Security Awareness Programs, Training & Awareness.

Εάν επιθυμείτε το COMMUNICATION SOLUTIONS να δημοσιεύσει περισσότερα άρθρα για την **Κρυπτογραφία** κυκλώστε το **No 25** στην ***κάρτα αναγνωστών***