Εισαγωγή στο CrypTool

Ασφάλεια & Έλεγχος
Πληροφορικών Συστημάτων (Ε)

ΤΕΙ Δυτικής Μακεδονίας
Τμήμα Εφαρμογών Πληροφορικής
Στην Διοίκηση και την Οικονομία

Βασικές έννοιες (1/2)

- **Αλγόριθμος**: σύνολο μαθηματικών κανόνων που χρησιμοποιούνται στην κρυπτογράφηση
- **Κρυπτοσύστημα**: η υλοποίηση ενός αλγορίθμου κρυπτογράφησης
- **Κρυπτανάλυση**: η μελέτη των μαθηματικών τεχνικών που αποσκοπούν στην αποκρυπτογράφηση δεδομένων χωρίς την χρήση κλειδιών
- **Κρυπτογράφηση**: η μετατροπή δεδομένων σε μη αναγνώσιμη μορφή
- **Αποκρυπτογράφηση**: η μετατροπή δεδομένων σε αναγνώσιμη μορφή
- **Plaintext**: το αρχικό μήνυμα
- **Ciphertext**: το κρυπτογαφημένο μήνυμα

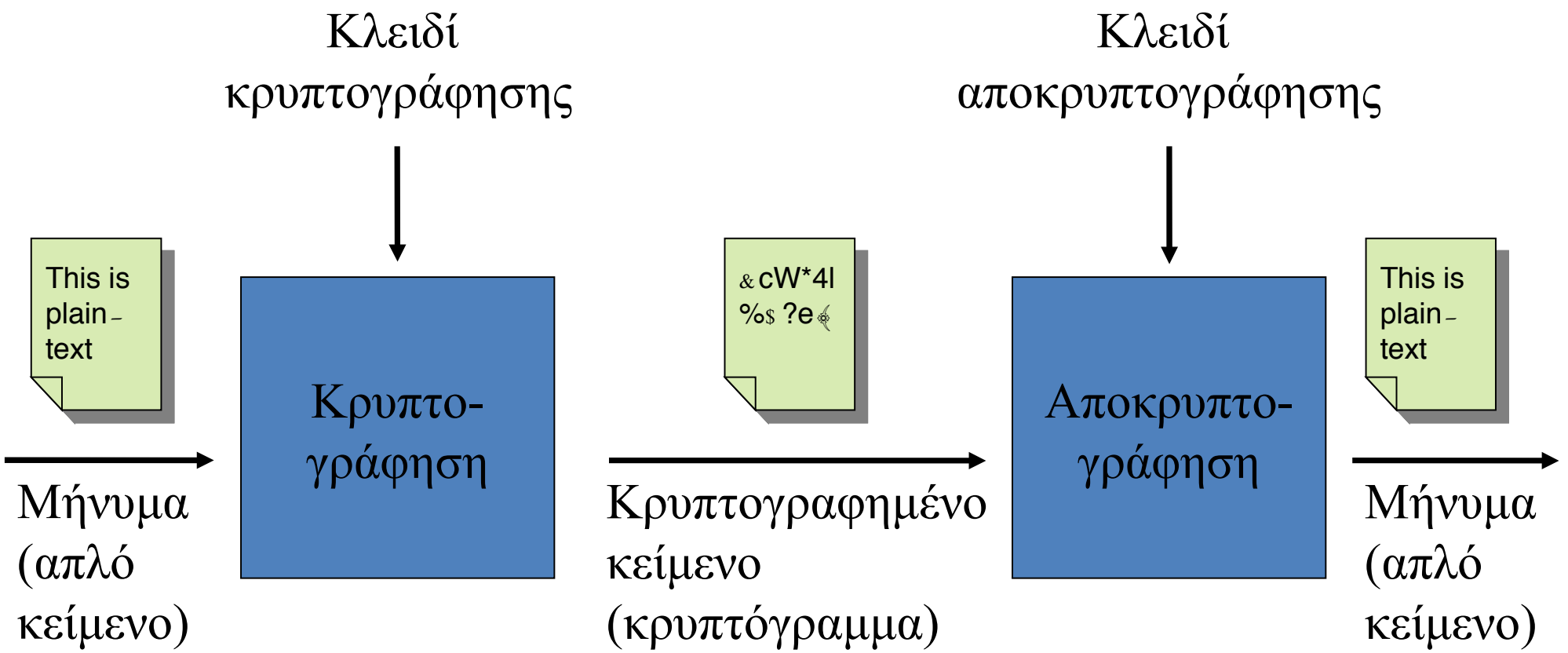
Βασικές έννοιες (2/2)

- **Κλειδί:** Ποσότητα πληροφορίας (σύνολο bytes) που καθορίζει τους μετασχηματισμούς που θα πραγματοποιηθούν κατά τη διαδικασία της κρυπτογράφησης ή αποκρυπτογράφησης.
- **Χώρος μη κρυπτογραφημένων μηνυμάτων M:** Όλα τα δυνατά μηνύματα απλού κειμένου.
- **Χώρος κρυπτογραφημένων μηνυμάτων C:** Όλα τα δυνατά μηνύματα κρυπτογραφημένου κειμένου.
- **Οικογένεια μετασχηματισμών κρυπτογράφησης**: Μια ομάδα συναρτήσεων E_k με πεδίο ορισμού το M και πεδίο τιμών το C. Υπάρχει μία συνάρτηση για κάθε κλειδί. Η κρυπτογράφηση ενός απλού κειμένου μπορεί να γραφεί ως $E_k(m)=c$ όπου με M, c ε C.
- **Οικογένεια μετασχηματισμών αποκρυπτογράφησης**: Μια ομάδα συναρτήσεων D_k με πεδίο ορισμού το C και πεδίο τιμών το M. Υπάρχει μία συνάρτηση για κάθε κλειδί. Η αποκρυπτογράφηση ενός κρυπτογραφημένου κειμένου μπορεί να γραφεί ως $D_k(c)=m$ όπου με M, c ε C.

Επιθυμητές ιδιότητες

- Αποδοτικοί αλγόριθμοι για τις λειτουργίες κωδικοποίησης και αποκωδικοποίησης.
- Το σύστημα να είναι εύχρηστο.
- Η προστασία που παρέχει το σύστημα πρέπει να προϋποθέτει μόνο τη μυστικότητα των κλειδιών, όχι του αλγορίθμου.

Βασική αναπαράσταση



CrypTool

- Αναπτύχθηκε από την Deutsche Bank για τους πελάτες της προκειμένου να αυξηθεί η κατανόηση τους σε κρυπτογραφικές διαδικασίες και ζητήματα ασφάλειας
- Εκπαιδευτικό εργαλείο, δωρεάν
  - http://www.cryptool.de
  - http://www.cryptool.org
  - http://www.cryptool.com
- Διαβάζει μόνο αρχεία απλού κειμένου (τύπου .txt)

Μηχανισμοί και Αλγόριθμοι Κρυπτογράφησης στο CryptTool

- Συμμετρικοί αλγόριθμοι κρυπτογραφίας
- Δημιουργία ασύμμετρου ζεύγους κλειδιών
- Εμφάνιση πληροφοριών που σχετίζονται με το ζεύγος κλειδιών
- Ασύμμετροι αλγόριθμοι κρυπτογραφίας
- Υβριδική κρυπτογραφία

Συμμετρική κρυπτογράφηση

- Είναι επίσης γνωστή ως κρυπτογράφηση:
  - συμμετρικού κλειδιού
  - μυστικού κλειδιού
  - ενός κλειδιού
- Ένας αλγόριθμος κρυπτογράφησης λέγεται συμμετρικός εάν γνωρίζοντας το κλειδί κρυπτογράφησης k είναι υπολογιστικά “εύκολο” να προσδιορίσουμε το κλειδί αποκρυπτογράφησης k', και αντίστροφα.
- Πρακτικά, για τους περισσότερους συμμετρικούς αλγόριθμους $k = k'$.
- Αποστολέας και παραλήπτης μοιράζονται ένα κοινό κλειδί.

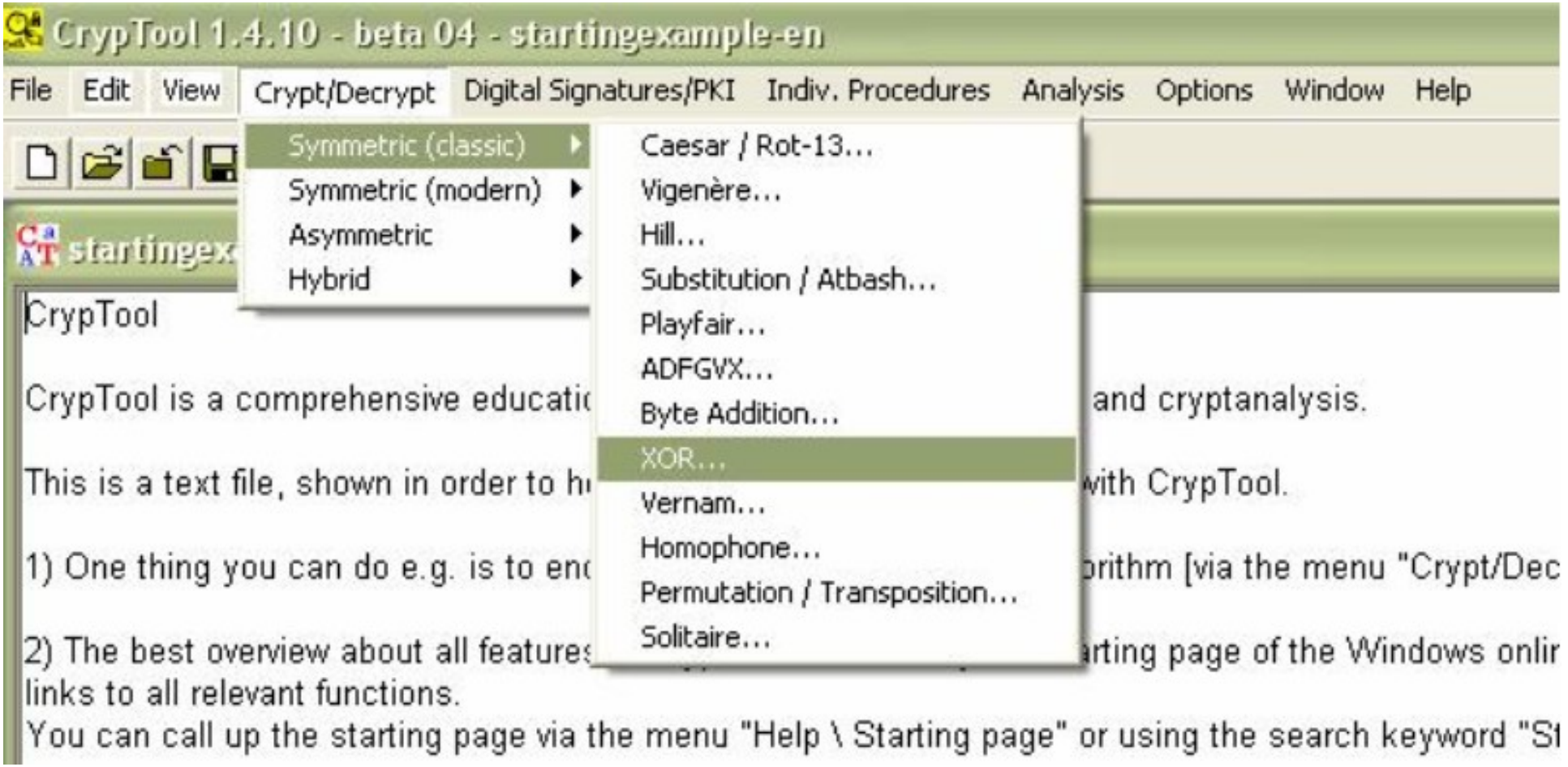
Συμμετρικά κρυπτοσυστήματα

- Πλεονεκτήματα
  - Ταχύτητα κρυπτογράφησης/αποκρυπτογράφησης
  - Μέγεθος κλειδιών
  - Μπορούν να χρησιμοποιηθούν ως βάση για τη κατασκευή άλλων μηχανισμών όπως παραγωγής τυχαίων αριθμών, συναρτήσεων κατακερματισμού, και ψηφιακών υπογραφών.
- Μειονεκτήματα
  - Μυστικότητα του κλειδιού.
  - Διαχείριση των κλειδιών:
    - Κατανομή/Διανομή
    - Αλλαγή/Ανανέωση
    - Περίοδος ζωής

Συμμετρικοί αλγόριθμοι κρυπτογραφίας

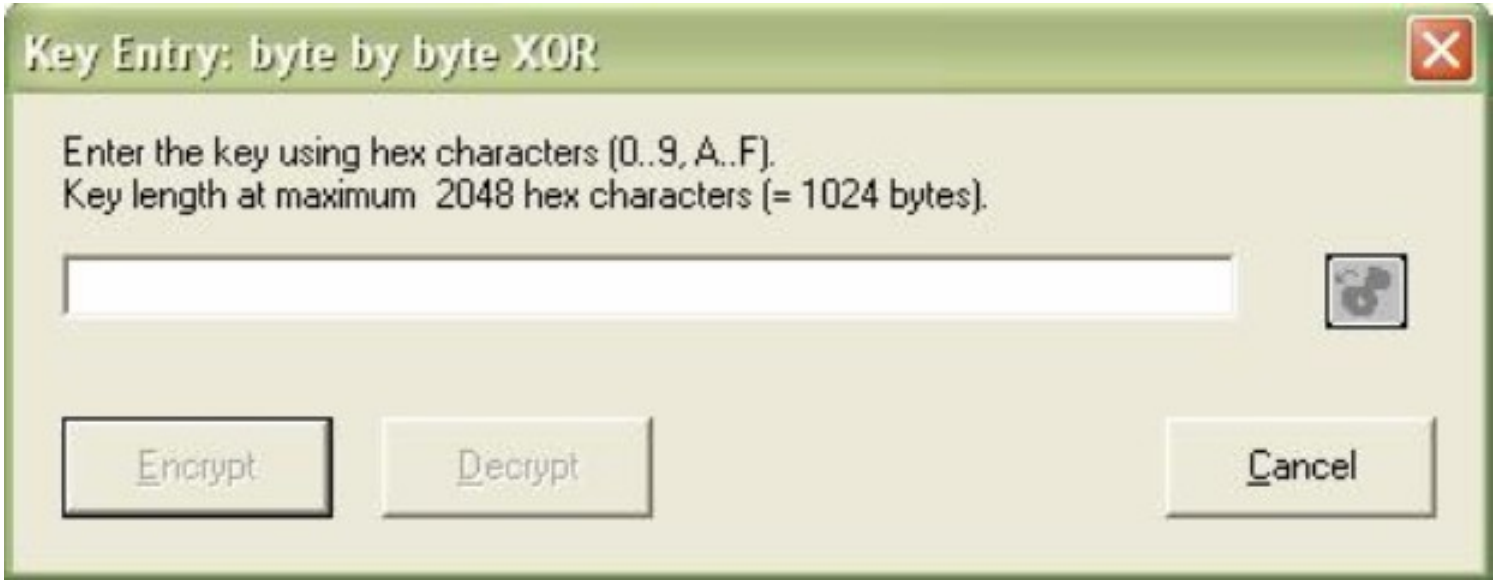
- Η λογική πράξη XOR
- Ο αλγόριθμος DES
  - ECB mode
  - CDC mode
- Ο αλγόριθμος RC2
- Ο αλγόριθμος AES

XOR (1/2)


CrypTool 1.4.10 - beta 04 - startingexample-en
File
Edit
View
Crypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
Caesar / Rot-13...
Vigenère...
Hill...
Substitution / Atbash...
Playfair...
ADFGVX...
Byte Addition...
XOR...
Vernam...
Homophone...
Permutation / Transposition...
Solitaire...
CrypTool
CrypTool is a comprehensive educati
and cryptanalysis.
This is a text file, shown in order to h
with CrypTool.
1) One thing you can do e.g. is to en
orithm [via the menu "Crypt/Dec
2) The best overview about all feature
arting page of the Windows onlir
links to all relevant functions.
You can call up the starting page via the menu "Help \ Starting page" or using the search keyword "St

XOR (2/2)

- Μας ζητείτε να εισάγουμε ένα κλειδί το οποίο μπορεί να πάρει σαν παραμέτρους είτε αριθμούς (0,1,...,9) είτε χαρακτήρες από A μέχρι F
- Κάνουμε ακριβώς την ίδια διαδικασία για την αποκρυπτογράφηση του μηνύματος

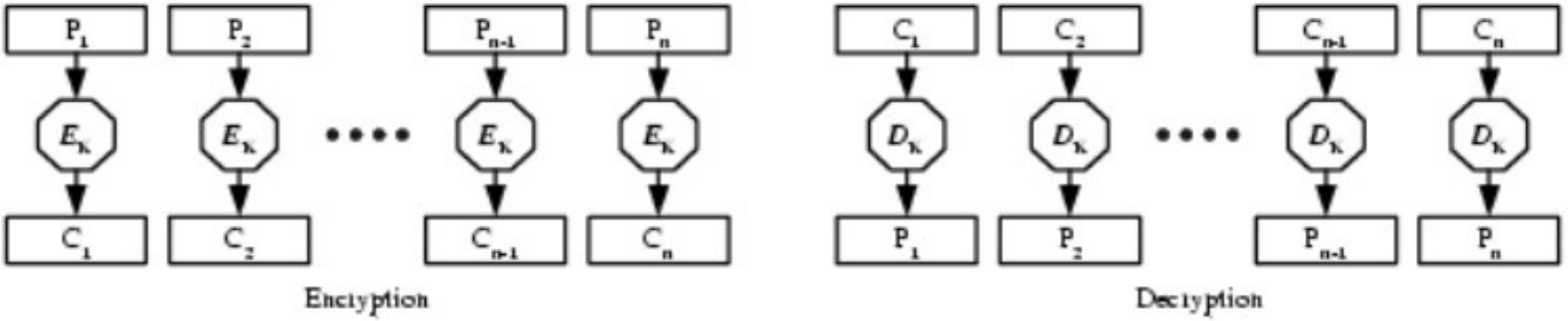


Ο αλγόριθμος DES

- Data Encryption Standard
- Ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος
- Χρησιμοποιεί κλειδί με μέγεθος 64 bit από τα οποία τα 8 αποτελούν bit ισοτιμίας
- Αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί
- Κρυπτογράφηση μηνυμάτων ΚΑΙ αρχείων στο δίσκο (σε περιβάλλον ενός χρήστη)
- Σε περιβάλλον πολλών χρηστών για διανομή κλειδιών συνδυάζεται με ασυμμετρικό κρυπτοσύστημα

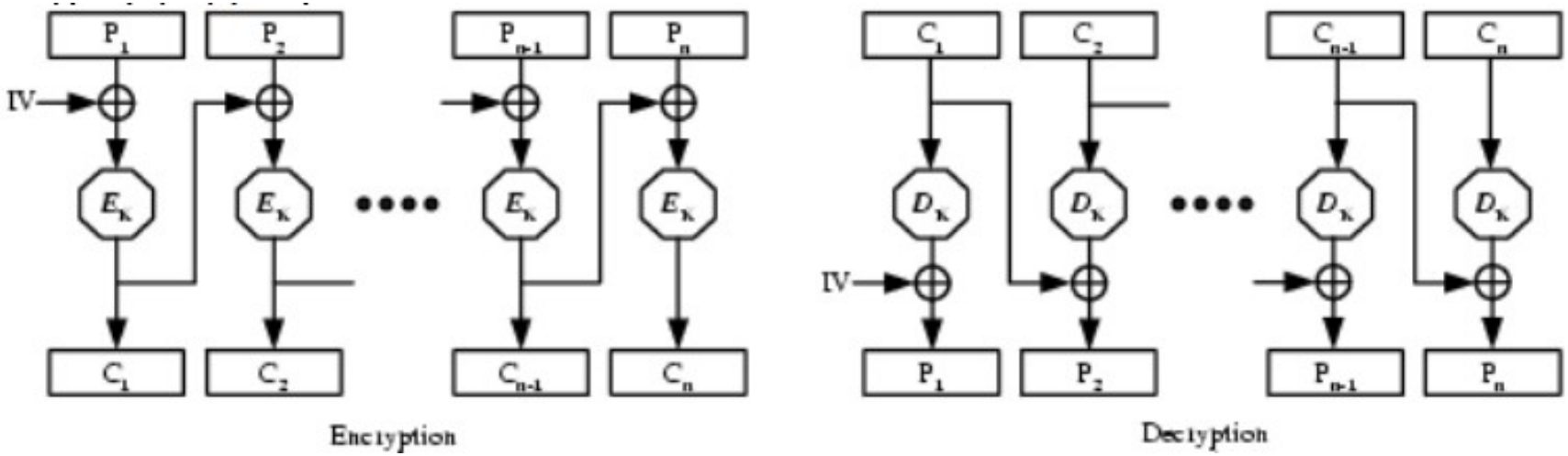
DES (ECB mode)

- Το κείμενο χωρίζεται σε τμήματα ίδιου μήκους (blocks)
- Κάθε τμήμα κρυπτογραφείται ανεξάρτητα



DES (CBC mode)

- Κάθε block συνδυάζεται μέσω της λογικής πράξης XOR με το πρωτύτερα κρυπτογραφημένο block
- Απαιτείται μια αρχική τιμή για την πρώτη XOR πράξη που καλείται διάνυσμα αρχικοποίησης (initialization vector)



Ο αλγόριθμος RC2

- Κλειδί μεταβλητού μήκους από 8 έως 128 bit
- Σχεδιάστηκε από τον Ron Rivest και τα αρχικά σημαίνουν Ron's Code ή Rivest's Cipher
- Είναι γρηγορότερος από τον DES και μπορεί να γίνε περισσότερο ή λιγότερο ασφαλής ανάλογα με το μήκος του κλειδιού
- Χρησιμοποιεί μέγεθος block 64 bit

Ο αλγόριθμος AES

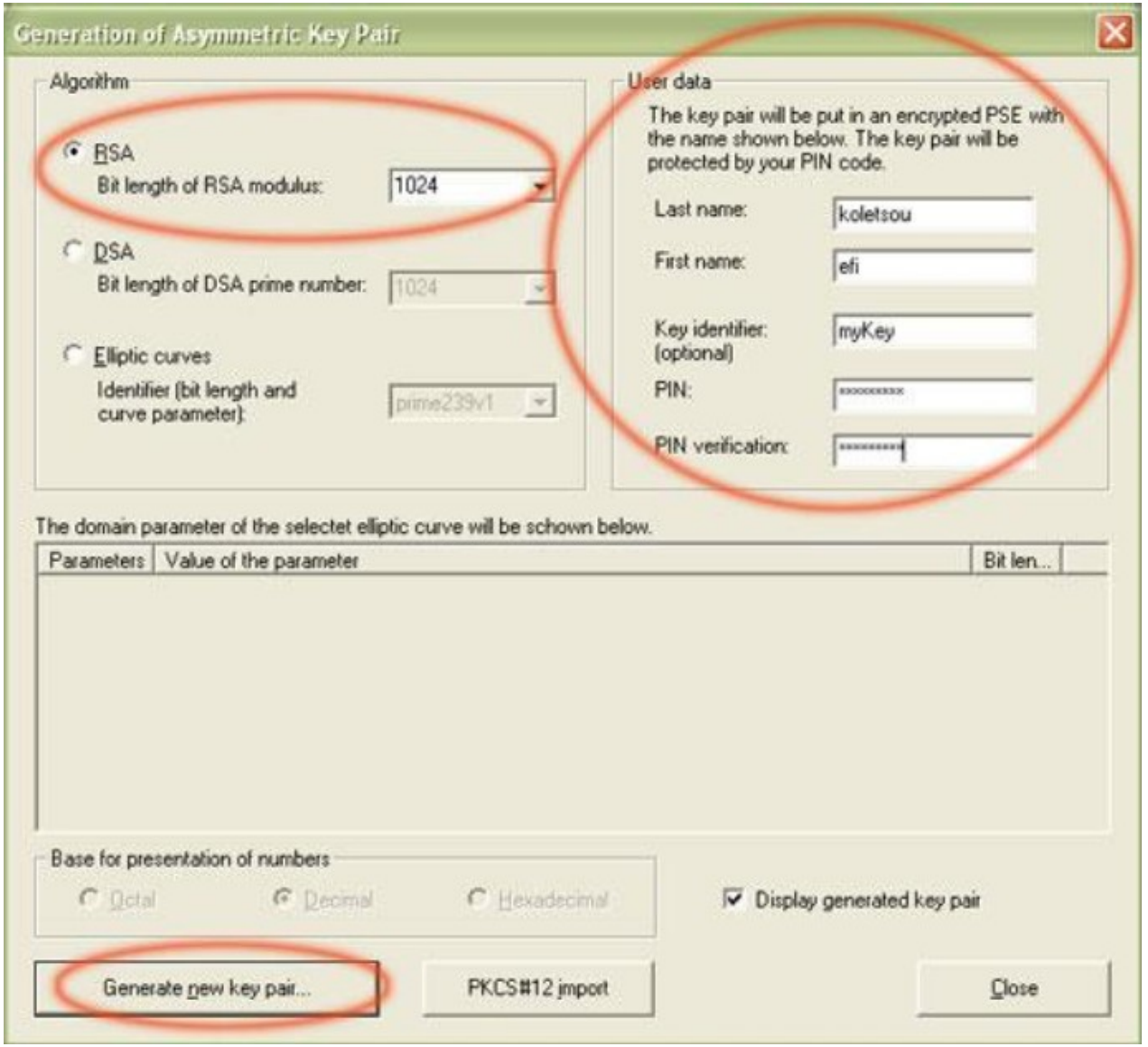
- Advanced Encryption Standard
- Κωδικοποίηση ομάδων δεδομένων με κάποιο μυστικό κλειδί
- Υποστηρίζει χρήση κλειδιών μήκους 128, 192 και 256 bit
- Μήκος των block δεδομένων 128 bits
- Η διαδικασία κρυπτογράφησης είναι επαναληπτική (rounds)

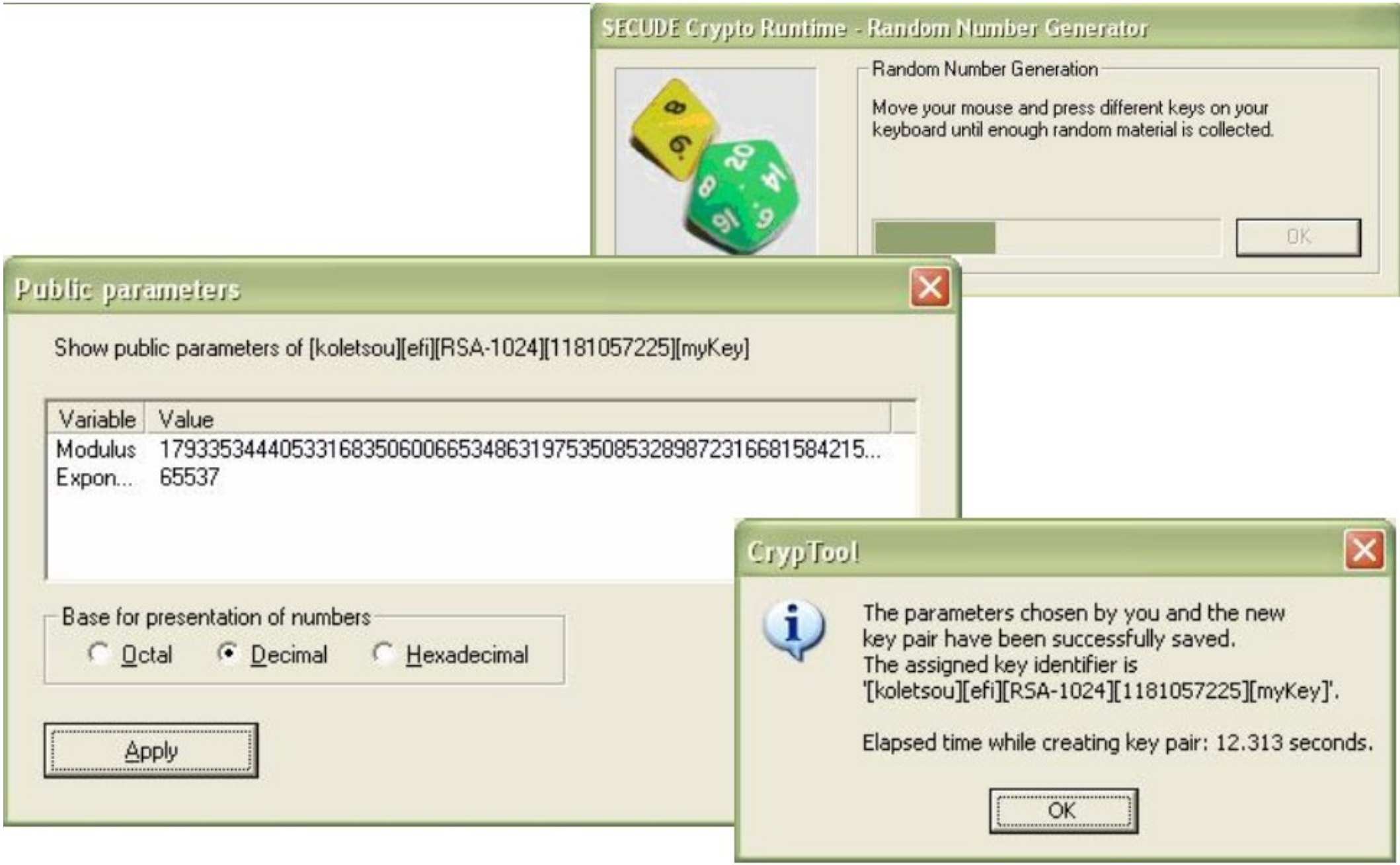
Δημιουργία ασύμμετρου ζεύγους κλειδιών



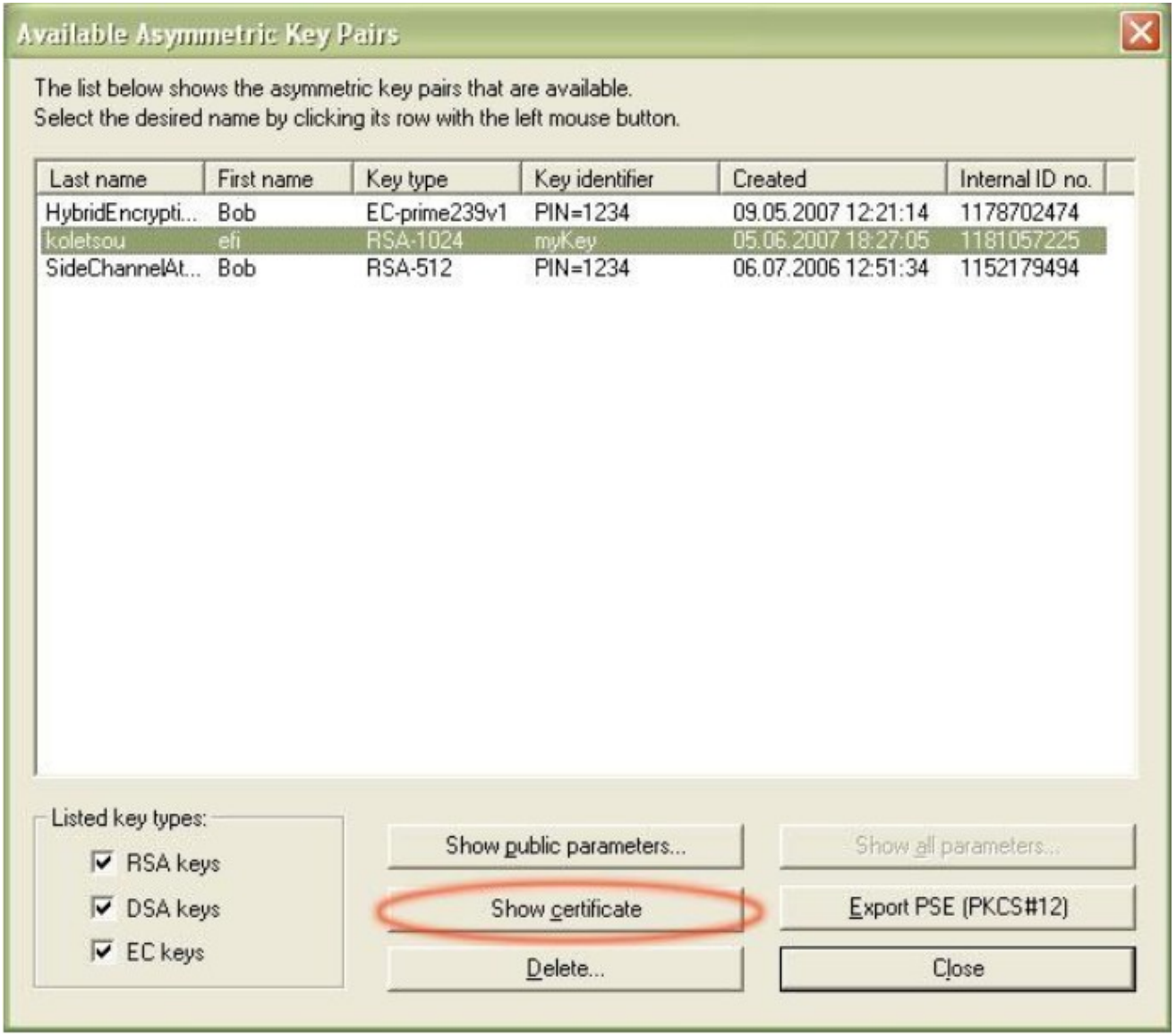
- Στην καρτέλα που εμφανίζεται επιλέγουμε τον τύπο του αλγορίθμου (RSA, DSA και Elliptic curves)

Δημιουργία ασύμμετρου ζεύγους κλειδιών




SECUDE Crypto Runtime - Random Number Generator
Random Number Generation
Move your mouse and press different keys on your keyboard until enough random material is collected.
OK
Public parameters
Show public parameters of [koletsou][efi][RSA-1024][1181057225][myKey]
Variable
Value
Modulus
179335344405331683506006653486319753508532898723166815842 15...
Expon...
65537
Base for presentation of numbers
Octal
Decimal
Hexadecimal
Apply
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.
OK

Εμφάνιση πληροφοριών για το ζεύγος κλειδιών (Key Display/Export...)

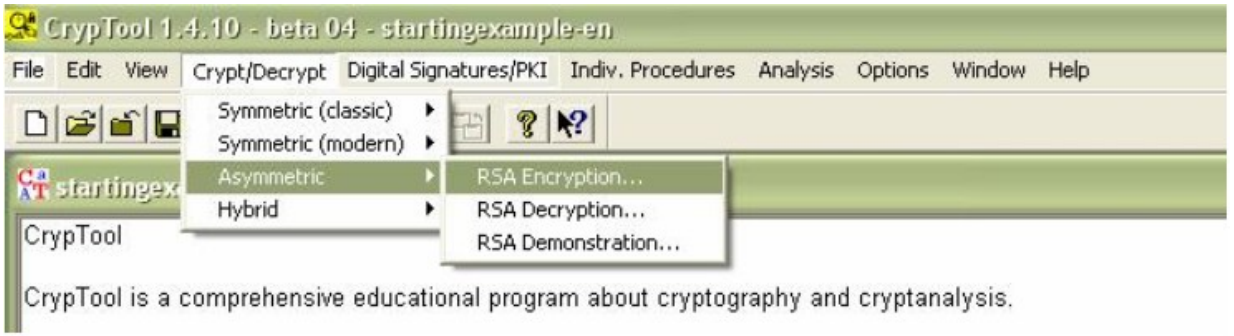


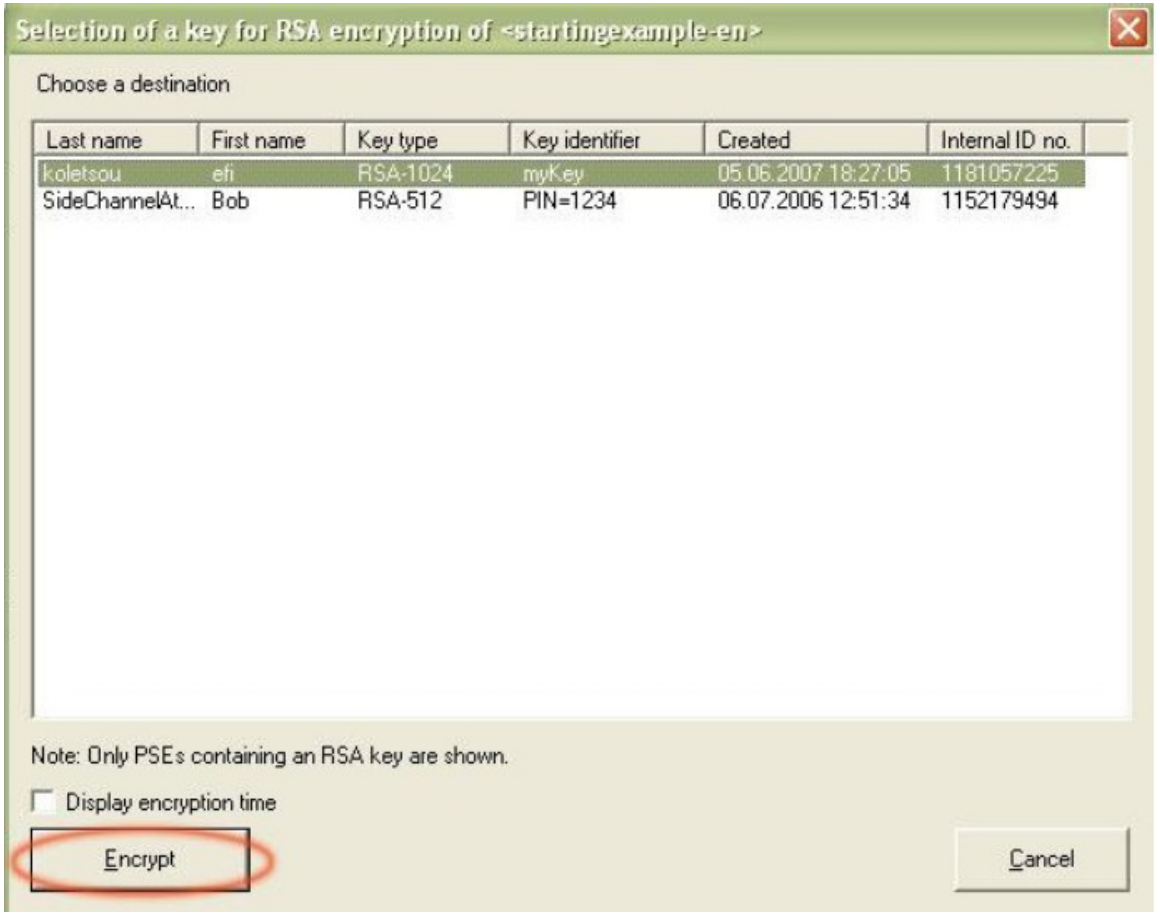
Ασύμμετροι Αλγόριθμοι Κρυπτογραφίας

- Ο αλγόριθμος RSA

Ο αλγόριθμος RSA

- Σχεδιάστηκε από τους: Ron **R**ivest, Adi **S**hamin και Leonard **A**dleman
- Η ασφάλεια του έγκειται στην δυσκολία παραγοντοποίησης πολύ μεγάλων φυσικών αριθμών
- Το μέγεθος των κλειδιών διαφέρει σημαντικά σε σχέση με την συμμετρική κρυπτογραφία (ένα κλειδί μήκους 512bit θεωρείται αναξιόπιστο)
- Αποστολέας και παραλήπτης δεν έχουν κοινά ιδιωτικά κλειδιά
- Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα αλλά μόνο ο κάτοχος του σωστού ιδιωτικού κλειδιού μπορεί να το αποκρυπτογραφήσει


CrypTool 1.4.10 - beta 04 - startingexample-en
File Edit View Crypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
RSA Encryption...
RSA Decryption...
RSA Demonstration...
CrypTool
CrypTool is a comprehensive educational program about cryptography and cryptanalysis.


Selection of a key for RSA encryption of <startingexample-en>
Choose a destination
Last name | First name | Key type | Key identifier | Created | Internal ID no.
koletsou | efi | RSA-1024 | myKey | 05.06.2007 18:27:05 | 1181057225
SideChannelAt... | Bob | RSA-512 | PIN=1234 | 06.07.2006 12:51:34 | 1152179494
Note: Only PSEs containing an RSA key are shown.
Display encryption time
Encrypt
Cancel

Υβριδική Κρυπτογραφία

- Αξιοποιεί ταυτόχρονα τεχνικές συμμετρικής και ασύμμετρης κρυπτογραφίας
- Μπορεί να χρησιμοποιηθεί για πολλούς παραλήπτες ταυτόχρονα
- Είναι γνωστή και ως **ψηφιακός φάκελος** (digital envelope)

Δημιουργία Ψηφιακού Φακέλου

- Δημιουργία συμμετρικού κλειδιού με χρήση ενός αλγορίθμου συμμετρικής κρυπτογραφίας (πχ του DES, του AES)
- Η αρχική πληροφορία κρυπτογραφείται με το συμμετρικό κλειδί που έχει δημιουργηθεί
- Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη
- Τα δύο κρυπτογραφημένα κείμενα (κρυπτογραφημένη πληροφορία και κρυπτογραφημένο κλειδί) αποτελούν τον ψηφιακό φάκελο του παραλήπτη

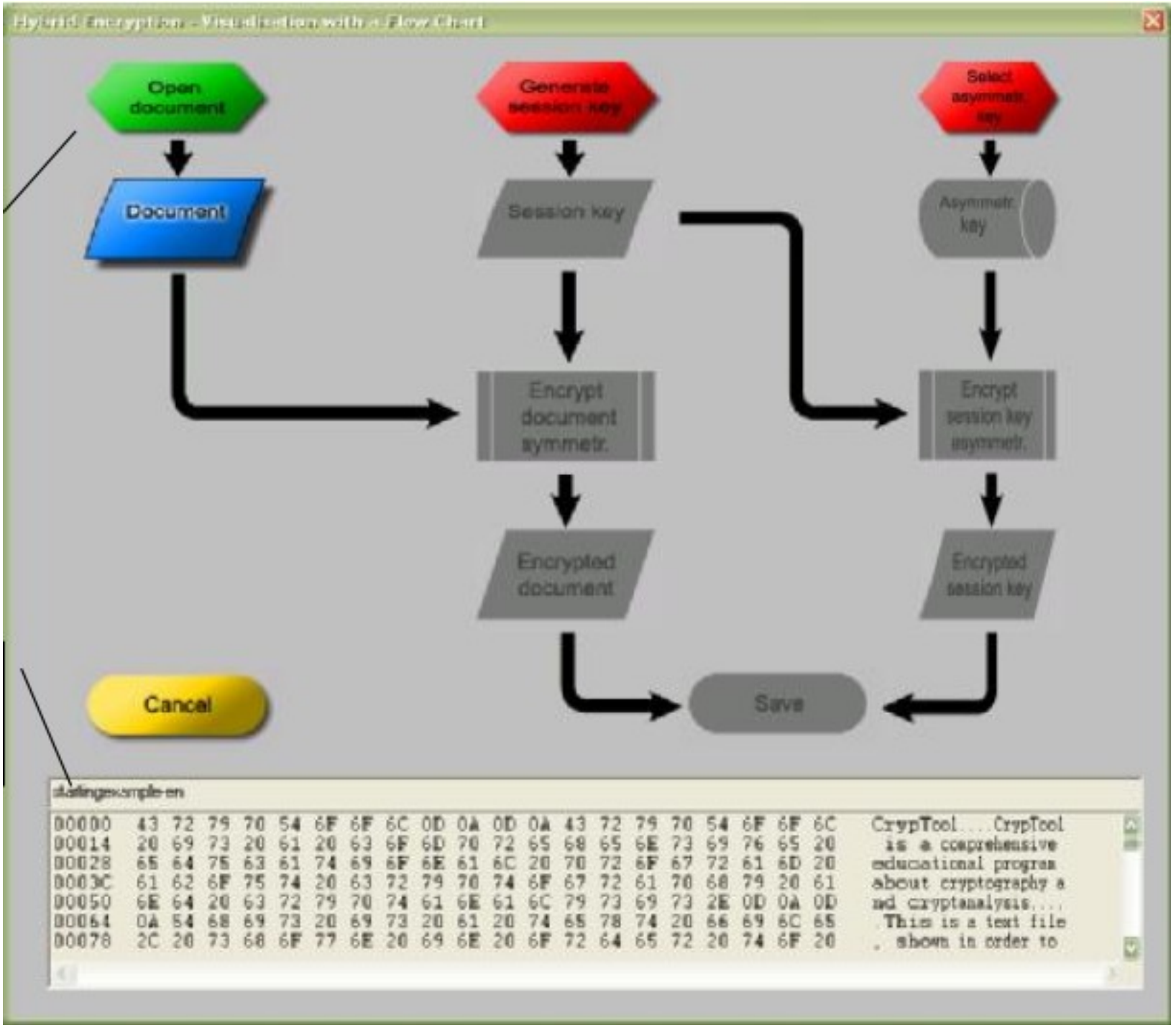
Αποκρυπτογράφηση

- Ο παραλήπτης ανοίγει τον ψηφιακό φάκελο
- Αποκρυπτογραφεί με το ιδιωτικό κλειδί του το κρυπτογραφημένο συμμετρικό κλειδί
- Χρησιμοποιεί το συμμετρικό κλειδί για την αποκρυπτογράφηση του αρχικού κειμένου
- Μετά την ασφαλή επικοινωνία μεταξύ αποστολέα και παραλήπτη το συμμετρικό κλειδί καταστρέφεται

Υβριδική Κρυπτογράφηση μέσω του CrypTool



- Άνοιγμα του εγγράφου
- Δημιουργία συμμετρικού κλειδιού
- Κρυπτογράφηση του αρχικού κειμένου
- Επιλογή ασύμμετρου κλειδιού
- Κρυπτογράφηση του συμμετρικού κλειδιού με το ασύμμετρο κλειδί
- Δημιουργία κρυπτογραφημένου κειμένου (ψηφιακός φάκελος)


Open document
Generate session key
Select asymmetr. key
Document
Session key
Asymmetr. key
Encrypt document symmetr.
Encrypt session key asymmetr.
Encrypted document
Encrypted session key
Cancel
Save
00000 43 72 79 70 54 6F 6F 6C 0D 0A 0D 0A 43 72 79 70 54 6F 6F 6C CrypTool....CrypTool
00014 20 69 73 20 61 20 63 6F 6D 70 72 65 68 65 6E 73 69 76 65 20 is a comprehensive
00028 65 64 75 63 61 74 69 6F 6E 61 6C 20 70 72 6F 67 72 61 6D 20 educational program
0003C 61 62 6F 75 74 20 63 72 79 70 74 6F 67 72 61 70 68 79 20 61 about cryptography a
00050 6E 64 20 63 72 79 70 74 61 6E 61 6C 79 73 69 73 2E 0D 0A 0D nd cryptanalysis....
00064 0A 54 68 69 73 20 69 73 20 61 20 74 65 78 74 20 66 69 6C 65 .This is a text file
00078 2C 20 73 68 6F 77 6E 20 69 6E 20 6F 72 64 65 72 20 74 6F 20 , shown in order to

Συναρτήσεις κατακερματισμού ***hash functions***

- Ένας μετασχηματισμός **h** που παίρνει σαν είσοδο ένα μήνυμα **m** οποιουδήποτε μήκους και επιστρέφει σαν έξοδο μια ακολουθία χαρακτήρων **h(m)** περιορισμένου μήκους που καλείται τιμή κατακερματισμού (hash value)

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

Σύνοψη μηνύματος
message digest

- Η τιμή κατακερματισμού παρουσιάσει συνοπτικά ένα μεγαλύτερο μήνυμα ή έγγραφο γι αυτό καλείται και σύνοψη μηνύματος
- Ψηφιακό αποτύπωμα (digital fingerprint) του εγγράφου
- Γνωστές συναρτήσεις κατακερματισμού: MD2, MD4, MD5, SHA, SHA-1, RIPEMD-

MD2, MD4, MD5

- **M**essage **D**igest
- Αναπτύχθηκαν από τον Ron Rivest
- Χρησιμοποιούνται κυρίως για την παραγωγή ψηφιακών υπογραφών
- Δέχονται μήνυμα αυθαίρετου μήκους κι εξάγουν μια σύνοψη 128 bits
- Η σύνοψη κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα

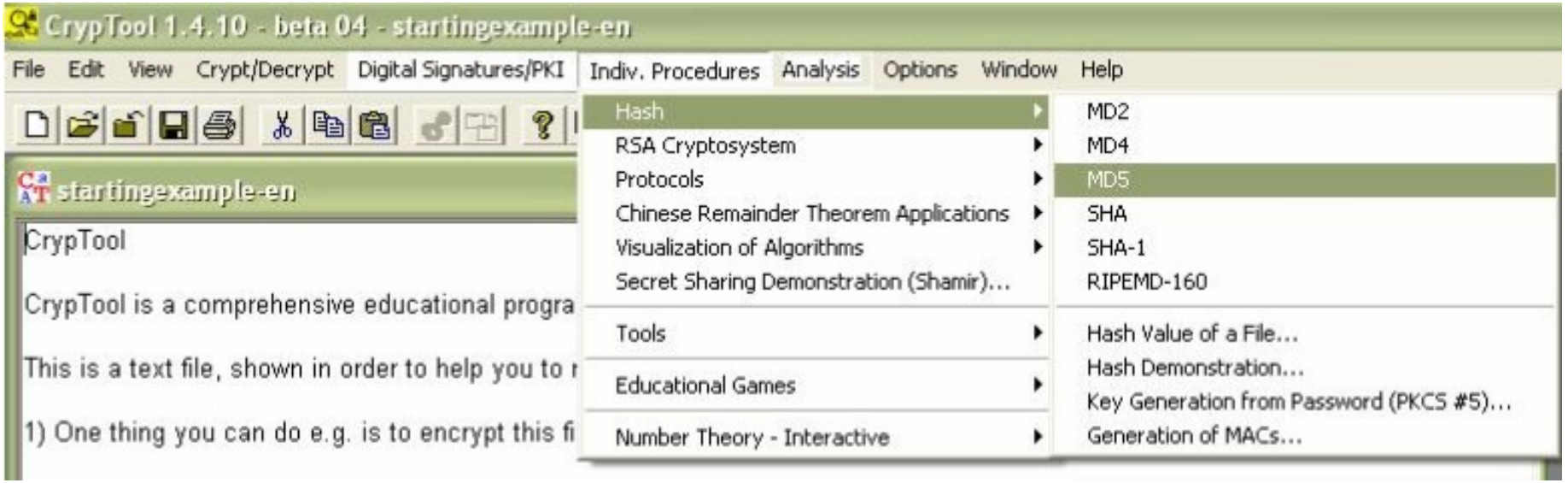
SHA και SHA-1

- **S**ecure **H**ash **A**lgorithm
- Είσοδος: μήνυμα μήκους μέχρι 264 bits
- Παράγει message digest 160 bits
- Πιο αργός από MD5 αλλά πιο ασφαλής

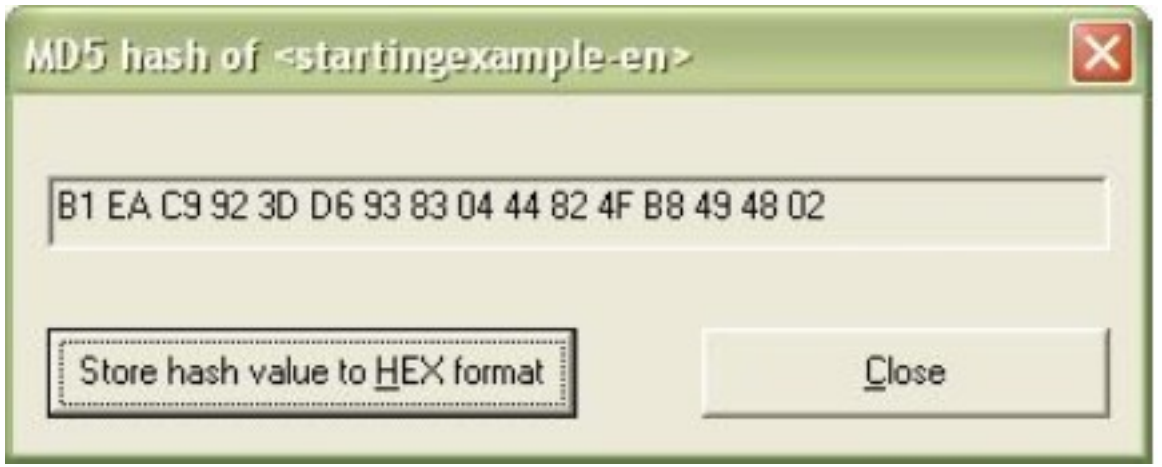
RIPEMD-

- Αναπτύχθηκε από τους Hans Dobbertin, Antoon Bosselaers και Bart Preneel
- Υπάρχει σε εκδόσεις των 128, 160, 256 και 320 bit εκ των οποίων παίρνει και την αντίστοιχη ονομασία κάθε φορά

Δημιουργία σύνοψης μέσω MD5



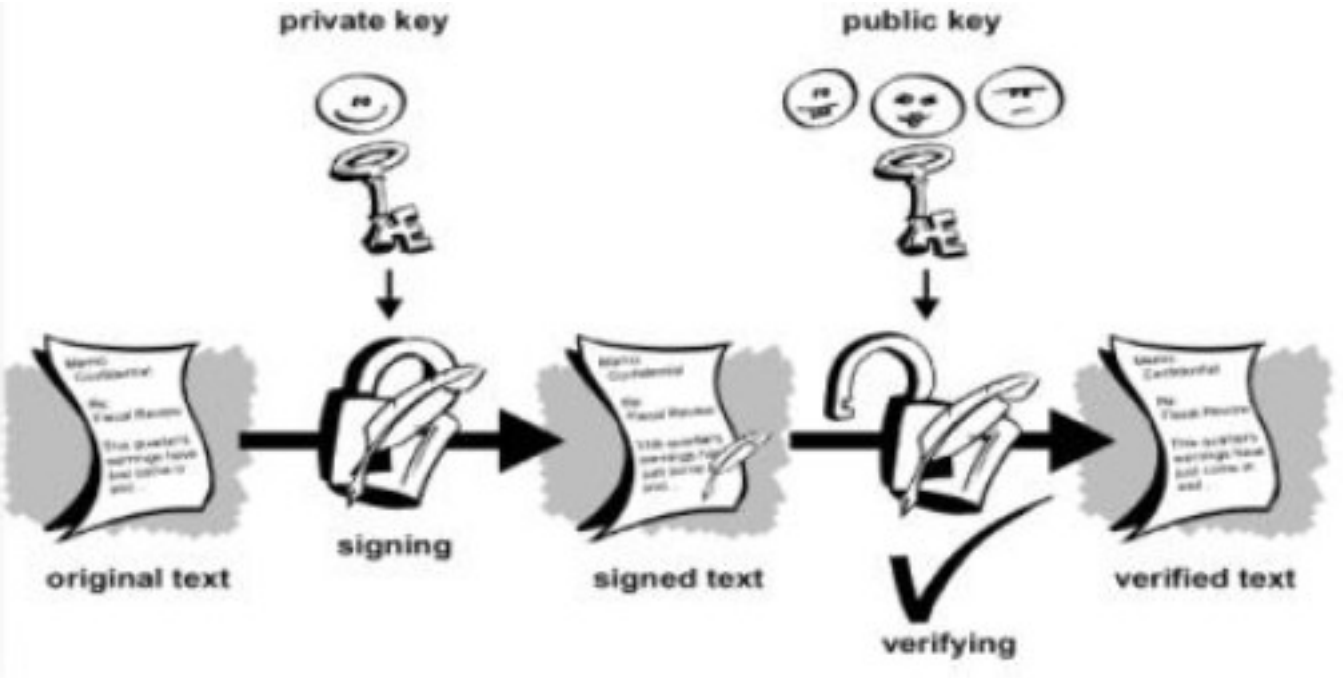
- Αφού επιλέξουμε το αρχικό κείμενο και την συνάρτηση κατακερματισμού που θέλουμε να χρησιμοποιήσουμε, εμφανίζεται σε ένα νέο παράθυρο η σύνοψη του μηνύματος

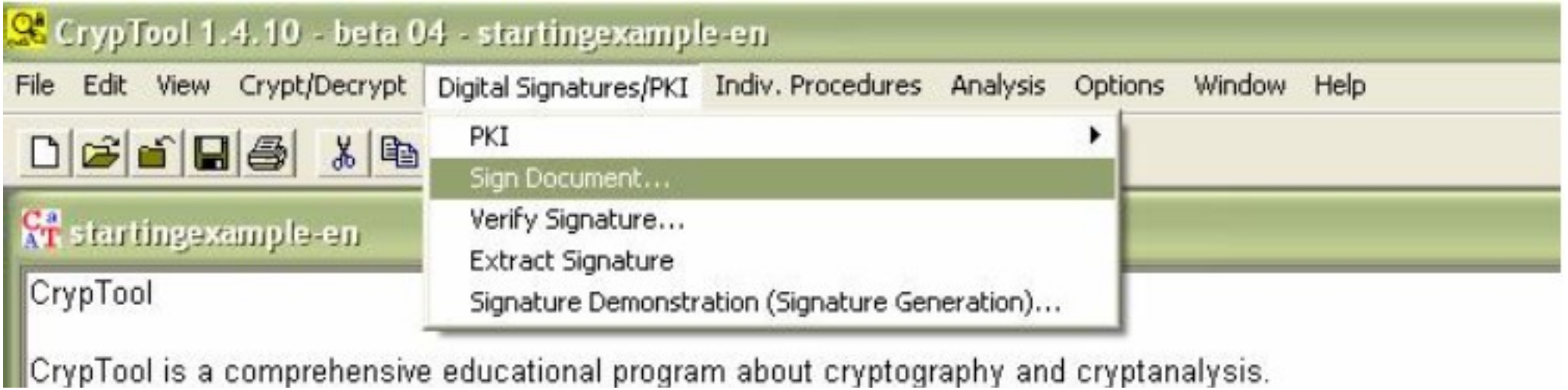


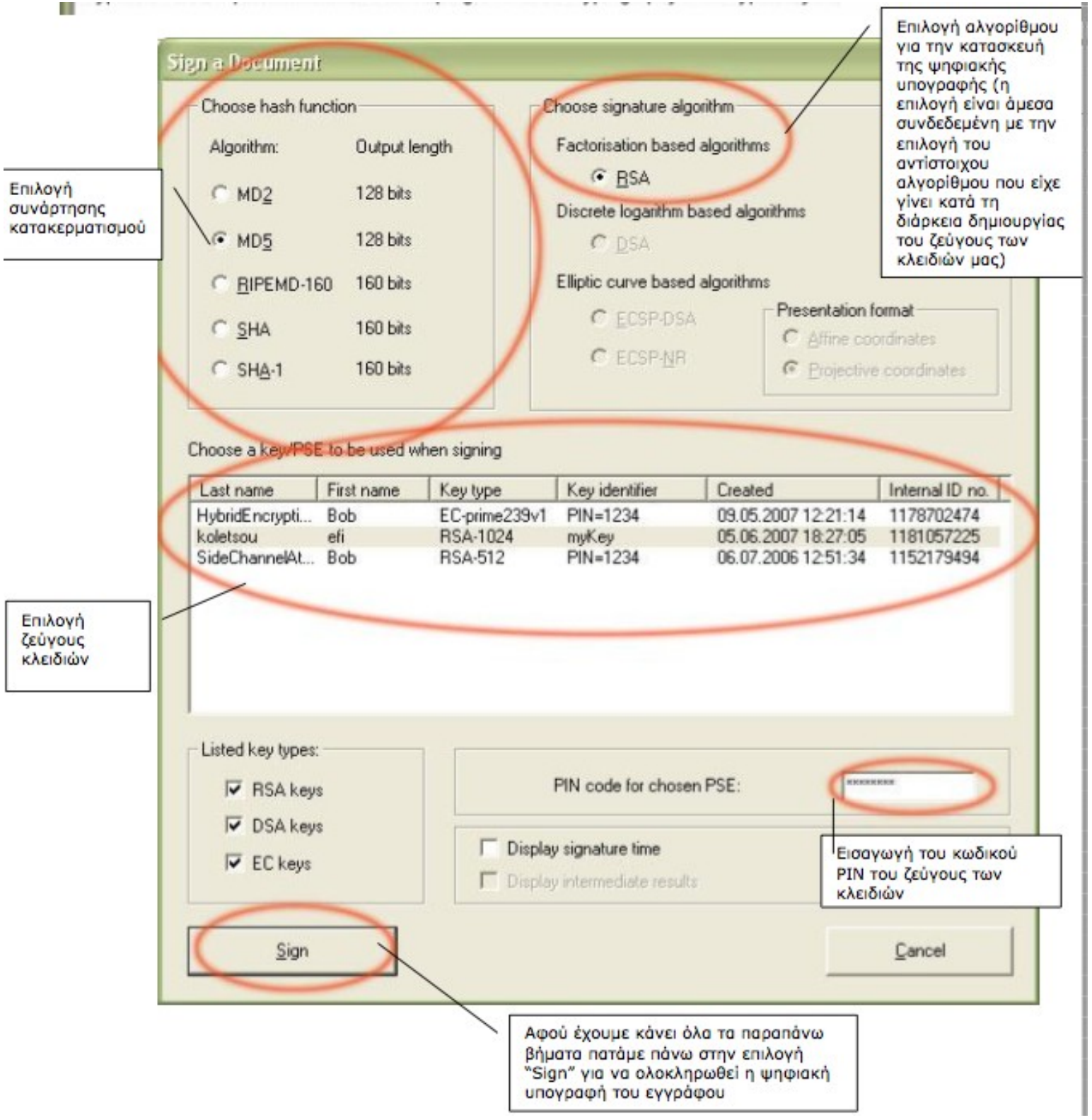
Ψηφιακή Υπογραφή Κειμένου
digital signature

