Experiment No.10

Create and verify digital signature using cryptool

Minimum Theoretical Background

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity). Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement electronic signatures, which include any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including South Africa, the United States, Algeria, Turkey, India, Brazil, Indonesia, Mexico, Saudi Arabia, Uruguay, Switzerland and the countries of the European Union electronic signatures have legal significance.

As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. The United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures. Universities including Penn State, University of Chicago, and Stanford are publishing electronic student transcripts with digital signatures.

Below are some common reasons for applying a digital signature to communications:

Applications:

1. Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

2. Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to *change* an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

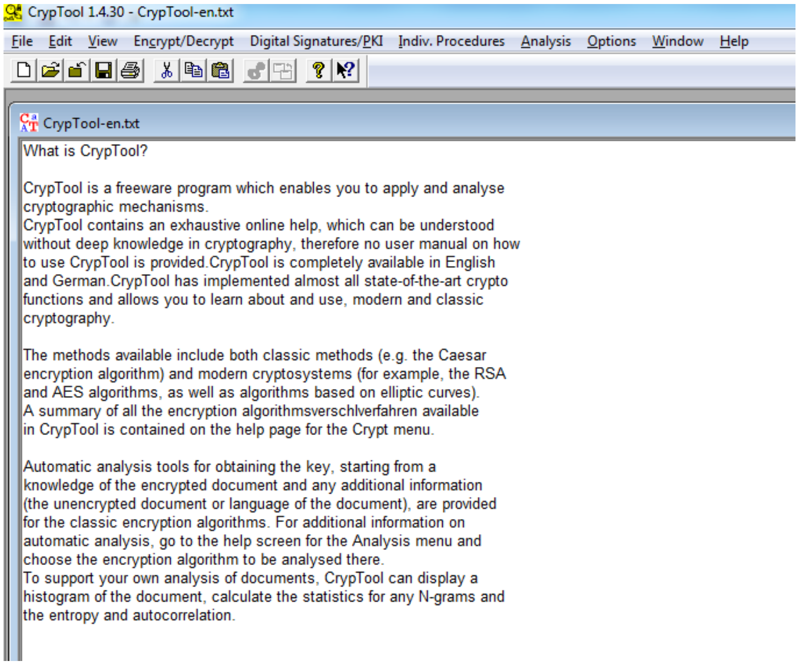
3. Non-repudiation

Non-repudiation or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that these authentications, non-repudiation etc. properties rely on the secret key *not having been revoked* prior to its usage. Public revocation of a key-pair is a required ability; else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check; e.g., checking a certificate revocation list or via the Online Certificate Status Protocol. Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purpose.

II. Procedure

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


CrypTool 1.4.30 - CrypTool-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
CrypTool-en.txt

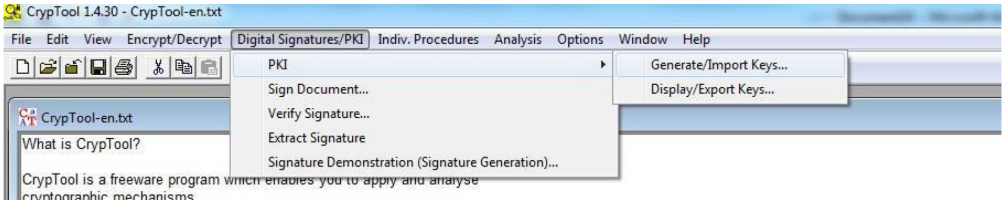
What is CrypTool?

CrypTool is a freeware program which enables you to apply and analyse cryptographic mechanisms.
CrypTool contains an exhaustive online help, which can be understood without deep knowledge in cryptography, therefore no user manual on how to use CrypTool is provided.CrypTool is completely available in English and German.CrypTool has implemented almost all state-of-the-art crypto functions and allows you to learn about and use, modern and classic cryptography.

The methods available include both classic methods (e.g. the Caesar encryption algorithm) and modern cryptosystems (for example, the RSA and AES algorithms, as well as algorithms based on elliptic curves).
A summary of all the encryption algorithmsverschlverfahren available in CrypTool is contained on the help page for the Crypt menu.

