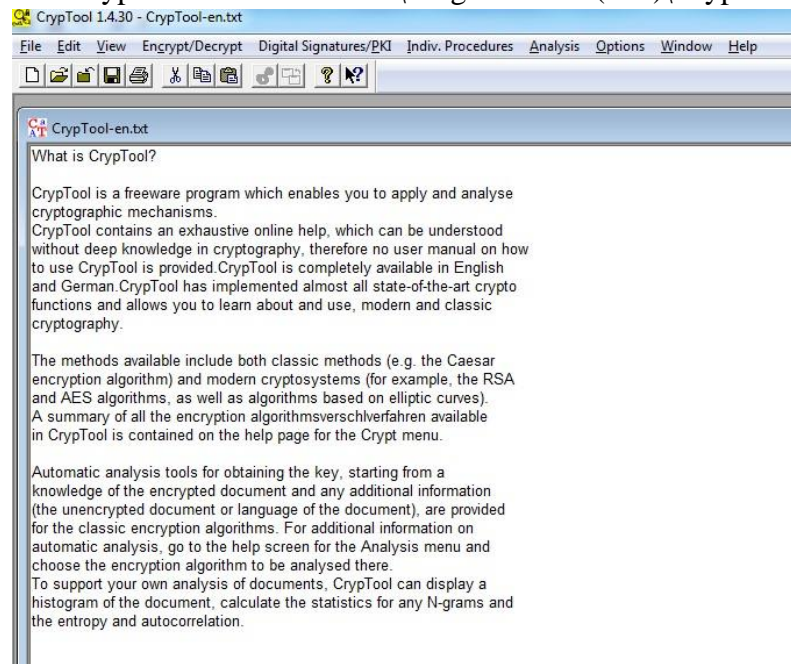
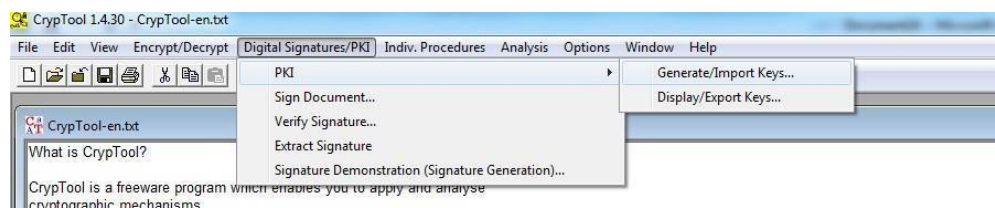


## Procedure

1. Open the file CrypTool-en.txt under C:\Program Files (x86)\CrypTool\examples.



2. Click from menu Digital Signatures/PKI/Generate/Import Keys.



3. Enter the following Last name: Smith

First name:

John

Key identifier: Smith Key

PIN code: cryptool

PIN: cryptool

4. And click on the Generate new key pair button.

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: Smith

First name: John

Key identifier (optional): Smith Key

PIN: 12345678

PIN verification: 12345678

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

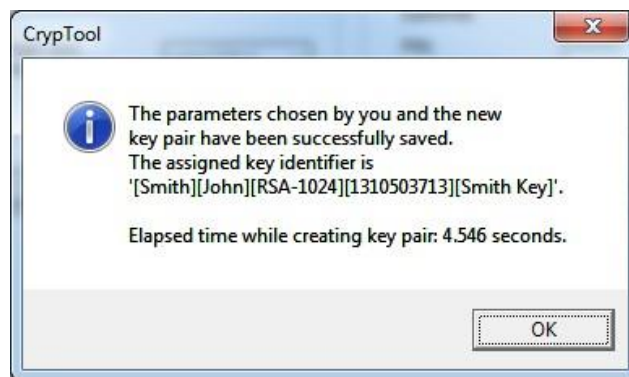
Parameters	Value of the parameter	Bit len...

Base for presentation of numbers

☒ Octal ☐ Decimal ☐ Hexadecimal

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

5. The following window shows up and click OK:



6. Click Show Key Pair, you will see

Available Asymmetric Key Pairs

The list below shows the asymmetric key pairs that are available.  
Select the desired name by clicking its row with the left mouse button.

Last name	First name	Key type	Key identifier	Created	Internal ID no.
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 05:21:14	1178702474
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 05:51:34	1152179494
Smith	John	RSA-1024	Smith Key	12.07.2011 16:48:33	1310503713

Listed key types:

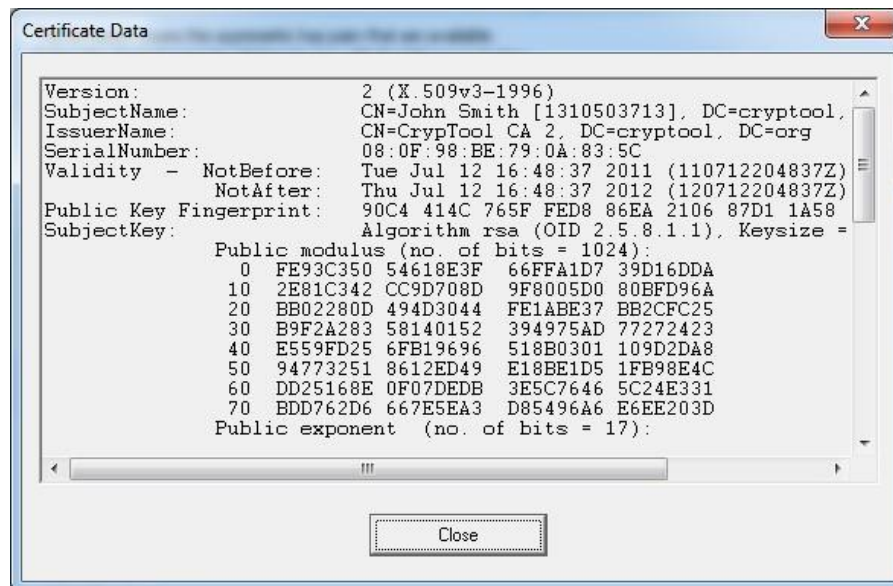
☒ RSA keys

☒ DSA keys

☒ EC keys

Show public parameters... Show all parameters... Show certificate Export PSE (PKCS #12) Delete... Close

