Khoa Khoa học & Kỹ thuật máy tính

Trường ĐH Bách Khoa TP.HCM

Cryptography and Network Security
Lab 6
Digital Signature

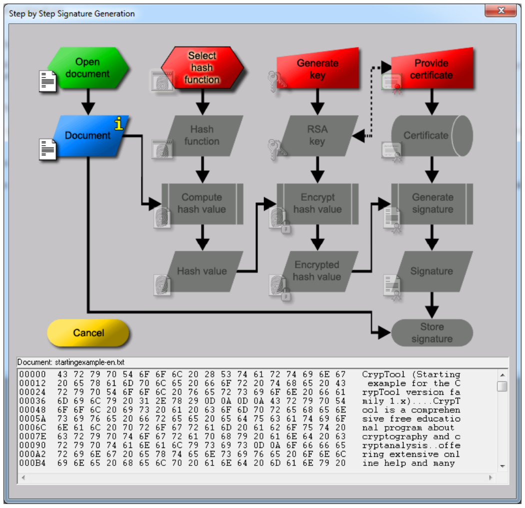
INTRODUCTION

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

EXPERIENCE

A. Digital Signature Visualization

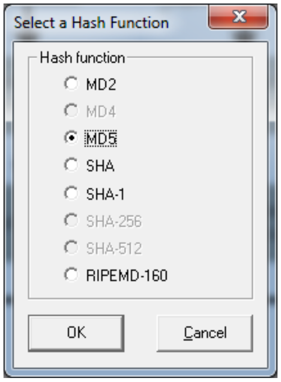
1. Select from menu of CrypTool “**Digital Signatures/PKI” \ “Signature Demonstration (Signature Generation)**”



Document: startingexample-en.txt

```
00000   43 72 79 70 54 6F 6F 6C 20 28 53 74 61 72 74 69 6E 67   CrypTool (Starting
00012   20 65 78 61 6D 70 6C 65 20 66 6F 72 20 74 68 65 20 43    example for the C
00024   72 79 70 54 6F 6F 6C 20 76 65 72 73 69 6F 6E 20 66 61   rypTool version fa
00036   6D 69 6C 79 20 31 2E 78 29 0D 0A 0D 0A 43 72 79 70 54   mily 1.x)....CrypT
00048   6F 6F 6C 20 69 73 20 61 20 63 6F 6D 70 72 65 68 65 6E   ool is a comprehen
0005A   73 69 76 65 20 66 72 65 65 20 65 64 75 63 61 74 69 6F   sive free educatio
0006C   6E 61 6C 20 70 72 6F 67 72 61 6D 20 61 62 6F 75 74 20   nal program about
0007E   63 72 79 70 74 6F 67 72 61 70 68 79 20 61 6E 64 20 63   cryptography and c
00090   72 79 70 74 61 6E 61 6C 79 73 69 73 0D 0A 6F 66 66 65   ryptanalysis..offe
000A2   72 69 6E 67 20 65 78 74 65 6E 73 69 76 65 20 6F 6E 6C   ring extensive onl
000B4   69 6E 65 20 68 65 6C 70 20 61 6E 64 20 6D 61 6E 79 20   ine help and many
```

2. Click on "**Select hash function**". Choose **MD5** (or others) and click **OK**.

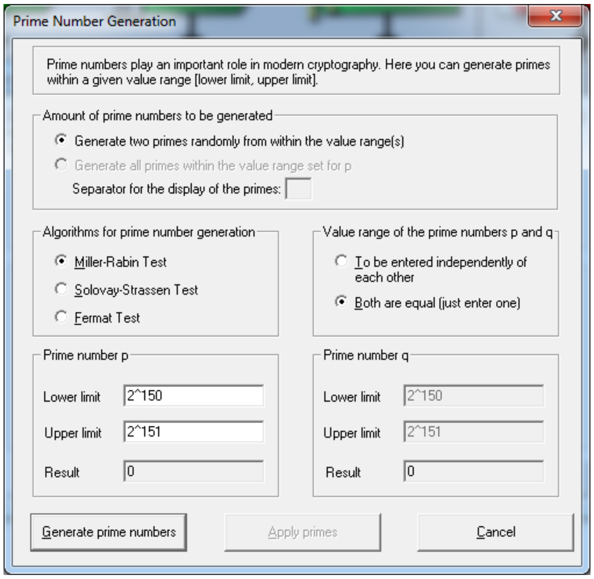


Select a Hash Function

Hash function

○ MD2
○ MD4
● MD5
○ SHA
○ SHA-1
○ SHA-256
○ SHA-512
○ RIPEMD-160

3. Click "**Generate Key**" and "**Generate prime numbers**" in **step by step Signature Generation** dialog.



Prime Number Generation

Prime numbers play an important role in modern cryptography. Here you can generate primes within a given value range [lower limit, upper limit].

Amount of prime numbers to be generated

● Generate two primes randomly from within the value range(s)
○ Generate all primes within the value range set for p

Separator for the display of the primes:

Algorithms for prime number generation

● Miller-Rabin Test
○ Solovay-Strassen Test
○ Fermat Test

Value range of the prime numbers p and q

○ To be entered independently of each other
● Both are equal (just enter one)

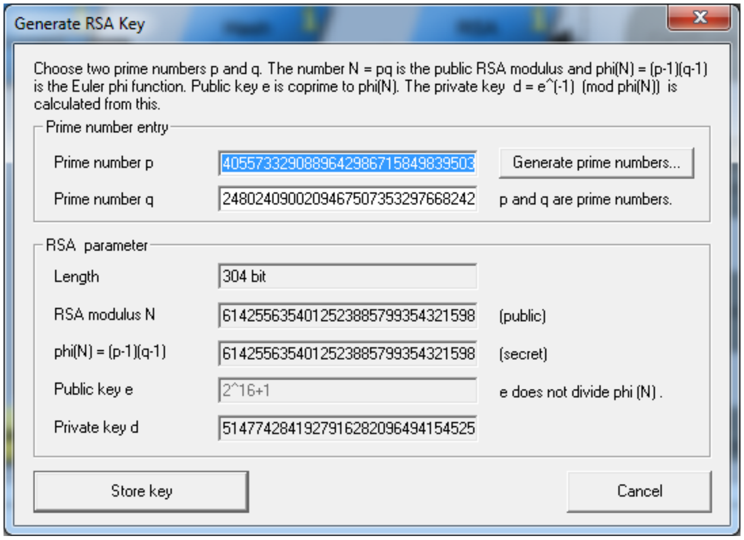
Prime number p

Lower limit 2^150
Upper limit 2^151
Result 0

Prime number q

Lower limit 2^150
Upper limit 2^151
Result 0

4. Enter **2^150** as the <u>lower limit</u> and **2^151** as <u>upper limit</u>. And click **Generate prime numbers** and **apply primes**.



Generate RSA Key

Choose two prime numbers p and q. The number N = pq is the public RSA modulus and phi(N) = (p-1)(q-1) is the Euler phi function. Public key e is coprime to phi(N). The private key d = e^(-1) (mod phi(N)) is calculated from this.

Prime number entry

Prime number p 405573329088964298671584983950З

Prime number q 2480240900209467507353297668242 p and q are prime numbers.

RSA parameter

Length 304 bit

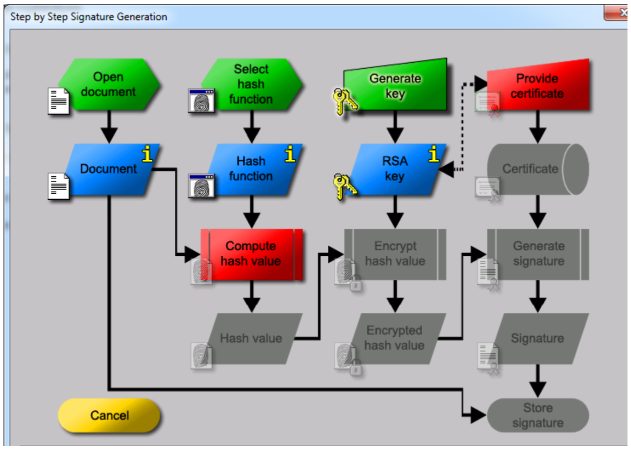
RSA modulus N 6142556354012523885799354321598 (public)

phi(N) = (p-1)(q-1) 6142556354012523885799354321598 (secret)

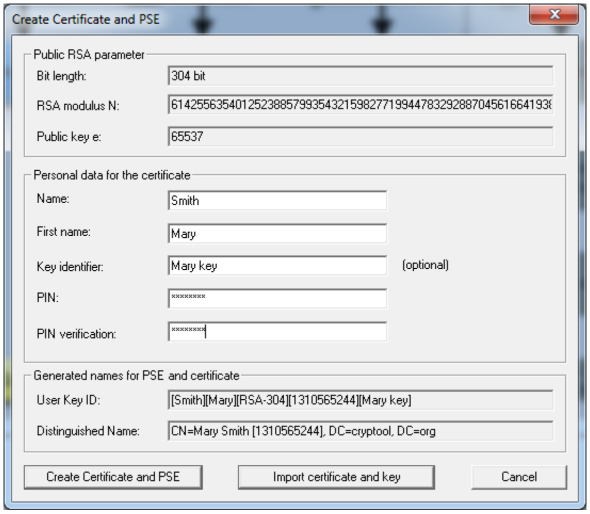
Public key e 2^16+1 e does not divide phi (N) .

Private key d 5147742841927916282096494154525

5. Click **Store key** button.



6. Click **Provide certificate** button. Enter
Name: **Smith** - First name: **Mary** - Key identifier: **Mary key**
PIN: **cryptool** - PIN verification: **cryptool**



Create Certificate and PSE

Public RSA parameter

Bit length:	304 bit
RSA modulus N:	61425563540125238857993543215982771994478329288704561664193
Public key e:	65537

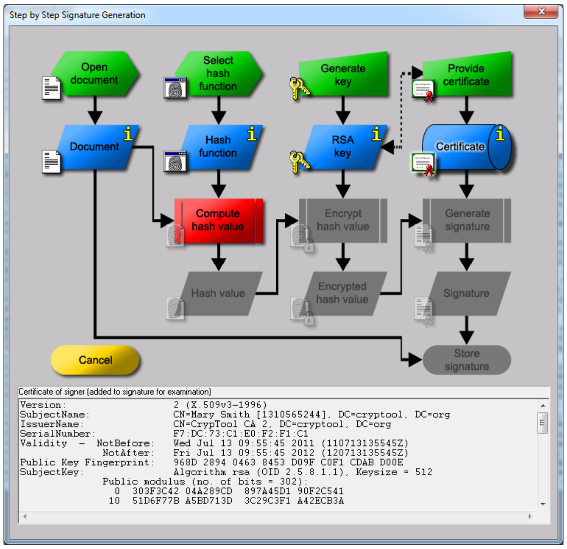
Personal data for the certificate

Name:	Smith	
First name:	Mary	
Key identifier:	Mary key	(optional)
PIN:	********	
PIN verification:	********	

Generated names for PSE and certificate

User Key ID:	[Smith][Mary][RSA-304][1310565244][Mary key]
Distinguished Name:	CN=Mary Smith [1310565244], DC=cryptool, DC=org

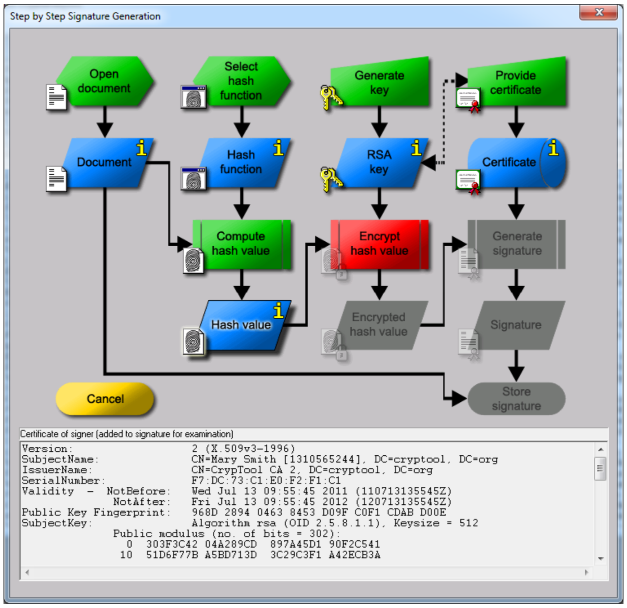
7. And click “**Create Certificate and PSE**”.



Certificate of signer (added to signature for examination)

```
Version:                    2 (X.509v3-1996)
SubjectName:                CN=Mary Smith [1310565244], DC=cryptool, DC=org
IssuerName:                 CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber:               F7:DC:73:C1:E0:F2:F1:C1
Validity  -  NotBefore:     Wed Jul 13 09:55:45 2011 (110713135545Z)
             NotAfter:      Fri Jul 13 09:55:45 2012 (120713135545Z)
Public Key Fingerprint:     968D 2894 0463 8453 D09F C0F1 CDAB D00E
SubjectKey:                 Algorithm rsa (OID 2.5.8.1.1), Keysize = 512
             Public modulus (no. of bits = 302):
               0  303F3C42 04A289CD  897A45D1 90F2C541
              10  51D6F77B A5BD713D  3C29C3F1 A42ECB3A
```

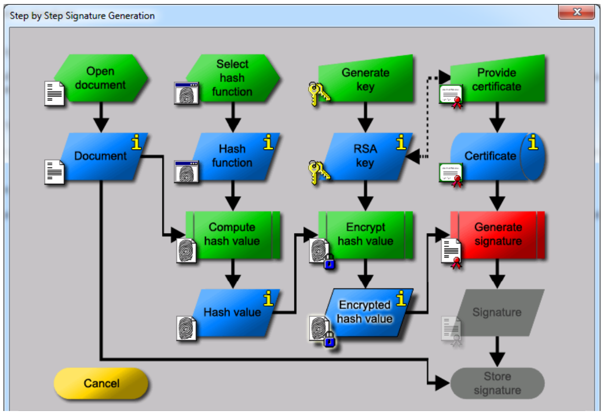
8. click “**Compute hash value**”.



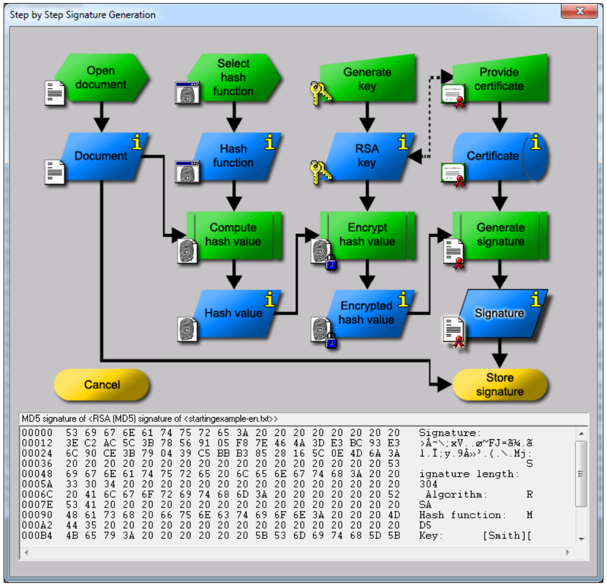
Certificate of signer (added to signature for examination)

```
Version:                    2 (X.509v3-1996)
SubjectName:                CN=Mary Smith [1310565244], DC=cryptool, DC=org
IssuerName:                 CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber:               F7:DC:73:C1:E0:F2:F1:C1
Validity  -  NotBefore:     Wed Jul 13 09:55:45 2011 (110713135545Z)
             NotAfter:      Fri Jul 13 09:55:45 2012 (120713135545Z)
Public Key Fingerprint:     968D 2894 0463 8453 D09F C0F1 CDAB D00E
SubjectKey:                 Algorithm rsa (OID 2.5.8.1.1), Keysize = 512
             Public modulus (no. of bits = 302):
               0  303F3C42 04A289CD  897A45D1 90F2C541
              10  51D6F77B A5BD713D  3C29C3F1 A42ECB3A
```

9. Click “**Encrypt hash value**”.



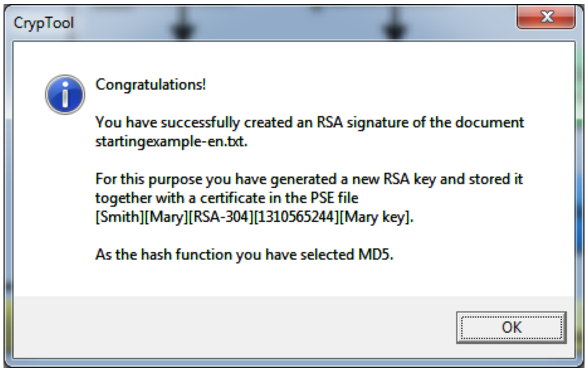
10. Click “**Generate signature**”.



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

```
00000  53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 20   Signature:
00012  3E C2 AC 5C 3B 78 56 91 05 F8 7E 46 4A 3D E3 BC 93 E3   >Â¬\;xV..ø~FJ=ã¼.ã
00024  6C 90 CE 3B 79 04 39 C5 BB B3 85 28 16 5C 0E 4D 6A 3A   l.Î;y.9Å»³.(.\.Mj:
00036  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53                    S
00048  69 67 6E 61 74 75 72 65 20 6C 65 6E 67 74 68 3A 20 20   ignature length:
0005A  33 30 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   304
0006C  20 41 6C 67 6F 72 69 74 68 6D 3A 20 20 20 20 20 20 52    Algorithm:      R
0007E  53 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   SA
00090  48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20 20 4D   Hash function:   M
000A2  44 35 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   D5
000B4  4B 65 79 3A 20 20 20 20 20 20 5B 53 6D 69 74 68 5D 5B   Key:      [Smith][
```

11. Click “**Store signature**”.



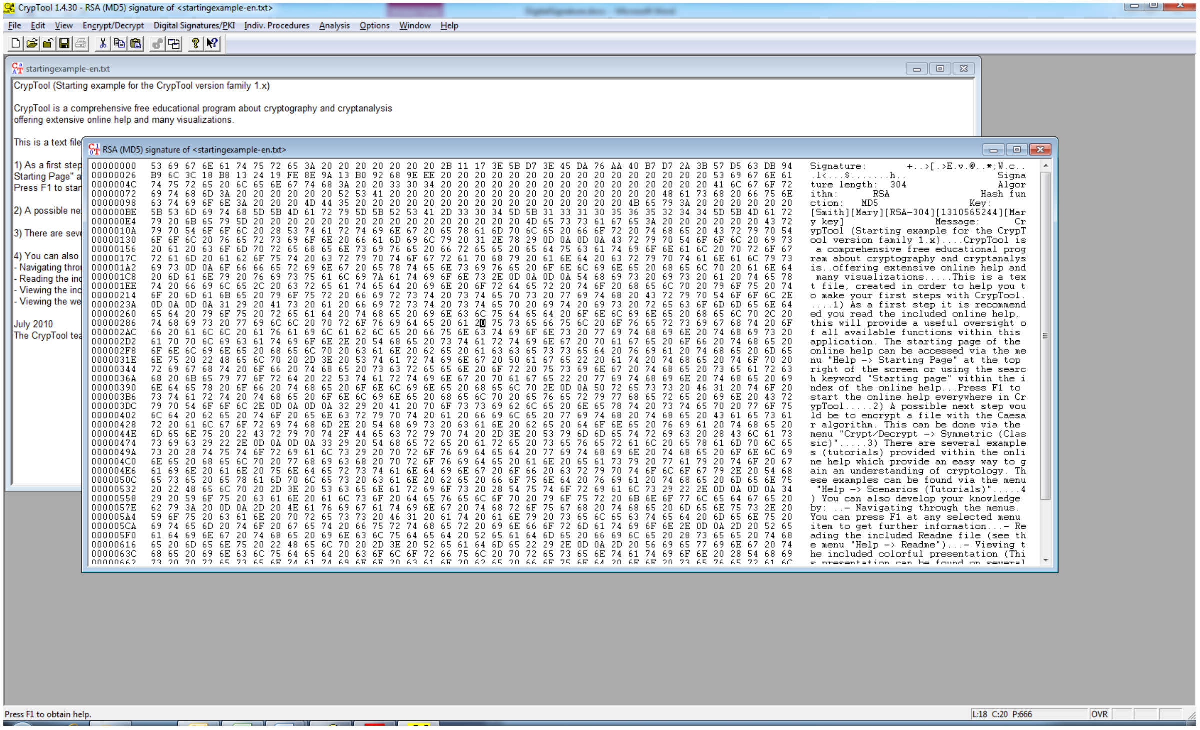
Congratulations!

You have successfully created an RSA signature of the document startingexample-en.txt.

For this purpose you have generated a new RSA key and stored it together with a certificate in the PSE file [Smith][Mary][RSA-304][1310565244][Mary key].

As the hash function you have selected MD5.

12 click “OK”, you will see RSA (md5)signature of <startingexample-en.txt>.



CrypTool 1.4.30 - RSA (MD5) signature of <startingexample-en.txt>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
RSA (MD5) signature of <startingexample-en.txt>
Press F1 to obtain help.
L:18 C:20 P:666
OVR

CrypTool (Starting example for the CrypTool version family 1.x)

CrypTool is a comprehensive free educational program about cryptography and cryptanalysis
offering extensive online help and many visualizations.

This is a text file

1) As a first step
Starting Page" a
Press F1 to star

2) A possible ne

3) There are seve

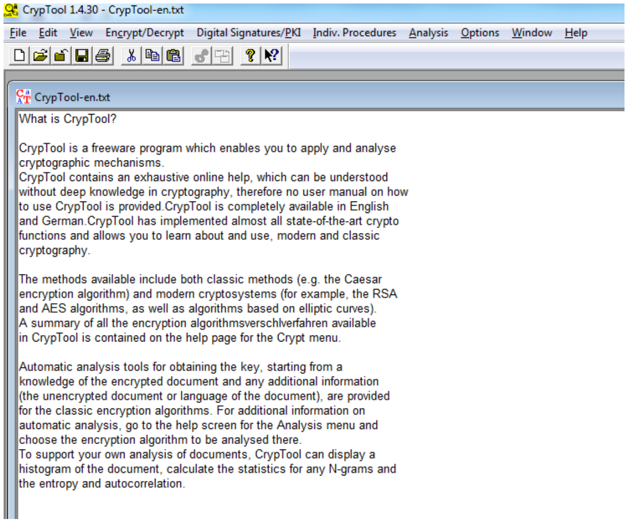
4) You can also
- Navigating thro
- Reading the inc
- Viewing the inc
- Viewing the we

July 2010
The CrypTool tea

```
00000000   53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 2B 11 17 3E 5B D7 3E 45 DA 76 AA 40 B7 D7 2A 3B 57 D5 63 DB 94   Signature:       +..>[.>E.v.@..*;W.c..
00000026   B9 6C 3C 18 B8 13 24 19 FE 8E 9A 13 B0 92 68 9E EE 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 69 67 6E 61   .l<...$.......h..                 Signa
0000004C   74 75 72 65 20 6C 65 6E 67 74 68 3A 20 20 33 30 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 41 6C 67 6F 72   ture length:  304                 Algor
00000072   69 74 68 6D 3A 20 20 20 20 20 20 52 53 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 48 61 73 68 20 66 75 6E   ithm:      RSA                Hash fun
00000098   63 74 69 6F 6E 3A 20 20 20 4D 44 35 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4B 65 79 3A 20 20 20 20 20 20   ction:   MD5                 Key:      
000000BE   5B 53 6D 69 74 68 5D 5B 4D 61 72 79 5D 5B 52 53 41 2D 33 30 34 5D 5B 31 33 31 30 35 36 35 32 34 34 5D 5B 4D 61 72   [Smith][Mary][RSA-304][1310565244][Mar
000000E4   79 20 6B 65 79 5D 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4D 65 73 73 61 67 65 3A 20 20 20 20 20 20 43 72   y key]                  Message:      Cr
0000010A   79 70 54 6F 6F 6C 20 28 53 74 61 72 74 69 6E 67 20 65 78 61 6D 70 6C 65 20 66 6F 72 20 74 68 65 20 43 72 79 70 54   ypTool (Starting example for the CrypT
00000130   6F 6F 6C 20 76 65 72 73 69 6F 6E 20 66 61 6D 69 6C 79 20 31 2E 78 29 0D 0A 0D 0A 43 72 79 70 54 6F 6F 6C 20 69 73   ool version family 1.x)....CrypTool is
00000156   20 61 20 63 6F 6D 70 72 65 68 65 6E 73 69 76 65 20 66 72 65 65 20 65 64 75 63 61 74 69 6F 6E 61 6C 20 70 72 6F 67    a comprehensive free educational prog
0000017C   72 61 6D 20 61 62 6F 75 74 20 63 72 79 70 74 6F 67 72 61 70 68 79 20 61 6E 64 20 63 72 79 70 74 61 6E 61 6C 79 73   ram about cryptography and cryptanalys
000001A2   69 73 0D 0A 6F 66 66 65 72 69 6E 67 20 65 78 74 65 6E 73 69 76 65 20 6F 6E 6C 69 6E 65 20 68 65 6C 70 20 61 6E 64   is..offering extensive online help and
000001C8   20 6D 61 6E 79 20 76 69 73 75 61 6C 69 7A 61 74 69 6F 6E 73 2E 0D 0A 0D 0A 54 68 69 73 20 69 73 20 61 20 74 65 78    many visualizations.....This is a tex
000001EE   74 20 66 69 6C 65 2C 20 63 72 65 61 74 65 64 20 69 6E 20 6F 72 64 65 72 20 74 6F 20 68 65 6C 70 20 79 6F 75 20 74   t file, created in order to help you t
00000214   6F 20 6D 61 6B 65 20 79 6F 75 72 20 66 69 72 73 74 20 73 74 65 70 73 20 77 69 74 68 20 43 72 79 70 54 6F 6F 6C 2E   o make your first steps with CrypTool.
0000023A   0D 0A 0D 0A 31 29 20 41 73 20 61 20 66 69 72 73 74 20 73 74 65 70 20 69 74 20 69 73 20 72 65 63 6F 6D 6D 65 6E 64   ....1) As a first step it is recommend
00000260   65 64 20 79 6F 75 20 72 65 61 64 20 74 68 65 20 69 6E 63 6C 75 64 65 64 20 6F 6E 6C 69 6E 65 20 68 65 6C 70 2C 20   ed you read the included online help, 
00000286   74 68 69 73 20 77 69 6C 6C 20 70 72 6F 76 69 64 65 20 61 20 75 73 65 66 75 6C 20 6F 76 65 72 73 69 67 68 74 20 6F   this will provide a useful oversight o
000002AC   66 20 61 6C 6C 20 61 76 61 69 6C 61 62 6C 65 20 66 75 6E 63 74 69 6F 6E 73 20 77 69 74 68 69 6E 20 74 68 69 73 20   f all available functions within this 
000002D2   61 70 70 6C 69 63 61 74 69 6F 6E 2E 20 54 68 65 20 73 74 61 72 74 69 6E 67 20 70 61 67 65 20 6F 66 20 74 68 65 20   application. The starting page of the 
000002F8   6F 6E 6C 69 6E 65 20 68 65 6C 70 20 63 61 6E 20 62 65 20 61 63 63 65 73 73 65 64 20 76 69 61 20 74 68 65 20 6D 65   online help can be accessed via the me
0000031E   6E 75 20 22 48 65 6C 70 20 2D 3E 20 53 74 61 72 74 69 6E 67 20 50 61 67 65 22 20 61 74 20 74 68 65 20 74 6F 70 20   nu "Help -> Starting Page" at the top 
00000344   72 69 67 68 74 20 6F 66 20 74 68 65 20 73 63 72 65 65 6E 20 6F 72 20 75 73 69 6E 67 20 74 68 65 20 73 65 61 72 63   right of the screen or using the searc
0000036A   68 20 6B 65 79 77 6F 72 64 20 22 53 74 61 72 74 69 6E 67 20 70 61 67 65 22 20 77 69 74 68 69 6E 20 74 68 65 20 69   h keyword "Starting page" within the i
00000390   6E 64 65 78 20 6F 66 20 74 68 65 20 6F 6E 6C 69 6E 65 20 68 65 6C 70 2E 0D 0A 50 72 65 73 73 20 46 31 20 74 6F 20   ndex of the online help...Press F1 to 
000003B6   73 74 61 72 74 20 74 68 65 20 6F 6E 6C 69 6E 65 20 68 65 6C 70 20 65 76 65 72 79 77 68 65 72 65 20 69 6E 20 43 72   start the online help everywhere in Cr
000003DC   79 70 54 6F 6F 6C 2E 0D 0A 0D 0A 32 29 20 41 20 70 6F 73 73 69 62 6C 65 20 6E 65 78 74 20 73 74 65 70 20 77 6F 75   ypTool.....2) A possible next step wou
00000402   6C 64 20 62 65 20 74 6F 20 65 6E 63 72 79 70 74 20 61 20 66 69 6C 65 20 77 69 74 68 20 74 68 65 20 43 61 65 73 61   ld be to encrypt a file with the Caesa
00000428   72 20 61 6C 67 6F 72 69 74 68 6D 2E 20 54 68 69 73 20 63 61 6E 20 62 65 20 64 6F 6E 65 20 76 69 61 20 74 68 65 20   r algorithm. This can be done via the 
0000044E   6D 65 6E 75 20 22 43 72 79 70 74 2F 44 65 63 72 79 70 74 20 2D 3E 20 53 79 6D 6D 65 74 72 69 63 20 28 43 6C 61 73   menu "Crypt/Decrypt -> Symmetric (Clas
00000474   73 69 63 29 22 2E 0D 0A 0D 0A 33 29 20 54 68 65 72 65 20 61 72 65 20 73 65 76 65 72 61 6C 20 65 78 61 6D 70 6C 65   sic)".....3) There are several example
0000049A   73 20 28 74 75 74 6F 72 69 61 6C 73 29 20 70 72 6F 76 69 64 65 64 20 77 69 74 68 69 6E 20 74 68 65 20 6F 6E 6C 69   s (tutorials) provided within the onli
000004C0   6E 65 20 68 65 6C 70 20 77 68 69 63 68 20 70 72 6F 76 69 64 65 20 61 6E 20 65 61 73 79 20 77 61 79 20 74 6F 20 67   ne help which provide an easy way to g
000004E6   61 69 6E 20 61 6E 20 75 6E 64 65 72 73 74 61 6E 64 69 6E 67 20 6F 66 20 63 72 79 70 74 6F 6C 6F 67 79 2E 20 54 68   ain an understanding of cryptology. Th
0000050C   65 73 65 20 65 78 61 6D 70 6C 65 73 20 63 61 6E 20 62 65 20 66 6F 75 6E 64 20 76 69 61 20 74 68 65 20 6D 65 6E 75   ese examples can be found via the menu
00000532   20 22 48 65 6C 70 20 2D 3E 20 53 63 65 6E 61 72 69 6F 73 20 28 54 75 74 6F 72 69 61 6C 73 29 22 2E 0D 0A 0D 0A 34    "Help -> Scenarios (Tutorials)".....4
00000558   29 20 59 6F 75 20 63 61 6E 20 61 6C 73 6F 20 64 65 76 65 6C 6F 70 20 79 6F 75 72 20 6B 6E 6F 77 6C 65 64 67 65 20   ) You can also develop your knowledge 
0000057E   62 79 3A 20 0D 0A 2D 20 4E 61 76 69 67 61 74 69 6E 67 20 74 68 72 6F 75 67 68 20 74 68 65 20 6D 65 6E 75 73 2E 20   by: ..- Navigating through the menus. 
000005A4   59 6F 75 20 63 61 6E 20 70 72 65 73 73 20 46 31 20 61 74 20 61 6E 79 20 73 65 6C 65 63 74 65 64 20 6D 65 6E 75 20   You can press F1 at any selected menu 
000005CA   69 74 65 6D 20 74 6F 20 67 65 74 20 66 75 72 74 68 65 72 20 69 6E 66 6F 72 6D 61 74 69 6F 6E 2E 0D 0A 2D 20 52 65   item to get further information...- Re
000005F0   61 64 69 6E 67 20 74 68 65 20 69 6E 63 6C 75 64 65 64 20 52 65 61 64 6D 65 20 66 69 6C 65 20 28 73 65 65 20 74 68   ading the included Readme file (see th
00000616   65 20 6D 65 6E 75 20 22 48 65 6C 70 20 2D 3E 20 52 65 61 64 6D 65 22 29 2E 0D 0A 2D 20 56 69 65 77 69 6E 67 20 74   e menu "Help -> Readme")...- Viewing t
0000063C   68 65 20 69 6E 63 6C 75 64 65 64 20 63 6F 6C 6F 72 66 75 6C 20 70 72 65 73 65 6E 74 61 74 69 6F 6E 20 28 54 68 69   he included colorful presentation (Thi
```

B. RSA Signature

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

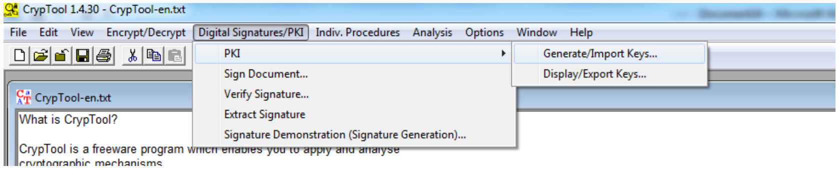
What is CrypTool?

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.**

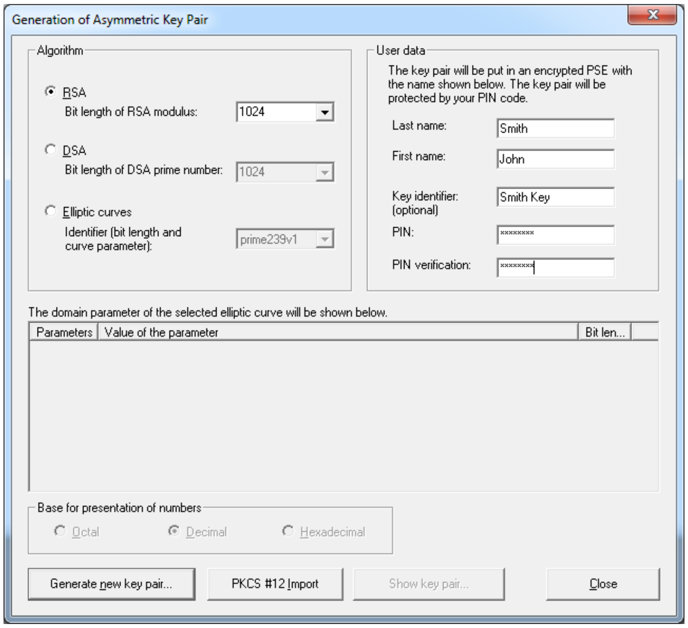

CrypTool 1.4.30 - CrypTool-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
PKI
Sign Document...
Verify Signature...
Extract Signature
Signature Demonstration (Signature Generation)...
Generate/Import Keys...
Display/Export Keys...
CrypTool-en.txt
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**

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



● RSA
Bit length of RSA modulus: 1024

○ DSA
Bit length of DSA prime number: 1024

○ Elliptic curves
Identifier (bit length and curve parameter): prime239v1

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.

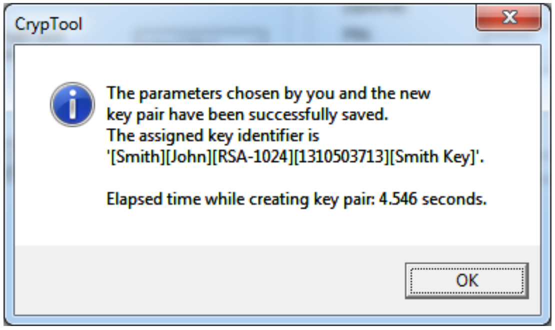
Last name: Smith
First name: John
Key identifier (optional): Smith Key
PIN: ********
PIN verification: ********

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

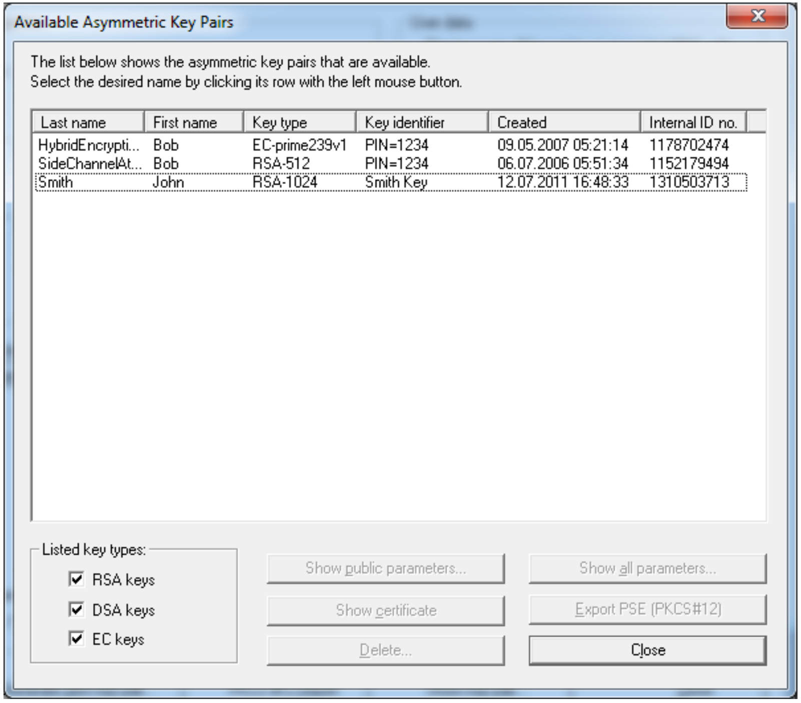
4. The following window shows up and click **OK**:



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.

5. Click **Show Key Pair**, you will see

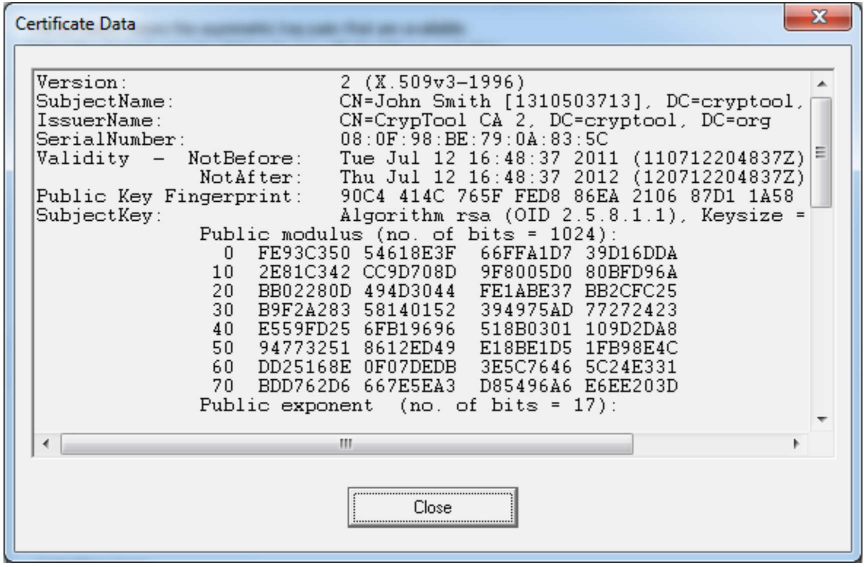


The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.

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

6. The certificate is displayed by clicking on the **Show certificate** pushbutton.



```
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):
```

7. Close both dialogs on **Certificate Data** and **Available Asymmetric Key Pairs**.

8. To sign the document of CrypTool-en.txt, select **Digital Signatures/PKI\Sign Message**. Enter the following

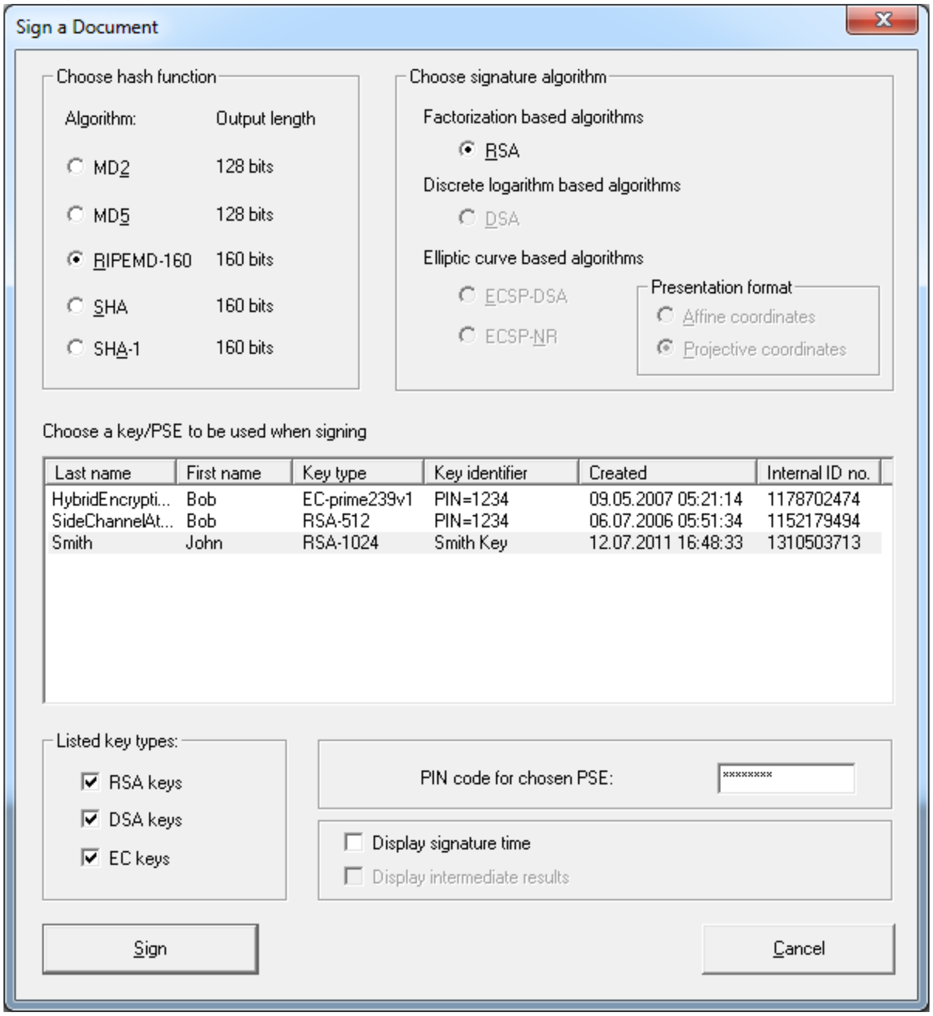
Choose hash function: **RIPEMD-160**

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

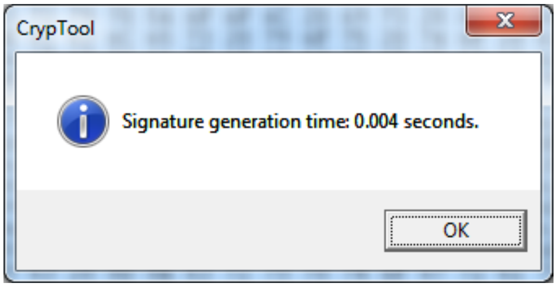
☑ DSA keys

☑ EC keys

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

☐ Display signature time

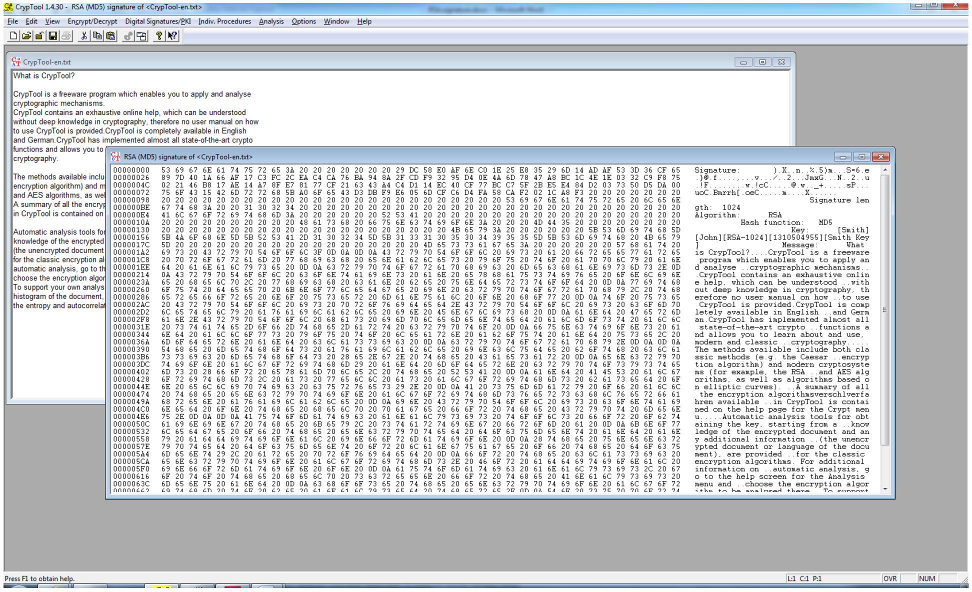
☐ Display intermediate results



CrypTool

Signature generation time: 0.004 seconds.

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



What is CrypTool?

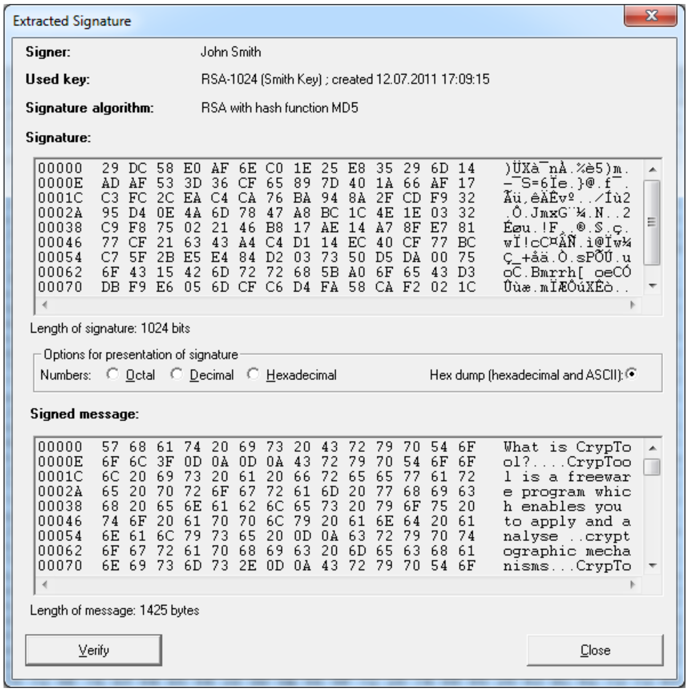
CrypTool is a freeware program which enables you to apply and analyse
cryptographic mechanisms.
CrypTool contains an exhaustive online help, which can be understood
without deep knowledge in cryptography, therefore no user manual on how
to use CrypTool is provided.CrypTool is completely available in 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 wel
A summary of all the encryp
in CrypTool is contained on

Automatic analysis tools for
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

```
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
00000026  89 7D 40 1A 66 AF 17 C3 FC 2C EA C4 CA 76 BA 94 8A 2F CD F9 32 95 D4 0E 4A 6D 78 47 A8 BC 1C 4E 1E 03 32 C9 F8 75   .}@.f....,...v.../..2...JmxG...N..2..u
0000004C  02 21 46 B8 17 AE 14 A7 8F E7 81 77 CF 21 63 43 A4 C4 D1 14 EC 40 CF 77 BC C7 5F 2B E5 E4 84 D2 03 73 50 D5 DA 00   .!F........w.!cC.....@.w.._+.....sP...
00000072  75 6F 43 15 42 6D 72 72 68 5B A0 6F 65 43 D3 DB F9 E6 05 6D CF C6 D4 FA 58 CA F2 02 1C A8 F3 20 20 20 20 20 20 20   uoC.Bmrrh[.oeC.....m....X......
00000098  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 69 67 6E 61 74 75 72 65 20 6C 65 6E                            Signature len
000000BE  67 74 68 3A 20 20 31 30 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   gth:  1024
000000E4  41 6C 67 6F 72 69 74 68 6D 3A 20 20 20 20 20 20 52 53 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   Algorithm:      RSA
0000010A  20 20 20 20 20 20 20 20 20 20 48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20 20 4D 44 35 20 20 20 20 20 20 20 20             Hash function:   MD5
00000130  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4B 65 79 3A 20 20 20 20 20 20 5B 53 6D 69 74 68 5D                        Key:      [Smith]
00000156  5B 4A 6F 68 6E 5D 5B 52 53 41 2D 31 30 32 34 5D 5B 31 33 31 30 35 30 34 39 35 35 5D 5B 53 6D 69 74 68 20 4B 65 79   [John][RSA-1024][1310504955][Smith Key
0000017C  5D 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4D 65 73 73 61 67 65 3A 20 20 20 20 20 20 57 68 61 74 20   ]                  Message:      What 
000001A2  69 73 20 43 72 79 70 54 6F 6F 6C 3F 0D 0A 0D 0A 43 72 79 70 54 6F 6F 6C 20 69 73 20 61 20 66 72 65 65 77 61 72 65   is CrypTool?....CrypTool is a freeware
000001C8  20 70 72 6F 67 72 61 6D 20 77 68 69 63 68 20 65 6E 61 62 6C 65 73 20 79 6F 75 20 74 6F 20 61 70 70 6C 79 20 61 6E    program which enables you to apply an
000001EE  64 20 61 6E 61 6C 79 73 65 20 0D 0A 63 72 79 70 74 6F 67 72 61 70 68 69 63 20 6D 65 63 68 61 6E 69 73 6D 73 2E 0D   d analyse ..cryptographic mechanisms..
00000214  0A 43 72 79 70 54 6F 6F 6C 20 63 6F 6E 74 61 69 6E 73 20 61 6E 20 65 78 68 61 75 73 74 69 76 65 20 6F 6E 6C 69 6E   .CrypTool contains an exhaustive onlin
0000023A  65 20 68 65 6C 70 2C 20 77 68 69 63 68 20 63 61 6E 20 62 65 20 75 6E 64 65 72 73 74 6F 6F 64 20 0D 0A 77 69 74 68   e help, which can be understood ..with
00000260  6F 75 74 20 64 65 65 70 20 6B 6E 6F 77 6C 65 64 67 65 20 69 6E 20 63 72 79 70 74 6F 67 72 61 70 68 79 2C 20 74 68   out deep knowledge in cryptography, th
00000286  65 72 65 66 6F 72 65 20 6E 6F 20 75 73 65 72 20 6D 61 6E 75 61 6C 20 6F 6E 20 68 6F 77 20 0D 0A 74 6F 20 75 73 65   erefore no user manual on how ..to use
000002AC  20 43 72 79 70 54 6F 6F 6C 20 69 73 20 70 72 6F 76 69 64 65 64 2E 43 72 79 70 54 6F 6F 6C 20 69 73 20 63 6F 6D 70    CrypTool is provided.CrypTool is comp
000002D2  6C 65 74 65 6C 79 20 61 76 61 69 6C 61 62 6C 65 20 69 6E 20 45 6E 67 6C 69 73 68 20 0D 0A 61 6E 64 20 47 65 72 6D   letely available in English ..and Germ
000002F8  61 6E 2E 43 72 79 70 54 6F 6F 6C 20 68 61 73 20 69 6D 70 6C 65 6D 65 6E 74 65 64 20 61 6C 6D 6F 73 74 20 61 6C 6C   an.CrypTool has implemented almost all
0000031E  20 73 74 61 74 65 2D 6F 66 2D 74 68 65 2D 61 72 74 20 63 72 79 70 74 6F 20 0D 0A 66 75 6E 63 74 69 6F 6E 73 20 61    state-of-the-art crypto ..functions a
00000344  6E 64 20 61 6C 6C 6F 77 73 20 79 6F 75 20 74 6F 20 6C 65 61 72 6E 20 61 62 6F 75 74 20 61 6E 64 20 75 73 65 2C 20   nd allows you to learn about and use, 
0000036A  6D 6F 64 65 72 6E 20 61 6E 64 20 63 6C 61 73 73 69 63 20 0D 0A 63 72 79 70 74 6F 67 72 61 70 68 79 2E 0D 0A 0D 0A   modern and classic ..cryptography.....
00000390  54 68 65 20 6D 65 74 68 6F 64 73 20 61 76 61 69 6C 61 62 6C 65 20 69 6E 63 6C 75 64 65 20 62 6F 74 68 20 63 6C 61   The methods available include both cla
000003B6  73 73 69 63 20 6D 65 74 68 6F 64 73 20 28 65 2E 67 2E 20 74 68 65 20 43 61 65 73 61 72 20 0D 0A 65 6E 63 72 79 70   ssic methods (e.g. the Caesar ..encryp
000003DC  74 69 6F 6E 20 61 6C 67 6F 72 69 74 68 6D 29 20 61 6E 64 20 6D 6F 64 65 72 6E 20 63 72 79 70 74 6F 73 79 73 74 65   tion algorithm) and modern cryptosyste
00000402  6D 73 20 28 66 6F 72 20 65 78 61 6D 70 6C 65 2C 20 74 68 65 20 52 53 41 20 0D 0A 61 6E 64 20 41 45 53 20 61 6C 67   ms (for example, the RSA ..and AES alg
00000428  6F 72 69 74 68 6D 73 2C 20 61 73 20 77 65 6C 6C 20 61 73 20 61 6C 67 6F 72 69 74 68 6D 73 20 62 61 73 65 64 20 6F   orithms, as well as algorithms based o
0000044E  6E 20 65 6C 6C 69 70 74 69 63 20 63 75 72 76 65 73 29 2E 20 0D 0A 41 20 73 75 6D 6D 61 72 79 20 6F 66 20 61 6C 6C   n elliptic curves). ..A summary of all
00000474  20 74 68 65 20 65 6E 63 72 79 70 74 69 6F 6E 20 61 6C 67 6F 72 69 74 68 6D 73 76 65 72 73 63 68 6C 76 65 72 66 61    the encryption algorithmsverschlverfa
0000049A  68 72 65 6E 20 61 76 61 69 6C 61 62 6C 65 20 0D 0A 69 6E 20 43 72 79 70 54 6F 6F 6C 20 69 73 20 63 6F 6E 74 61 69   hren available ..in CrypTool is contai
000004C0  6E 65 64 20 6F 6E 20 74 68 65 20 68 65 6C 70 20 70 61 67 65 20 66 6F 72 20 74 68 65 20 43 72 79 70 74 20 6D 65 6E   ned on the help page for the Crypt men
000004E6  75 2E 0D 0A 0D 0A 41 75 74 6F 6D 61 74 69 63 20 61 6E 61 6C 79 73 69 73 20 74 6F 6F 6C 73 20 66 6F 72 20 6F 62 74   u.....Automatic analysis tools for obt
0000050C  61 69 6E 69 6E 67 20 74 68 65 20 6B 65 79 2C 20 73 74 61 72 74 69 6E 67 20 66 72 6F 6D 20 61 20 0D 0A 6B 6E 6F 77   aining the key, starting from a ..know
00000532  6C 65 64 67 65 20 6F 66 20 74 68 65 20 65 6E 63 72 79 70 74 65 64 20 64 6F 63 75 6D 65 6E 74 20 61 6E 64 20 61 6E   ledge of the encrypted document and an
00000558  79 20 61 64 64 69 74 69 6F 6E 61 6C 20 69 6E 66 6F 72 6D 61 74 69 6F 6E 20 0D 0A 28 74 68 65 20 75 6E 65 6E 63 72   y additional information ..(the unencr
0000057E  79 70 74 65 64 20 64 6F 63 75 6D 65 6E 74 20 6F 72 20 6C 61 6E 67 75 61 67 65 20 6F 66 20 74 68 65 20 64 6F 63 75   ypted document or language of the docu
000005A4  6D 65 6E 74 29 2C 20 61 72 65 20 70 72 6F 76 69 64 65 64 20 0D 0A 66 6F 72 20 74 68 65 20 63 6C 61 73 73 69 63 20   ment), are provided ..for the classic 
000005CA  65 6E 63 72 79 70 74 69 6F 6E 20 61 6C 67 6F 72 69 74 68 6D 73 2E 20 46 6F 72 20 61 64 64 69 74 69 6F 6E 61 6C 20   encryption algorithms. For additional 
000005F0  69 6E 66 6F 72 6D 61 74 69 6F 6E 20 6F 6E 20 0D 0A 61 75 74 6F 6D 61 74 69 63 20 61 6E 61 6C 79 73 69 73 2C 20 67   information on ..automatic analysis, g
00000616  6F 20 74 6F 20 74 68 65 20 68 65 6C 70 20 73 63 72 65 65 6E 20 66 6F 72 20 74 68 65 20 41 6E 61 6C 79 73 69 73 20   o to the help screen for the Analysis 
0000063C  6D 65 6E 75 20 61 6E 64 20 0D 0A 63 68 6F 6F 73 65 20 74 68 65 20 65 6E 63 72 79 70 74 69 6F 6E 20 61 6C 67 6F 72   menu and ..choose the encryption algor
00000662  69 74 68 6D 20 74 6F 20 62 65 20 61 6E 61 6C 79 73 65 64 20 74 68 65 72 65 2E 0D 0A 54 6F 20 73 75 70 70 6F 72 74   ithm to be analysed there..To support
```

10. 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**.



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

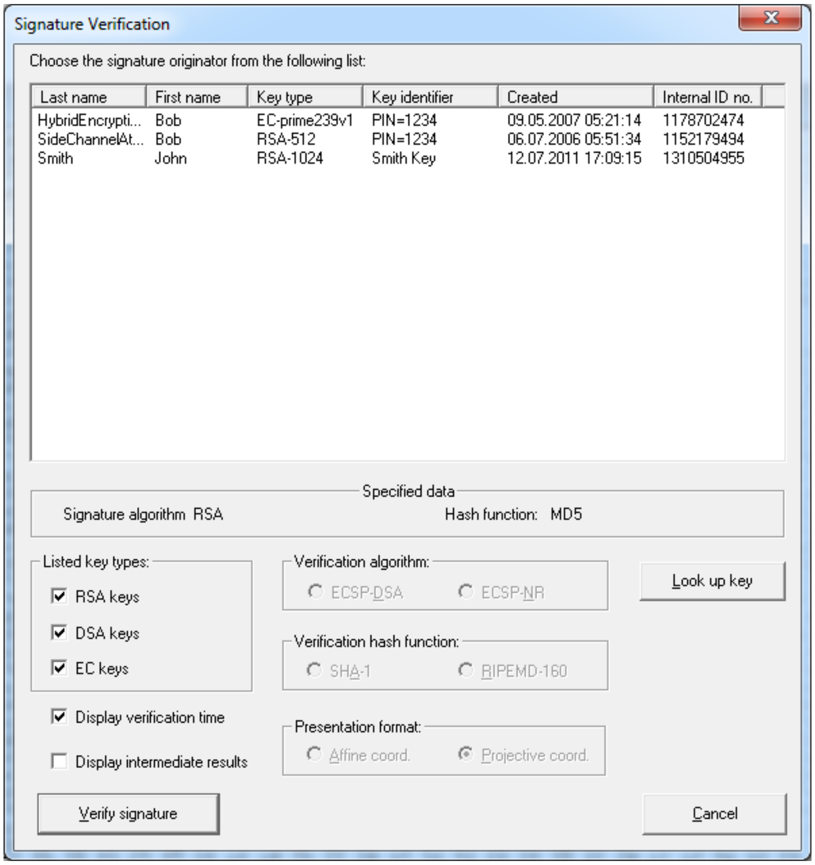
Numbers: ○ Octal ○ Decimal ○ Hexadecimal   Hex dump (hexadecimal and ASCII): ●

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

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



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

Verification algorithm:

○ ECSP-DSA ○ ECSP-NR

Verification hash function:

○ SHA-1 ○ RIPEMD-160

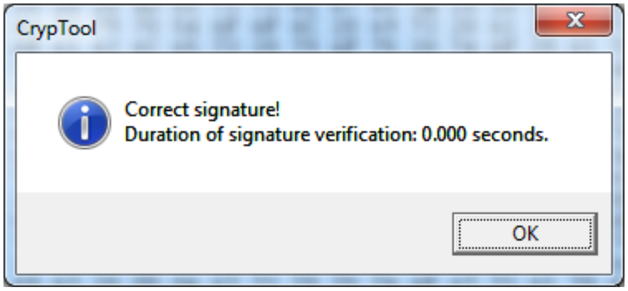
Presentation format:

○ Affine coord. ● Projective coord.

☑ Display verification time

☐ Display intermediate results

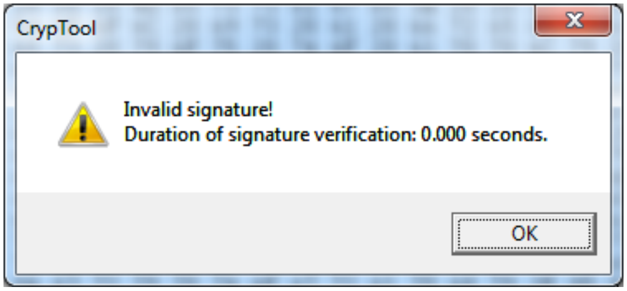
12. Select John Smith from the list of signatures and click on the Verify signature button. The following dialog appears.



Correct signature!
Duration of signature verification: 0.000 seconds.

