

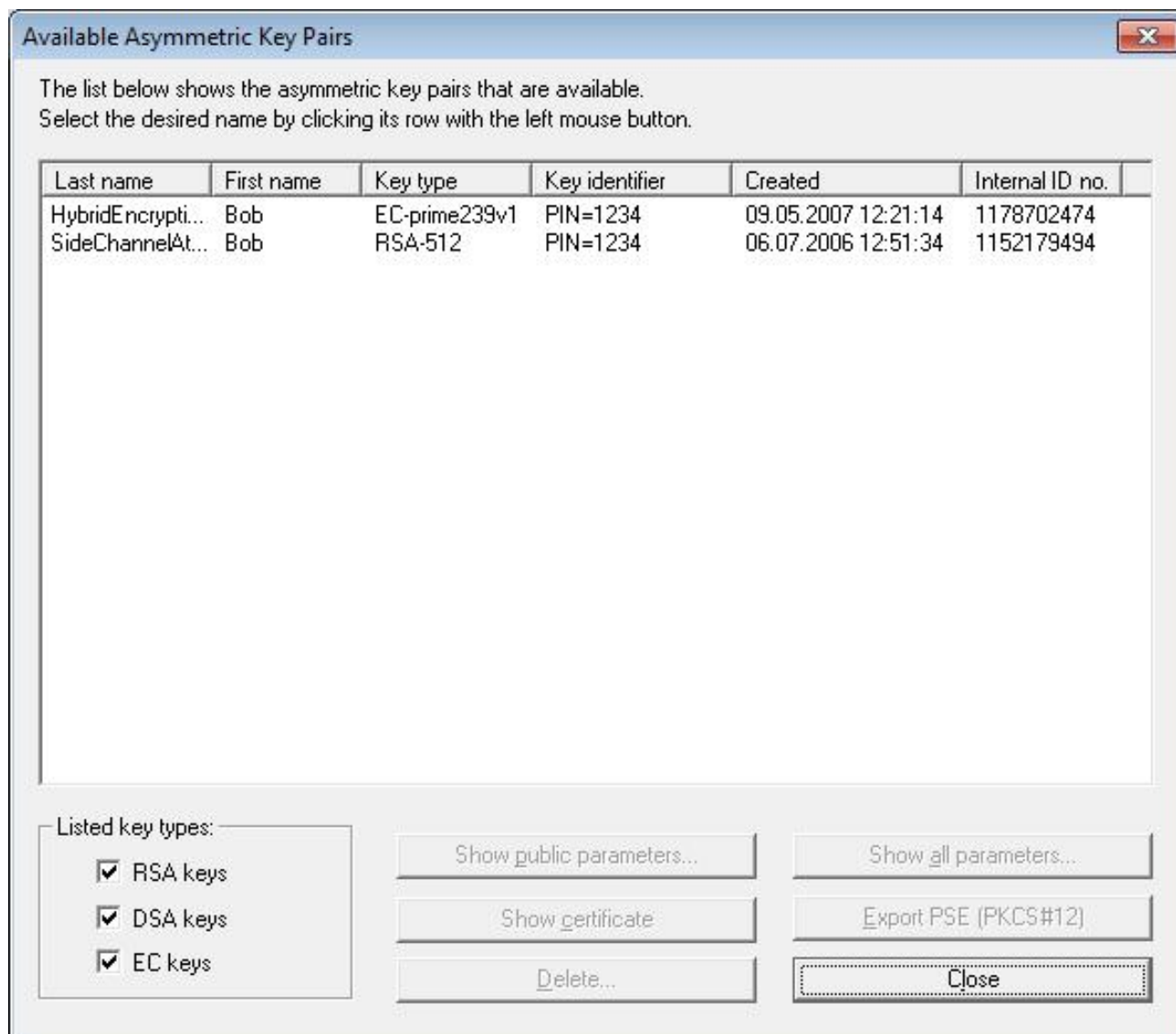
## Δραστηριότητα για το επόμενο μάθημα

### 1. Δημιουργία ζεύγους κλειδιών RSA

Εκτελούμε το εργαλείο Cryptool και από το μενού επιλέγουμε:

**Digital Signatures / PKI → PKI → Display /Export Keys**

Από το παράθυρο που εμφανίζεται, ενημερωνόμαστε για τα ζεύγη κλειδιών που υπάρχουν στον υπολογιστή μας και για τα οποία είναι ενήμερο το Cryptool



**Εικόνα 1.** Εγκατεστημένα ζεύγη κλειδιών.

Στη συνέχεια, θα δημιουργήσουμε ένα ζεύγος ιδιωτικού & δημοσίου κλειδιού. Από το μενού επιλέγουμε: **Digital Signatures / PKI → PKI → Generate / Import Keys**

**Generation of Asymmetric Key Pair**

**Algorithm**

- ☒ **RSA**  
Bit length of RSA modulus: 2048
- ☐ **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: Bell  
First name: Jim  
Key identifier (optional): NSA  
PIN: xxxx  
PIN verification: xxxx

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

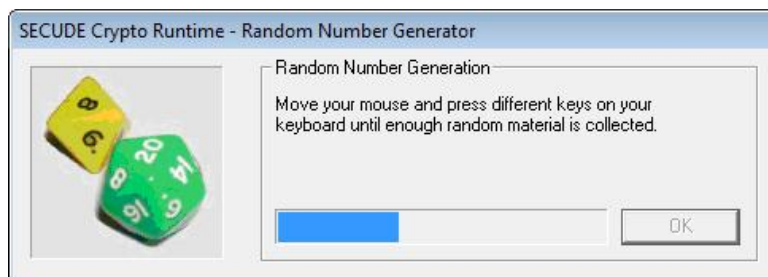
Generate new key pair... PKCS #12 Import Show key pair... Close

**Εικόνα 2.** Δημιουργία ζεύγους κλειδιών στο *Cryptool*.

Επιλέγουμε τη χρήση του RSA με modulus ίσο με 2048 bits. Εισάγουμε τα στοιχεία μας (User data). Αν, για παράδειγμα, είμαστε ο Jim Bell της NSA, θα μπορούσαμε να εισάγουμε:

- Last name: Bell
- First name: Jim
- Key Identifier: NSA
- PIN: protect

Πατάμε το κουμπί **Generate new key pair...** Μετά από ελάχιστα δευτερόλεπτα, αφού μετακινήσουμε το ποντίκι ή πατήσουμε τυχαία πλήκτρα ώστε να συλλεγούν τυχαίες τιμές, το ζεύγος κλειδιών δημιουργείται (Εικόνα 3).