- Πιστοποίηση της αυθεντικότητας ενός μηνύματος
- Ακολουθία χαρακτήρων άμεσα συσχετισμένη με το περιεχόμενο του μηνύματος και την ταυτότητα αυτού που το υπογράφει
- Αποστέλλεται μαζί με το μήνυμα
- Ο παραλήπτης ελέγχοντας την υπογραφή μπορεί 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 υπογράφτηκε με το αντίστοιχο ιδιωτικό κλειδί

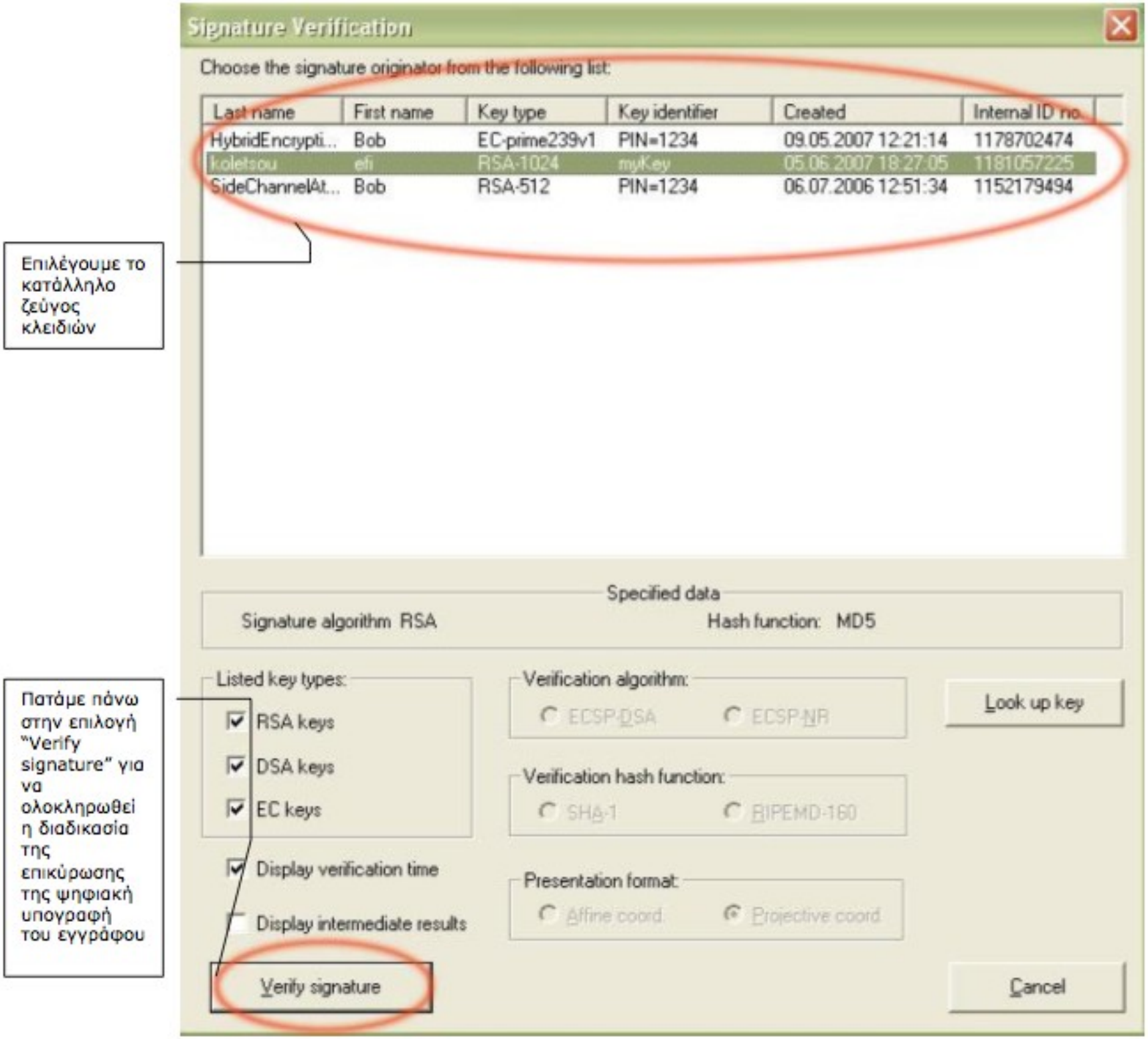



CrypTool 1.4.10 - beta 04 - startingexample-en
File Edit View Crypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
PKI
Sign Document...
Verify Signature...
Extract Signature
Signature Demonstration (Signature Generation)...
startingexample-en
CrypTool
CrypTool is a comprehensive educational program about cryptography and cryptanalysis.


Sign a Document
Choose hash function
Algorithm:
Output length
MD2
128 bits
MD5
128 bits
RIPEMD-160
160 bits
SHA
160 bits
SHA-1
160 bits
Choose signature algorithm
Factorisation based algorithms
RSA
Discrete logarithm based algorithms
DSA
Elliptic curve based algorithms
ECSP-DSA
ECSP-NR
Presentation format
Affine coordinates
Projective coordinates
Choose a key/PSE to be used when signing
Last name
First name
Key type
Key identifier
Created
Internal ID no.
HybridEncrypti...
Bob
EC-prime239v1
PIN=1234
09.05.2007 12:21:14
1178702474
koletsou
efi
RSA-1024
myKey
05.06.2007 18:27:05
1181057225
SideChannelAt...
Bob
RSA-512
PIN=1234
06.07.2006 12:51:34
1152179494
Listed key types:
RSA keys
DSA keys
EC keys
PIN code for chosen PSE:
Display signature time
Display intermediate results
Sign
Cancel
Επιλογή αλγορίθμου για την κατασκευή της ψηφιακής υπογραφής (η επιλογή είναι άμεσα συνδεδεμένη με την επιλογή του αντίστοιχου αλγορίθμου που είχε γίνει κατά τη διάρκεια δημιουργίας του ζεύγους των κλειδιών μας)
Επιλογή συνάρτησης κατακερματισμού
Επιλογή ζεύγους κλειδιών
Εισαγωγή του κωδικού PIN του ζεύγους των κλειδιών
Αφού έχουμε κάνει όλα τα παραπάνω βήματα πατάμε πάνω στην επιλογή "Sign" για να ολοκληρωθεί η ψηφιακή υπογραφή του εγγράφου

Επικύρωση της ψηφιακής υπογραφής




Signature Verification
Choose the signature originator from the following list:
Last name
First name
Key type
Key identifier
Created
Internal ID no.
HybridEncrypti...
Bob
EC-prime239v1
PIN=1234
09.05.2007 12:21:14
1178702474
koletsou
efi
RSA-1024
myKey
05.06.2007 18:27:05
1181057225
SideChannelAt...
Bob
RSA-512
PIN=1234
06.07.2006 12:51:34
1152179494
Επιλέγουμε το κατάλληλο ζεύγος κλειδιών
Specified data
Signature algorithm RSA
Hash function: MD5
Listed key types:
RSA keys
DSA keys
EC keys
Verification algorithm:
ECSP-DSA
ECSP-NR
Look up key
Verification hash function:
SHA-1
RIPEMD-160
Display verification time
Presentation format:
Affine coord.
Projective coord.
Display intermediate results
Πατάμε πάνω στην επιλογή "Verify signature" για να ολοκληρωθεί η διαδικασία της επικύρωσης της ψηφιακή υπογραφή του εγγράφου
Verify signature
Cancel