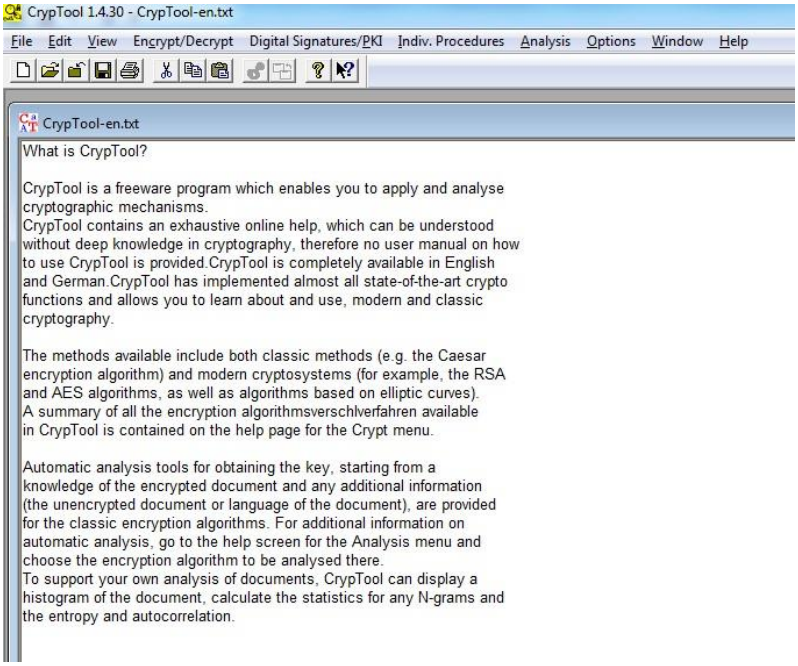
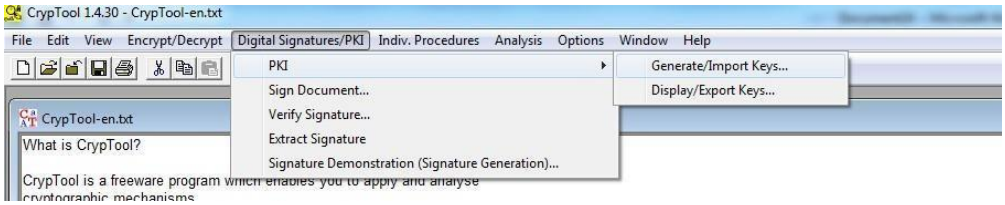
Procedure

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



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



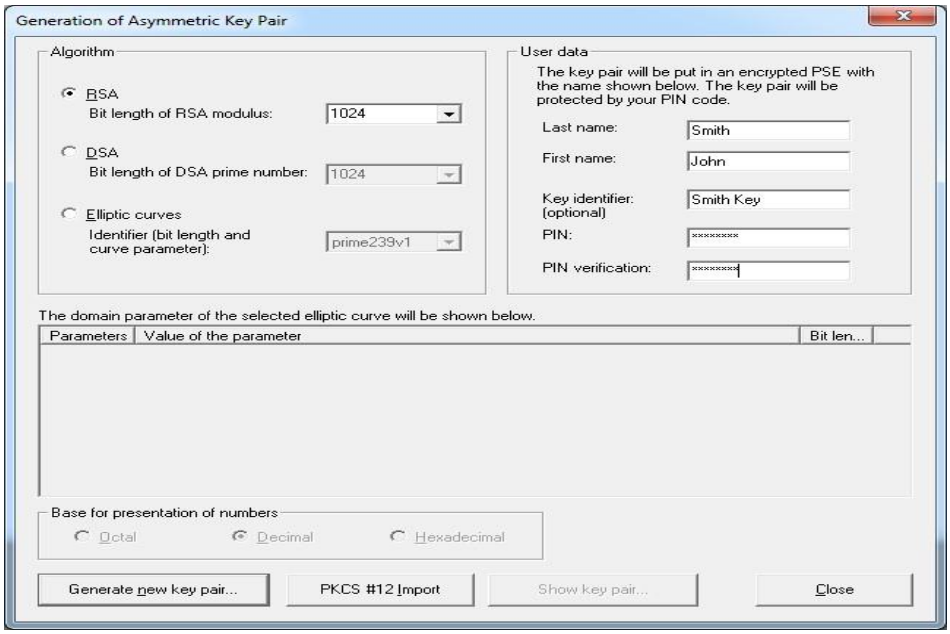
3. Enter the following Last name: Smith

First name:

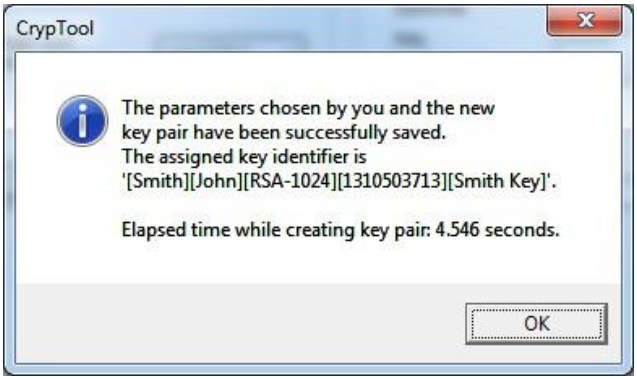
John

Key identifier: Smith Key
PIN code: cryptool
PIN: cryptool

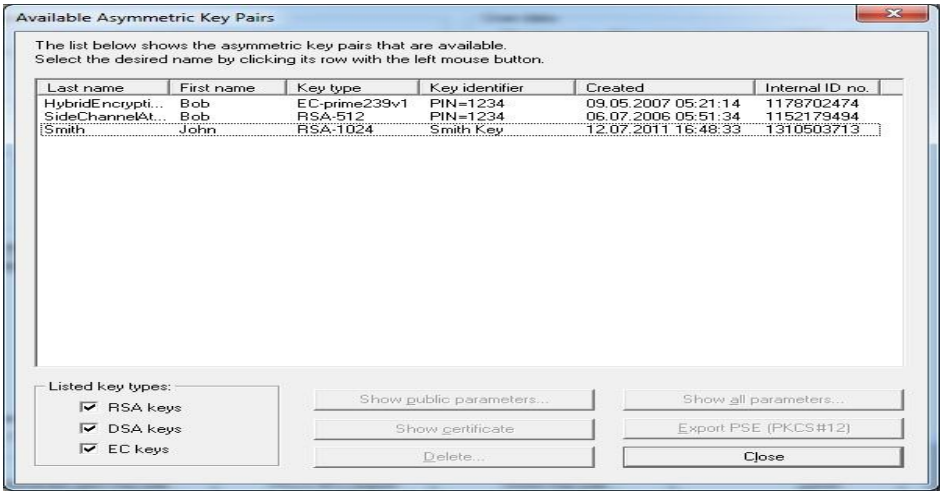
4. And click on the Generate new key pair button.



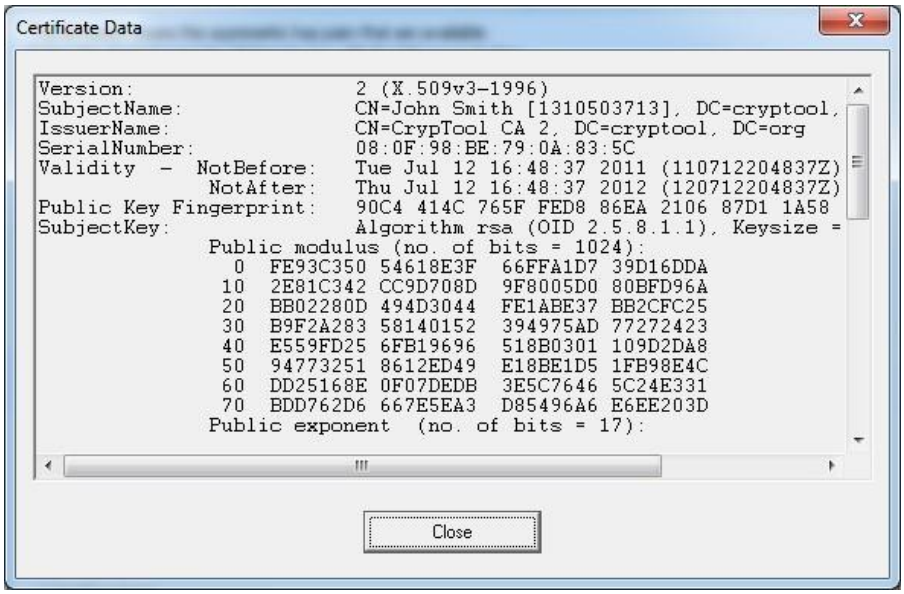
5. The following window shows up and click OK:



6. Click Show Key Pair, you will see



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

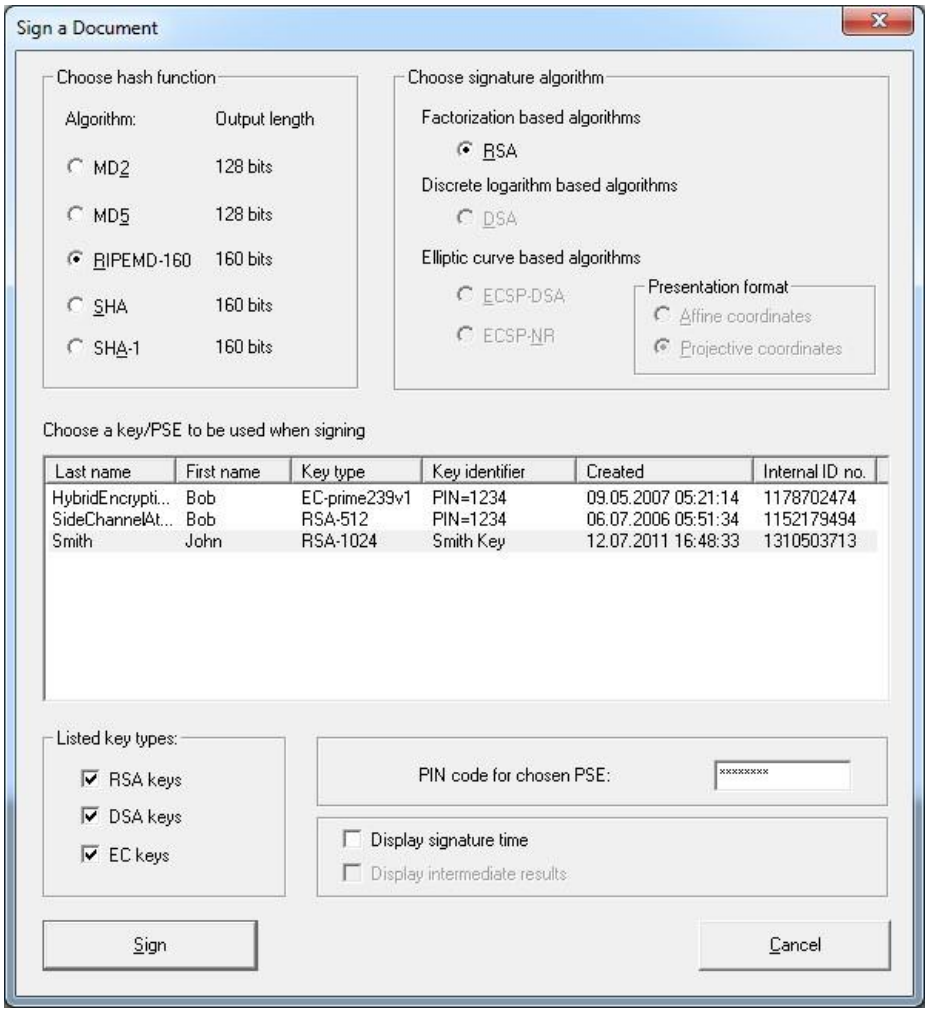
Choose hash function: RIPEMD-160

Choose signature algorithm: RSA

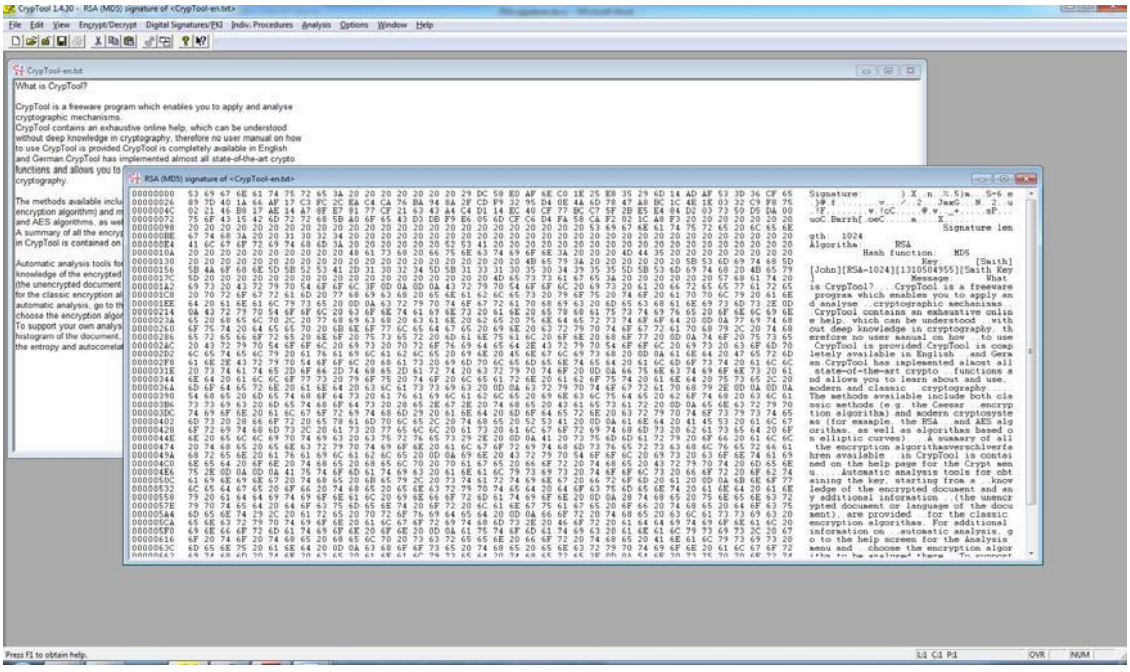
Choose a key/PSE to be used when signing: Smith John