7. The certificate is displayed by clicking on the Show certificate pushbutton.



8. Close both dialogs on Certificate Data and Available Asymmetric Key Pairs.
9. To sign the document of CrypTool-en.txt, select Digital Signatures/PKI\Sign Message.  
Enter the following

Choose hash function: RIPEMD-160

Choose signature algorithm: RSA

Choose a key/PSE to be used when signing: Smith John

PIN code: cryptool

And click on Sign button.



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

Factorization 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.
HybridEncrypt...	Bob	EC-prime239v1	PIN=1234	09.05.2007 05:21:14	1178702474
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 05:51:34	1152179494
Smith	John	RSA-1024	Smith Key	12.07.2011 16:48:33	1310503713

Listed key types:

☒ RSA keys
 ☒ DSA keys
 ☒ EC keys

PIN code for chosen PSE:

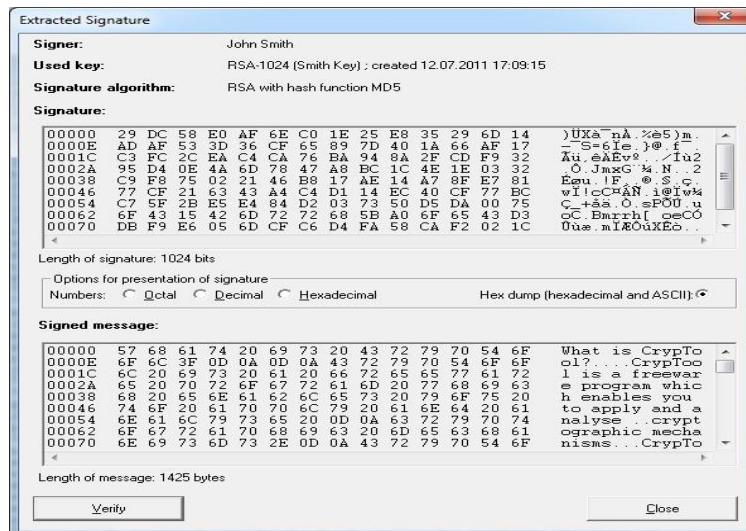
☐ Display signature time
 ☐ Display intermediate results

Sign

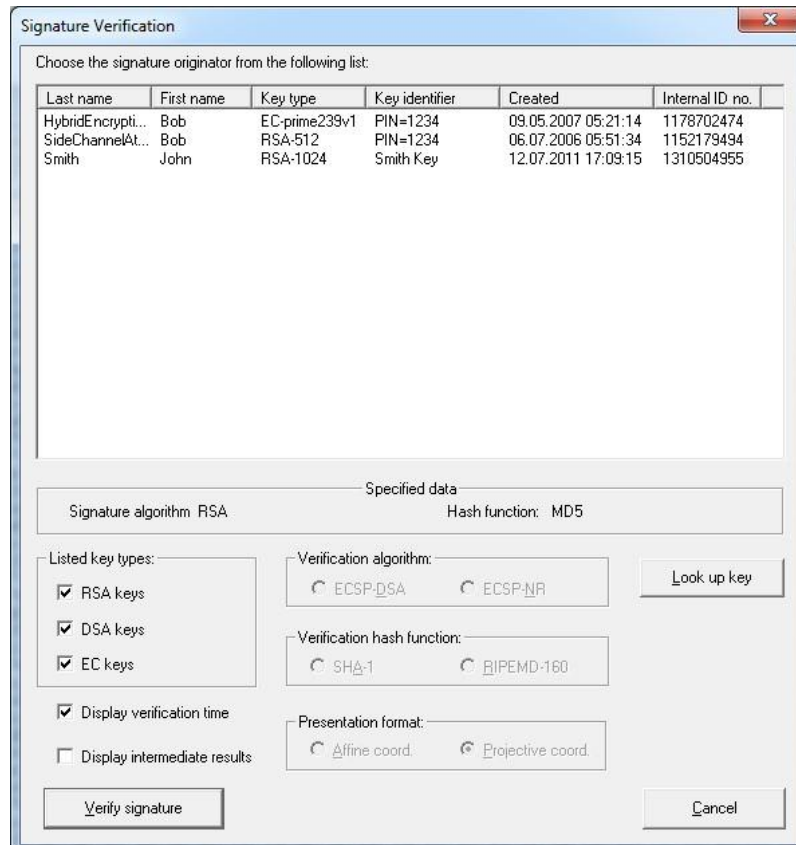
Cancel

10. Click OK button. The dialog box closes and the signed document is displayed.

11. The signature is at the start of the document and the document to be signed is at the end, as can be verified easily by comparing with the original document. A clearer presentation, with the separation of the signature and the document, can be obtained by selecting Digital Signature/PKI\Extract Signature.



12. Select Digital Signature/PKI\Verify Signature to check that the document has not been altered.





13. Select John Smith from the list of signatures and click on the Verify signature button. The following dialog appears.



14. modify the message by deleting "What".
15. Select Digital Signature/PKI\Verify Signature, the following dialog box appears:

