

---

## Εισαγωγή Στην Κρυπτογραφία

---

**Περίληψη.** Στην παρούσα εργαστηριακή ενότητα επιχειρείται η εισαγωγή του αναγνώστη στην κρυπτογραφία ως επιστημονικός κλάδος αλλά και ως μεθοδολογία διασφάλισης των πληροφοριακών συστημάτων. Αρχικά επιχειρείται να καταστεί κατανοητή η αναγκαιότητα ύπαρξης αυτής της μεθοδολογίας, στη συνέχεια παρουσιάζονται κάποιοι βασικοί κρυπταλγόριθμοι και σχήματα κρυπτογράφησης καθώς και εφαρμογές όπως οι ψηφιακές υπογραφές. Στα πλαίσια του εργαστηρίου θα δούμε πως αυτά υλοποιούνται με κατάλληλο λογισμικό.

### 1. Εισαγωγή

Δεδομένου ότι οι υπολογιστές και η επικοινωνία μεταξύ τους χρησιμοποιούνται όλο και περισσότερο για αποθήκευση και ανταλλαγή πολύτιμων στοιχείων, πρέπει να λαμβάνονται μέτρα για να προστατεύονται τα στοιχεία αυτά από εσκεμμένη ή συμπωματική τροποποίηση ή κακή χρήση. Τα στοιχεία που πρέπει να προστατευθούν ποικίλλουν, αναφορικά με τη φύση τους. Μπορεί να συνίστανται σε πόρους συστήματος που ανήκουν σε παροχές υπηρεσιών, οι οποίοι προσφέρουν πρόσβαση σε βάσεις δεδομένων, πληροφοριακά συστήματα ή, γενικώς, υπολογιστικές υπηρεσίες που περιλαμβάνουν πληροφορίες που αποθηκεύονται και ανταλλάσσονται με τη βοήθεια υπολογιστών. Μπορούν ακόμη να περιλαμβάνουν ηλεκτρονικά υπογεγραμμένα και υποθηκευμένα συμβόλαια, τα οποία αφορούν τρίτους ή ψηφιακή πληροφορία για νομικές δεσμεύσεις σε επιχειρησιακά πλαίσια.

Τα τελευταία παραδείγματα καταδεικνύουν ότι δεν χρειάζονται απλά νέες τεχνικές ασφάλειας για τις περιοχές όπου οι κλασικές προσεγγίσεις, όπως η χρήση συνθηματικών, έχουν αποδειχθεί ανεπαρκείς. Οι προηγμένες τεχνικές ασφάλειας είναι μια αναγκαιότητα.

Η ασφάλεια είναι χρήσιμη τόσο για τους χρήστες των υπολογιστικών συστημάτων όσο και για τους παροχείς υπολογιστικών υπηρεσιών. Η κλασική μέθοδος επίτευξης της ασφάλειας εξυπηρετεί καλύτερα τα συμφέροντα των παροχών συστημάτων παρά αυτά των χρηστών. Πρώτον, οι χρήστες είναι συνήθως αυστηρά περιορισμένοι σε υπηρεσίες και πόρους συστήματος για τους οποίους έχουν πληρώσει ή για τους οποίους πιστεύεται από τους διαχειριστές των συστημάτων ότι είναι επαρκείς για τις ανάγκες των χρηστών. Δεύτερον, η πρόσβαση σε πόρους και πληροφορίες προστατεύεται με μηχανισμούς που βασίζονται σε συνθηματικά, οι οποίοι προστατεύουν τα συστήματα από μη εξουσιοδοτημένους χρήστες και κάθε χρήστη από τους υπολοίπους αλλά δεν παρέχουν καμία προστασία στους χρήστες απέναντι στους διαχειριστές των συστημάτων. Τρίτον, τα συστήματα δίνουν τη δυνατότητα στους διαχειριστές να καταγράψουν λεπτομερώς τις κινήσεις των χρηστών, κάτι που δίνει τη δυνατότητα προστασίας των πόρων και επακριβούς χρέωσης για τους πόρους που χρησιμοποιήθηκαν, ενέχει όμως τον κίνδυνο της παραβίασης της ιδιωτικότητας των χρηστών. Όλα αυτά οδηγούν σε κλειστά συστήματα. Από την άλλη πλευρά, τα ανοικτά συστήματα που δεν παρέχουν στους χρήστες τη δυνατότητα να δημιουργήσουν κλειστά περιβάλλοντα, δεν μπορούν να φιλοξενήσουν τις περισσότερες εφαρμογές. Τα ανοικτά συστήματα στα οποία οι χρήστες έχουν τη δυνατότητα να απαιτούν υπηρεσίες, χωρίς χρονικούς ή άλλους περιορισμούς, πιθανώς με ανώνυμο τρόπο αν αυτό επιθυμείται, χωρίς προϋποθέσεις για εκ των προτέρων εγγραφή και χωρίς να είναι δυνατόν να καταγραφούν οι ενέργειές τους δεν είναι δυνατόν να στηριχθούν σε μηχανισμούς που βασίζονται στα συνθηματικά.

#### 1.1 Κύρια ζητήματα για την ασφάλεια

Μπορούμε να ορίσουμε τέσσερις κύριες κατηγορίες απειλών για την ασφάλεια των επικοινωνιών στα ανοικτά συστήματα:

1. Μη εξουσιοδοτημένη απόκτηση της πληροφορίας μέσω παθητικής παρακολούθησης.
2. Μη εξουσιοδοτημένη τροποποίηση της πληροφορίας, π.χ. αλλαγή, αναπαραγωγή ή επαναποστολή της πληροφορίας που ανταλλάσσεται μεταξύ δύο οντοτήτων.
3. Μεταμφίηση, δηλ. διενέργεια πράξεων υπό ταυτότητα διαφορετική από την πραγματική. Η μεταμφίηση μπορεί να λάβει διάφορες μορφές.

4. Αποκήρυξη της επικοινωνίας (δηλ. άρνηση συμμετοχής σ' αυτή), από οποιοδήποτε από τα ενεχόμενα μέρη.

Η αυθεντικότητα είναι ένα από τα σημεία-κλειδιά της ασφάλειας. Η αυθεντικότητα των υποκειμένων (προσώπων, οργανισμών, τμημάτων υλικού) και των αντικειμένων (αρχείων, πληροφορίας, προγραμμάτων, κλειδιών) στα συστήματα διαχείρισης πληροφοριών είναι η βάση στην οποία στηρίζεται η υπευθυνότητα, που με τη σειρά της είναι η βάση για τη συλλογική εργασία. Οι απαιτήσεις που σχετίζονται με την ασφάλεια, όπως η ακεραιότητα των δεδομένων, ο έλεγχος πρόσβασης, η απουσία δυνατότητας αποκήρυξης της επικοινωνίας και η παρεμπόδιση της μεταμφίσεως μπορούν να καλυφθούν μόνο αν υπάρχει αξιόπιστη διακρίβωση της ταυτότητας των εταίρων.

Η εμπιστευτικότητα είναι επίσης σημαντικό ζήτημα για πολλές εφαρμογές. Πληροφορίες που είναι απόρρητες, όπως προσωπικά δεδομένα, ιατρικά στοιχεία κ.τ.λ. δεν πρέπει να μεταδίδονται χωρίς κρυπτογράφηση μέσα από δημόσια δίκτυα, αν η διαρροή αυτών των πληροφοριών είναι δυνατόν να οδηγήσει σε οικονομικές ή άλλου τύπου ζημιές. Σε πολλές περιπτώσεις η επικοινωνία μεταξύ δύο συστημάτων διέρχεται από πολλαπλά επικοινωνιακά κανάλια, με κυμαινόμενες δυνατότητες για επίδοξους υποκλοπείς να αντλήσουν την πληροφορία που επιθυμούν. Με την πρόοδο των δικτυακών συστημάτων αρχείων, όπως π.χ. τα NFS και CIFS, οι χρήστες πολλές φορές αγνοούν ότι μία ενέργεια που φαίνεται να εκτελείται «τοπικά» στον υπολογιστή τους, στην πραγματικότητα μετακινεί πολλά δεδομένα μέσα από το δίκτυο, από ή προς τον υπολογιστή όπου πραγματικά αποθηκεύεται το αρχείο. Η κρυπτογράφηση από άκρου εις άκρον είναι απαραίτητη στις περισσότερες περιπτώσεις, ενώ και μηχανισμοί κρυπτογράφησης μεταξύ δικτυακών στοιχείων επικοινωνίας μπορεί να είναι καλό να χρησιμοποιηθούν για προστασία από τεχνικές όπως η ανάλυση ροής πληροφορίας. Θα πρέπει ωστόσο να σημειώσουμε ότι η εμπιστευτικότητα προϋποθέτει την αυθεντικότητα. Ο κάθε ένας πρέπει να είναι σίγουρος για την ταυτότητα αυτού με τον οποίο ανταλλάσσει ή μοιράζεται κλειδιά για την επίτευξη της εμπιστευτικότητας. Η αυθεντικότητα είναι προαπαιτούμενο για άλλες υπηρεσίες ασφάλειας και ως εκ τούτου το κεντρικό ζήτημα στην ασφάλεια.

Συνοψίζοντας μπορούμε να εντοπίσουμε την αναγκαιότητα για:

1. Δυνατότητα ισχυρής διακρίβωσης της ταυτότητας των χρηστών ή άλλων ενεργών οντοτήτων (π.χ. εκτελούμενων προγραμμάτων) με αποκεντρωμένο τρόπο και υπό τον έλεγχο του χρήστη. Κατά τη διακρίβωση της ταυτότητας δεν πρέπει να αποκαλύπτονται περισσότερα στοιχεία απ' ότι είναι απαραίτητο για να εξυπηρετηθούν τα έννομα συμφέροντα των ενεχομένων μερών, και δεν πρέπει να παρεμβαίνουν ασκόπως, ή να καταγράφουν τα τεκταινόμενα κεντρικές αρχές.
2. Δυνατότητα παροχής και επαλήθευσης αποδείξεων αυθεντικότητας και ακεραιότητας της πληροφορίας.
3. Δυνατότητα εγγύησης της εμπιστευτικότητας και του απορρήτου σε ένα πολυχρηστικό περιβάλλον.

## 2 Κρυπτογραφία

Ο βασικός μηχανισμός για την παροχή ασφάλειας με τα χαρακτηριστικά που περιγράφηκαν πιο πάνω είναι η κρυπτογραφία. Οι αλγόριθμοι κρυπτογραφίας χρησιμοποιούνται για δύο σκοπούς. Ο **πρώτος** είναι για να αποδείξει κάποιος στους υπόλοιπους ότι είναι κάτοχος κάποιου συγκεκριμένου κλειδιού. Αν ο εταίρος ή ο επαληθευτής είναι σε θέση να αποκρυπτογραφήσει δεδομένα που έχουν κρυπτογραφηθεί με χρήση του συγκεκριμένου κλειδιού, τότε θεωρείται ότι η κατοχή του κλειδιού έχει αποδειχθεί. Αν επιπρόσθετα μπορεί να εξασφαλισθεί, με άλλα μέσα, ότι κανείς άλλος χρήστης ή οντότητα δεν μπορεί να έχει στη διάθεσή του το ίδιο κλειδί, η χρήση αυτού του κλειδιού συνιστά ταυτόχρονα και σύνδεσμο προς τον χρήστη του κλειδιού. Με τον τρόπο αυτό επιτυγχάνεται η *αυθεντικοποίηση*. Ο **δεύτερος** σκοπός για τον οποίο χρησιμοποιείται η κρυπτογραφία είναι η απόκρυψη της πληροφορίας, δηλαδή η προσπάθεια να αποφευχθεί η αποκάλυψή της σε μη εξουσιοδοτημένες οντότητες.

Στην κρυπτογραφία γενικά χρησιμοποιούνται οι εξής όροι:

**1.Απλό ή μη κρυπτογραφημένο κείμενο (plaintext).** Τα δεδομένα όπως χρησιμοποιούνται από τους ανθρώπους ή τις εφαρμογές.

**2.Κρυπτογραφημένο κείμενο (cipher text).** Τα δεδομένα σε ακατάληπτη για τους ανθρώπους ή τις εφαρμογές μορφή.

**3.Κρυπτογράφηση.** Ο μετασχηματισμός του απλού κειμένου σε κρυπτογραφημένο κείμενο.

**4.Αποκρυπτογράφηση.** Ο μετασχηματισμός του κρυπτογραφημένου κειμένου σε απλό.

**5.Κλειδί.** Μια ποσότητα πληροφορίας (σύνολο bytes) που καθορίζει τους μετασχηματισμούς που θα πραγματοποιηθούν κατά τη διαδικασία της κρυπτογράφησης ή αποκρυπτογράφησης.

Αναφορικά με τις κρυπτογραφικές μεθόδους μπορούμε να διακρίνουμε δύο μείζονες κατηγορίες: η πρώτη είναι οι **συμμετρικοί αλγόριθμοι**, όπου η κρυπτογράφηση και η αποκρυπτογράφηση γίνεται χρησιμοποιώντας το ίδιο κλειδί αλλά αντίστροφες λειτουργίες. Ο πιο διαδεδομένος αλγόριθμος συμμετρικής κρυπτογραφίας είναι ο DES που επινοήθηκε το 1977. Η δεύτερη κατηγορία είναι οι **ασύμμετροι αλγόριθμοι**. Ο πρώτος επινοήθηκε από τους Diffie και Hellmann το 1976. Οι αλγόριθμοι αυτοί χρησιμοποιούν διαφορετικά κλειδιά για τις λειτουργίες της κρυπτογράφησης και της αποκρυπτογράφησης. Τα κλειδιά είναι μαθηματικώς συναρτώμενα μεταξύ τους, αλλά υπάρχει η πρόσθετη απαίτηση να το πολύ ένα εξ αυτών να είναι δυνατόν να υπολογιστεί από το άλλο με «υπολογιστικά εφικτό» τρόπο, ενώ η άλλη κατεύθυνση υπολογισμού θα πρέπει να είναι υπολογιστικά ανέφικτη. Η ιδιότητα αυτή επιτρέπει να δημοσιοποιηθεί το ένα κλειδί (αυτό που υπολογίζεται βάσει του άλλου), ενώ το άλλο κλειδί τηρείται μυστικό και συνδέεται άρρηκτα με την οντότητα που προσδιορίζει. Λόγω του σχήματος λειτουργίας αυτού, οι αλγόριθμοι αυτοί πολλές φορές ονομάζονται αλγόριθμοι δημόσιου κλειδιού.

Ένας ακόμη διαχωρισμός που μπορεί να γίνει στους αλγόριθμους κρυπτογραφίας είναι μεταξύ των αλγορίθμων κρυπτογράφησης κατά μπλοκ και των αλγορίθμων κρυπτογράφησης αλυσιδωτών μπλοκ.

## **2.1 Συμμετρικοί αλγόριθμοι κρυπτογραφίας**

Στα επόμενα εδάφια παρουσιάζονται μερικοί από τους συμμετρικούς αλγόριθμους κρυπτογραφίας που έχουν κατά καιρούς χρησιμοποιηθεί.

### **2.1.1 Κρυπτογράφηση με μεταθέσεις**

Η κρυπτογράφηση με μεταθέσεις βασίζεται στη γενική ιδέα ότι τα bytes του αρχικού μηνύματος αναδιατάσσονται με κάποιον τρόπο που προσδιορίζει ο αλγόριθμος και το κλειδί. Οι πιο γνωστοί αλγόριθμοι είναι : **η απλή μετάθεση**, το «**συρματόπλεγμα**» και η **μετάθεση κατά στήλες**.

#### **Απλή μετάθεση**

Στη διαδικασία της απλής μετάθεσης χρησιμοποιείται ως κλειδί ένα διάνυσμα  $n$ -θέσεων, όπου σε κάθε θέση περιέχεται ένας αριθμός από το ένα έως το  $n$ . Το διάνυσμα πρέπει να περιέχει όλους τους αριθμούς από το ένα έως το  $n$ , και έτσι κάθε αριθμός εμφανίζεται μία μόνο φορά.

Στη διαδικασία κρυπτογράφησης το μήνυμα αρχικά κατατμείται σε μπλοκ μεγέθους  $n$ , και εντός κάθε τμήματος τα bytes αναδιατάσσονται όπως ορίζει το κλειδί. Αν, για παράδειγμα το πρώτο στοιχείο του κλειδιού είναι ίσο με 2, το πρώτο byte στο κρυπτογραφημένο τμήμα θα ισούται με το δεύτερο byte του μη κρυπτογραφημένου τμήματος.

#### **Παράδειγμα:**

Έστω ότι το κλειδί είναι ίσο με (2 5 4 1 3) και το μη κρυπτογραφημένο κείμενο είναι ίσο με ΜΥΣΤΙΚΟ ΜΗΝΥΜΑ. Αρχικά πρέπει να κατατμηθεί το μη κρυπτογραφημένο κείμενο σε τεμάχια των 5 bytes, όσο δηλαδή και το μήκος του κλειδιού. Επειδή το μήνυμα έχει μήκος 14 bytes, το οποίο δεν είναι ακέραιο πολλαπλάσιο του 5, θα συμπληρωθεί με τον ειδικό χαρακτήρα  $\emptyset$ , ο οποίος κανονικά δεν είναι δυνατόν να εμφανισθεί ανάμεσα στους παραδεκτούς χαρακτήρες του μη

κρυπτογραφημένου μηνύματος. Έτσι τα τεμάχια του μη κρυπτογραφημένου μηνύματος θα έχουν ως ακολούθως:

ΜΥΣΤΙ	ΚΟ ΜΗ	ΝΥΜΑØ
-------	-------	-------

Το κάθε τμήμα πλέον αναδιατάσσεται όπως ορίζει το κλειδί, καταλήγοντας στο κρυπτογραφημένο μήνυμα:

ΥΙΤΜΣ	ΟΗΜΚ	ΥØΑΝΜ
-------	------	-------

Η διαδικασία της αποκρυπτογράφησης ακολουθεί ακριβώς την αντίστροφη διαδικασία, ακολουθούμενη από την εξάλειψη των χαρακτήρων «Ø» που υπάρχουν στο τέλος του μηνύματος.

### «Συρματοπλέγμα»

Στην κρυπτογράφηση βάσει της μεθόδου του «συρματοπλέγματος» το μη κρυπτογραφημένο μήνυμα αρχικά γράφεται κατά μήκος ενός νοητού «σύρματος» που έχει την ακόλουθη μορφή:



Το πλήθος των χαρακτήρων που γράφονται σε κάθε τμήμα του σύρματος καθορίζεται από το κλειδί. Αφού το απλό κείμενο γραφεί κατ' αυτή την έννοια, διαβάζεται ακολούθως κατά γραμμές, διαμορφώνοντας έτσι το κρυπτογραφημένο κείμενο.

### Παράδειγμα:

Έστω ότι το κλειδί μας υποδεικνύει να γράφονται τρία bytes σε κάθε τμήμα του «συρματοπλέγματος» και ότι το απλό κείμενο είναι ΜΥΣΤΙΚΟ ΜΗΝΥΜΑ. Η γραφή στο «συρματοπλέγμα» θα έχει ως εξής:

Μ				Ι				Μ				Μ	
	Υ		Τ		Κ				Η		Υ		Α
		Σ				Ο					Ν		

Στη συνέχεια, διαβάζοντας τον ανωτέρω πίνακα κατά γραμμές (αρχικά η πρώτη γραμμή, ακολούθως η δεύτερη κ.λπ.) καταλήγουμε στο ακόλουθο κρυπτογραφημένο μήνυμα:

ΜΙΜΜΥΤΚ ΗΥΑΣΟΝ

Το κλειδί σε μία τέτοια κρυπτογράφηση αποτελείται από δύο ακεραίους, ο πρώτος από τους οποίους προσδιορίζει το πλήθος των bytes που γράφουμε σε κάθε «τμήμα σύρματος» ( ισοδύναμο με το πλήθος των γραμμών του ανωτέρω πίνακα) και ο δεύτερος τη μετατόπιση έναρξης, που ουσιαστικά υποδεικνύει πόσες στήλες στον ως άνω πίνακα θα αφήσουμε κενές πριν αρχίσουμε να γραφούμε τα bytes του απλού κειμένου.

### Μετάθεση κατά στήλες

Στη μετάθεση κατά στήλες ως κλειδί χρησιμοποιείται μία λέξη, της οποίας τα γράμματα αντιστοιχίζονται σε αριθμούς, ανάλογα με τη σειρά εμφάνισής τους στο αλφάβητο. Για παράδειγμα, αν η λέξη-κλειδί είναι:

ΠΟΛΥΜΕΡΕΣ

η αντιστοιχία των γραμμάτων του κλειδιού σε αριθμούς εκφράζεται από το διάνυσμα (6 5 3 9 4 1 7 2 8)

(Το Ε αντιστοιχίζεται στο 1 γιατί είναι το μικρότερο λεξικογραφικά γράμμα της λέξης, ενώ η δεύτερη εμφάνιση του Ε αντιστοιχίζεται με το 2. Το επόμενο λεξικογραφικά γράμμα είναι το Λ, που αντιστοιχίζεται στον αριθμό 3 κ.ο.κ.). Στη συνέχεια, το μη κρυπτογραφημένο κείμενο γράφεται σε έναν πίνακα που έχει τόσες στήλες όσες τα γράμματα του κλειδιού, ενώ το πλήθος γραμμών καθορίζεται από το μήκος του μη κρυπτογραφημένου κειμένου. Τέλος, το κρυπτογραφημένο κείμενο παράγεται με ανάγνωση του πίνακα κατά στήλες, με τη σειρά που ορίζεται από την απεικόνιση του κλειδιού. Για παράδειγμα, αν το μη κρυπτογραφημένο κείμενο είναι ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ

για να κρυπτογραφηθεί με το κλειδί ΠΟΛΥΜΕΡΕΣ θα γραφεί σε έναν πίνακα ως εξής:

Π	Ο	Λ	Υ	Μ	Ε	Ρ	Ε	Σ
6	5	3	9	4	1	7	2	8
Α	Σ	Π	Ρ	Η		Π	Ε	Τ
Ρ	Α		Ξ	Ε	Ξ	Α	Σ	Π
Ρ	Η	∅	∅	∅	∅	∅	∅	∅

και το κρυπτογραφημένο κείμενο που θα παραχθεί θα είναι Ξ∅ΕΣ∅Π  
∅ΗΕ∅ΣΑΗΑΡΡΠΑ∅ΤΠ∅ΡΞ∅

Βλέπουμε ότι το μη κρυπτογραφημένο κείμενο συμπληρώνεται με τον ειδικό χαρακτήρα ∅ προκειμένου να αποκτήσει μήκος πολλαπλάσιο του κλειδιού.

### 2.1.2 Κρυπτογράφηση με αντικατάσταση

Η κρυπτογράφηση με αντικατάσταση βασίζεται στη γενική ιδέα ότι η παραγωγή του κρυπτογραφημένου κειμένου γίνεται αντικαθιστώντας κάθε ένα byte του μη κρυπτογραφημένου κειμένου με κάποιο άλλο byte, όπως προκύπτει από μία συνάρτηση αντικατάστασης. Στη συνέχεια παρουσιάζονται τα πιο χαρακτηριστικά παραδείγματα.

#### Απλή αντικατάσταση

Στην απλή αντικατάσταση, για κάθε γράμμα του αλφαβήτου των μηνυμάτων ορίζουμε την απεικόνισή του, συνήθως μέσω ενός πίνακα. Αν, για παράδειγμα, το αλφάβητο των μηνυμάτων είναι το Ελληνικό αλφάβητο, ο πίνακας απεικόνισης θα μπορούσε να έχει την εξής μορφή:

Α	Β	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
Δ	Κ	Ρ	Ο	Υ	Λ	Ω	Ε	Π	Η	Α	Φ	Ζ	Μ	Τ	Β	Χ	Θ	Ν	Ψ	Γ	Ι	Σ	Ξ

Με βάση τον πίνακα αυτόν, η κρυπτογράφηση του απλού κειμένου:

ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ

παράγει το κρυπτογραφημένο κείμενο:

ΔΘΒΧΩ ΒΥΝΧΔ ΜΥΜΔΘΒΧΩ

Η συγκεκριμένη μέθοδος κρυπτογράφησης έχει το μειονέκτημα να είναι ιδιαίτερα ευάλωτη σε επιθέσεις βασισμένες σε στατιστικές αναλύσεις εμφάνισης μεμονωμένων χαρακτήρων, ζευγών, τριάδων, κ.λπ.