PIN code: cryptool

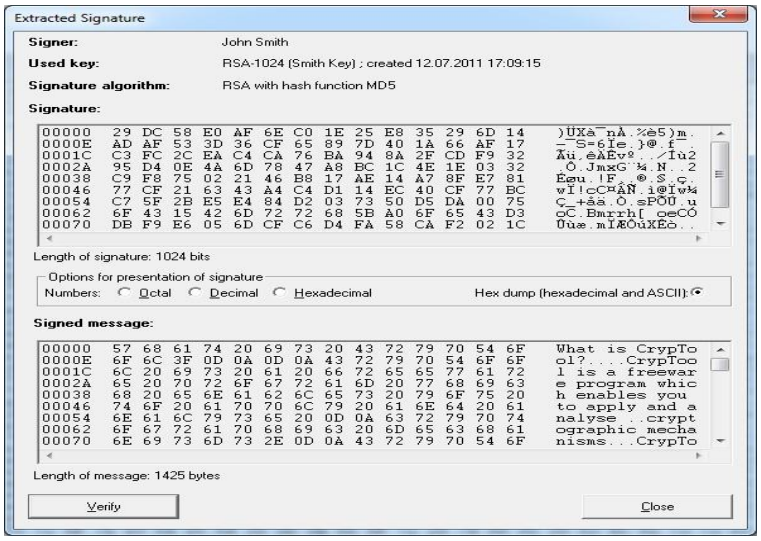
And click on Sign button.



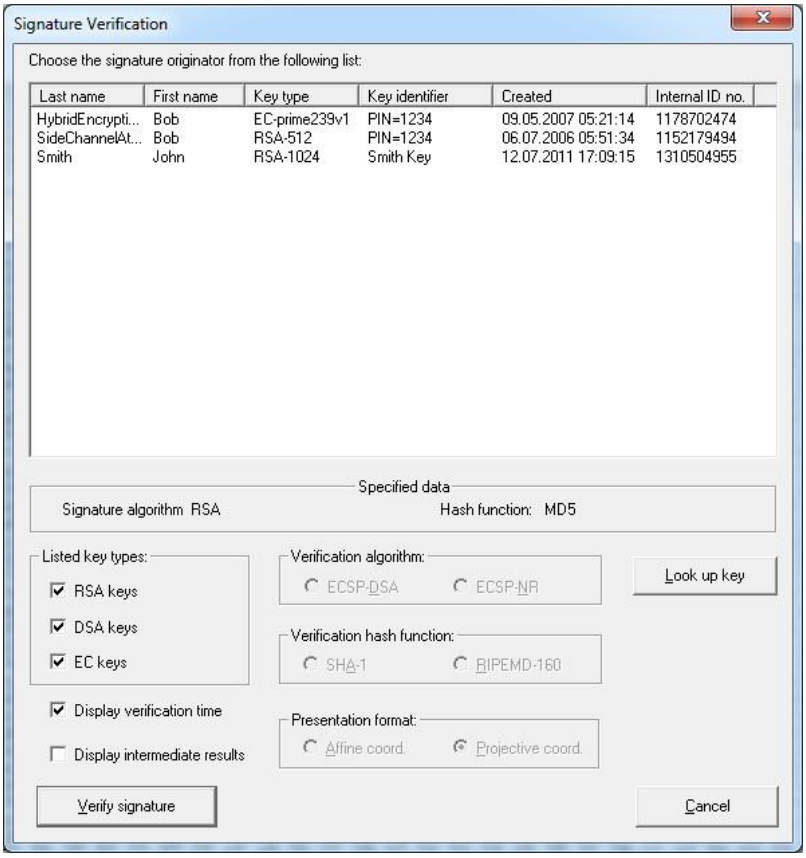
10. Click OK button. The dialog box closes and the signed document is displayed.



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: