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

1. 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.

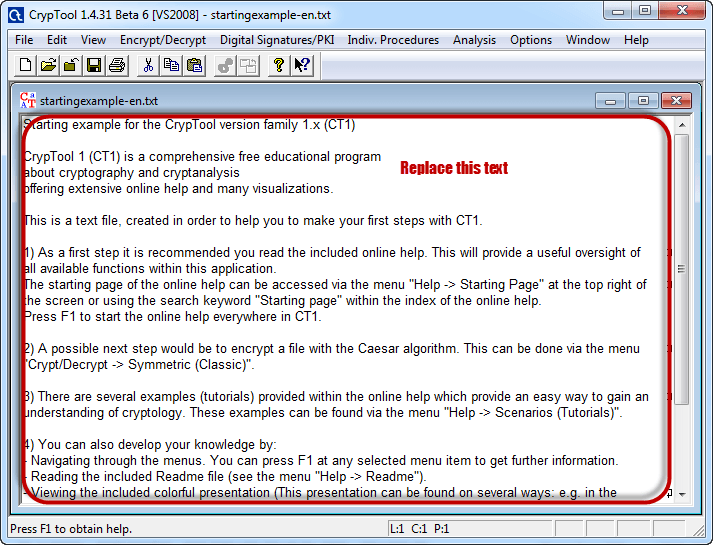
## Creating the RC4 stream ciphertext

We will encrypt the following phrase

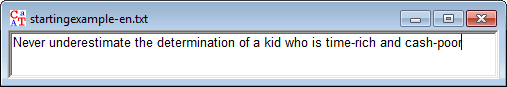
Never underestimate the determination of a kid who is time-rich and cash-poor

We will use 00 00 00 as the encryption key.

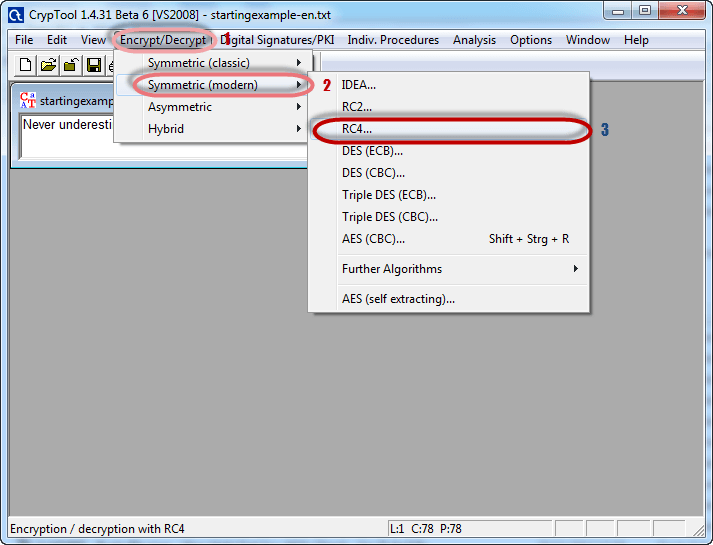
* Open CrypTool 1

[](https://www.guru99.com/images/EthicalHacking/Cryptool1.png)

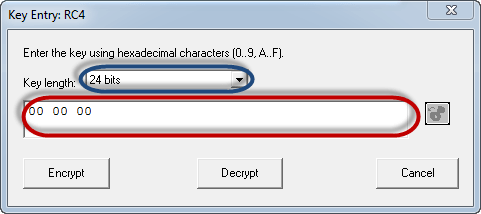
* Replace the text with Never underestimate the determination of a kid who is time-rich and cash-poor

[](https://www.guru99.com/images/EthicalHacking/Cryptool2.png)

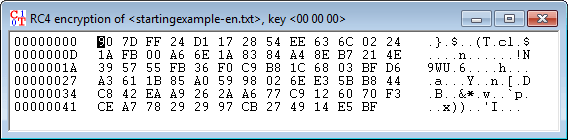
* Click on Encrypt/Decrypt menu

[](https://www.guru99.com/images/EthicalHacking/Cryptool3.png)

* Point to Symmetric (modern) then select RC4 as shown above
* The following window will appear

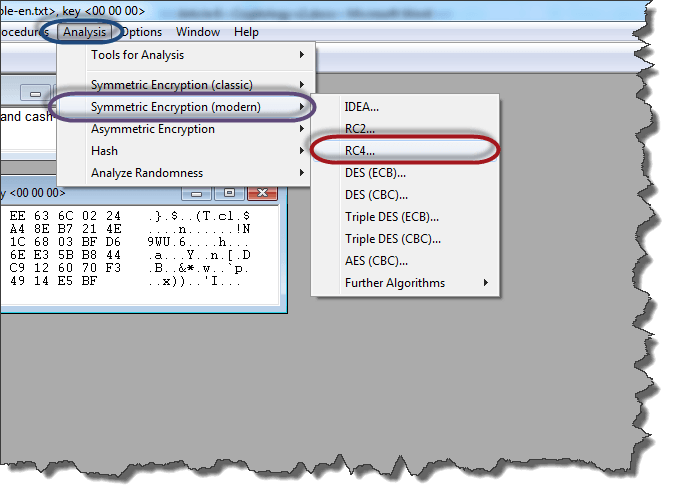
[](https://www.guru99.com/images/EthicalHacking/Cryptool4.png)

* 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

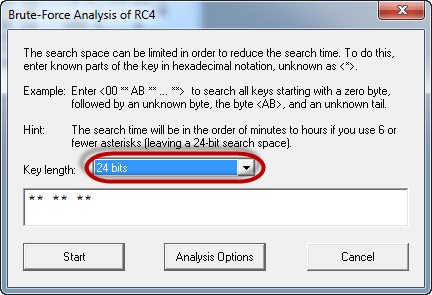
[](https://www.guru99.com/images/EthicalHacking/Cryptool5.png)

## Attacking the stream cipher

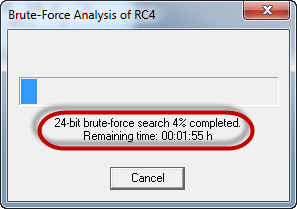
* Click on Analysis menu

[](https://www.guru99.com/images/EthicalHacking/Analysys_menu.png)

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

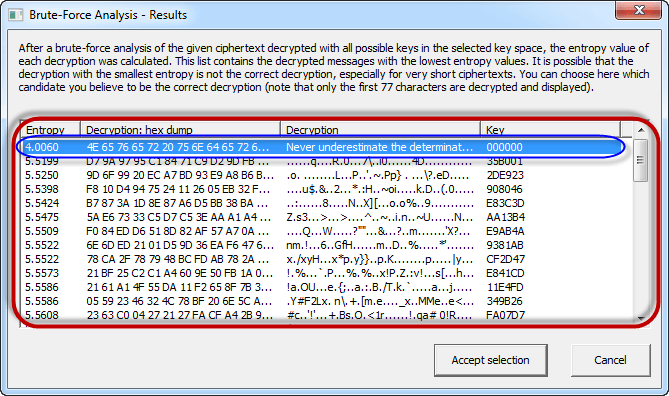
[](https://www.guru99.com/images/EthicalHacking/Analysys_of_rc4.png)

* 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

[](https://www.guru99.com/images/EthicalHacking/Analysys_of_rc4_1.png)

* 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.

[](https://www.guru99.com/images/EthicalHacking/Analysys_result.png)

* 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