Ηλεκτρονικό εμπόριο και ασφάλεια: κρυπτογράφηση

Του κ. **Αντωνίου ΠΑΛΛΗΚΑΡΩΝΑ**
Φοιτ. Τμήμ. Μαθηματ. Πανεπ. Πατρών

Η ασφάλεια[1] αποτελεί ένα σημαντικό παράγοντα σε κάθε οικονομικό σύστημα ανεξάρτητα με το αν βασίζεται σε φυσικές ή ηλεκτρονικές οικονομικές συναλλαγές. Για τις φυσικές συναλλαγές βασιζόμαστε σε μία σειρά φυσικών μεθόδων ασφαλείας, ενώ για τις ηλεκτρονικέ συναλλαγές είναι εύλογο, ότι η χρησιμοποίηση επιπρόσθετων μέσων είναι επιτακτική για την ικανοποιητική προστασία και διασφάλιση του απαραβίαστου των δεδομένων, της επικοινωνίας και των εμπορικών συναλλαγών. Η υλοποίηση ψηφιακών συναλλαγών διά μέσου του διαδικτύου σημαίνει πολύ απλά, έναν αυξημένο αριθμό απειλών και κινδύνων για την ασφάλεια του δεδομένου συστήματος συναλλαγών. Ο ακόλουθος πίνακας προβάλλει μία σειρά από κινδύνους, που απειλούν την ασφάλεια του συστήματος, μαζί με πιθανές λύσεις που μπορούν να χρησιμοποιηθούν.

ΑΠΕΙΛΗ	ΛΥΣΗ ΑΣΦΑΛΕΙΑΣ	ΛΕΙΤΟΥΡΓΙΑ	ΤΕΧΝΟΛΟΓΙΑ
ΥΠΟΚΛΟΠΗ ΠΛΗΡΟΦΟΡΙΩΝ, ΠΑΡΑΝΟΜΗ ΑΝΑΓΝΩΣΗ Η ΤΡΟΠΟΠΟΙΗΣΗ	ΚΡΥΠΤΟΓΡΑΦΗΣΗ	ΚΩΔΙΚΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ ΓΙΑ ΑΠΟΤΡΟΠΗ ΞΕΝΩΝ ΕΠΕΜΒΑΣΕΩΝ	ΣΥΜΜΕΤΡΙΚΗ-ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ
ΧΡΗΣΤΕΣ ΔΙΑΣΤΡΕΒΛΩΝΟΥΝ ΤΗΝ ΤΑΥΤΟΤΗΤΑ ΤΟΥΣ ΔΙΕΞΑΓΩΝΤΑΣ ΑΠΑΤΗ	ΠΙΣΤΟΠΟΙΗΣΗ	ΠΙΣΤΟΠΟΙΗΣΗ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ ΤΟΥ ΑΠΟΣΤΟΛΕΑ ΚΑΙ ΤΟΥ ΑΠΟΔΕΚΤΗ	ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ
ΜΗ ΕΞΟΥΣΙΟΔΟΤΗΜΕΝΟ ΧΡΗΣΤΕΣ ΑΠΟΚΤΟΥΝ ΠΑΡΑΝΟΜΗ ΠΡΟΣΒΑΣΗ ΣΕ ΞΕΝΟ ΔΙΚΤΥΟ	FIREWALL	ΦΙΛΤΡΑΡΙΣΜΑ ΚΑΙ ΑΠΟΤΡΟΠΗ ΣΥΓΚΕΚΡΙΜΕΝΕΣ ΚΥΚΛΟΦΟΡΙΑΣ ΣΤΟ ΔΙΚΤΥΟ Η ΣΤΟΝ SERVER	FIREWALLS ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΥΚΤΙΑ

1. Το κείμενο προέρχεται από σχετική εκτενή εργασία του Συγγραφέα με τίτλο: Έρευνα και ανάλυση για το ηλεκτρονικό εμπόριο στην Ελλάδα.

Οι βασικές απαιτήσεις για την διεξαγωγή εμπορίου περιλαμβάνουν εμπιστοσύνη, ακεραιότητα, πιστοποίηση, εξουσιοδότηση, εγγύηση και μυστικότητα. Οι τέσσερις πρώτες απαιτήσεις για το ηλεκτρονικό εμπόριο μπορούν να διασφαλισθούν με την βοήθεια της τεχνολογίας. Αλλά οι δύο τελευταίες, εγγύηση και μυστικότητα, εξαρτώνται από τις καλές προθέσεις των ατόμων και των οργανισμών να δραστηριοποιούνται υπεύθυνα και να επιδεικνύουν την πρέπουσα υπακοή στους νόμους, που είτε έχουν δημιουργηθεί, είτε θα δημιουργηθούν μελλοντικά κατά της απάτης από κακόβουλους εμπόρους.