Automatic analysis tools for obtaining the key, starting from a knowledge of the encrypted document and any additional information (the unencrypted document or language of the document), are provided for the classic encryption algorithms. For additional information on automatic analysis, go to the help screen for the Analysis menu and choose the encryption algorithm to be analysed there.
To support your own analysis of documents, CrypTool can display a histogram of the document, calculate the statistics for any N-grams and the entropy and autocorrelation.

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


CrypTool 1.4.30 - CrypTool-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
PKI
Sign Document...
Verify Signature...
Extract Signature
Signature Demonstration (Signature Generation)...
Generate/Import Keys...
Display/Export Keys...
CrypTool-en.txt
What is CrypTool?
CrypTool is a freeware program which enables you to apply and analyse
cryptographic mechanisms

3.Enter the

following Last

name: **Smith**

First name:

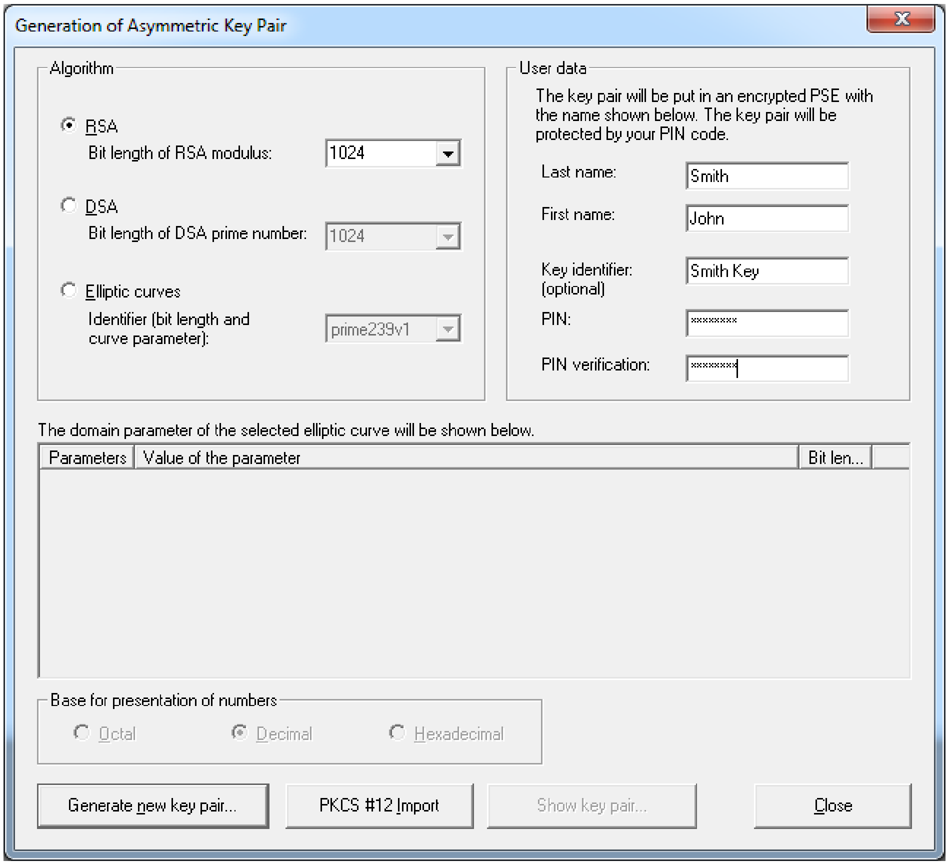
John

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: ********

PIN verification: ********

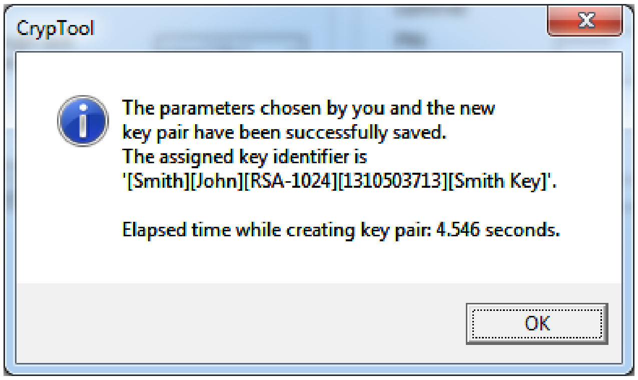
The domain parameter of the selected elliptic curve will be shown below.

Parameters	Value of the parameter	Bit len...

Base for presentation of numbers

○ Octal ● Decimal ○ Hexadecimal

5. The following window shows up and click OK:

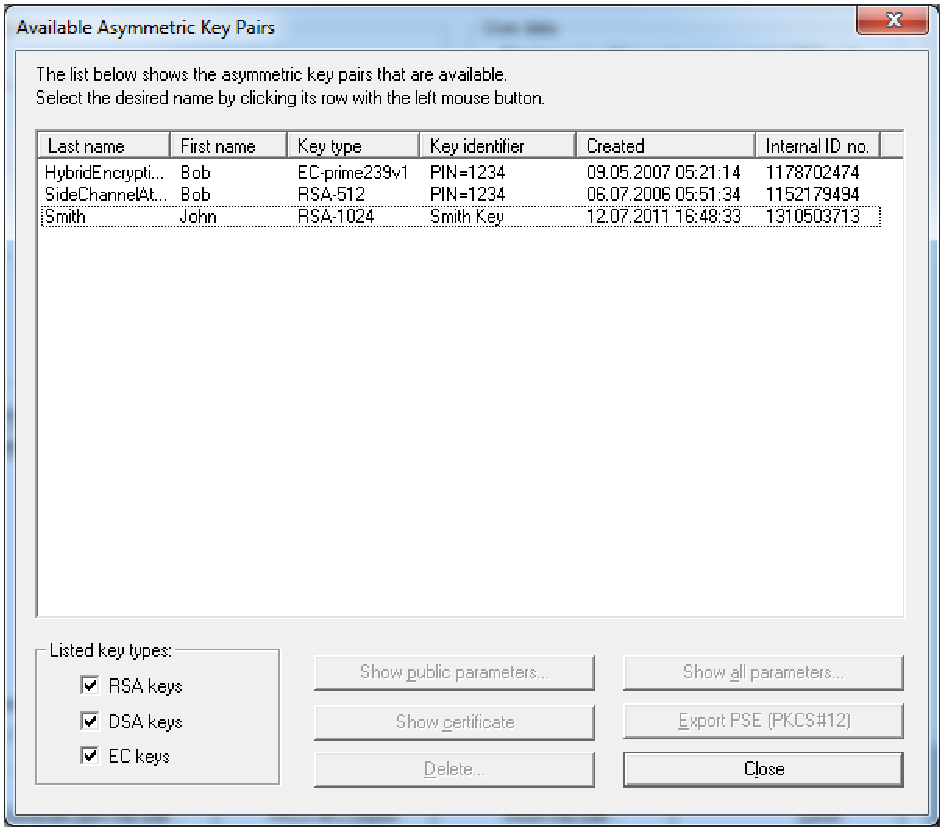


CrypTool

The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is '[Smith][John][RSA-1024][1310503713][Smith Key]'.

Elapsed time while creating key pair: 4.546 seconds.

6. Click Show Key Pair, you will see



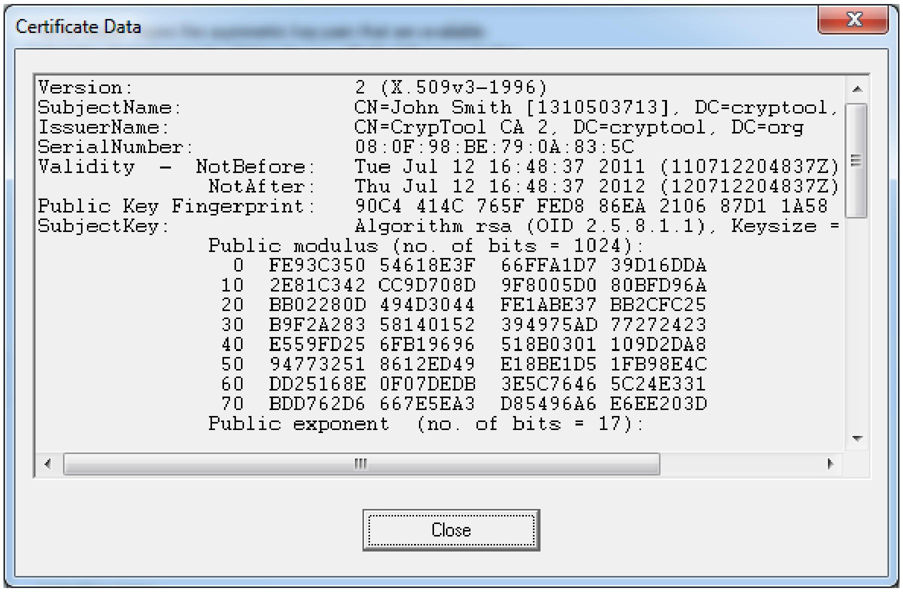
Available Asymmetric Key Pairs

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

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



Certificate Data

```
Version:                     2 (X.509v3-1996)
SubjectName:                 CN=John Smith [1310503713], DC=cryptool,
IssuerName:                  CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber:                08:0F:98:BE:79:0A:83:5C
Validity  -  NotBefore:      Tue Jul 12 16:48:37 2011 (110712204837Z)
              NotAfter:      Thu Jul 12 16:48:37 2012 (120712204837Z)
Public Key Fingerprint:      90C4 414C 765F FED8 86EA 2106 87D1 1A58
SubjectKey:                  Algorithm rsa (OID 2.5.8.1.1), Keysize =
              Public modulus (no. of bits = 1024):
                0   FE93C350 54618E3F  66FFA1D7 39D16DDA
               10   2E81C342 CC9D708D  9F8005D0 80BFD96A
               20   BB02280D 494D3044  FE1ABE37 BB2CFC25
               30   B9F2A283 58140152  394975AD 77272423
               40   E559FD25 6FB19696  518B0301 109D2DA8
               50   94773251 8612ED49  E18BE1D5 1FB98E4C
               60   DD25168E 0F07DEDB  3E5C7646 5C24E331
               70   BDD762D6 667E5EA3  D85496A6 E6EE203D
              Public exponent  (no. of bits = 17):
```

