1 Brute force attacking Triple DES

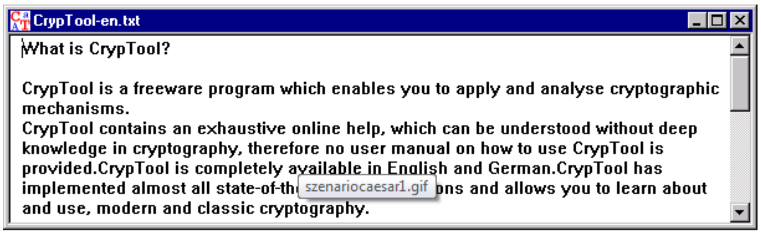
2 Example illustrating the Triple-DES encryption algorithm in CBC Mode

This section provides an example which illustrates the use of the Triple-DES encryption algorithm in CBC mode.

In this tutorial it will be shown using the frequency distribution and autocorrelation of the letters in the encrypted document that an attack on Triple-DES encryption in CBC mode is more difficult than an attack on the classical encryption algorithms.

Before you do the tutorial, you should previously have completed the tutorial on the Caesar Algorithm and simple Cryptanalysis.

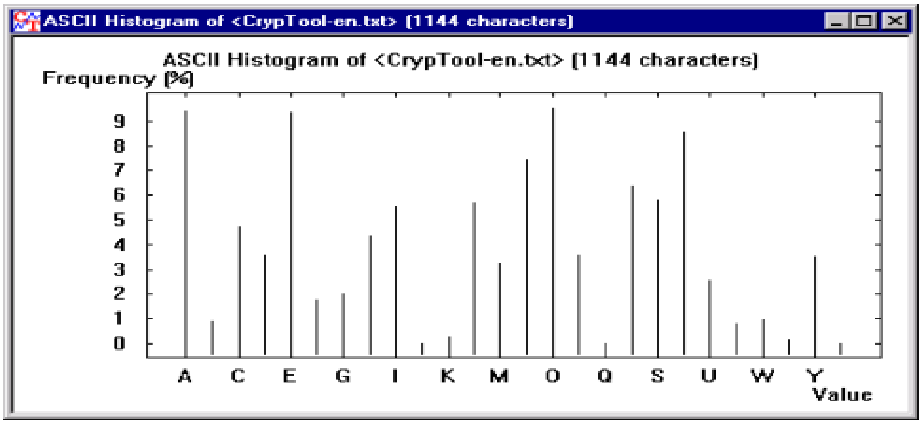
2.1 Open the file CrypTool-en.txt out of the directory: CrypTool\examples via the menu File→Open.



What is CrypTool?

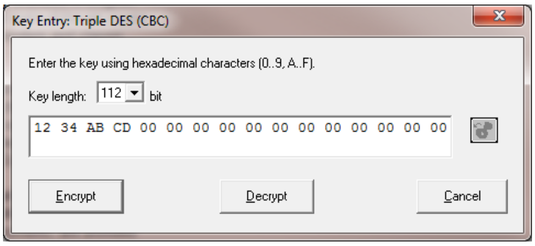
CrypTool is a freeware program which enables you to apply and analyse cryptographic mechanisms.
CrypTool contains an exhaustive online help, which can be understood without deep knowledge in cryptography, therefore no user manual on how to use CrypTool is provided.CrypTool is completely available in English and German.CrypTool has implemented almost all state-of-th szenariocaesar1.gif ons and allows you to learn about and use, modern and classic cryptography.

2.2 Next we analyse the frequency distribution of the letters (Analysis→Tools for Analysis→Histogram).



The correlation is of course the same as we found in the previous tutorial and is quite typical of what we would expect of most documents.

2.3 To encrypt the document using Triple-DES encryption in CBC mode, select Crypt/Decrypt→Symmetric (modern)→Triple DES (CBC)



Key Entry: Triple DES (CBC)

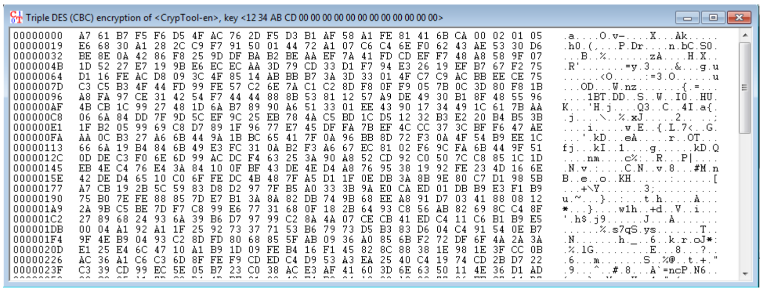
Enter the key using hexadecimal characters (0..9, A..F).

Key length: 112 bit

12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00

2.4 Enter 12 34 AB CD into the dialog box as the key.

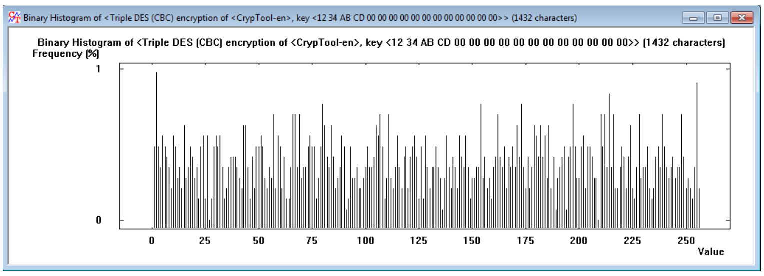
This causes a window containing the encrypted document to open.



Triple DES (CBC) encryption of <CrypTool-en>, key <12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00>

```
00000000  A7 61 B7 F5 F6 D5 4F AC 76 2D F5 D3 B1 AF 58 A1 FE 81 41 6B CA 00 02 01 05   .a....O.v-....X...Ak.....
00000019  E6 68 30 A1 28 2C C9 F7 91 50 01 44 72 A1 07 C6 C4 6E F0 62 43 AE 53 30 D6   .h0.(,...P.Dr....n.bC.S0.
00000032  BE 8E 0A 42 86 F8 25 9D DF BA B2 BE AA EF 7A 41 FD CD EF F7 48 A8 58 9F 07   ...B..%.......zA....H.X..
0000004B  1D 52 27 E7 19 9B E6 EC EC AA 3D 79 CD 33 D1 F7 94 E3 26 19 EF B7 67 F2 75   .R'........=y.3....&...g.u
00000064  D1 16 FE AC D8 09 3C 4F 85 14 AB BB B7 3A 3D 33 01 4F C7 C9 AC BB EE CE 75   ......<O.....:=3.O......u
0000007D  C3 C5 B3 4F 44 FD 99 FE 57 C2 6E 7A C1 C2 8D F8 0F F9 05 7B 0C 3D 80 F8 1B   ...OD...W.nz.......{.=...
00000096  A8 FA 97 CE 31 42 54 F7 44 44 88 8B 53 81 12 57 A9 DE 49 30 B1 8F 48 55 96   ....1BT.DD..S..W..I0..HU.
000000AF  4B CB 1C 99 27 48 1D 6A B7 89 90 A6 51 33 01 EE 43 90 17 34 49 1C 61 7B AA   K...'H.j....Q3..C..4I.a{.
000000C8  06 6A 84 DD 7F 9D 5C EF 9C 25 EB 78 4A C5 BD 1C D5 12 32 B3 E2 20 B4 B5 3B   .j....\..%.xJ.....2.....;
000000E1  1F B2 05 99 69 C8 D7 89 1F 96 77 E7 45 DF FA 7B EF 4C CC 37 3C BF F6 47 AE   ....i.....w.E..{.L.7<..G.
000000FA  AA 0C B3 27 A6 6B 44 9A 1B BC 65 41 7F 0A 96 BB 8D 72 F3 0A 4F 54 B9 EE 1C   ...'.kD...eA.....r..OT...
00000113  66 6A 19 B4 84 6B 49 E3 FC 31 0A B2 F3 A6 67 EC 81 02 F6 9C FA 6B 44 9F 51   fj...kI..1....g......kD.Q
0000012C  0D DE C3 F0 6E 6D 99 AC DC F4 63 25 3A 90 A8 52 CD 92 C0 50 7C C8 85 1C 1D   ....nm....c%:..R...P|....
00000145  EB 4E C4 76 E4 3A 84 10 0F BF 43 DE 4E D4 A8 76 95 38 19 92 FE 23 4D 16 6E   .N.v.:....C.N..v.8...#M.n
0000015E  42 DE D4 65 10 C0 6F FE DC 4B 48 7F A5 D1 1F 0E DB 3A 8B 9E 80 C7 D1 98 5B   B..e..o..KH..........:.......[
00000177  A7 CB 19 2B 5C 59 83 D8 D2 97 7F B5 A0 33 3B 9A E0 CA ED 01 DB B9 E3 F1 B9   ...+\Y.......3;..........
00000190  75 B0 7E FE 88 85 7D E7 B1 3A 8A 82 DB 74 9B 68 EE A8 91 D7 03 41 88 08 12   u.~...}..:...t.h.....A...
000001A9  2A 9B C5 BE 7D F7 C8 99 E6 77 31 68 0F 18 2B 64 93 C8 56 AB 82 69 8C C4 8F   *...}....w1h..+d..V..i...
000001C2  27 89 68 24 93 6A 39 B6 D7 97 99 C2 8A 4A 07 CE CB 41 ED C4 11 C6 B1 B9 E5   '.h$.j9......J...A.......
000001DB  00 04 A1 92 A1 1F 25 92 73 37 71 53 B6 79 73 D5 B3 83 D6 04 C4 91 54 0E B7   ......%.s7qS.ys.......T..
000001F4  9F 4E B9 04 93 C2 8D FD 80 68 85 5F AB 09 36 A0 85 6B F2 72 DF 6F 4A 2A 3A   .N.......h._..6..k.r.oJ*:
0000020D  E1 25 E4 6C 47 10 A1 B9 1D 09 FE B4 16 F1 45 82 8C 88 38 1E 98 1E 3F CC 0B   .%.lG.........E...8...?..
00000226  AC 36 A1 C6 C3 6D 8F FE F9 CD ED C4 D9 53 A3 EA 25 40 C4 19 74 CD 2B D7 22   .6...m.......S..%@..t.+."
0000023F  C3 39 CD 99 EC 5E 05 B7 23 C0 38 AC E3 AF 41 60 3D 6E 63 50 11 4E 36 D1 AD   .9...^..#.8...A`=ncP.N6..
```

2.5 Next we analyse the frequency distribution of the letters (Analysis→Tools for Analysis→Histogram).

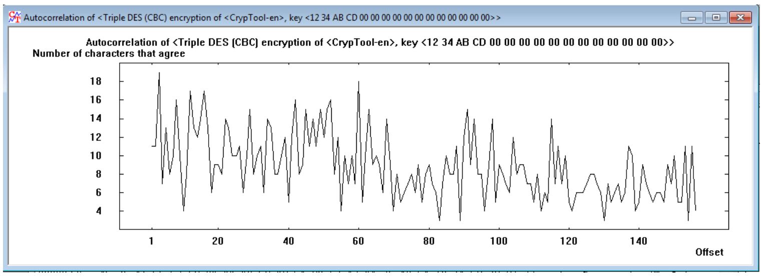


Binary Histogram of <Triple DES (CBC) encryption of <CrypTool-en>, key <12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00>> (1432 characters)

This bears no resemblance at all to the histogram of the unencrypted document as, for example, was the case in the example we used to illustrate the Caesar encryption algorithm.

Next we perform an autocorrelation of the encrypted text (again to get sighters of any patterns that might suggest that the key is)

2.6 Select Analysis→Symmetric Encryption (classic)→Ciphertext-Only→Byte Addition, and the autocorrelation will be calculated and displayed.

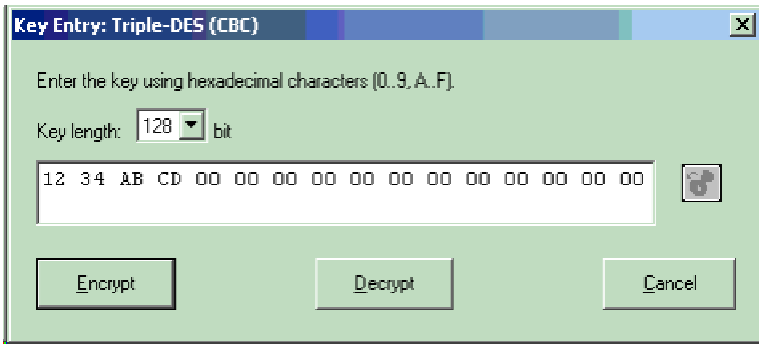


Autocorrelation of <Triple DES (CBC) encryption of <CrypTool-en>, key <12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00>>

The autocorrelation exhibits no regularity which could provide a clue as to the key length, as, for example, was the case in the example of encryption using binary addition.

The document can be decrypted in the same manner as the encryption.

2.7 To decrypt the document using Triple-DES encryption in CBC mode, select Crypt/Decrypt→Symmetric (modern)→Triple DES (CBC)



Key Entry: Triple-DES (CBC)

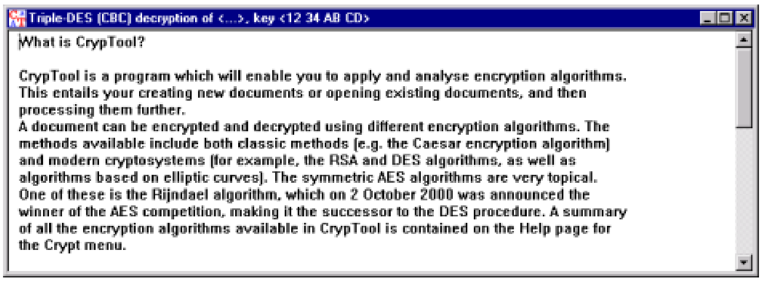
Enter the key using hexadecimal characters (0..9, A..F).

Key length: 128 bit

12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00

2.8 Enter 12 34 AB CD into the dialog box as the key.

2.9 Click on decrypt, this produces a new window containing the plaintext.



Triple-DES (CBC) decryption of <...>, key <12 34 AB CD>

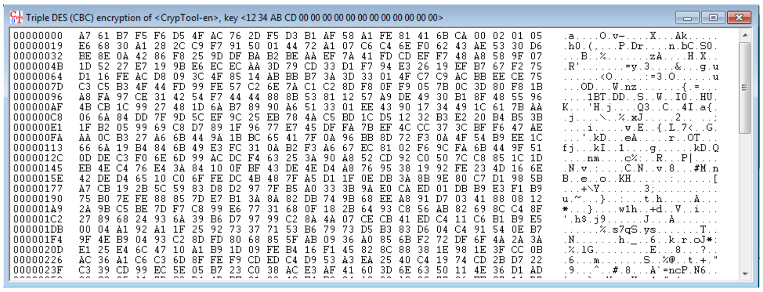
What is CrypTool?

CrypTool is a program which will enable you to apply and analyse encryption algorithms. This entails your creating new documents or opening existing documents, and then processing them further.
A document can be encrypted and decrypted using different encryption algorithms. The methods available include both classic methods (e.g. the Caesar encryption algorithm) and modern cryptosystems (for example, the RSA and DES algorithms, as well as algorithms based on elliptic curves). The symmetric AES algorithms are very topical. One of these is the Rijndael algorithm, which on 2 October 2000 was announced the winner of the AES competition, making it the successor to the DES procedure. A summary of all the encryption algorithms available in CrypTool is contained on the Help page for the Crypt menu.

3 Brute force attacking Triple DES (CBC)

One of the most popular forms of attacking encryption is a brute force attack where (typically) every combination of key is applied to the ciphertext. CrypTool allows us to perform simple brute force attacks on even the more modern encryption systems.

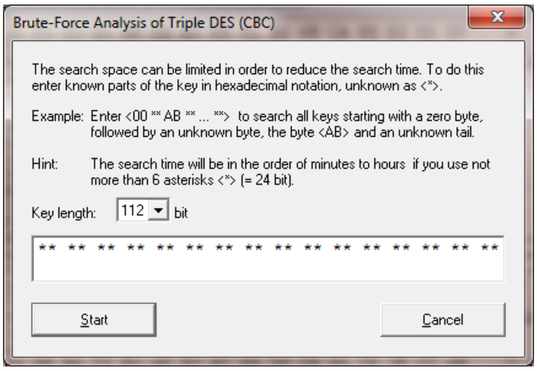
3.1 Activate the encrypted document.