Οι ψηφιακές επικοινωνίες, που γίνονται είτε με τα νέα τηλέφωνα του ΟΤΕ, είτε με τα κινητά, είτε μέσω δικτύων ηλεκτρονικών υπολογιστών, έχουν ένα μοναδικό χαρακτηριστικό: στην ουσία μεταφέρουν αριθμούς. Ότι δήποτε γράφουμε στον υπολογιστή ή προφέρουμε στο τηλέφωνο, μετατρέπονται σε ψηφία, μεταφέρονται μέσω της γραμμής και αποκωδικοποιούνται όταν φτάσουν στο δέκτη. Οι αριθμοί όμως αυτοί μπορούν να «αναμειχθούν» στην πηγή τους με βάση μία εξίσωση που ονομάζεται αλγόριθμος και να «τοποθετηθούν σε σειρά» με βάση την ίδια εξίσωση όταν φτάσουν στον προορισμό τους. Αν στο ενδιάμεσο κάποιος υποκλέψει τη μετάδοση και δεν έχει τον αλγόριθμο δεν μπορεί να καταλάβει το μήνυμα.

Η τεχνολογία για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων είναι πολύ παλιά, αλλά το υψηλό της κόστος την έκανε κρατικό μονοπώλιο. Με την έλευση των προσωπικών υπολογιστών και των ψηφιακών τηλεφώνων η διαδικασία γινόταν πολύ απλή. Όποιος δήποτε πλέον μπορεί να κρυπτογραφεί τα μηνύματά του αρκεί να έχει το κατάλληλο πρόγραμμα.

Όταν αναφερόμαστε στον όρο κρυπτογραφία, το πρώτο πράγμα που σκεφτόμαστε είναι, ότι πρόκειται για μία μέθοδο που κωδικοποιεί έναν αριθμό δεδομένων με τέτοιο τρόπο, ώστε να είναι δύσκολο να διαβαστούν και κατά συνέπεια μία μέθοδο που να διασφαλίζει την μυστικότητά τους. Στην πραγματικότητα η κρυπτογραφία ικανοποιεί και άλλες ανάγκες, όπως η ανάγκη για εξακρίβωση και πιστοποίηση προσώπων για παράδειγμα, που επιδιώκουν την πραγματοποίηση συναλλαγών μέσα στο διαδίκτυο.

Οι κρυπτογραφικές τεχνικές προσφέρουν τρεις βασικούς τύπους υπηρεσιών στο ηλεκτρονικό εμπόριο: πιστοποίηση (που περιλαμβάνει και εξακρίβωση), επιβεβαίωση αποστολής και μυστικότητα. Η εξακρίβωση (identification), ένας τύπος της πιστοποίησης, επιβεβαιώνει, ότι ο αποστολέας ενός μηνύματος είναι στην πραγματικότητα αυτός, που υποστηρίζει ότι είναι, δηλαδή εξακριβώνει αν είναι ο αληθινός. Η πιστοποίηση προχωρά ένα βήμα περαιτέρω: επιβεβαιώνει όχι μόνο την ταυτότητα του αποστολέα, αλλά και ότι το μήνυμα που έχει μεταφερθεί δεν έχει τροποποιηθεί. Η επιβεβαίωση αποστολής (non-repudiation) αποτελεί ένα απαραίτητο εφόδιο για το ηλεκτρονικό εμπόριο. Η εφαρμογή της εμποδίζει όποιον δήποτε να αρνηθεί, ότι έχει στείλει ή έχει δεχτεί ένα συγκεκριμένο αρχείο ή δεδομένο. Τέλος, η μυστικότητα (privacy) λειτουργεί σαν ασπίδα που θωρακίζει την επικοινωνία από μη εξουσιοδοτημένα μέλη.

Η κρυπτογράφηση ή κωδικοποίηση πληροφοριών προκειμένου να αποτραπεί η ανάγνωση τους από μη-εξουσιοδοτημένα άτομα αποτελεί μία διαδικασία ιδιαίτερα παλιά. Ο Ιούλιος Καίσαρας π.χ. χρησιμοποιούσε για τις στρατιωτικές του επιχειρήσεις έναν απλό κρυπτογραφικό κώδικα, που αντικαθιστούσε ένα γράμμα με κάποιο άλλο που βρίσκονταν 3 ή 4 θέσεις μπροστά του στο αλφάβητο, δηλαδή αντικαθιστούσε το γράμμα α με το γράμμα δ ή ε.

Για να είναι εφικτή η λειτουργία της κρυπτογραφίας πρέπει τόσο ο αποστολέας, όσο και ο αποδέκτης του μηνύματος να γνωρίζουν τους κανόνες, που διέπουν το συγκεκρι-

Ευγενία Γ. Αθανασοπούλου
(1916-1992 μ.Χ.)

Γεώργιος Κ. Αθανασόπουλος
(1916-1983 μ.Χ.)

ΔΗΜΟΤΙΚΑ ΤΡΑΓΟΥΔΙΑ ΠΕΡΙΟΧΗΣ ΣΟΦΑΔΩΝ

Αθήναι, Ιούνιος 1997

μένο κρυπτογράφημα. Στην αναφερθείσα περίπτωση θα έπρεπε να γνωρίζουν, ότι το γράμμα α έχει αντικατασταθεί από το γράμμα δ.

Η κρυπτογραφία βασίζεται σε δύο συστατικά στοιχεία: τον αλγόριθμο και το κλειδί. Ο αλγόριθμος αποτελεί μία μαθηματική λειτουργία-πρόγραμμα, που συνδυάζει ένα απλό κείμενο ή κάποια καταληπτή πληροφορία με μία σειρά ψηφίων, που καλείται κλειδί έτσι, ώστε να δημιουργηθεί ένα ακατάληπτο κρυπτογραφημένο κείμενο. Στο ιστορικό παράδειγμα, που ήδη αναφέρθηκε μπορούμε να θεωρήσουμε σαν αλγόριθμο την διαδικασία αντικατάστασης ενός γράμματος με ένα άλλο και σαν κλειδί μπορούμε να θεωρήσουμε τον αριθμό 3, δηλαδή την αντικατάσταση ενός όποιου δήποτε γράμματος με ένα άλλο, που όμως βρίσκεται 3 θέσεις μπροστά του στο αλφάβητο. Η κρυπτογράφηση, που χρησιμοποιεί κλειδί, αποτελεί τον πιο σημαντικό και εύχρηστο τύπο κρυπτογράφησης για το ηλεκτρονικό εμπόριο γιατί προσφέρει δύο σημαντικά πλεονεκτήματα. Πρώτον είναι δύσκολο να επινοούμε συνεχώς νέους αλγορίθμους κάθε στιγμή, που θέλουμε να επικοινωνούμε ιδιαιτέρως με έναν νέο ανταποκριτή. Με την χρήση του κλειδιού είναι εφικτή η χρησιμοποίηση του ίδιου αλγόριθμου για να επικοινωνούμε με πολλούς ανθρώπους. Το μόνο που χρειάζεται είναι η χρήση διαφορετικού κλειδιού για κάθε διαφορετικό ανταποκριτή. Δεύτερον εάν κάποιος καταφέρει να αποκρυπτογραφήσει το τροποποιημένο μήνυμα το μόνο που χρειάζεται είναι να αντικατασταθεί το παλιό κλειδί με ένα νέο. Κατά συνέπεια δεν χρειάζεται η αντικατάσταση του αλγόριθμου εκτός εάν αυτός αποδειχτεί ανασφαλής κάτι, που όμως σήμερα θεωρείται σχεδόν απίθανο.

Ο αριθμός των πιθανών κλειδιών, που κάθε αλγόριθμος μπορεί να υποστηρίξει εξαρτάται από τον αριθμό των ψηφίων (bits) που διαθέτει το κλειδί. Π.χ. ένα οκταψήφιο κλειδί επιτρέπει 256 πιθανούς αριθμητικούς συνδυασμούς (2 υψωμένο στην δύναμη του 8, λόγω του δυαδικού συστήματος), καθένας από τους οποίους καλείται κλειδί. Όσο μεγαλύτερος είναι ο αριθμός των κλειδιών, που μπορούν να δημιουργηθούν από τον συνδυασμό των ψηφίων τόσο πιο δύσκολη είναι το «σπάσιμο» του κρυπτογραφημένου μηνύματος. Κατά συνέπεια ο βαθμός δυσκολίας εξαρτάται από το μάκρος του κλειδιού. Για έναν υπολογιστή δεν είναι δύσκολο ούτε χρονοβόρο να μαντέψει διαδοχικά κάθε ένα από τα 256 κλειδιά και να αποκωδικοποιήσει το μήνυμα: θα χρειαστεί λιγότερο από 1 χιλιοστό του δευτερολέπτου.