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

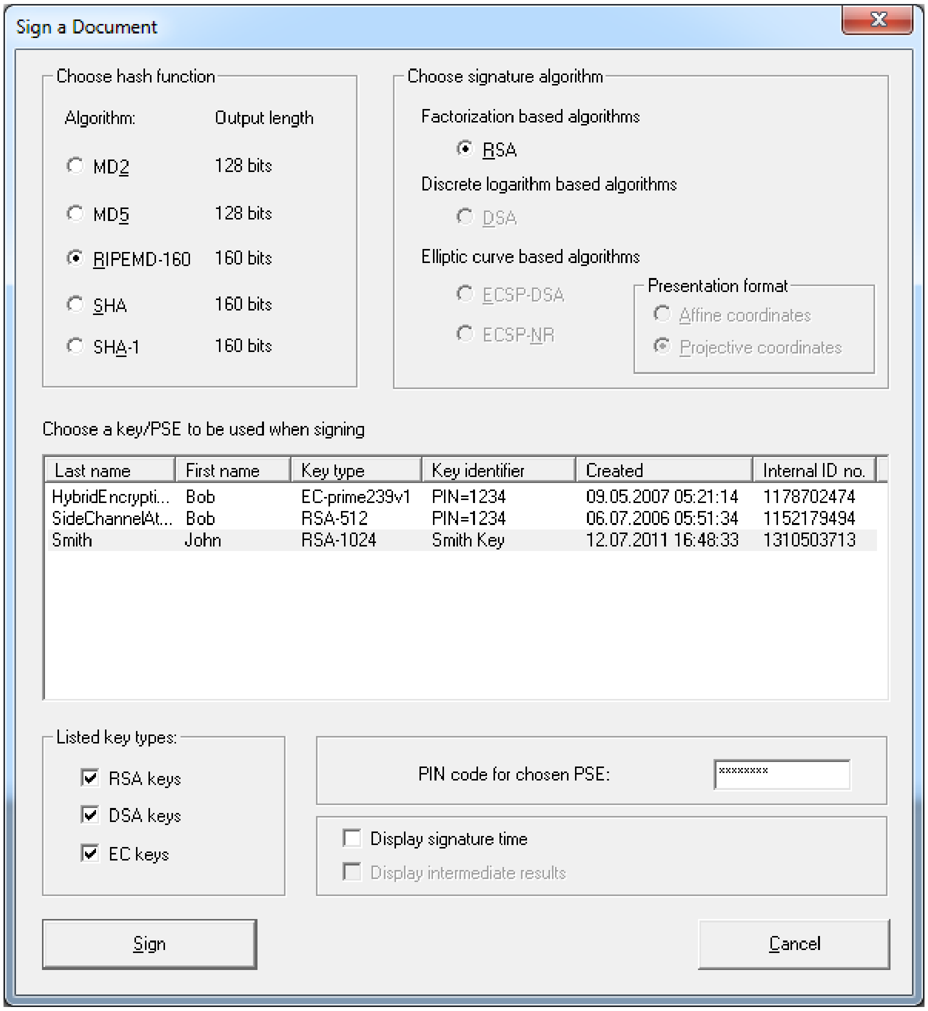
Choose hash function: RIPEMD-160

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.
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

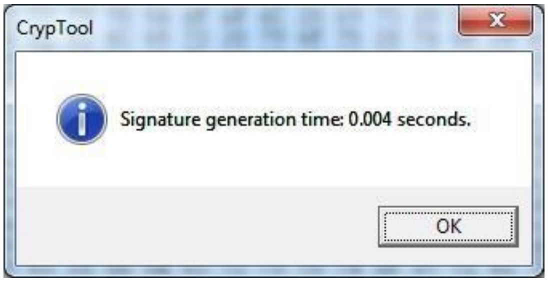
☑ DSA keys

☑ EC keys

PIN code for chosen PSE: ********

☐ Display signature time

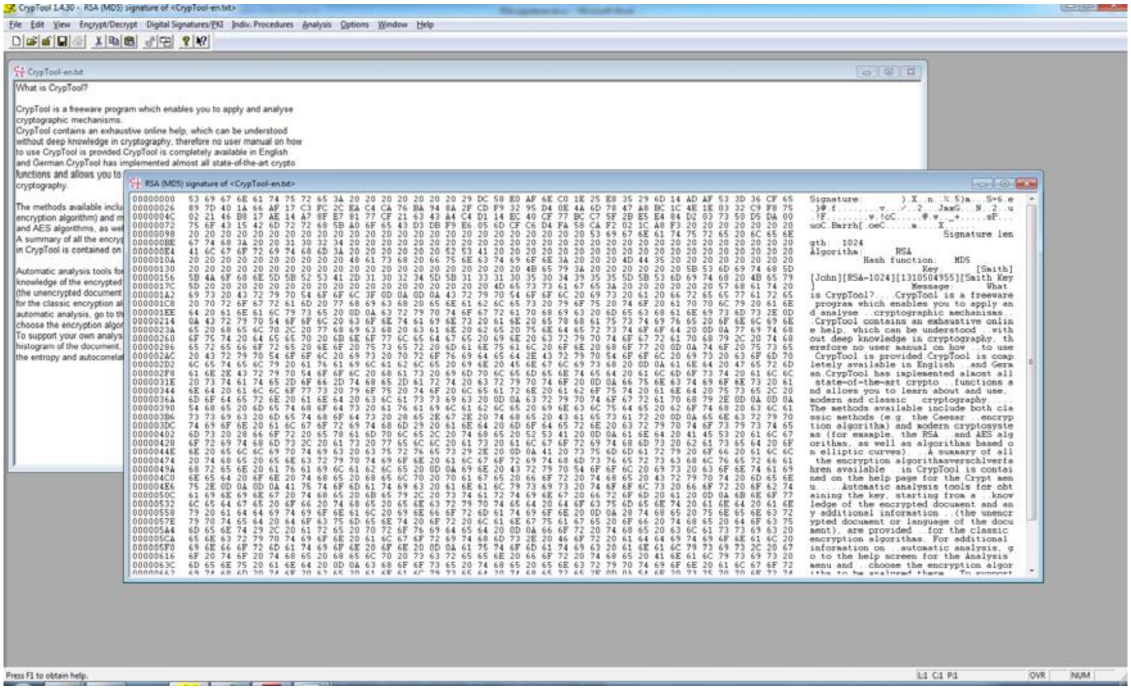
☐ Display intermediate results



CrypTool

Signature generation time: 0.004 seconds.

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



CrypTool 1.4.30 - RSA (MD5) signature of <CrypTool-en.txt>

CrypTool-en.txt

What is CrypTool?

CrypTool is a freeware program which enables you to apply and analyse cryptographic mechanisms.
CrypTool contains an exhaustive online help, which can be understood without deep knowledge in cryptography, therefore no user manual on how to use CrypTool is provided.CrypTool is completely available in English and German.CrypTool has implemented almost all state-of-the-art crypto functions and allows you to
cryptography.

The methods available inclu
encryption algorithm) and m
and AES algorithms, as we
A summary of all the encry
in CrypTool is contained on

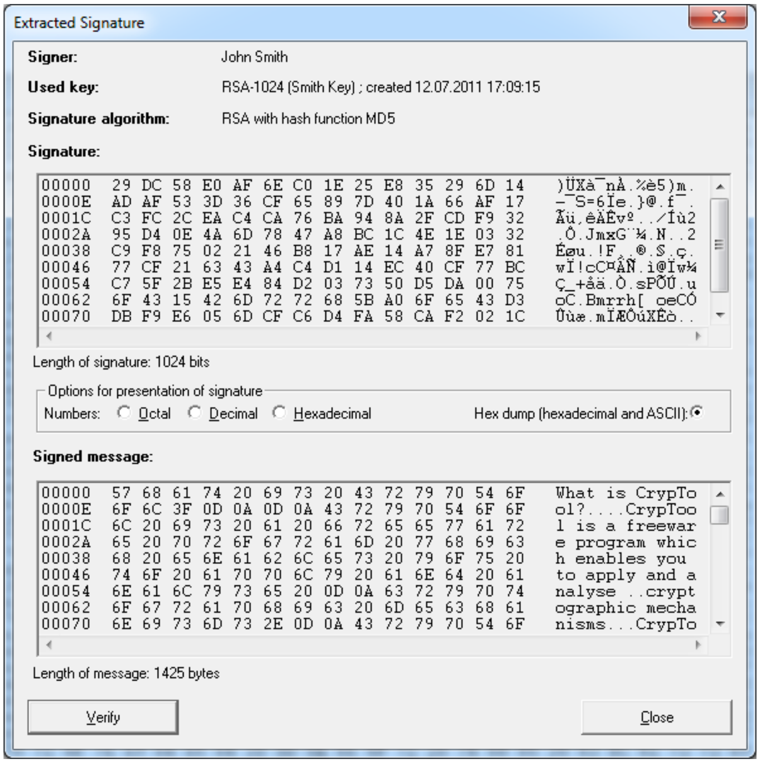
Automatic analysis tools fo
knowledge of the encrypted
(the unencrypted document
for the classic encryption al
automatic analysis, go to th
choose the encryption algor
To support your own analys
histogram of the document,
the entropy and autocorrelat

RSA (MD5) signature of <CrypTool-en.txt>

```
00000000  53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 29 DC 58 E0 AF 6E C0 1E 25 E8 35 29 6D 14 AD AF 53 3D 36 CF 65   Signature:        ).X..n..%.5)m...S=6.e
```

Press F1 to obtain help.

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.



Extracted Signature

Signer: John Smith

Used key: RSA-1024 (Smith Key) ; created 12.07.2011 17:09:15

Signature algorithm: RSA with hash function MD5

Signature:

```
00000   29 DC 58 E0 AF 6E C0 1E 25 E8 35 29 6D 14   )ÜXà¯nÀ.%è5)m.
0000E   AD AF 53 3D 36 CF 65 89 7D 40 1A 66 AF 17   -¯S=6Ïe.}@.f¯.
0001C   C3 FC 2C EA C4 CA 76 BA 94 8A 2F CD F9 32   Ãü,êÄÊvº../Íù2
0002A   95 D4 0E 4A 6D 78 47 A8 BC 1C 4E 1E 03 32   .Ô.JmxG¨¼.N..2
00038   C9 F8 75 02 21 46 B8 17 AE 14 A7 8F E7 81   Éøu.!F¸.®.§.ç.
00046   77 CF 21 63 43 A4 C4 D1 14 EC 40 CF 77 BC   wÏ!cC¤ÄÑ.ì@Ïw¼
00054   C7 5F 2B E5 E4 84 D2 03 73 50 D5 DA 00 75   Ç_+åä.Ò.sPÕÚ.u
00062   6F 43 15 42 6D 72 72 68 5B A0 6F 65 43 D3   oC.Bmrrh[ oeCÓ
00070   DB F9 E6 05 6D CF C6 D4 FA 58 CA F2 02 1C   Ûùæ.mÏÆÔúXÊò..
```

Length of signature: 1024 bits

Options for presentation of signature

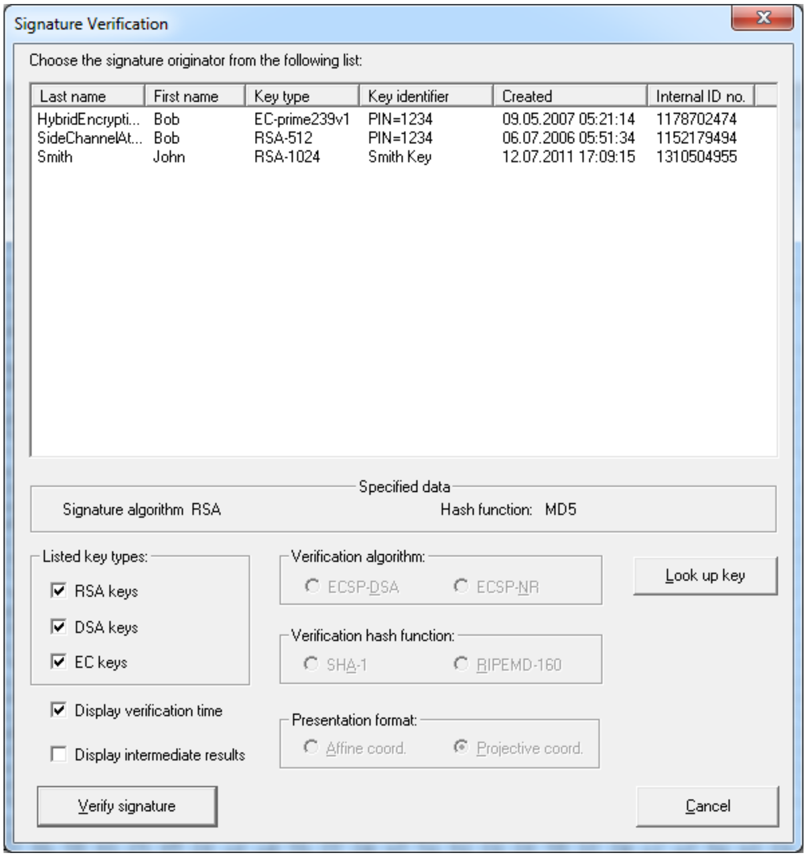
Numbers: ○ Octal ○ Decimal ○ Hexadecimal   Hex dump (hexadecimal and ASCII): ●