Triple DES (CBC) encryption of <CrypTool-en>, key <12 34 AB CD 00 00 00 00 00 00 00 00 00 00 00 00>

```
00000000  A7 61 B7 F5 F6 D5 4F AC 76 2D F5 D3 B1 AF 58 A1 FE 81 41 6B CA 00 02 01 05  .a....O.v-....X...Ak.....
00000019  E6 68 30 A1 28 2C C9 F7 91 50 01 44 72 A1 07 C6 C4 6E F0 62 43 AE 53 30 D6  .h0.(,...P.Dr....n.bC.S0.
00000032  BE 8E 0A 42 86 F8 25 9D DF BA B2 BE AA EF 7A 41 FD CD EF F7 48 A8 58 9F 07  ...B..%.......zA....H.X..
0000004B  1D 52 27 E7 19 9B E6 EC EC AA 3D 79 CD 33 D1 F7 94 E3 26 19 EF B7 67 F2 75  .R'.......=y.3....&...g.u
00000064  D1 16 FE AC D8 09 3C 4F 85 14 AB BB B7 3A 3D 33 01 4F C7 C9 AC BB EE CE 75  ......<O.....:=3.O......u
0000007D  C3 C5 B3 4F 44 FD 99 FE 57 C2 6E 7A C1 C2 8D F8 0F F9 05 7B 0C 3D 80 F8 1B  ...OD...W.nz.......{.=...
00000096  A8 FA 97 CE 31 42 54 F7 44 44 88 8B 53 81 12 57 A9 DE 49 30 B1 8F 48 55 96  ....1BT.DD..S..W..I0..HU.
000000AF  4B CB 1C 99 27 48 1D 6A B7 89 90 A6 51 33 01 EE 43 90 17 34 49 1C 61 7B AA  K...'H.j....Q3..C..4I.a{.
000000C8  06 6A 84 DD 7F 9D 5C EF 9C 25 EB 78 4A C5 BD 1C D5 12 32 B3 E2 20 B4 B5 3B  .j....\..%.xJ.....2.. ..;
000000E1  1F B2 05 99 69 C8 D7 89 1F 96 77 E7 45 DF FA 7B EF 4C CC 37 3C BF F6 47 AE  ....i.....w.E..{.L.7<..G.
000000FA  AA 0C B3 27 A6 6B 44 9A 1B BC 65 41 7F 0A 96 BB 8D 72 F3 0A 4F 54 B9 EE 1C  ...'.kD...eA.....r..OT...
00000113  66 6A 19 B4 84 6B 49 E3 FC 31 0A B2 F3 A6 67 EC 81 02 F6 9C FA 6B 44 9F 51  fj...kI..1....g......kD.Q
0000012C  0D DE C3 F0 6E 6D 99 AC DC F4 63 25 3A 90 A8 52 CD 92 C0 50 7C C8 85 1C 1D  ....nm....c%:..R...P|....
00000145  EB 4E C4 76 E4 3A 84 10 0F BF 43 DE 4E D4 A8 76 95 38 19 92 FE 23 4D 16 6E  .N.v.:....C.N..v.8...#M.n
0000015E  42 DE D4 65 10 C0 6F FE DC 4B 48 7F A5 D1 1F 0E DB 3A 8B 9E 80 C7 D1 98 5B  B..e..o..KH......:......[
00000177  A7 CB 19 2B 5C 59 83 D8 D2 97 7F B5 A0 33 3B 9A E0 CA ED 01 DB B9 E3 F1 B9  ...+\Y.......3;..........
00000190  75 B0 7E FE 88 85 7D E7 B1 3A 8A 82 DB 74 9B 68 EE A8 91 D7 03 41 88 08 12  u.~...}..:...t.h.....A...
000001A9  2A 9B C5 BE 7D F7 C8 99 E6 77 31 68 0F 18 2B 64 93 C8 56 AB 82 69 8C C4 8F  *...}....w1h..+d..V..i...
000001C2  27 89 68 24 93 6A 39 B6 D7 97 99 C2 8A 4A 07 CE CB 41 ED C4 11 C6 B1 B9 E5  '.h$.j9......J...A.......
000001DB  00 04 A1 92 A1 1F 25 92 73 37 71 53 B6 79 73 D5 B3 83 D6 04 C4 91 54 0E B7  ......%.s7qS.ys.......T..
000001F4  9F 4E B9 04 93 C2 8D FD 80 68 85 5F AB 09 36 A0 85 6B F2 72 DF 6F 4A 2A 3A  .N.......h._..6..k.r.oJ*:
0000020D  E1 25 E4 6C 47 10 A1 B9 1D 09 FE B4 16 F1 45 82 8C 88 38 1E 98 1E 3F CC 0B  .%.lG.........E...8...?..
00000226  AC 36 A1 C6 C3 6D 8F FE F9 CD ED C4 D9 53 A3 EA 25 40 C4 19 74 CD 2B D7 22  .6...m.......S..%@..t.+."
0000023F  C3 39 CD 99 EC 5E 05 B7 23 C0 38 AC E3 AF 41 60 3D 6E 63 50 11 4E 36 D1 AD  .9...^..#.8...A`=ncP.N6..
```

3.2 We now select Analysis→Symmetric Modern→Triple DES (CBC).



Brute-Force Analysis of Triple DES (CBC)

The search space can be limited in order to reduce the search time. To do this enter known parts of the key in hexadecimal notation, unknown as <*>.

Example: Enter <00 ** AB ** ... **> to search all keys starting with a zero byte, followed by an unknown byte, the byte <AB> and an unknown tail.

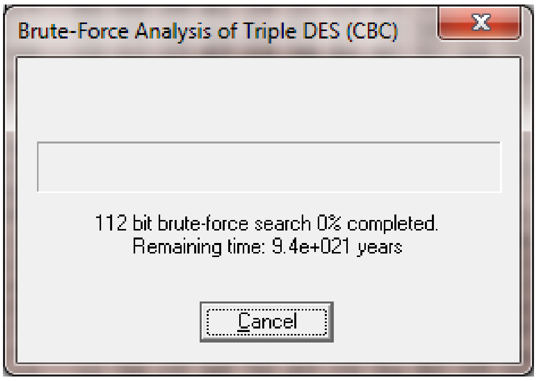
Hint: The search time will be in the order of minutes to hours if you use not more than 6 asterisks <*> (= 24 bit).

Key length: 112 bit

** ** ** ** ** ** ** ** ** ** ** ** ** **

In the dialog box which appears we are able to set a key range – this is the range of keys which we want the software to apply. An asterisk (*) means apply every possible value for the key in that position. In this example, the search key is automatically set to: ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** this means that the software will apply every single possible key.

3.3 Click on Start



Brute-Force Analysis of Triple DES (CBC)

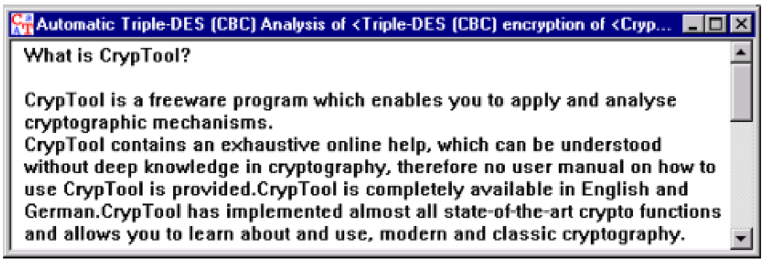
112 bit brute-force search 0% completed.
Remaining time: 9.4e+021 years

You will notice that the dialogue box suggests that it will take around approximately 9000000000000000000000 years to complete this exercise. This is clearly too long (!). Hence we need to limit the key search somewhat.

3.4 Repeat this stem, but now enter ** ** AB CD ** ** ** ** ** ** ** ** ** ** ** ** as the range to be searched through

This reduces the time significantly (approx. 5000000000000000000 years!). Clearly this is not good enough and unless we apply more significant processing power to this, we will not realistically be able to brute force attack this.

3.5 Repeat the process one last time with the correct key (as established in the steps above) and note that this does of course present the correct plaintext result.


Automatic Triple-DES (CBC) Analysis of <Triple-DES (CBC) encryption of <Cryp...

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.