UNIVERSITY of GUYANA

CSE 2203 (2018-2019)

TUTORIAL 3 – SYMMETRIC CRYPTOGRAPHY (MODERN)

Please note that downloading and installing software on the laboratory computers is strictly forbidden and if found doing so, you will be penalized. Special permission was sought to conduct this tutorial session. Please install ONLY the tools specified in this tutorial.

1. Navigate to cryptool.org
2. Download and Install CrypTool 1, if not already installed.
3. Complete the following exercise:

Videos

1) The politics of Cryptography

Tutor Note: Cryptography has traditionally been developed and used by the Military and by Government Intelligence Agencies. Advances in modern cryptography have been governed by strict export controls. For example, the US Government once banned the export of any cryptography. However, with the commercialization of the internet, governments have had to relax their controls. There is always a battle between individual and commercial use of cryptography and Government's need to provide national security.

Video Link: https://www.youtube.com/watch?v=lWImmWpIbYs

https://www.youtube.com/watch?v=ASfAPOiq_eQ

https://www.youtube.com/watch?v=mXZNayEPFKc

2) The pioneers of Cryptography

Tutor Note: The NSA (National Security Agency) wanted to control cryptography. However, they came into conflict with the Academic Community. Martin Hellman and Whitfield Diffie challenged the government on weakening DES (the Data Encryption Standard), a symmetric cryptographic algorithm in use by the commercial sector, by shortening its key to 56 bits. Diffie and Hellman also solved the problem of symmetric cryptography - they provided a mathematical way of doing key-exchange without needing to pre-share a secret key.

Video Link: https://www.youtube.com/watch?v=w3JcMetfl00

ACTIVITY 1: CRYPTANALYSIS OF RC4 (STREAM CIPHER) USING CRYPTOOL 1

Hacking Activity: Use CrypTool

In this practical scenario, we will create a simple encryption using the RC4 stream cipher algorithm. We will then attempt to decrypt it using brute-force attack. For this exercise, let us assume that we know the encryption secret key is 24 bits. We will use this information to break the cipher.

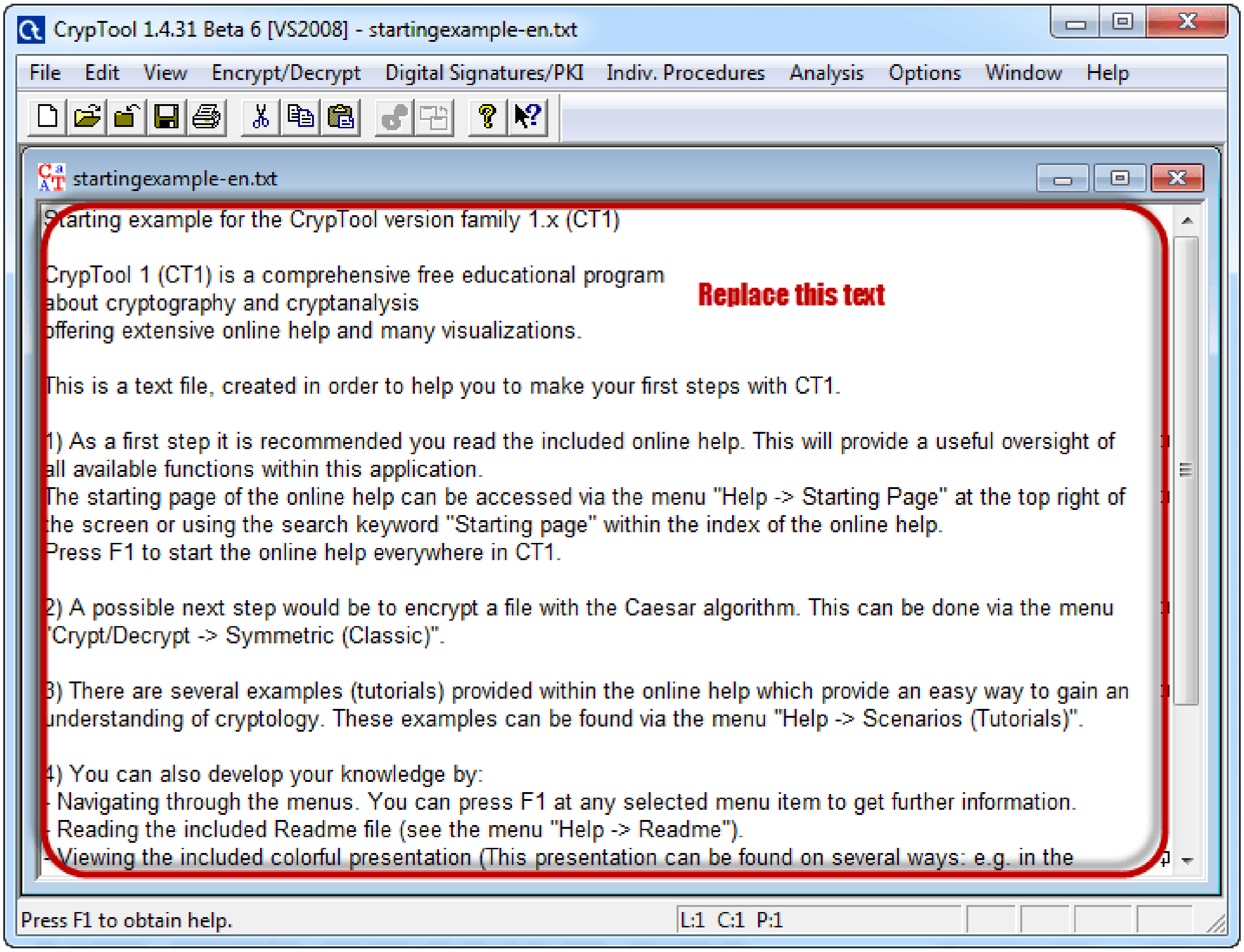
Creating the RC4 stream ciphertext

We will encrypt the following phrase

Never underestimate the determination of a kid who is time-rich and cash-poor

We will use 00 00 00 as the encryption key.

- Open CrypTool 1


CrypTool 1.4.31 Beta 6 [VS2008] - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
Replace this text
Press F1 to obtain help.
L:1 C:1 P:1

Starting example for the CrypTool version family 1.x (CT1)

CrypTool 1 (CT1) is a comprehensive free educational program
about cryptography and cryptanalysis
offering extensive online help and many visualizations.

This is a text file, created in order to help you to make your first steps with CT1.

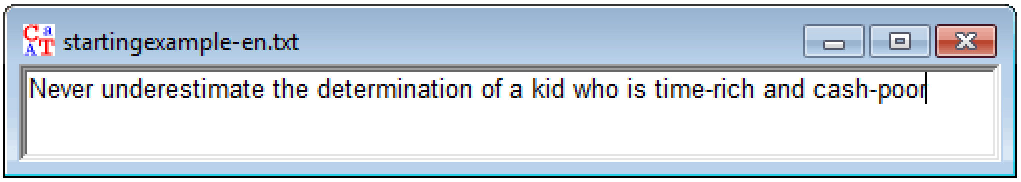
1) As a first step it is recommended you read the included online help. This will provide a useful oversight of all available functions within this application.
The starting page of the online help can be accessed via the menu "Help -> Starting Page" at the top right of the screen or using the search keyword "Starting page" within the index of the online help.
Press F1 to start the online help everywhere in CT1.

2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (Classic)".

3) There are several examples (tutorials) provided within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found via the menu "Help -> Scenarios (Tutorials)".

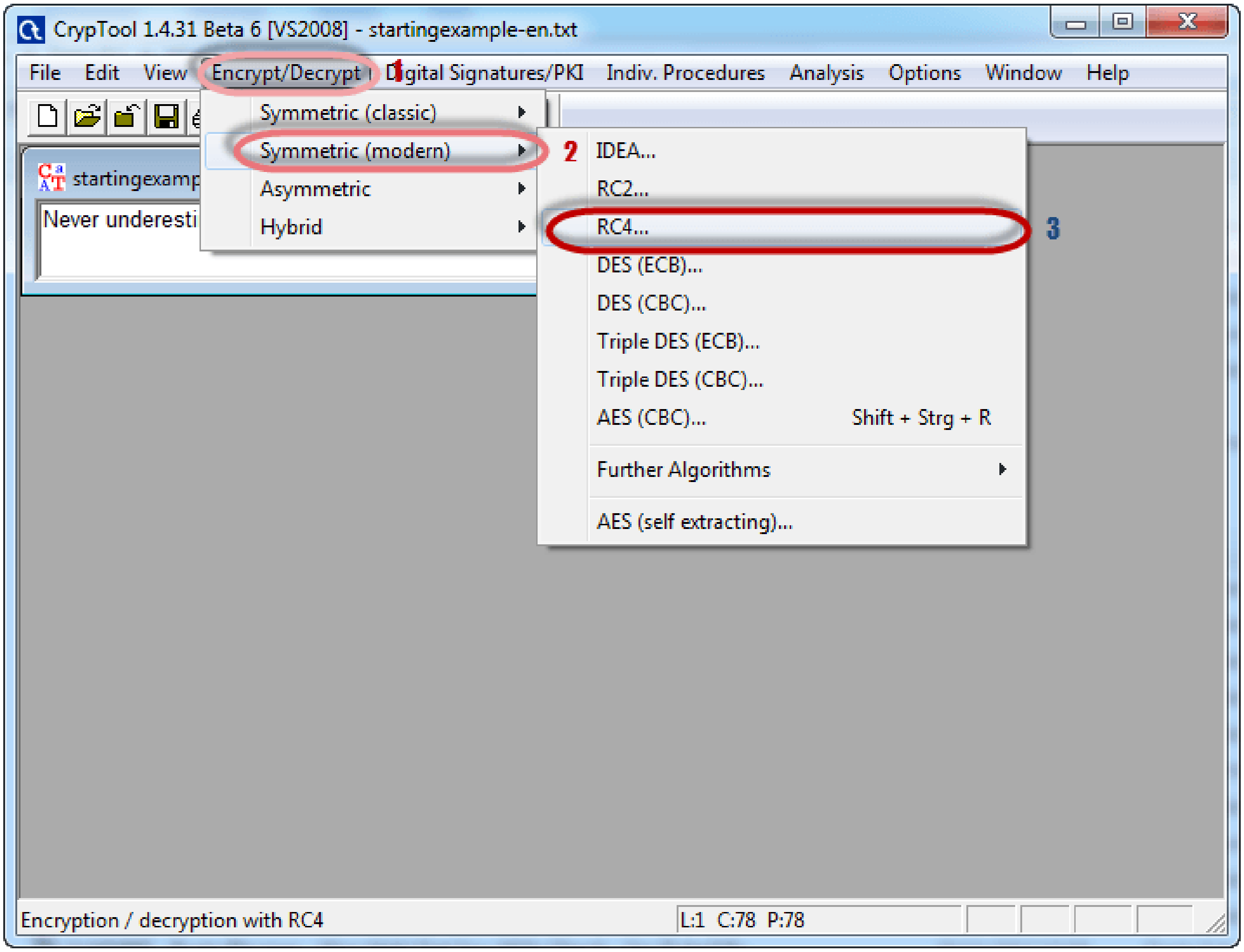
4) You can also develop your knowledge by:
- Navigating through the menus. You can press F1 at any selected menu item to get further information.
- Reading the included Readme file (see the menu "Help -> Readme").
- Viewing the included colorful presentation (This presentation can be found on several ways: e.g. in the

- Replace the text with Never underestimate the determination of a kid who is time-rich and cash-poor



Never underestimate the determination of a kid who is time-rich and cash-poor

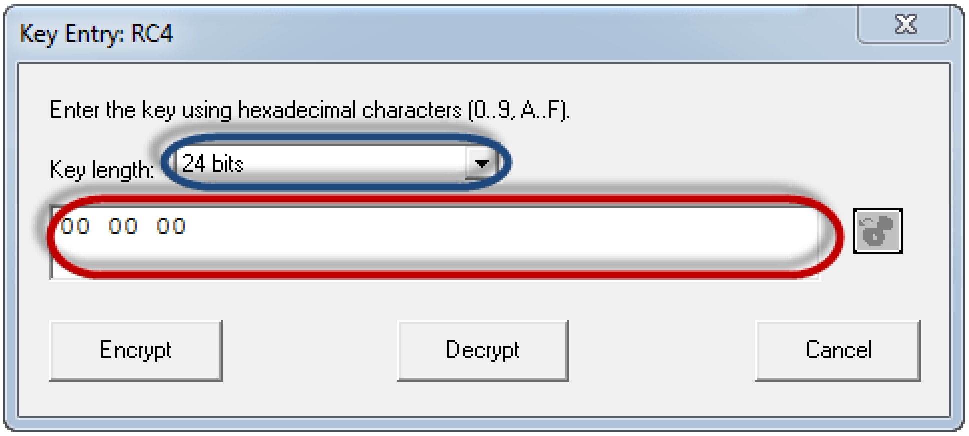
- Click on Encrypt/Decrypt menu



Encryption / decryption with RC4 L:1 C:78 P:78

- Point to Symmetric (modern) then select RC4 as shown above

- The following window will appear



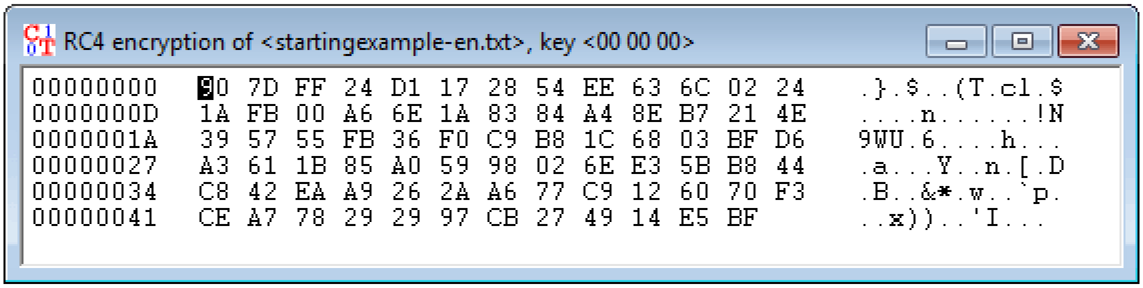
Key Entry: RC4

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

Key length: 24 bits

00 00 00

- Select 24 bits as the encryption key
- Set the value to 00 00 00
- Click on Encrypt button
- You will get the following stream cipher

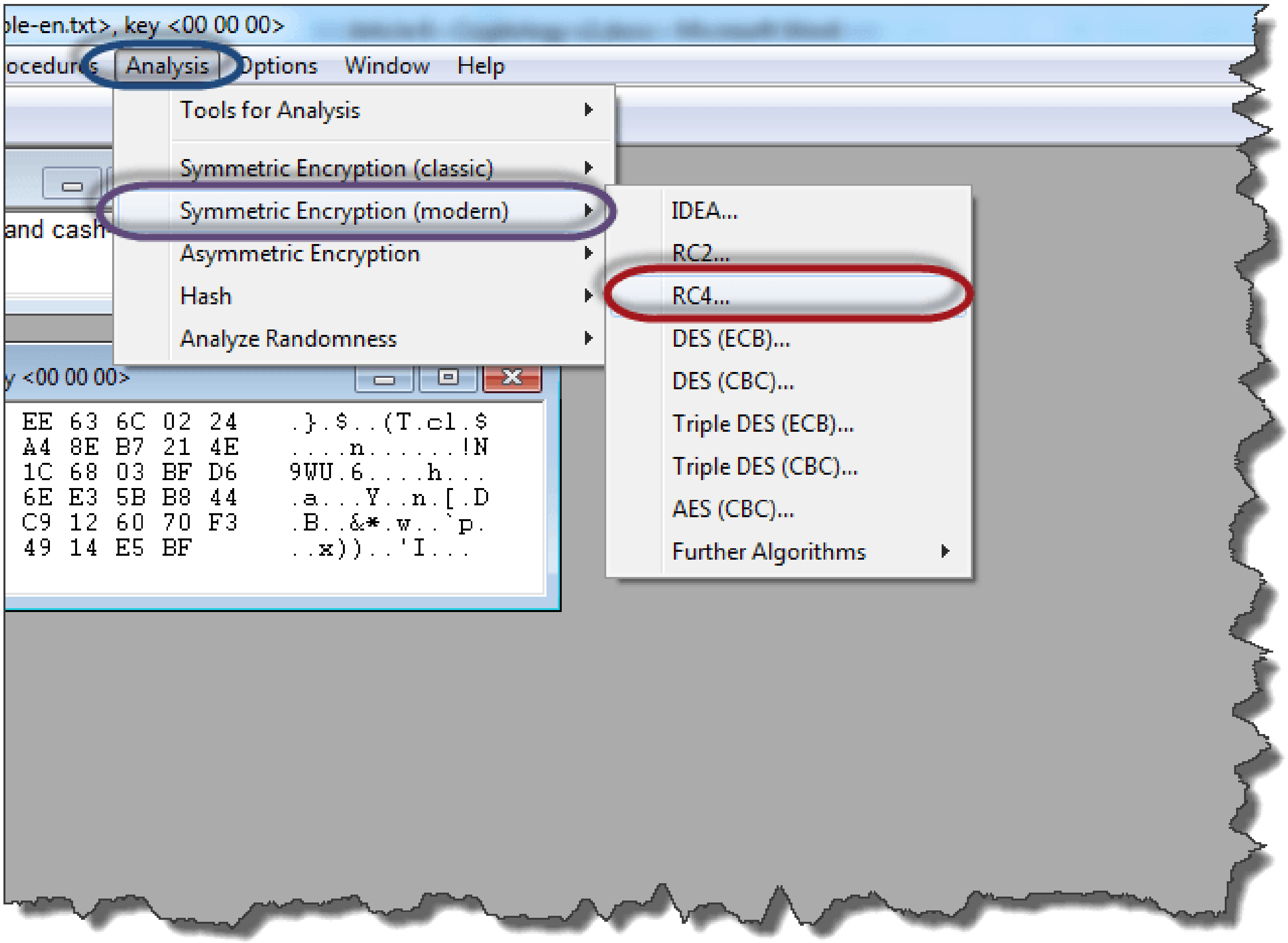


RC4 encryption of <startingexample-en.txt>, key <00 00 00>

```
00000000   90 7D FF 24 D1 17 28 54 EE 63 6C 02 24    .}.$..(T.cl.$
0000000D   1A FB 00 A6 6E 1A 83 84 A4 8E B7 21 4E    ....n......!N
0000001A   39 57 55 FB 36 F0 C9 B8 1C 68 03 BF D6    9WU.6....h...
00000027   A3 61 1B 85 A0 59 98 02 6E E3 5B B8 44    .a...Y..n.[.D
00000034   C8 42 EA A9 26 2A A6 77 C9 12 60 70 F3    .B..&*.w..`p.
00000041   CE A7 78 29 29 97 CB 27 49 14 E5 BF       ..x))..'I...
```

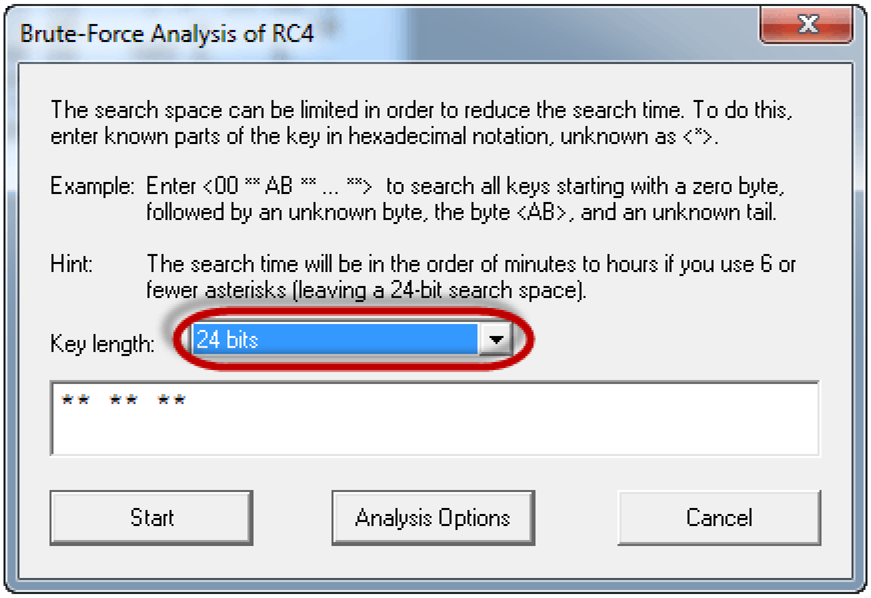
Attacking the stream cipher

- Click on Analysis menu



```
EE 63 6C 02 24    .}.$..(T.cl.$
A4 8E B7 21 4E    ....n......!N
1C 68 03 BF D6    9WU.6....h...
6E E3 5B B8 44    .a...Y..n.[.D
C9 12 60 70 F3    .B..&*.w..`p.
49 14 E5 BF       ..x))..'I...
```

- Point to Symmetric Encryption (modern) then select RC4 as shown above
- You will get the following window



Brute-Force Analysis of RC4

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 <*>.

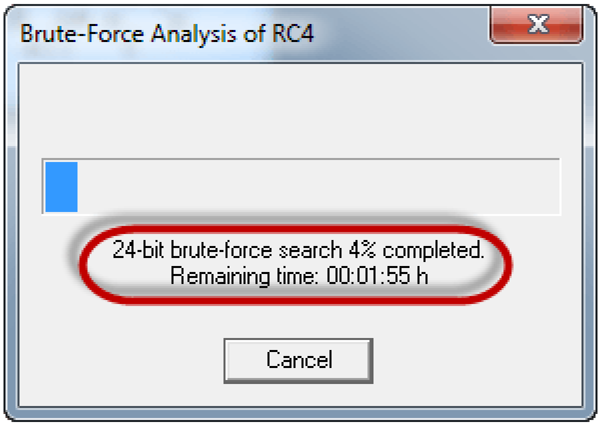
Example: Enter <00 ** AB ** ... **> to search all keys starting with a zero byte, followed by an unknown byte, the byte <AB>, and an unknown tail.

Hint: The search time will be in the order of minutes to hours if you use 6 or fewer asterisks (leaving a 24-bit search space).

Key length: 24 bits

```
** ** **
```

- Remember the assumption made is the secret key is 24 bits. So make sure you select 24 bits as the key length.
- Click on the Start button. You will get the following window

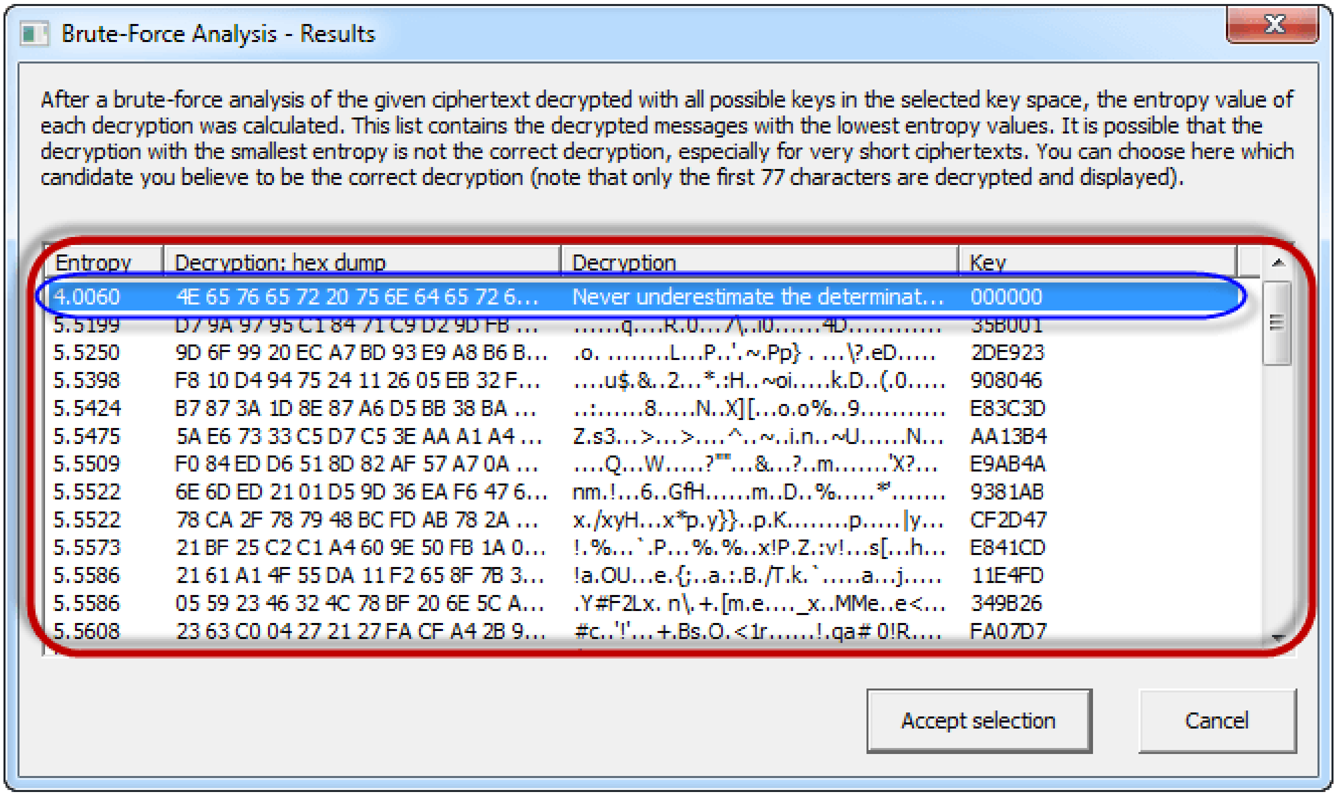


Brute-Force Analysis of RC4

24-bit brute-force search 4% completed.
Remaining time: 00:01:55 h

- Note: the time taken to complete the Brute-Force Analysis attack depends on the processing capacity of the machine been used and the key length. The longer the key length, the longer it takes to complete the attack.

- When the analysis is complete, you will get the following results.



Brute-Force Analysis - Results

After a brute-force analysis of the given ciphertext decrypted with all possible keys in the selected key space, the entropy value of each decryption was calculated. This list contains the decrypted messages with the lowest entropy values. It is possible that the decryption with the smallest entropy is not the correct decryption, especially for very short ciphertexts. You can choose here which candidate you believe to be the correct decryption (note that only the first 77 characters are decrypted and displayed).

Entropy	Decryption: hex dump	Decryption	Key
4.0060	4E 65 76 65 72 20 75 6E 64 65 72 6...	Never underestimate the determinat...	000000
5.5199	D7 9A 97 95 C1 84 71 C9 D2 9D FB ...	......q....R.0.../\..i0......4D...........	35B001
5.5250	9D 6F 99 20 EC A7 BD 93 E9 A8 B6 B...	.o. ........L...P..'.~.Pp} . ...\?.eD.....	2DE923
5.5398	F8 10 D4 94 75 24 11 26 05 EB 32 F...	....u$.&..2...*.:H..~oi.....k.D..(.0.....	908046
5.5424	B7 87 3A 1D 8E 87 A6 D5 BB 38 BA ...	..:......8.....N..X][...o.o%..9..........	E83C3D
5.5475	5A E6 73 33 C5 D7 C5 3E AA A1 A4 ...	Z.s3...>...>....^..~..i.n..~U......N...	AA13B4
5.5509	F0 84 ED D6 51 8D 82 AF 57 A7 0A ...	....Q...W.....?""...&...?..m.......'X?...	E9AB4A
5.5522	6E 6D ED 21 01 D5 9D 36 EA F6 47 6...	nm.!...6..GfH......m..D..%.....*'.......	9381AB
5.5522	78 CA 2F 78 79 48 BC FD AB 78 2A ...	x./xyH...x*p.y}}..p.K........p.....|y...	CF2D47
5.5573	21 BF 25 C2 C1 A4 60 9E 50 FB 1A 0...	!.%...`.P...%.%..x!P.Z.:v!...s[...h...	E841CD
5.5586	21 61 A1 4F 55 DA 11 F2 65 8F 7B 3...	!a.OU...e.{;..a.:.B./T.k.`.....a...j.....	11E4FD
5.5586	05 59 23 46 32 4C 78 BF 20 6E 5C A...	.Y#F2Lx. n\.+.[m.e...._x..MMe..e<...	349B26
5.5608	23 63 C0 04 27 21 27 FA CF A4 2B 9...	#c..'!'...+.Bs.O.<1r......!.qa# 0!R....	FA07D7

- Note: a lower Entropy number means it is the most likely correct result. It is possible a higher than the lowest found Entropy value could be the correct result.
- Select the line that makes the most sense then click on Accept selection button when done

QUESTION: What assumption was needed in this activity's cryptanalysis?

ANSWER: One possible answer is that we needed to know the key length.

ACTIVITY 2: VISUALISATION OF DES / AES USING CRYPTOOL 1

On the Individual Procedures Menu item of CrypTool 1, Navigate to Visualisation of Algorithms. Work through the DES and AES Visualisations.

REFERENCE:

https://www.guru99.com/how-to-make-your-data-safe-using-cryptography.html