Signed message:

```
00000   57 68 61 74 20 69 73 20 43 72 79 70 54 6F   What is CrypTo
0000E   6F 6C 3F 0D 0A 0D 0A 43 72 79 70 54 6F 6F   ol?....CrypToo
0001C   6C 20 69 73 20 61 20 66 72 65 65 77 61 72   l is a freewar
0002A   65 20 70 72 6F 67 72 61 6D 20 77 68 69 63   e program whic
00038   68 20 65 6E 61 62 6C 65 73 20 79 6F 75 20   h enables you 
00046   74 6F 20 61 70 70 6C 79 20 61 6E 64 20 61   to apply and a
00054   6E 61 6C 79 73 65 20 0D 0A 63 72 79 70 74   nalyse ..crypt
00062   6F 67 72 61 70 68 69 63 20 6D 65 63 68 61   ographic mecha
00070   6E 69 73 6D 73 2E 0D 0A 43 72 79 70 54 6F   nisms...CrypTo
```

Length of message: 1425 bytes

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



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 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 17:09:15	1310504955

Specified data

Signature algorithm RSA Hash function: MD5

Listed key types:

☑ RSA keys

☑ DSA keys

☑ EC keys

☑ Display verification time

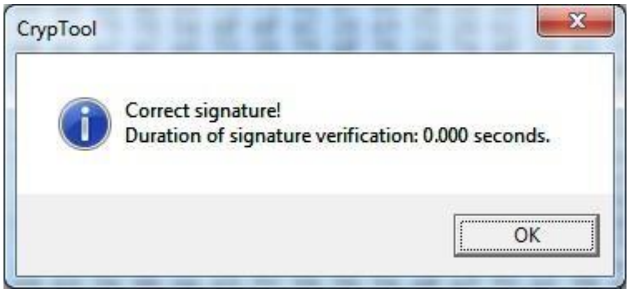
☐ Display intermediate results

Verification algorithm: ○ ECSP-DSA ○ ECSP-NR

Verification hash function: ○ SHA-1 ○ RIPEMD-160

Presentation format: ○ Affine coord. ● Projective coord.

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

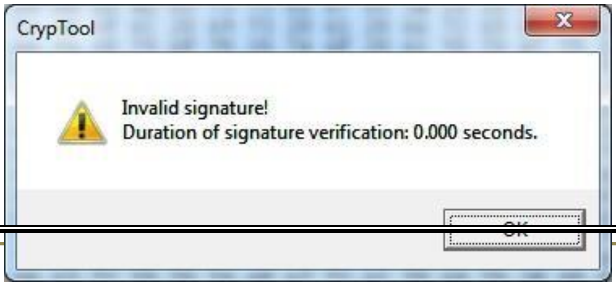


CrypTool

Correct signature!
Duration of signature verification: 0.000 seconds.

14. **modify the message by deleting “What”.**

15. **Select Digital Signature/PKI\Verify Signature, the following dialog box appears:**



CrypTool

Invalid signature!
Duration of signature verification: 0.000 seconds.

III. Conclusion

Hence we have successfully create and verify digital signature..

IV. Exercise

Q.1 What is digital signature certificate?

Q.2 What are the types of digital signature certificate?

Q.3 What are the benefits of a digital signature?

Q4. What is the application of a digital signature?

Q5. What is the Message authentication?

Q6. What is the Data Integrity?

Q7. Explain Authentication.

Answers

………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
………………………………………………………………………………………………....
……………………………………………………………………………………………...…
……………………………………………………………………………………………...…
……………………………………………………………………………………………...…
……………………………………………………………………………………………...…

Network and Information Security(22620)

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………....

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

…………………………………………………………………………………………………...….

………………………………………………………………………………………………...…….

………………………………………………………………………………………………...…….

………………………………………………………………………………………………...…….

………………………………………………………………………………………………...…….

………………………………………………………………………………………………...…….

Marks obtained			**Dated signature of Teacher**
Process Related (15)	**Product Related (10)**	**Total(25)**	