#### Πολυαλφαβητική αντικατάσταση

Η πολυαλφαβητική αντικατάσταση είναι μία φυσική επέκταση της απλής αντικατάστασης, όπου πέρα από τον πίνακα αντικατάστασης χρησιμοποιεί και ένα επιπλέον κλειδί Κ, του οποίου τα στοιχεία ανήκουν σε ένα αλφάβητο Α<sub>κ</sub>. Ο πίνακας αντικαταστάσεων έχει τόσες στήλες όσα τα στοιχεία του αλφαβήτου μηνυμάτων και τόσες γραμμές όσα τα στοιχεία του Α<sub>κ</sub>, το κάθε δε στοιχείο

του πίνακα περιέχει τον χαρακτήρα του αλφαβήτου κρυπτογραφημένων μηνυμάτων που πρέπει να χρησιμοποιηθεί όταν κρυπτογραφείται το στοιχείο του αλφαβήτου μηνυμάτων που αντιστοιχεί στη στήλη με το στοιχείο του αλφαβήτου κλειδιών που αντιστοιχεί στη γραμμή. Αν  $M_i$  είναι ο υπ' αριθμόν  $i$  χαρακτήρας του μη κρυπτογραφημένου μηνύματος και  $K_i$  ο υπ' αριθμόν  $i$  χαρακτήρας του κλειδιού, ο υπ' αριθμόν  $i$  χαρακτήρας του κρυπτογραφημένου μηνύματος είναι η καταχώρηση στη θέση  $(K_i, M_i)$  του πίνακα.

### Παράδειγμα:

Έστω ότι το αλφάβητο των μη κρυπτογραφημένων μηνυμάτων και των κρυπτογραφημένων μηνυμάτων είναι το ελληνικό αλφάβητο, το αλφάβητο των κλειδιών είναι το  $\{A, B\}$ , και ο πίνακας αντικατάστασης είναι ο εξής:

	A	B	Γ	Δ	Ε	Ζ	Η	Θ	Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω
A	Δ	Κ	Ρ	Ο	Υ	Λ	Ω	Ε	Π	Η	Α	Φ	Ζ	Μ	Τ	Β	Χ	Θ	Ν	Ψ	Γ	Ι	Σ	Ξ
B	Η	Λ	Θ	Ρ	Δ	Ξ	Κ	Α	Φ	Ο	Γ	Ψ	Π	Ι	Υ	Χ	Μ	Β	Σ	Ω	Ε	Ν	Ζ	Τ

τότε η κρυπτογράφηση του απλού κειμένου

ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ

με το κλειδί:

ABBA BBAAB BAABBAAB

παράγει το κρυπτογραφημένο κείμενο :

ΔΒΧΧΩ ΧΔΝΧΗ ΙΘΜΗΒΒΧΚ

Ένα ζήτημα που τίθεται στην πολυαλφαβητική αντικατάσταση είναι τι συμβαίνει αν το μήκος του μη κρυπτογραφημένου κειμένου είναι μεγαλύτερο από αυτό του κλειδιού. Στην περίπτωση αυτή υπάρχουν οι κάτωθι επιλογές:

το κλειδί χρησιμοποιείται εξ αρχής, π.χ. αν το κλειδί είναι ABBA μπορεί να επεκταθεί σε ABBAABBAABBAABBA...

το κλειδί χρησιμοποιείται μετασχηματισμένο, π.χ. αυξάνοντας όλους τους χαρακτήρες του κατά ένα, π.χ. το κλειδί HAL θα γίνει HALIBMJCN...

χρησιμοποιούνται ως κλειδί οι αρχικοί χαρακτήρες του μη κρυπτογραφημένου κειμένου, π.χ. αν το κείμενο είναι ΑΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑΣΠΡΗ και το κλειδί είναι ABBA, το τελικό κλειδί που θα χρησιμοποιηθεί θα είναι BBAAΣΠΡΗ ΠΕΤΡΑ ΞΕΞΑ. Για να είναι εφικτή αυτή η μέθοδος θα πρέπει το αλφάβητο των κλειδιών και το αλφάβητο των μη κρυπτογραφημένων μηνυμάτων να ταυτίζονται.

## 2.2 Ασύμμετροι αλγόριθμοι κρυπτογραφίας

Οι ασύμμετροι αλγόριθμοι κρυπτογραφίας, σε αντίθεση με τους συμμετρικούς, χρησιμοποιούν δύο διαφορετικά κλειδιά για τις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης. Τα κλειδιά αυτά χρησιμοποιούνται κατά ζεύγη με το ένα κλειδί συνήθως να τηρείται μυστικό (στην κατοχή του ιδιοκτήτη) και το άλλο να δημοσιοποιείται.

Οι ασύμμετροι αλγόριθμοι μπορούν περαιτέρω να διαχωρισθούν σε δύο υποκατηγορίες, τους αντιστρέψιμους και τους μη αντιστρέψιμους. Αν  $E$  είναι η συνάρτηση κρυπτογράφησης και  $D$  είναι η συνάρτηση αποκρυπτογράφησης, και  $E_k$  και  $D_k$  τα αντίστοιχα κλειδιά, για έναν αντιστρέψιμο αλγόριθμο ισχύει:

$$D(E(\text{data}, E_k), D_k) = E(D(\text{data}, D_k), E_k) = \text{data}$$

Με άλλα λόγια δηλαδή, η σειρά εφαρμογής των πράξεων κρυπτογράφησης και αποκρυπτογράφησης δεν επηρεάζει το αποτέλεσμα. Η ιδιότητα αυτή επιτρέπει σε έναν μοναδικό αλγόριθμο - και ενδεχομένως ένα ζεύγος κλειδιών - να χρησιμοποιηθεί τόσο για στόχους αυθεντικότητας όσο και για εμπιστευτικότητας, υπό το σχήμα ότι χρησιμοποιεί κανείς το δικό του μυστικό κλειδί για να δημιουργήσει μια δική του ψηφιακή υπογραφή η οποία μπορεί να επαληθευτεί από οποιονδήποτε βάσει του δημόσιου κλειδιού, ενώ παράλληλα οποιοσδήποτε μπορεί να κρυπτογραφήσει πληροφορία με το δημόσιο κλειδί και να την αποστείλει στον κάτοχο του ιδιωτικού

κλειδιού, ο οποίος είναι ο μόνος που μπορεί να την αποκρυπτογραφήσει. Ο πιο γνωστός αντιστρέψιμος ασύμμετρος αλγόριθμος είναι ο RSA. Οι μη αντιστρέψιμοι ασύμμετροι αλγόριθμοι δεν έχουν αυτή την ιδιότητα, δηλ. δεν είναι δυνατόν να ανακτηθούν τα αρχικώς κρυπτογραφημένα δεδομένα από τα κρυπτογραφημένα, και συνεπώς δεν υπάρχουν συναρτήσεις κρυπτογράφησης-αποκρυπτογράφησης με την ανωτέρω έννοια. Οι αλγόριθμοι αυτοί επιτρέπουν την διακρίβωση ότι μία ψηφιακή υπογραφή δημιουργήθηκε με ένα συγκεκριμένο μυστικό κλειδί, χρησιμοποιώντας το αντίστοιχο δημόσιο κλειδί. Για τον λόγο αυτό η συγκεκριμένη κατηγορία αλγορίθμων καλείται αλγόριθμοι υπογραφής μόνο.

### 3. Εισαγωγή στο CrypTool

Το CrypTool αποτελεί ένα πρόγραμμα με μία εξαιρετικά περιεκτική σε απευθείας σύνδεση βοήθεια που επιτρέπει στον χρήστη να χρησιμοποιήσει και να αναλύσει τις κρυπτογραφικές διαδικασίες μέσα σε ένα ενοποιημένο γραφικό περιβάλλον.

Το CrypTool αναπτύχθηκε κατά τη διάρκεια του προγράμματος συνειδητοποίησης των χρηστών της Deutsche Bank προκειμένου να αυξηθεί η κατανόησή τους σε ζητήματα ασφάλειας. Ένας περαιτέρω στόχος ήταν να δώσει τη δυνατότητα στους χρήστες να καταλάβουν τις κρυπτογραφικές διαδικασίες.

Το CrypTool χρησιμοποιείται αυτήν την περίοδο για εκπαιδευτικούς λόγους σε επιχειρήσεις και πανεπιστήμια, ενώ επιπλέον διάφορα πανεπιστήμια βοηθούν στην περαιτέρω ανάπτυξη του προγράμματος.

Πληροφορίες για το CrypTool θα βρείτε στις ιστοσελίδες:

<http://www.cryptool.de>  
<http://www.cryptool.org>  
<http://www.cryptool.com>

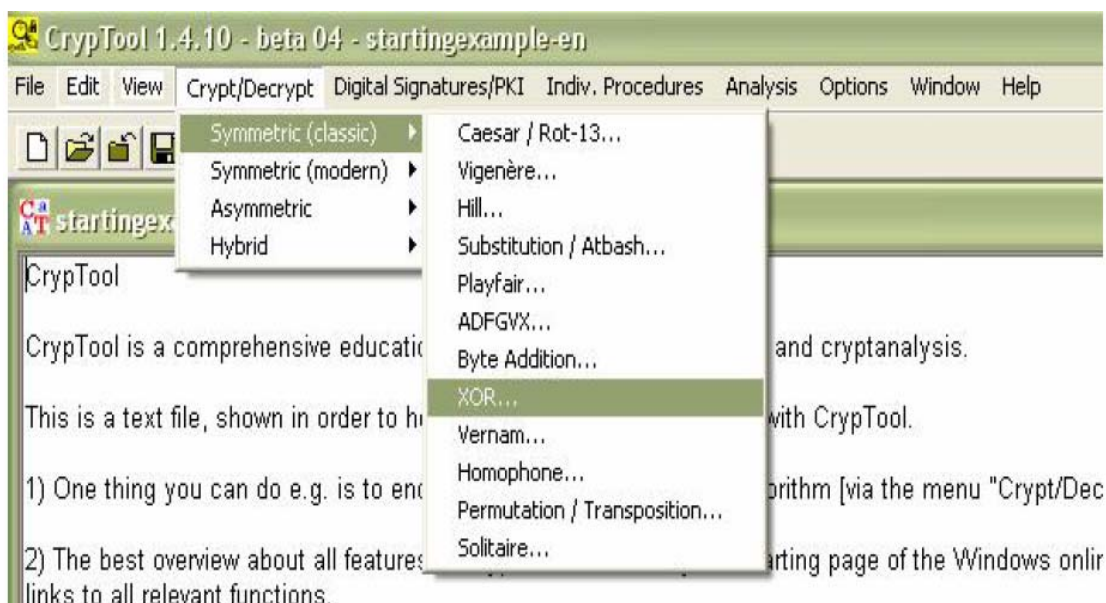
### Μηχανισμοί και Αλγόριθμοι Κρυπτογραφίας στο CrypTool

Το πρόγραμμα CrypTool μπορεί να διαβάσει μόνο αρχεία τύπου \*.txt, τα οποία είτε τα έχετε δημιουργήσει ήδη από πιο πριν στον υπολογιστή σας και θέλετε να τα επεξεργαστείτε μέσω του προγράμματος, είτε τα δημιουργείτε απ' ευθείας μέσω του CrypTool. Για να δημιουργήσετε ένα νέο μήνυμα, λοιπόν, μέσω του ίδιου του προγράμματος επιλέγετε από το βασικό μενού File New ή Ctrl+N.

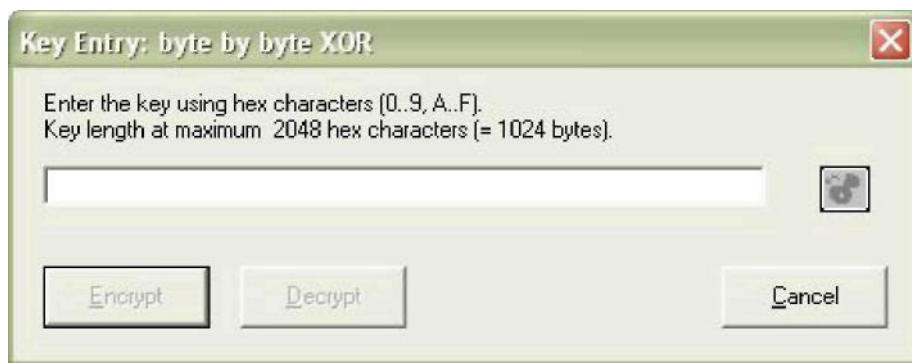
### Συμμετρικοί αλγόριθμοι κρυπτογραφίας

#### Η λογική πράξη XOR

Η κρυπτογράφηση του αρχικού κειμένου την χρήση του κλασσικού αλγόριθμου XOR γίνεται όπως βλέπετε στην εικόνα που ακολουθεί:







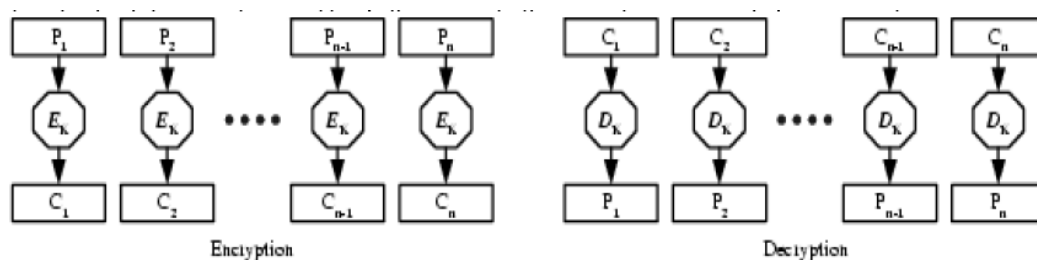
Μας ζητείτε να εισάγουμε ένα κλειδί το οποίο μπορεί να πάρει σαν παραμέτρους είτε αριθμούς (0,...,9) είτε χαρακτήρες από το γράμμα A μέχρι το γράμμα F à Encrypt. Κάνουμε ακριβώς την ίδια διαδικασία και για αποκρυπτογράφηση του μηνύματος (Decrypt).

## Ο αλγόριθμος DES

Ο DES (Data Encryption Standard) αντιπροσωπεύει την τυποποίηση Federal Information Processing Standard (FIPS) 46-1, που αναπτύχθηκε από την IBM, και είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος.

Ο DES χρησιμοποιεί κλειδί με μέγεθος 64 bit από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Ο DES, εκτός από κρυπτογράφηση μηνυμάτων, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα.

Σε ECB mode, το κείμενο χωρίζεται σε ισομήκη τμήματα. Κάθε μη κρυπτογραφημένο τμήμα (block) κρυπτογραφείται ανεξάρτητα από τη συνάρτηση του βασικού κώδικα τμήματος. Μειονέκτημα αυτού του τρόπου είναι ότι ομοιότητες του αρχικού κειμένου δεν καλύπτονται. Τα αποκρυπτογραφημένα τμήματα που είναι ταυτόσημα, δίνουν ταυτόσημα κρυπτογραφημένα τμήματα και το κείμενο μπορεί εύκολα να τροποποιηθεί με την αφαίρεση, πρόσθεση ή και ανακατάταξη των όμοιων κρυπτογραφημένων τμημάτων. Η ταχύτητα της κρυπτογράφησης για κάθε αρχικό τμήμα είναι ίδια με την ταχύτητα του κώδικα τμήματος. Ο ECB επιτρέπει την παράλληλη παραγωγή των κρυπτογραφημένων τμημάτων για καλύτερη απόδοση.



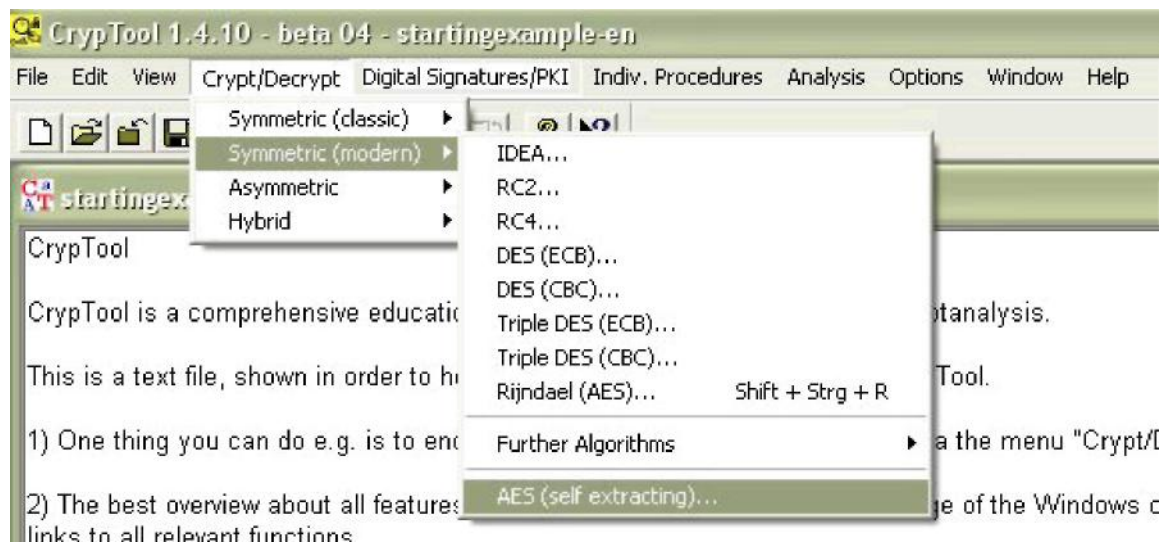
Σε CBC mode, κάθε μη κρυπτογραφημένο τμήμα (block) συνδυάζεται μέσω της λογικής πράξης XOR με το πρωτύττερα κρυπτογραφημένο block. Το αποτέλεσμα κρυπτογραφείται. Απαιτείται μια αρχική τιμή για την πρώτη XOR πράξη που καλείται Διάνυσμα Αρχικοποίησης (Initialization Vector),  $c_0$ . Τα όμοια αρχικά τμήματα καλύπτονται με τη χρήση της λογικής πράξης και αυξάνεται η ασφάλεια του αλγόριθμου. Η ταχύτητα της κρυπτογράφησης είναι ίδια με αυτή του κώδικα τμήματος, αλλά η διαδικασία δεν μπορεί να πραγματοποιηθεί παράλληλα παρόλο που η αποκρυπτογράφηση μπορεί.





Το πρότυπο AES περιγράφει μια συμμετρική block διαδικασία κρυπτογράφησης μυστικού κλειδιού. Το πρότυπο υποστηρίζει την χρήση κλειδιών μήκους 128, 192 και 256 bits. Ανάλογα με το ποιο μήκος κλειδιού χρησιμοποιείται, συνήθως χρησιμοποιείται η συντόμευση AES-128, AES-192 και AES-256 αντίστοιχα. Ανεξάρτητα από το μήκος κλειδιού, ο αλγόριθμος επενεργεί πάνω σε block δεδομένων μήκους 128 bits. Η διαδικασία κρυπτογράφησης είναι επαναληπτική. Αυτό σημαίνει ότι σε κάθε block δεδομένων γίνεται μια επεξεργασία η οποία επαναλαμβάνεται έναν αριθμό από φορές ανάλογα με το μήκος κλειδιού. Κάθε επανάληψη ονομάζεται γύρος (round). Στον πρώτο γύρο επεξεργασίας ως είσοδος είναι ένα μη κρυπτογραφημένο (plaintext) block και το αρχικό κλειδί, ενώ στους γύρους που ακολουθούν ως είσοδος είναι το block που έχει προκύψει από τον προηγούμενο γύρο καθώς και ένα κλειδί που έχει παραχθεί από το αρχικό με βάση κάποια διαδικασία που ορίζει ο αλγόριθμος. Το τελικό προϊόν της επεξεργασίας είναι το κρυπτογραφημένο block (ciphertext). Το block αυτό πρέπει να σημειωθεί ότι έχει ακριβώς το ίδιο μέγεθος (128 bits) με το plaintext block.

Η κρυπτογράφηση του αρχικού κειμένου την χρήση του συμμετρικού αλγόριθμου AES (self extracting) γίνεται όπως βλέπετε στην εικόνα που ακολουθεί:

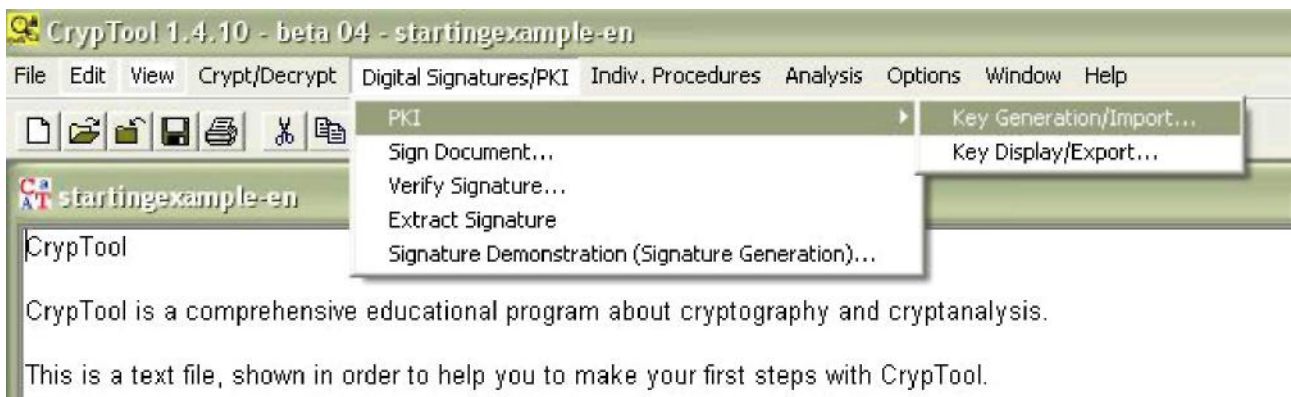


Με αυτόν τον τρόπο μας δίνεται η δυνατότητα να κρυπτογραφήσουμε ένα αρχείο ή έναν φάκελο, τον οποίο μπορούμε να αναζητήσουμε μέσα στον υπολογιστή μας. Στο παράθυρο που εμφανίζεται εισάγουμε έναν κωδικό για το κλειδί μας. Εμφανίζεται ένα νέο παράθυρο το οποίο μας ζητάει να αποθηκεύσουμε κάπου μέσα στον υπολογιστή μας το εκτελέσιμο αρχείο (\*.exe) που δημιουργείται. Αυτή η δυνατότητα μας δίνει την ευχέρεια να στείλουμε το αρχείο μας όπου θέλουμε χωρίς ο παραλήπτης του να έχει το ίδιο πρόγραμμα ή να έχει το αρχείο αποκρυπτογράφησης. Εξάλλου ένα αρχείο \*.exe δεν σημαίνει ότι είναι και κρυπτογραφημένο για να κινεί υποψίες. Κάνουμε ακριβώς την ίδια διαδικασία και για αποκρυπτογράφηση του μηνύματος (Decrypt).



### Δημιουργία ενός ασύμμετρου ζεύγους κλειδιών

Για τη δημιουργία ενός ασύμμετρου ζεύγους κλειδιών μέσω του προγράμματος CrypTool ακολουθούμε τα βήματα όπως φαίνονται στις παρακάτω εικόνες:



Στην καρτέλα που εμφανίζεται επιλέγουμε τον τύπο του αλγορίθμου που θέλουμε για τη δημιουργία του ζεύγους κλειδιών μεταξύ των RSA, DSA και της μεθόδου Elliptic curves. Στο πεδίο User Data συμπληρώνουμε τα στοιχεία μας (επώνυμο, όνομα, όνομα κλειδιού, PIN και επαλήθευση PIN) και τέλος πατάμε πάνω στην επιλογή "Generate new key pair...".

Στη συνέχεια εμφανίζεται ένα νέο παράθυρο που μας πληροφορεί για την κατάσταση της δημιουργίας του ζεύγους κλειδιών και μας παρακινεί στο να κουνήσουμε το ποντίκι του υπολογιστή μας ή να πατήσουμε διάφορα πλήκτρα από το πληκτρολόγιό μας ώστε να ολοκληρωθεί η διαδικασία.