Λόγω της πολυπλοκότητας της ανάλυσης των τεχνικών κρυπτογραφίας θα αναφερθούμε συνοπτικά στις δύο σημαντικότερες: την συμμετρική και την ασύμμετρη κρυπτογραφία:

Η συμμετρική κρυπτογραφία βασίζεται στην ύπαρξη ενός μοναδικού κλειδιού, το οποίο χρησιμοποιείται τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση των δεδομένων. Για το λόγο αυτό καλείται, επίσης, και κρυπτογραφία μυστικού κλειδιού ή διαμοιραζόμενου μυστικού.

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. Παρά την πολυπλοκότητά της αρχιτεκτονικής του DES, ο αλγόριθμος αυτός βασικά αποτελεί ένα κώδικα μονοαλφαβητικής αντικατάστασης χρησιμοποιώντας χαρακτήρες των 64 bits. Πρόσφατη εξέλιξη του συστήματος αυτού αποτελεί ο Triple-DES, ενώ εξαιρετικά δημοφιλείς είναι και οι IDEA (International Data Encryption Algorithm), RC2 και RC4.

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.

Τα σχήματα αυτά παρουσιάζουν το μειονέκτημα, ότι 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 εξυπηρέτηση.

Σε αντίθεση με την κρυπτογραφία μυστικού κλειδιού, η ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημόσιου κλειδιού είναι αρκετά πρόσφατη. Οι αλγόριθμοι και τα συστήματα της κατηγορίας αυτής βασίζονται στην ύπαρξη δύο ξεχωριστών κλειδιών για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης. Τα κλειδιά που ανήκουν στο ζεύγος αυτό έχουν την ιδιότητα, ότι είναι πρακτικά αδύνατος ο υπολογισμός του ενός κλειδιού γνωρίζοντας το άλλο. Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κελιδιού 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. Από τότε έχουν υπάρξει αρκετές προτάσεις για σχήματα δημόσιου κλειδιού, συμπεριλαμβανομένων των κρυπτοσυστημάτων EI Gamal και ελλειπτικών καμπυλών.

Κάθε κρυπτοσύστημα δημόσιου κλειδιού έχει τις δικές του ιδιαιτερότητες, όλα όμως βασίζονται στη δυνατότητα δημοσίευσης των δημόσιων κλειδιών, καθώς είναι πρακτικά αδύνατος ο υπολογισμός του αντίστοιχου ιδιωτικού κλειδιού. Ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για την κρυπτογράφηση του μηνύματος, εξασφαλίζοντας έτσι, ότι μόνο ο παραλήπτης που διαθέτει ο αντίστοιχο ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα.

Η κρυπτογραφία δημόσιου κλειδιού παρουσιάζει πολύ μεγαλύτερη υπολογιστική πολυπλοκότητα από την αντίστοιχη του μυστικού κλειδιού. Για το λόγο αυτό έχει επικρατήσει ως κοινή πρακτική η χρησιμοποίησή της για την κρυπτογράφηση των μυστικών κλειδιών, που χρησιμοποιούνται για την κρυπτογράφηση της πληροφορίας. Με τον τρόπο αυτό κάθε ασφαλές μήνυμα αποτελείται από δύο συστατικά: την πληροφορία (η οποία είναι κρυπτογραφημένη με σχήμα μυστικού κλειδιού) και το ίδιο το μυστικό κλειδί (το οποίο είναι κρυπτογραφημένο με σχήμα δημόσιου κλειδιού).

Τα πλεονεκτήματα της κρυπτογραφίας δημοσίου κλειδιού είναι τόσο σημαντικά, ώστε να έχουν ανοίξει το δρόμο για την υλοποίηση και άλλων πολύτιμων εφαρμογών α-