13. Modify the message by deleting “What”.

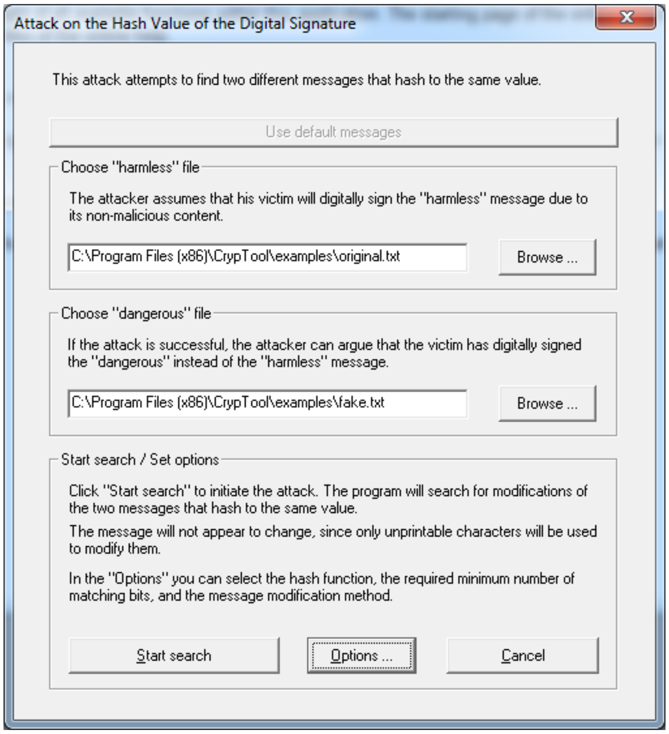
14. Select Digital Signature/PKI\Verify Signature, the following dialog box appears:



Invalid signature!
Duration of signature verification: 0.000 seconds.

C. Attack on Digital Signature/Hash Collision

Find two messages with the same hash value.
1. Select “**Analysis” \“Hash” \“Attack on the Hash Value of the Digital Signature**” from the menu.



Attack on the Hash Value of the Digital Signature

This attack attempts to find two different messages that hash to the same value.

Choose "harmless" file

The attacker assumes that his victim will digitally sign the "harmless" message due to its non-malicious content.

C:\Program Files (x86)\CrypTool\examples\original.txt

Choose "dangerous" file

If the attack is successful, the attacker can argue that the victim has digitally signed the "dangerous" instead of the "harmless" message.

C:\Program Files (x86)\CrypTool\examples\fake.txt

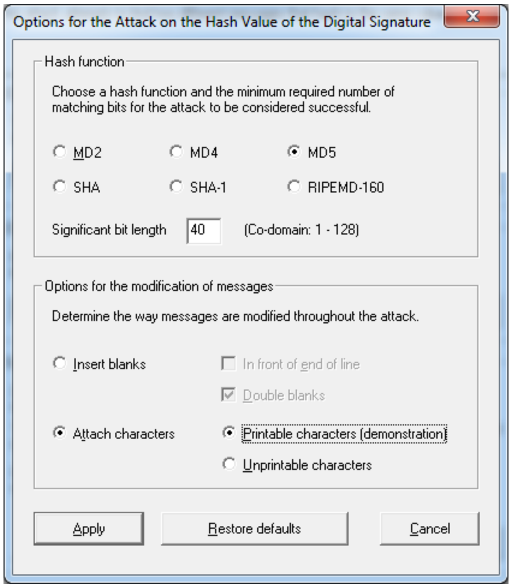
Start search / Set options

Click "Start search" to initiate the attack. The program will search for modifications of the two messages that hash to the same value.

The message will not appear to change, since only unprintable characters will be used to modify them.

In the "Options" you can select the hash function, the required minimum number of matching bits, and the message modification method.

2. Click “**Options**”.



Options for the Attack on the Hash Value of the Digital Signature

Hash function

Choose a hash function and the minimum required number of matching bits for the attack to be considered successful.

○ MD2 ○ MD4 ● MD5
○ SHA ○ SHA-1 ○ RIPEMD-160

Significant bit length 40 (Co-domain: 1 - 128)

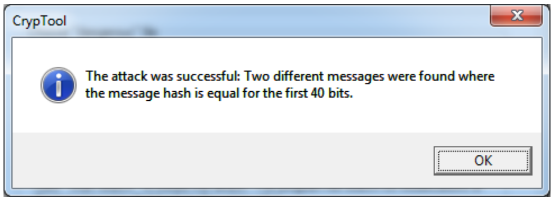
Options for the modification of messages

Determine the way messages are modified throughout the attack.

○ Insert blanks □ In front of end of line
☑ Double blanks
● Attach characters ● Printable characters (demonstration)
○ Unprintable characters

3. Choose **MD5** under Hash function and **40** for Significant bit length, and click **Apply**.

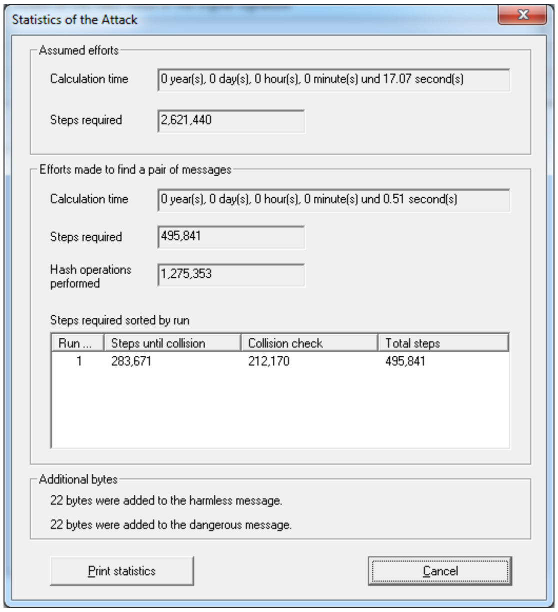
4. Click “**Start Search**” in dialog of Attack on the Hash Value of the Digital Signature.



CrypTool

The attack was successful: Two different messages were found where the message hash is equal for the first 40 bits.

5. Click “**OK**” and “**Print Statistics**”.



Statistics of the Attack

Assumed efforts

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 17.07 second(s)

Steps required: 2,621,440

Efforts made to find a pair of messages

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.51 second(s)

Steps required: 495,841

Hash operations performed: 1,275,353

Steps required sorted by run

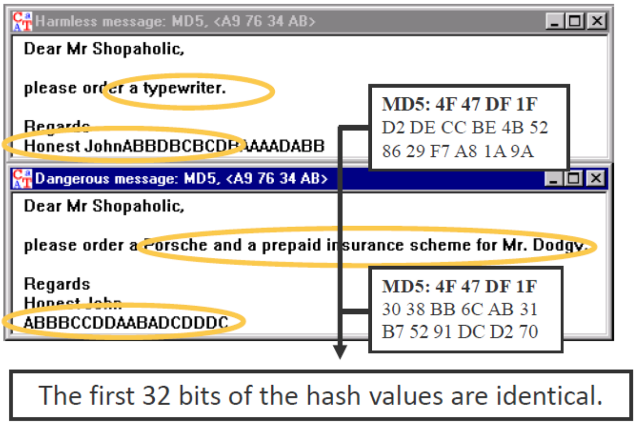
Run ...	Steps until collision	Collision check	Total steps
1	283,671	212,170	495,841

Additional bytes

22 bytes were added to the harmless message.

22 bytes were added to the dangerous message.

6. After modifying the two messages, the hash value of them are the same. The message will not appear to change, since only unprintable characters will be used to modify them.



Harmless message: MD5, <A9 76 34 AB>

Dear Mr Shopaholic,

please order a typewriter.

Regards
Honest JohnABBDBCBCDBAAAADABB

MD5: 4F 47 DF 1F
D2 DE CC BE 4B 52
86 29 F7 A8 1A 9A

Dangerous message: MD5, <A9 76 34 AB>

Dear Mr Shopaholic,

please order a Porsche and a prepaid insurance scheme for Mr. Dodgy.

Regards
Honest John
ABBBCCDDAABADCDDDC

MD5: 4F 47 DF 1F
30 38 BB 6C AB 31
B7 52 91 DC D2 70

The first 32 bits of the hash values are identical.

A 72-bit partial collision (i.e., the first 72 hash value bits are identical) was found in a couple of days using a single PC. Today signatures with hash values of 128 bits or less are vulnerable to a massive parallel search. It is therefore recommended to use hash values with a length of at least 160 bits.

HOMEWORK

1. List two disputes that can arise in the context of message authentication.

2. What are the properties a digital signature should have?

3. What requirements should a digital signature scheme satisfy?

4. What is the difference between direct and arbitrated digital signature?

5. In what order should the signature function and the confidentiality function be applied to a message, and why?

6. What are some threats associated with a direct digital signature scheme?

7. DSA specifies that if the signature generation process results in a value of s = 0, a new value of k should be generated and the signature should be recalculated. Why?

8. With DSA, because the value of k is generated for each signature, even if the same message is signed twice on different occasions, the signatures will differ. This is not true of RSA signatures. What is the practical implication of this difference?