Το επόμενο παράθυρο που εμφανίζεται ονομάζεται "Public parameters" και μας δίνει κάποιες πληροφορίες για το ζεύγος κλειδιών που μόλις δημιουργήσαμε. Πατάμε την επιλογή "Apply" και ένα νέο μήνυμα εμφανίζεται στην οθόνη μας που μας πληροφορεί για την επιτυχή δημιουργία του ζεύγους κλειδιών.

### Generation of Asymmetric Key Pair

Algorithm

☒ RSA  
Bit length of RSA modulus: 1024

☐ DSA  
Bit length of DSA prime number: 1024

☐ Elliptic curves  
Identifier (bit length and curve parameter): prime239v1

User data

The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.

Last name: koletsou

First name: efi

Key identifier (optional): myKey

PIN: .....

PIN verification: .....

The domain parameter of the selected elliptic curve will be shown below.

Parameters	Value of the parameter	Bit len...
------------	------------------------	------------

Base for presentation of numbers

☐ Octal ☒ Decimal ☐ Hexadecimal

☒ Display generated key pair

### SECURE Crypto Runtime - Random Number Generator

Random Number Generation

Move your mouse and press different keys on your keyboard until enough random material is collected.

### Public parameters

Show public parameters of [koletsou][efi][RSA-1024][1181057225][myKey]

Variable	Value
Modulus	17933534440533168350600665348631975350853289872316681584215...
Expon...	65537

Base for presentation of numbers

☐ Octal ☒ Decimal ☐ Hexadecimal

### CrypTool

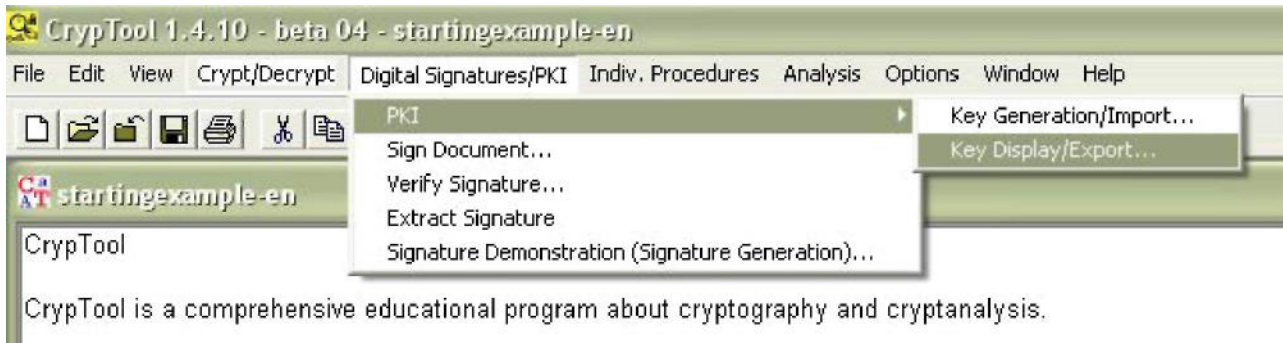
 The parameters chosen by you and the new key pair have been successfully saved. The assigned key identifier is '[koletsou][efi][RSA-1024][1181057225][myKey]'.

Elapsed time while creating key pair: 12.313 seconds.

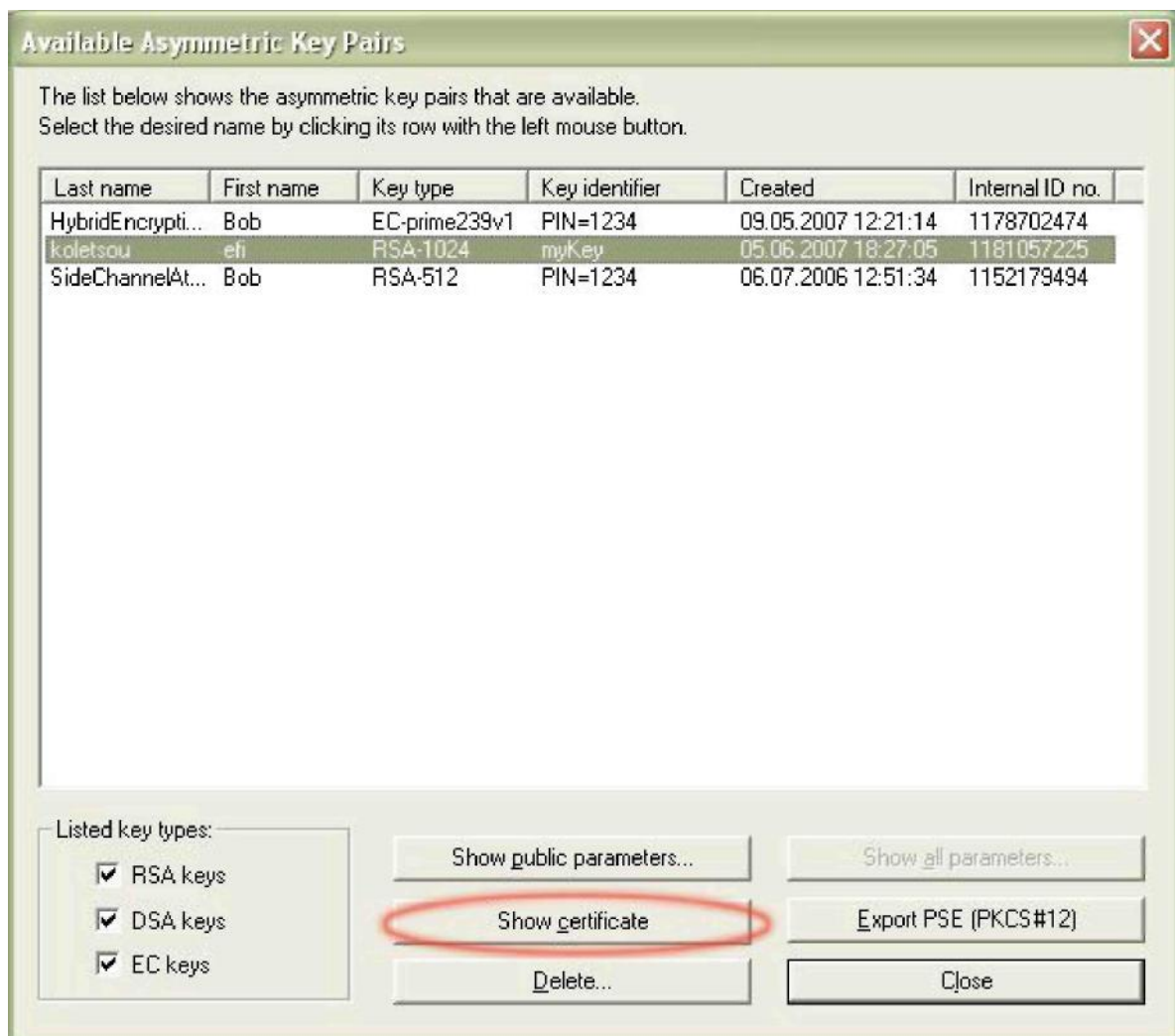


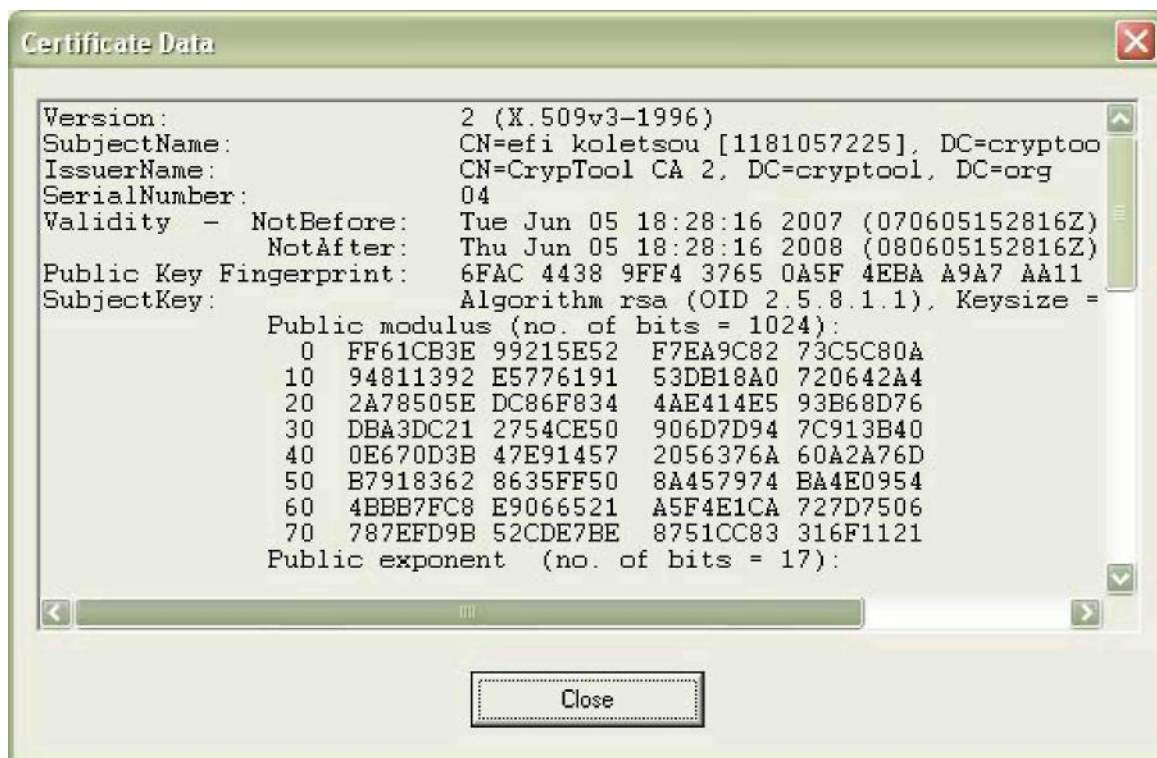
## Εμφάνιση των πληροφοριών που σχετίζονται με το ζεύγος κλειδιών

Για να εμφανίσουμε πληροφορίες που σχετίζονται με το ζεύγος κλειδιών που έχουμε κατασκευάσει μέσω του προγράμματος CrypTool ακολουθούμε τα βήματα που παρουσιάζονται στις παρακάτω εικόνες:



Επιλέγουμε το ζεύγος των κλειδιών μας και πατάμε πάνω στην επιλογή "Show certificate". Μας εμφανίζεται ένα νέο παράθυρο που μας δίνει όλες τις σχετικές λεπτομέρειες για το ζεύγος κλειδιών μας.