σφαλείας, απαραίτητων για την «ακέραιη» διεξαγωγή ηλεκτρονικού εμπορίου. Τα ζευγάρια κλειδιών έχουν ένα μοναδικό χαρακτηριστικό: τα δεδομένα, που κρυπτογραφούνται με το ένα κλειδί μπορούν να αποκρυπτογραφούν μόνο με το άλλο κλειδί του ζευγαριού. Με άλλα λόγια δεν έχει καμία διαφορά αν χρησιμοποιηθεί το δημόσιο κλειδί ή το μυστικό κλειδί για να κρυπτογραφηθεί ένα μήνυμα. Ο αποδέκτης μπορεί να χρησιμοποιήσει το άλλο κλειδί για να το αποκωδικοποιήσει. Τα κλειδιά μπορούν να χρησιμοποιηθούν με δύο διαφορετικούς τρόπους έτσι, ώστε να παρέχουν με τρόπο εμπιστευτικό ένα μήνυμα και έτσι ώστε να αποδεικνύουν την αυθεντικότητα του μηνύματος, δηλαδή την εξακρίβωση της προέλευσης της πληροφορίας. Στην πρώτη περίπτωση ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του αποδέκτη για να κρυπτογραφήσει το μήνυμα έτσι, ώστε αυτό να παραμείνει εμπιστευτικό μέχρι να αποκωδικοποιηθεί από τον τελευταίο. Στην δεύτερη περίπτωση ο αποστολέας κρυπτογραφεί ένα μήνυμα χρησιμοποιώντας ένα μυστικό κλειδί στο οποίο μόνο ο ίδιος έχει πρόσβαση.

Στην δεύτερη περίπτωση, η εξακρίβωση της προέλευσης του μηνύματος βασίζεται στην εξής βασική ιδέα:

Βάσει του γεγονότος, ότι υπάρχει ένα μοναδικό άτομο που μπορεί να κρυπτογραφήσει κάτι με το προσωπικό του μυστικό κλειδί, όποιος δήποτε άλλος χρησιμοποιήσει το δημόσιο κλειδί για να αποκρυπτογραφήσει το μήνυμα θα είναι σίγουρος, ότι το μήνυμα προέρχεται από τον κάτοχο του μυστικού κλειδιού. Κατά συνέπεια η χρήση του μυστικού κλειδιού για την κρυπτογράφηση ενός εγγράφου είναι αντίστοιχη με την υπογραφή σε ένα κανονικό έγγραφο και έτσι μας δίνεται η δυνατότητα για την απόκτηση της ψηφιακής υπογραφής (digital sign), μίας εφαρμογής, που όπως διαφαίνεται, η μελλοντική της χρήση αναπόφευκτα θα υπερκεράσει την χρήση της παραδοσιακής υπογραφής τουλάχιστον στις ηλεκτρονικές μας συναλλαγές.

Σε γενικές γραμμές η λειτουργία ενός πρότυπου συστήματος ψηφιακών υπογραφών ξεκινά όταν ο αποστολέας καθορίσει ακριβώς το πλήρες περιεχόμενο του μηνύματος. Από το λογισμικό του αποστολέα γίνεται η επεξεργασία του μηνύματος με βάση κάποιο αλγόριθμο Hash (γνωστός κρυπτογραφικός αλγόριθμος) και παράγεται ένα μοναδικό και σταθερού μήκους αποτέλεσμα, που ονομάζεται Message Digest, πρόκειται δηλαδή για μία μοναδική απεικόνιση του μηνύματος. Στη συνέχεια το λογισμικό του αποστολέα μετατρέπει το Message Digest σε ψηφιακή υπογραφή κάνοντας χρήση του μυστικού κλειδιού. Με αυτό τον τρόπο, η συγκεκριμένη ψηφιακή υπογραφή είναι μοναδικά αντιστοιχισμένη αφ' ενός με το Message Digest (συνεπώς και με το μήνυμα) και αφ' ετέρου με το μυστικό κλειδί που χρησιμοποιήθηκε για τη δημιουργία της. Τέλος, η ψηφιακή υπογραφή συνδέεται με το μήνυμα και αποστέλλεται στον παραλήπτη της. Με την χρήση του αλγόριθμου Hash, του αποτελέσματος και, τέλος, του αντίστοιχου δημοσίου κλειδιού ο παραλήπτης ελέγχει αν η ψηφιακή υπογραφή δημιουργήθηκε με τη χρήση του αντίστοιχου μυστικού κλειδιού και αν το αποτέλεσμα, που υπολογίστηκε κατά την λήψη είναι ίδιο με εκείνο που υπολογίστηκε κατά την αποστολή και ενσωματώθηκε στην ψηφιακή υπογραφή. Αν και οι δύο αυτοί παράμετροι ικανοποιούνται ο αποστολέας δεν μπορεί να αρνηθεί την αποστολή του συγκεκριμένου μηνύματος εφ' όσον δεν υπήρχε τρόπος αυτό να δημιουργηθεί χωρίς τη χρήση του μοναδικού μυστικού κλειδιού του οποίου είναι και μοναδικός κάτοχος.