**Εικόνα 3.** Εκτέλεση διαδικασίας δημιουργίας ζεύγους κλειδιών στο *Cryptool*.

Για να το δούμε, επιλέγουμε το κουμπί **Show key pair...**

## 2. Εξαγωγή δημοσίου κλειδιού RSA

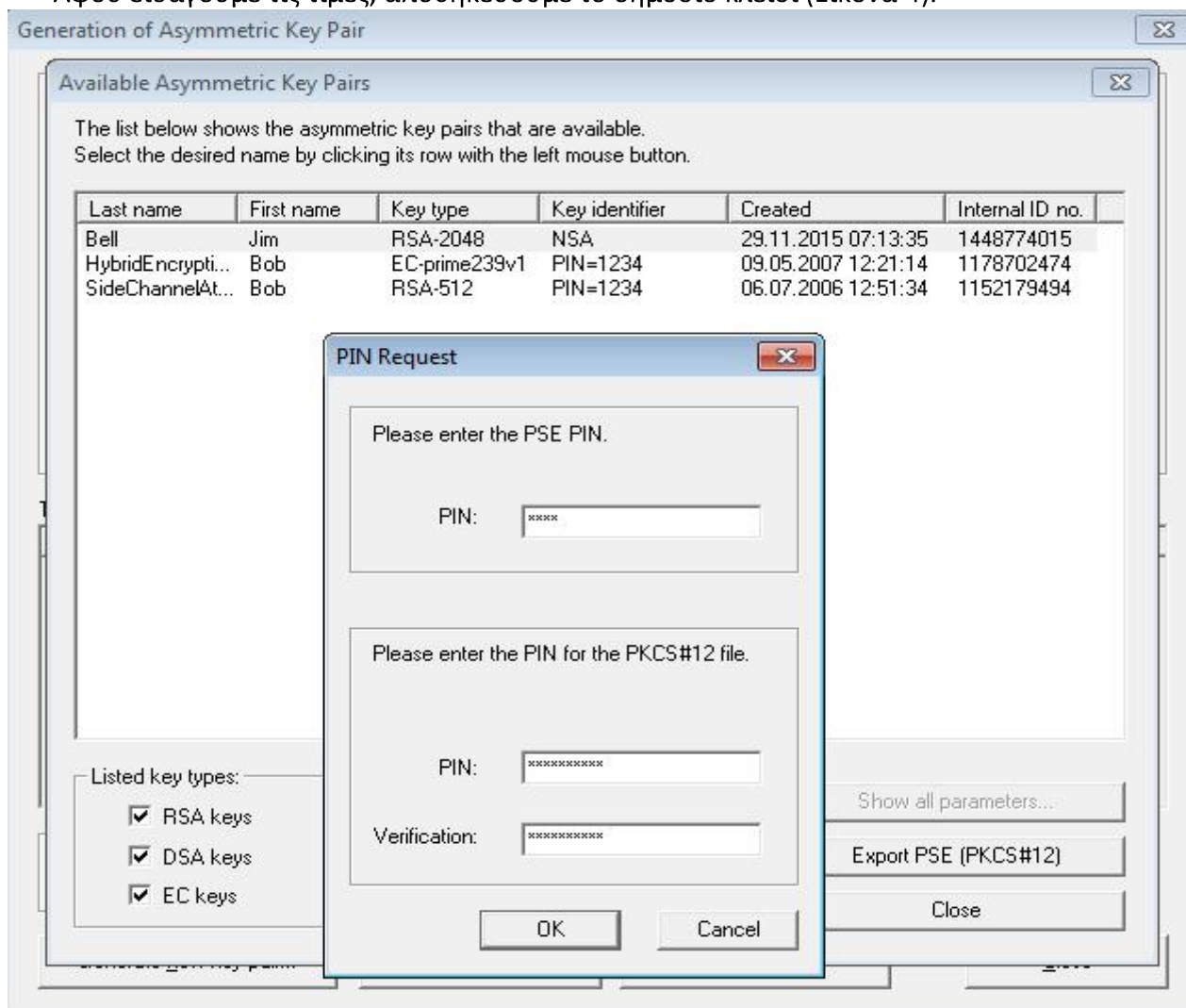
Στη ασύμμετρη κρυπτογραφία, για να αποστείλει κάποιος ένα κρυπτογραφημένο μήνυμα σε εμάς, θα πρέπει να γνωρίζει το δημόσιο κλειδί μας. Άρα, θα πρέπει με κάποιο τρόπο να το εξαγάγουμε και να μπορούμε να το διανεύουμε:

- Από το μενού επιλέγουμε: **Digital Signatures / PKI → PKI → Key Display / Export**
- Επιλέγουμε το ζεύγος κλειδιών που δημιουργήσαμε.

Πατάμε το κουμπί Export PSE (PKCS #12) και εισάγουμε το PIN που χρησιμοποιήσαμε κατά τη δημιουργία του ζεύγους κλειδιών.

Στη συνέχεια, εισάγουμε PIN για το PKCS#12 αρχείο. Το PIN αυτό χρησιμοποιείται προκειμένου να περιορίσουμε την χρήση του δημοσίου κλειδιού μας σε όσους διαθέτουν το PKCS#12 PIN.

Αφού εισάγουμε τις τιμές, αποθηκεύουμε το δημόσιο κλειδί (Εικόνα 4).



Εικόνα 4. Εξαγωγή κλειδιού σε αρχείο τύπου PKCS#12.

Μπορούμε να αποστείλουμε το δημόσιο αυτό κλειδί με οποιοδήποτε τρόπο σε όλους, όσοι επιθυμούν να το χρησιμοποιήσουν για να επικοινωνήσουν μαζί μας. Για παράδειγμα, μπορείτε να το αποστείλετε με email σε κάποιο συμφοιτητή σας.

### 3. Εισαγωγή δημοσίου κλειδιού RSA

Έστω ότι έχουμε στην κατοχή μας το δημόσιο κλειδί του προσώπου με το οποίο θα επικοινωνήσουμε. Στο εργαλείο CrypTool, από το μενού επιλέγουμε:

**Digital Signatures / PKI → PKI → Generate/ Import Keys**

και Πατάμε το κουμπί PKCS#12 Import.

Διαλέγουμε από την επιφάνεια εργασίας το δημόσιο κλειδί του άλλου προσώπου που αποθηκεύσαμε και εισάγουμε το απαραίτητο PIN προκειμένου να ολοκληρωθεί η εισαγωγή του δημόσιου κλειδιού.

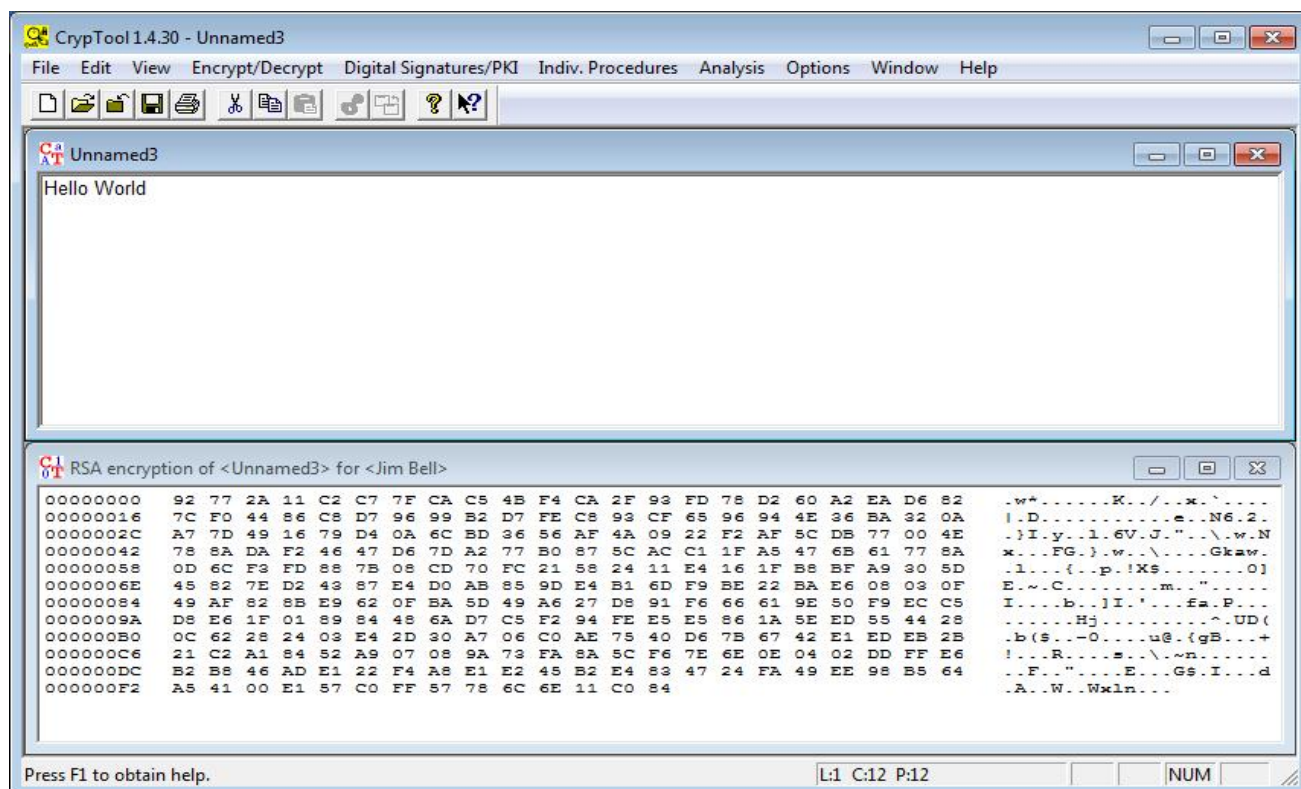
### 4. Κρυπτογράφηση με χρήση RSA

Από το μενού του CrypTool επιλέγουμε: **File → New** και γράφουμε μία φράση της αρεσκείας μας. Στη συνέχεια από το μενού επιλέγουμε:

**Encrypt / Decrypt → Asymmetric → RSA Encryption**

κι επιλέγουμε το δημόσιο κλειδί του παραλήπτη του κρυπτογραφήματος.

Πατάμε **Encrypt** και εμφανίζεται το μήνυμά μας κρυπτογραφημένο με το δημόσιο κλειδί του άλλου προσώπου (Εικόνα 5).



Εικόνα 5. Αρχικό μήνυμα και κρυπτογραφημένο με τον RSA.

Έχοντας επιλέξει το παράθυρο του κρυπτοκειμένου, από το μενού επιλέγουμε: **File → Save as** και αποθηκεύουμε το αρχείο το οποίο μπορούμε να αποστείλουμε στον παραλήπτη.

Προσπαθήστε να αποκρυπτογραφήσετε το αρχείο που μόλις κρυπτογραφήσατε.

- Είναι δυνατό;
- Συνάδει το αποτέλεσμα με όσα ξέρετε για την κρυπτογραφία δημόσιου κλειδιού;

## 5. Αποκρυπτογράφηση αρχείου με RSA

Ανοίξτε στο Cryptool ένα κρυπτογραφημένο μήνυμα που έχει κρυπτογραφηθεί με το δημόσιο κλειδί σας.

Από το μενού επιλέξτε: **Encrypt/Decrypt → Asymmetric → RSA Decryption**

Επιλέξτε το μυστικό κλειδί που θα χρησιμοποιήσετε για την αποκρυπτογράφηση, εισάγετε το PIN και πατάτε **Decrypt**.

- Ποιο κλειδί χρησιμοποιήσατε για την αποκρυπτογράφηση;
- Γιατί υπάρχουν επιπρόσθετα μηδενικά στο τέλος του αρχείου;

## 6. Αναπαράσταση της λειτουργίας του RSA

Στο Cryptool επιλέξτε **Indiv. Procedures → RSA Cryptosystem → RSA Demonstration...**

και πειραματιστείτε κρυπτογραφώντας και αποκρυπτογραφώντας το ονοματεπώνυμο σας.

## 7. Επίθεση στο RSA για μικρές τιμές του N

Η ανάλυση θα γίνει σε δύο μέρη:

- Πρώτα υπολογίζονται οι πρώτοι παράγοντες (factorization) του RSA και στη συνέχεια
- Υπολογίζεται το μυστικό κλειδί που έγινε η κρυπτογράφηση.

Είναι γνωστά εκ των προτέρων τα εξής:

*RSA modulus  $N = 63978486879527143858831415041$*

*Public exponent  $e = 17579$*

*Cipher Text = 21000659868873971790797821827,  
45841073649477115085555273031, 56556190677970417929536844197*

Βρείτε τα **p** και **q** υπολογίζοντας τους παράγοντες του **N**.

Επιλέξτε από το μενού **Indiv. Procedures → RSA Cryptosystem → Factorization of a Number...**

Αποκρυπτογραφήστε το κρυπτοκείμενο χρησιμοποιώντας τον RSA με τις κατάλληλες τιμές για τα **p**, **q** και **e**.

Στις επιλογές "**Alphabet and number system oprions...**"

επιλέξτε με τη σειρά "**Specify alphabet**", "**Normal**", "**Number system**", "**14**", "**Decimal**".