## Ασύμμετροι αλγόριθμοι κρυπτογραφίας

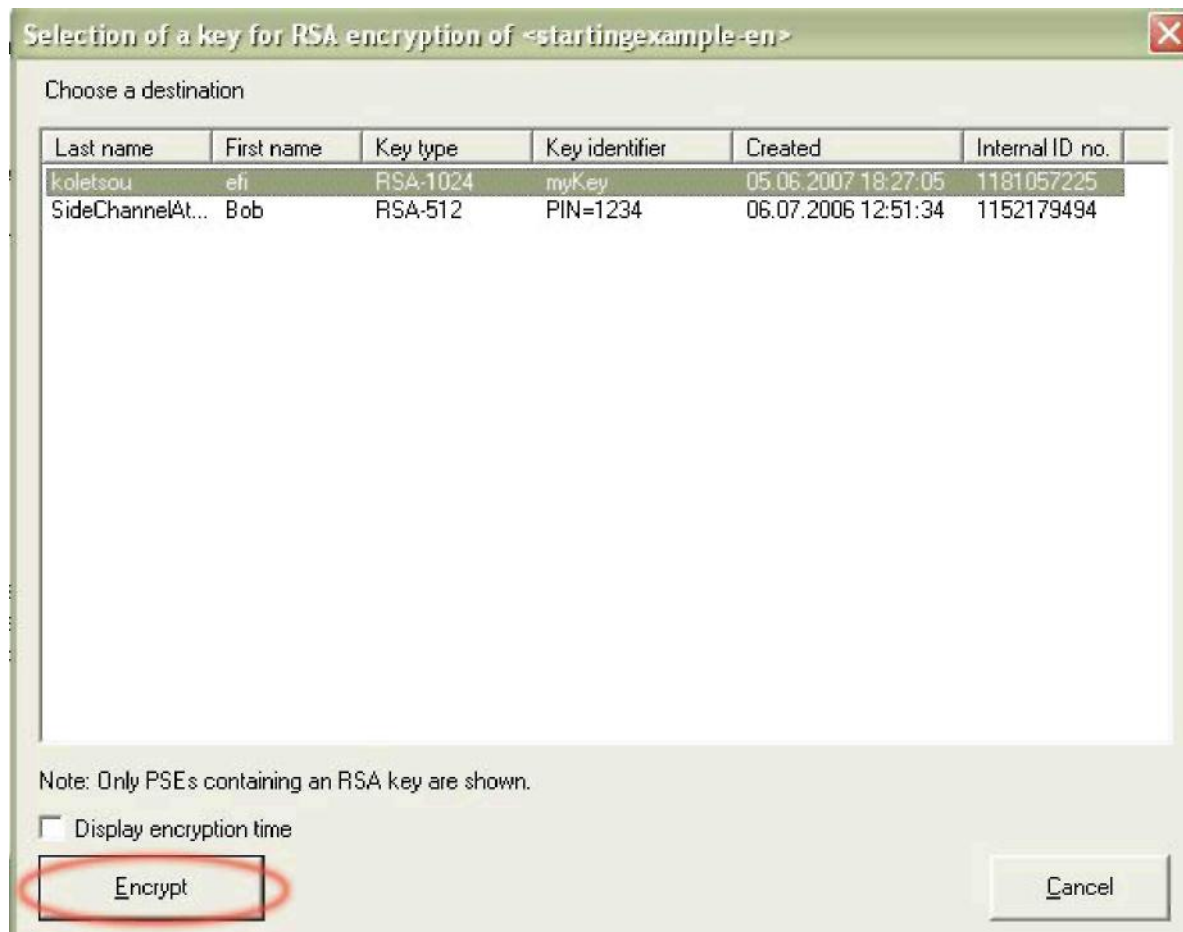
### Ο αλγόριθμος RSA

Ο RSA ανήκει στην οικογένεια των ασύμμετρων αλγορίθμων και προσφέρει τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Επινόηθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman, από τα αρχικά των οποίων προέρχεται και η ονομασία του. Η ασφάλειά του έγκειται στη δυσκολία της παραγοντοποίησης (factorization) πολύ μεγάλων φυσικών αριθμών. Το μέγεθος των κλειδιών διαφέρει σημαντικά σε σχέση με αυτό ενός κλειδιού του συστήματος της συμμετρικής κρυπτογραφίας. Στο σύστημα RSA ένα κλειδί με μήκος 512bit θεωρείται αναξιόπιστο, ένα με μήκος 768bit προσφέρει μέση ασφάλεια, ένα με 1024bit καλή, ενώ ένα με μήκος 2048bit θα παραμείνει απαραβίαστο για αρκετές δεκαετίες ακόμα (αν και με το ρυθμό ανάπτυξης της τεχνολογίας ποτέ δεν μπορεί να είναι κανείς σίγουρος).

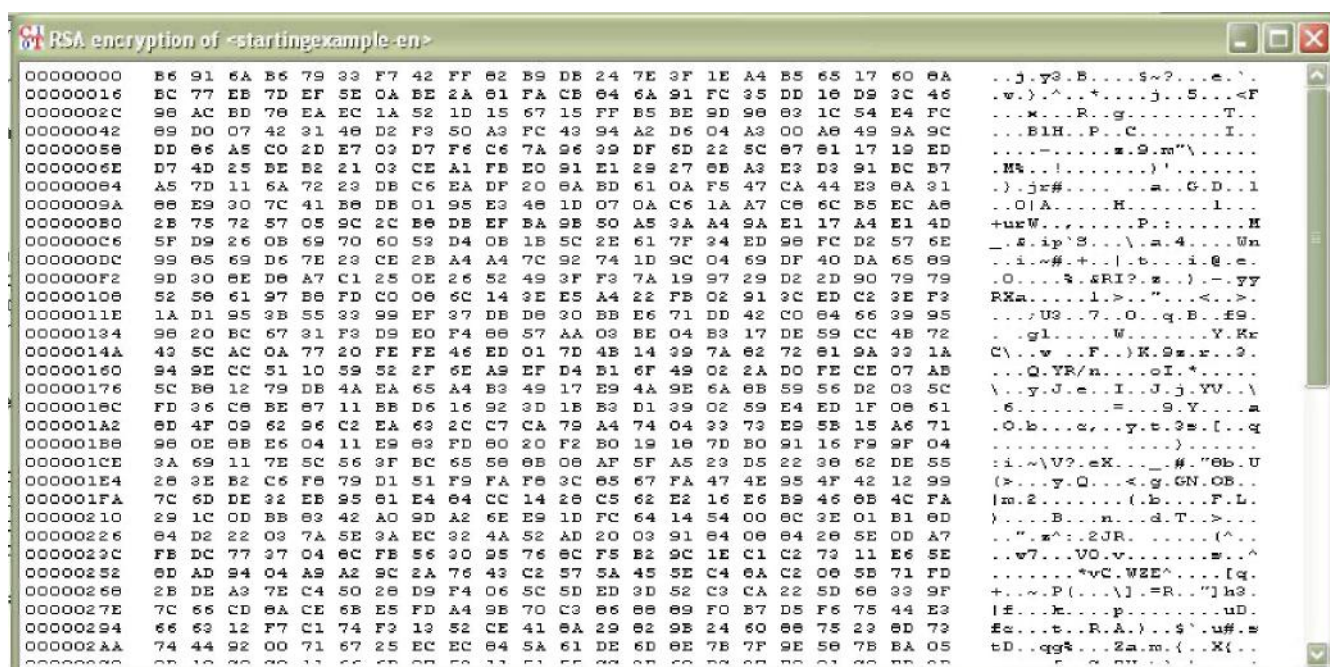
Με το RSA η κρυπτογράφηση και η πιστοποίηση ταυτότητας πραγματοποιούνται χωρίς την κοινή χρήση ιδιωτικών κλειδιών. Ο καθένας χρησιμοποιεί μόνο το δικό του ιδιωτικό κλειδί ή το δημόσιο κλειδί οποιουδήποτε άλλου. Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα ή να επαληθεύσουν μία υπογραφή, αλλά μόνο ο κάτοχος του σωστού ιδιωτικού κλειδιού μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα.

Η κρυπτογράφηση του αρχικού κειμένου την χρήση του ασύμμετρου αλγορίθμου RSA γίνεται όπως βλέπετε στην εικόνα που ακολουθεί:





Αφού επιλέξουμε το δικό μας ζεύγος κλειδιών πατάμε πάνω στην επιλογή "Encrypt" και σε ένα νέο παράθυρο μας εμφανίζεται το κρυπτογραφημένο κείμενο.



## Υβριδική κρυπτογραφία

Ιδιαίτερο ενδιαφέρον για την επίτευξη ασφαλούς επικοινωνίας μεταξύ δύο μερών παρουσιάζει η υβριδική κρυπτογραφία που είναι γνωστή και ως ψηφιακός φάκελος (digital envelope) και αξιοποιεί ταυτόχρονα τις τεχνικές συμμετρικής και ασύμμετρης κρυπτογραφίας. Η υβριδική αυτή



κρυπτογραφία μπορεί να χρησιμοποιηθεί για πολλούς παραλήπτες ταυτόχρονα. Τα βήματα που ακολουθούνται για τη δημιουργία ενός ψηφιακού φακέλου είναι τα εξής:

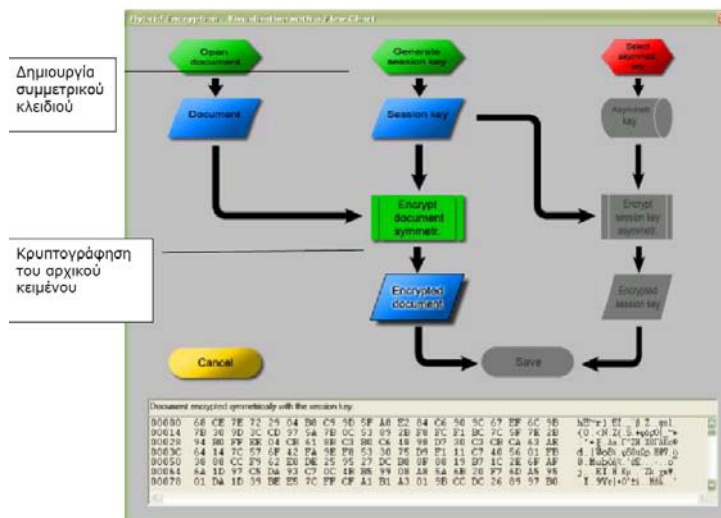
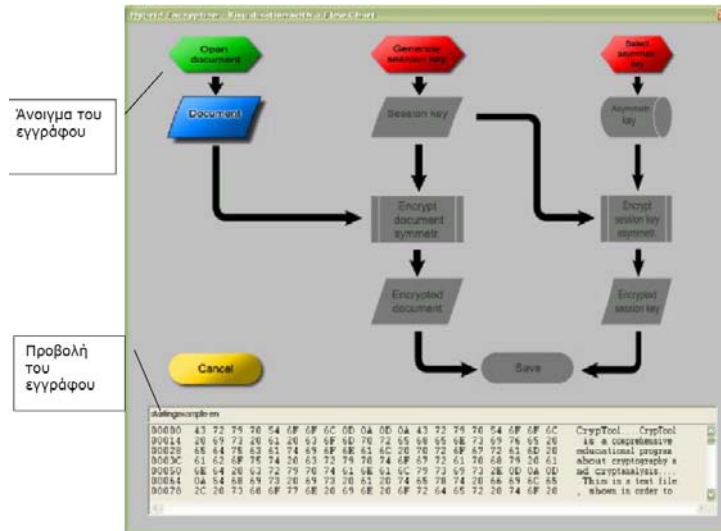
1. Δημιουργείται ένα συμμετρικό κλειδί κρυπτογραφίας με χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας (π.χ. του DES ή του AES).
2. Η αρχική πληροφορία κρυπτογραφείται με το συμμετρικό κλειδί που έχει δημιουργηθεί.
3. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.
4. Τα δύο κρυπτογραφημένα κείμενα αποτελούν τον ψηφιακό φάκελο του παραλήπτη.

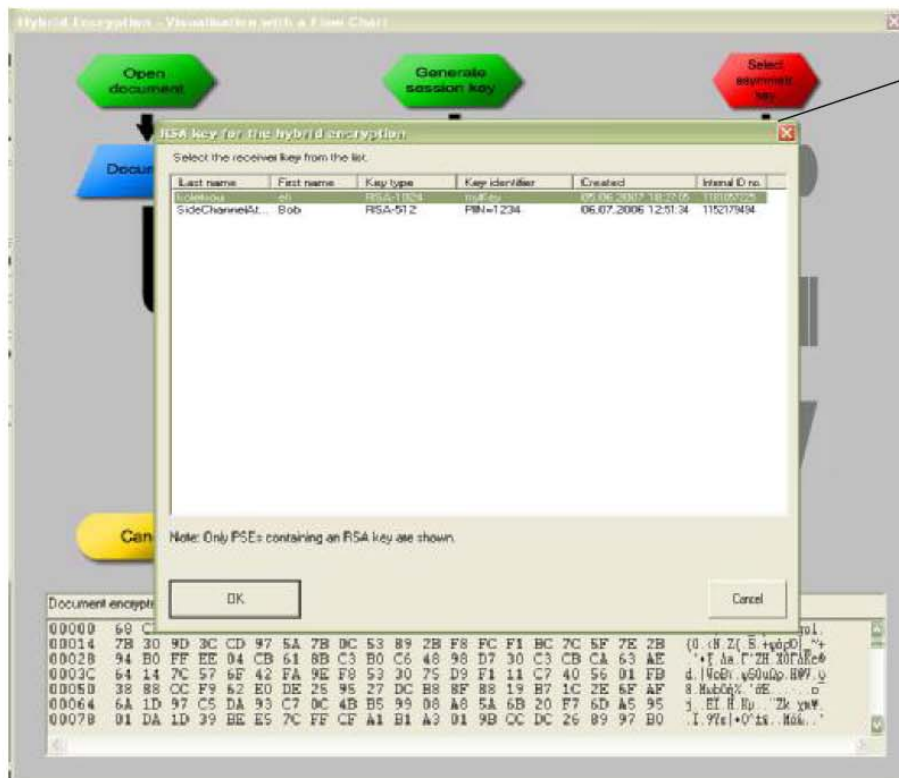
Ο παραλήπτης ανοίγει τον ψηφιακό του φάκελο αποκρυπτογραφώντας με το ιδιωτικό κλειδί του το κρυπτογραφημένο συμμετρικό κλειδί. Με χρήση του συμμετρικού κλειδιού ο παραλήπτης αποκρυπτογραφεί το αρχικό κείμενο. Μετά την επίτευξη μιας ασφαλούς επικοινωνίας μεταξύ αποστολέα και παραλήπτη το συμμετρικό κλειδί καταστρέφεται.

Η χρήση της υβριδικής κρυπτογραφίας βοηθά στο να ξεπεραστούν κάποιες σημαντικές αδυναμίες της κρυπτογραφίας δημοσίου κλειδιού. Συγκεκριμένα η κρυπτογραφία δημοσίου κλειδιού είναι αρκετά αργή σε σύγκριση με την συμμετρική κρυπτογραφία, ειδικά όταν πρόκειται να κρυπτογραφηθούν μεγάλα μηνύματα. Ακόμα όμως και στην περίπτωση που ο όγκος των προς κρυπτογράφηση δεδομένων είναι μικρός, έχει καθιερωθεί να χρησιμοποιείται η κρυπτογραφία ψηφιακού φακέλου. Με αυτόν τον τρόπο αποφεύγεται οποιαδήποτε σύγχυση ως προς το αν το αποτέλεσμα της αποκρυπτογράφησης είναι δεδομένα ή συμμετρικό κλειδί.

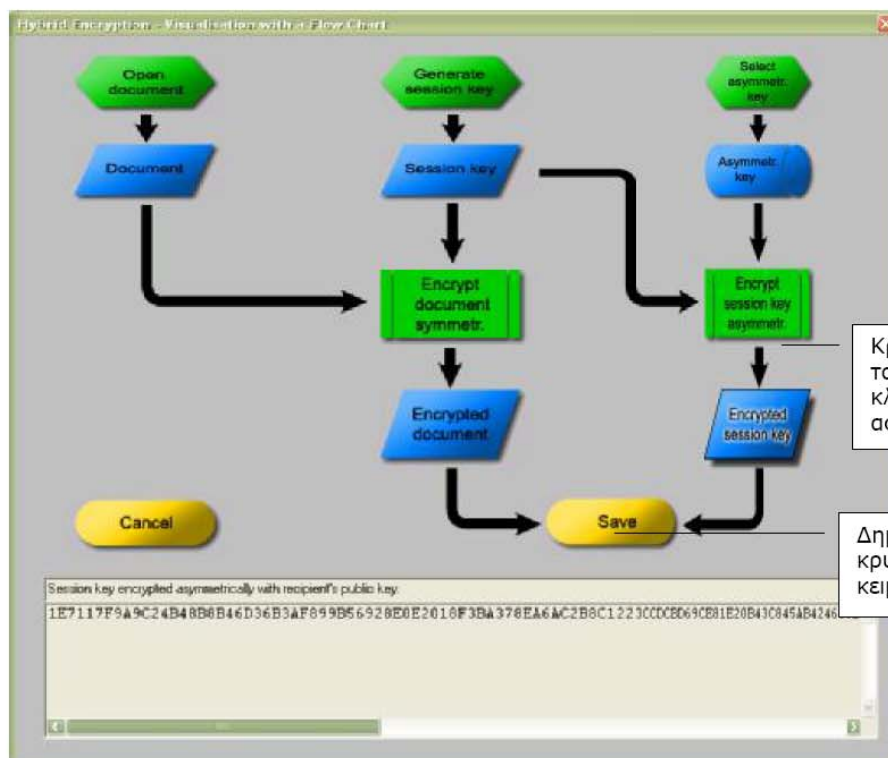
Η κρυπτογράφηση του αρχικού κειμένου με την χρήση υβριδικής κρυπτογραφίας γίνεται όπως βλέπετε στις εικόνες που ακολουθούν:







Επιλογή του ασύμμετρου κλειδιού



Κρυπτογράφηση του συμμετρικού κλειδιού με το ασύμμετρο κλειδί

Δημιουργία του κρυπτογραφημένου κειμένου

## Δημιουργία σύνοψης του αρχικού κειμένου

### Συναρτήσεις Κατακερματισμού

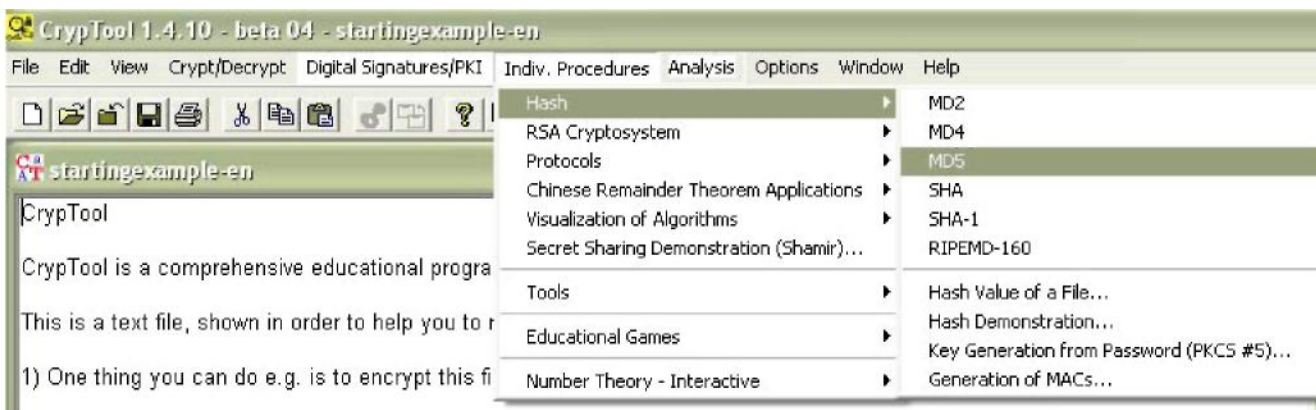
Ο όρος συνάρτηση κατακερματισμού (hash function) ή υποδηλώνει ένα μετασχηματισμό που παίρνει ως είσοδο ένα μήνυμα  $m$  οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων  $h(m)$  περιορισμένου μήκους που καλείται τιμή κατακερματισμού (hash value). Οι συναρτήσεις κατακερματισμού είναι συναρτήσεις με τις εξής ιδιότητες:

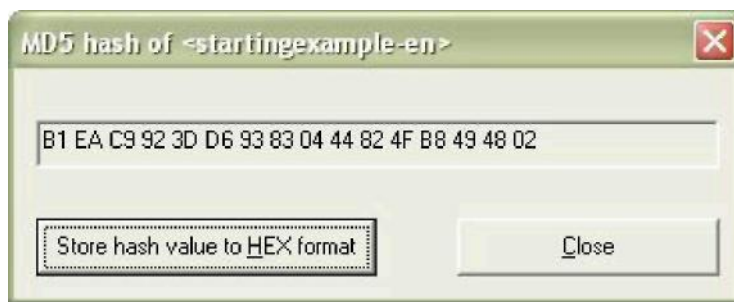
- Η είσοδος είναι οποιουδήποτε μήκους.
- Η έξοδος έχει περιορισμένο μήκος.
- Δεδομένου του  $m$ , ο υπολογισμός του  $h(m)$  είναι εύκολος.
- Η  $h$  είναι μη αντιστρέψιμη.
- Η  $h$  δεν είναι αμφιμονοσήμαντη (ένα προς ένα συνάρτηση).

Η τιμή κατακερματισμού παρουσιάζει συνοπτικά το μεγαλύτερο μήνυμα ή έγγραφο, για αυτό καλείται και σύνοψη μηνύματος (message digest). Μπορούμε να φανταστούμε τη σύνοψη του μηνύματος σαν "ψηφιακό αποτύπωμα" ("digital fingerprint") του εγγράφου. Γνωστές συναρτήσεις κατακερματισμού είναι οι MD2, MD4, MD5, SHA, SHA-1, RIPEMD, MD2, MD4, MD5 (Message Digest): Πρόκειται για Hash Function αλγόριθμους που αναπτύχθηκαν από τον Ron Rivest και χρησιμοποιούνται κυρίως για την παραγωγή ψηφιακών υπογραφών. Οι αλγόριθμοι αυτοί δέχονται ένα μήνυμα αυθαίρετου μήκους και εξάγουν ένα Message Digest 128 bits. Εν συνεχεία η σύνοψη αυτή του μηνύματος κρυπτογραφείται με την ιδιωτική κλειδα του αποστολέα. Μοιάζουν και οι τρεις αρκετά με την διαφορά αφ' ενός ότι πρόκειται για διαδοχικές βελτιώσεις και αφ' ετέρου ότι ο MD2 έχει σχεδιαστεί για 8 bit μηχανές ενώ οι MD4 και MD5 για μηχανές 32 bit.

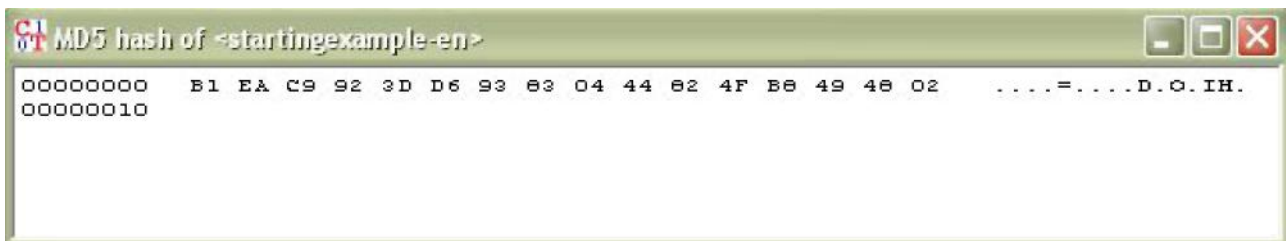
SHA – SHA-1 (Secure Hash Algorithm): Ο SHA-1 αποτελεί επανέκδοση του SHA και διόρθωσε μια ατέλεια του τελευταίου. Η δομή και η λειτουργία του είναι παρόμοια με την αντίστοιχη του MD4. Ο SHA-1 παίρνει ως είσοδο μήνυμα μήκους μικρότερο από 264 bits και παράγει message digest 160 bits. Είναι ελαφρά πιο αργός από τον MD5, αλλά το μεγαλύτερο message digest που παράγει τον κάνουν πιο ασφαλή απέναντι σε προσπάθειες αντιστροφής του.

RIPEMD - : αναπτύχθηκε στην Ευρώπη από τους Hans Dobbertin, Antoon Bosselaers, και Bart Preneel και υπάρχει σε εκδόσεις των 128, 160, 256 και 320 bit εκ των οποίων παίρνει και την αντίστοιχη ονομασία κάθε φορά. Για τη δημιουργία σύνοψης του αρχικού κειμένου με χρήση του προγράμματος CrypTool και για παράδειγμα με τη χρήση της συνάρτησης κατακερματισμού MD5, βλέπετε επακριβώς τα βήματα στις εικόνες που ακολουθούν:





Αφού επιλέξουμε τη συνάρτηση κατακερματισμού με την οποία θέλουμε να συνοψίσουμε το αρχικό μας κείμενο, εμφανίζεται ένα νέο παράθυρο το οποίο μας εμφανίζει τη σύνοψή του. Σε αυτό το παράθυρο πατάμε πάνω στην επιλογή "Store hash value to HEX format", και ουσιαστικά μας δίνει ένα την παραπάνω σύνοψη σε ένα \*.txt αρχείο το οποίο μπορούμε να αποθηκεύσουμε στον υπολογιστή μας και να το χρησιμοποιήσουμε όπως θέλουμε.

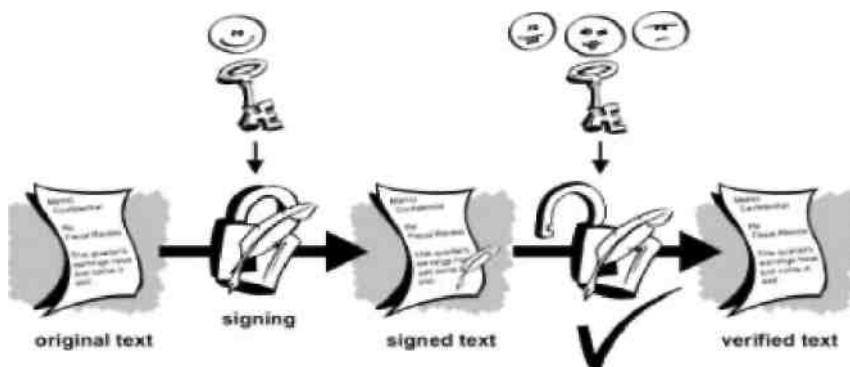


## Ψηφιακή υπογραφή κειμένου

### Υπογράφοντας ψηφιακά το κείμενο

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 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.

Ο αποστολέας υπογράφει το μήνυμα με το ιδιωτικό του κλειδί. Ο παραλήπτης διαθέτει το δημόσιο κλειδί του αποστολέα και μπορεί να επιβεβαιώσει ότι το μήνυμα υπογράφηκε με το αντίστοιχο ιδιωτικό κλειδί. Εφόσον το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του, μόνο αυτός θα μπορούσε να το χρησιμοποιήσει, για να υπογράψει κάποιο μήνυμα και επομένως μόνο αυτός θα μπορούσε να έχει στείλει το μήνυμα αυτό.

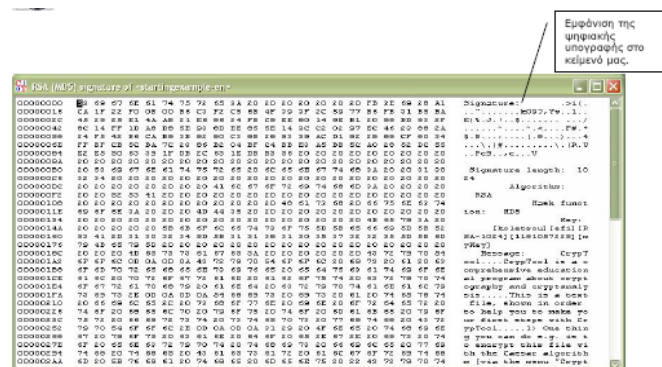
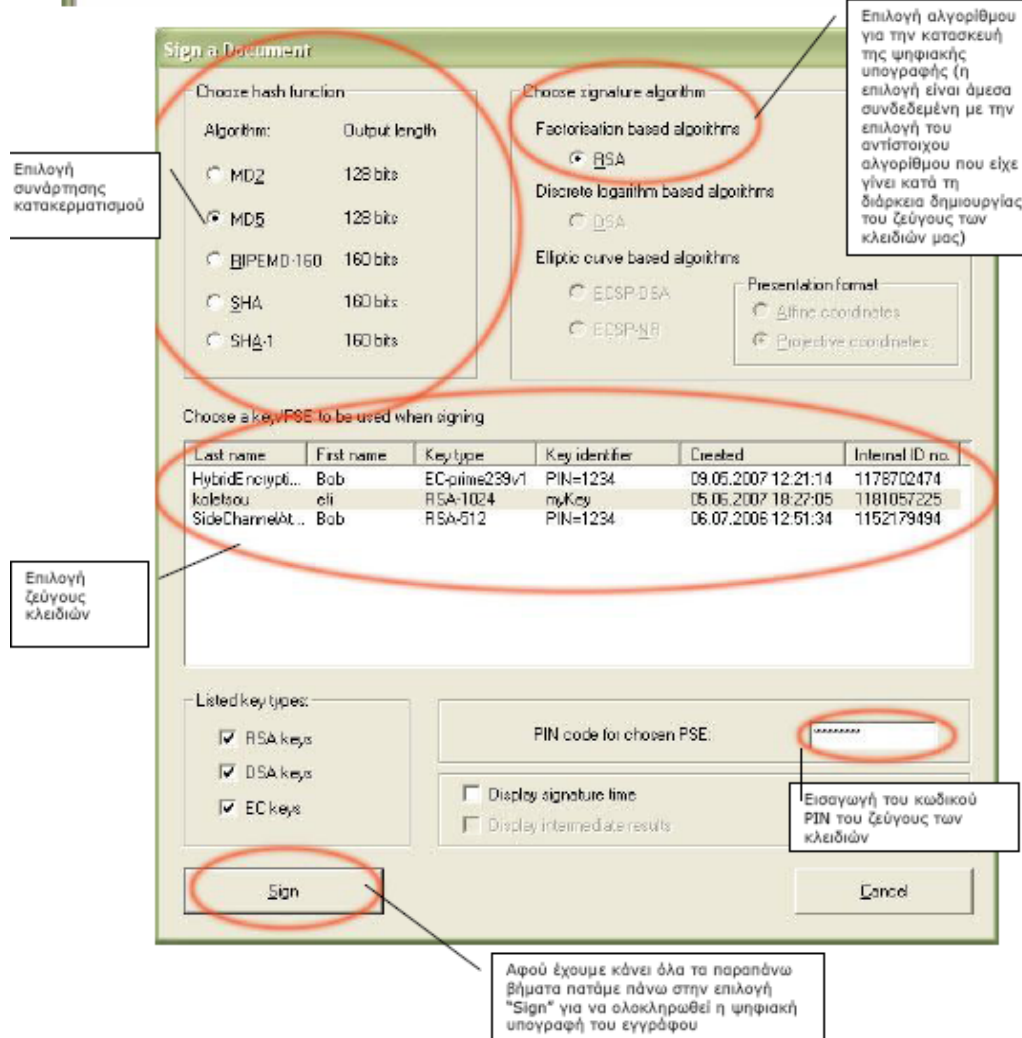
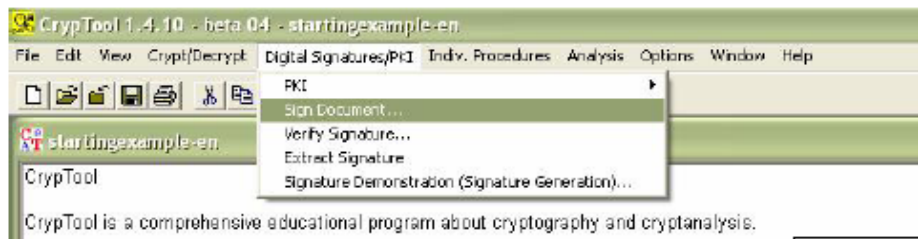


Πιο αναλυτικά, πρώτο βήμα για την δημιουργία της ψηφιακής υπογραφής είναι η παραγωγή μιας σύνοψης μηνύματος (message digest). Για το σκοπό αυτό, το λογισμικό που παράγει τις υπογραφές χρησιμοποιεί μία συνάρτηση κατακερματισμού (hash function). Η σύνοψη, κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα, αποτελεί την υπογραφή, η οποία επισυνάπτεται στο μήνυμα.

Ο παραλήπτης λαμβάνει τόσο το μήνυμα όσο και την υπογραφή. Χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει την υπογραφή, οπότε προκύπτει η σύνοψη του μηνύματος, όπως αυτή είχε παραχθεί πριν την αποστολή του μηνύματος. Εφόσον η υπογραφή έχει παραχθεί με το ιδιωτικό κλειδί του αποστολέα, μόνο το δημόσιο κλειδί του μπορεί να την αποκρυπτογραφήσει και να δώσει τη σύνοψη του μηνύματος. Η συνάρτηση κατακερματισμού χρησιμοποιείται για να παραχθεί μία σύνοψη του μηνύματος, όπως αυτό έχει φτάσει στα χέρια του παραλήπτη. Εφόσον το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί μετά την αποστολή του, η σύνοψη του μηνύματος θα είναι ίδια με αυτήν που είχε προκύψει κατά την υπογραφή του από τον αποστολέα. Με τον τρόπο αυτό, ο παραλήπτης βεβαιώνει την αυθεντικότητα του μηνύματος.

Για την ψηφιακή υπογραφή του αρχικού μας κειμένου με χρήση του προγράμματος CrypTool βλέπετε επακριβώς τα βήματα στις εικόνες που ακολουθούν:

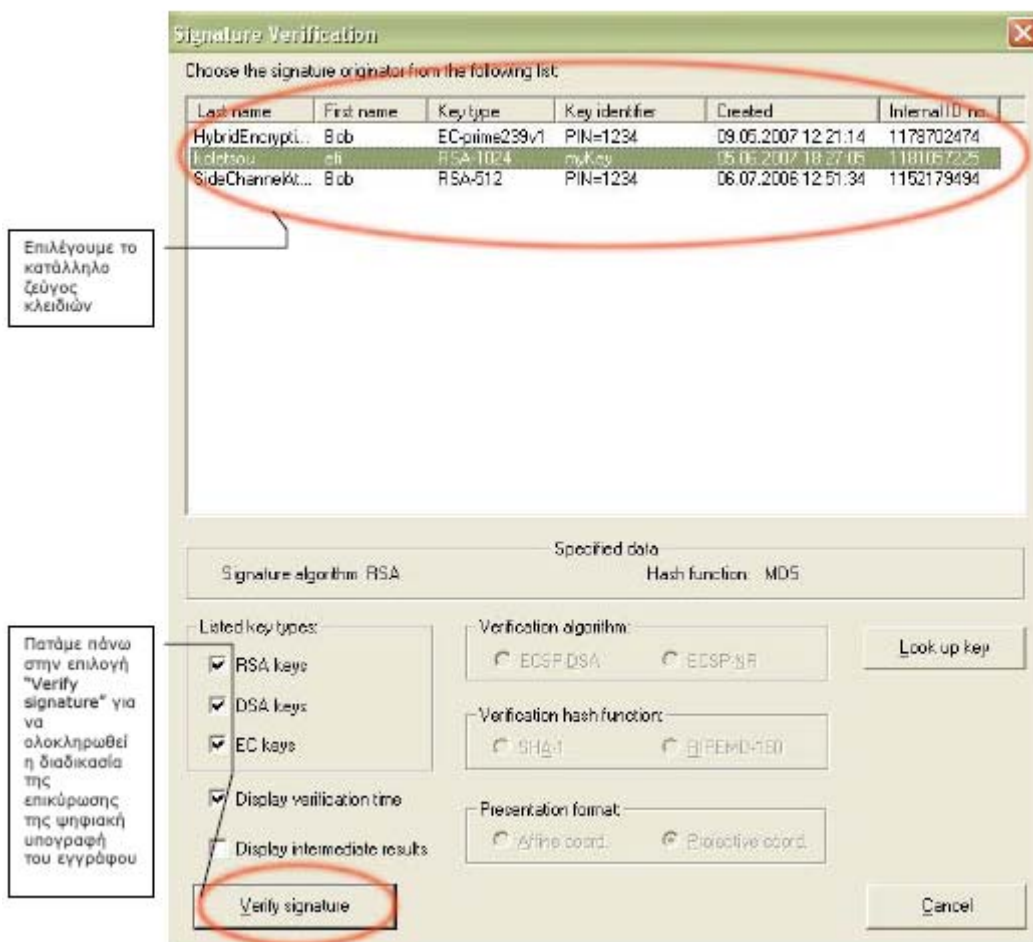






## Επικύρωση της ψηφιακής υπογραφής

Για την επικύρωση της ψηφιακής υπογραφής του κειμένου με χρήση του προγράμματος CrypTool βλέπετε επακριβώς τα βήματα στις εικόνες που ακολουθούν:



Οι ακόλουθες εικόνες είναι δύο διαφορετικά μηνύματα τα οποία εμφανίζονται, αφού έχουμε ολοκληρώσει την αμέσως προηγούμενη διαδικασία, όταν η υπογραφή είναι έγκυρη και όταν δεν είναι.



## **Βιβλιογραφία**

[1] Ν. Πολέμη, Χ. Δημητριάδης, Αλ. Καλιοντζόγλου, Αθ. Καραντιάς, Σπ. Παπαστεργίου, "Εργαστηριακές Ασκήσεις Ασφάλειας Πληροφοριακών Συστημάτων", Εκδόσεις Νέων Τεχνολογιών, Αθήνα 2007.

