



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



Internet Security (IS)

Lab – Cryptography

Faculty of Architecture, Computing & Engineering

School of Applied Computing

Mount Pleasant Campus

Swansea

SA1 6ED

Understanding Cryptography, Cryptanalysis and Cryptology

Information plays a vital role in the running of business, organizations, military operations etc. **Information in the wrong hands can lead to loss of business or catastrophic results. To secure communication, a business can use cryptology to cipher information.** Cryptology involves transforming information into non human readable format and vice versa.

In this article, we will introduce you to the world of cryptology and how you can secure information from falling into the wrong hands.

Topics covered in this tutorial

- What is cryptography?
- What is cryptanalysis?
- What is cryptology?
- Encryption Algorithms
- Hacking Lab Activity: Hack Now!

What is Cryptography?

Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into non human readable formats and vice versa.

Let's illustrate this with the aid of an example. Suppose you want to send the message "I LOVE APPLES", you can replace every letter in the phrase with the third successive letter in the alphabet. The encrypted message will be "K NQYG CRRNGV". To decrypt our message, we will have to go back three letters in the alphabet using the letter that we want to decrypt. The image below shows how the transformation is done.

Key: Replace every letter with 3rd successive letter

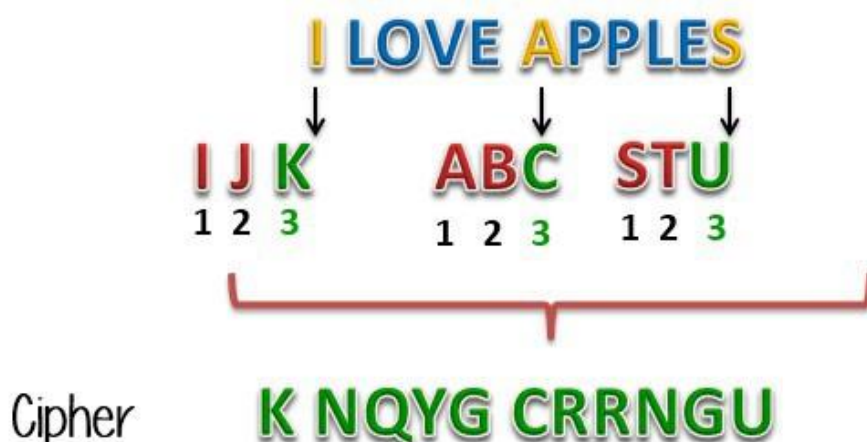


Figure 1: Basic Cryptographic concept.

The process of transforming information into non human readable form is called encryption.

The process of reversing encryption is called **decryption**.

Decryption is done using a **secret key** which is only known to the legitimate recipients of the information. The key is used to decrypt the hidden messages. This makes the communication secure because even if the attacker manages to get the information, it would not make sense to them.

The encrypted information is known as a **cipher**.

What is Cryptanalysis?

Cryptography encrypts messages using a secret key. **Cryptanalysis is the art of trying to decrypt the encrypted messages without the use of the key that was used to encrypt the messages.** Cryptanalysis uses mathematical analysis & algorithms to decipher the ciphers. The success of cryptanalysis attacks depends on;

- Amount of time available
- Computing power available
- Storage capacity available

The following is a list of the commonly used Cryptanalysis attacks;

- **Brute force attack**– this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.
- **Dictionary attack**– this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.
- **Rainbow table attack**– this type of attack compares the cipher text against pre-computed hashes to find matches.

What is Cryptology?

Cryptology combines the techniques of cryptography and cryptanalysis.

Encryption Algorithms

MD5– this is the acronym for Message-Digest 5. It is used to create 128 bit hash values. Theoretically, hashes cannot be reversed into the original plain text. MD5 is used to encrypt passwords as well as check data integrity. MD5 is not collision resistant. Collision resistance is the difficulties in finding two values that produce the same hash values.

- **SHA**– this is the acronym for Secure Hash Algorithm. SHA algorithms are used to generate condensed representations of a message (message digest). It has various versions such as;
 - **SHA-0**: produces 120 bit hash values. It was withdrawn from use due to significant flaws and replaced by SHA-1.

- **SHA-1:** produces 160 bit hash values. It is similar to earlier versions of MD5. It has cryptographic weakness and is not recommended for use since the year 2010.
- **SHA-2:** it has two hash functions namely SHA-256 and SHA-512. SHA-256 uses 32 bit words while SHA-512 uses 64 bit words.
- **SHA-3:** this algorithm was formally known as Keccak.
- **RC4**– this algorithm is used to create stream ciphers. It is mostly used in protocols such as **Secure Socket Layer (SSL)** to encrypt internet communication and **Wired Equivalent Privacy (WEP)** to secure wireless networks.
- **BLOWFISH**– this algorithm is used to create keyed, symmetric blocked ciphers. It can be used to encrypt passwords and other data.

Hacking Lab Activity: Hack Now!

In this practical scenario, we will create a simple cipher using the RC4 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.

We will use CrypTool 1 as our cryptology tool. CrypTool 1 is an open source educational tool for crypto logical studies. You can download it from <https://www.cryptool.org/en/ct1-downloads>

Creating the RC4 stream cipher

We will encrypt the following phrase. Don't include the quotation marks. *“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

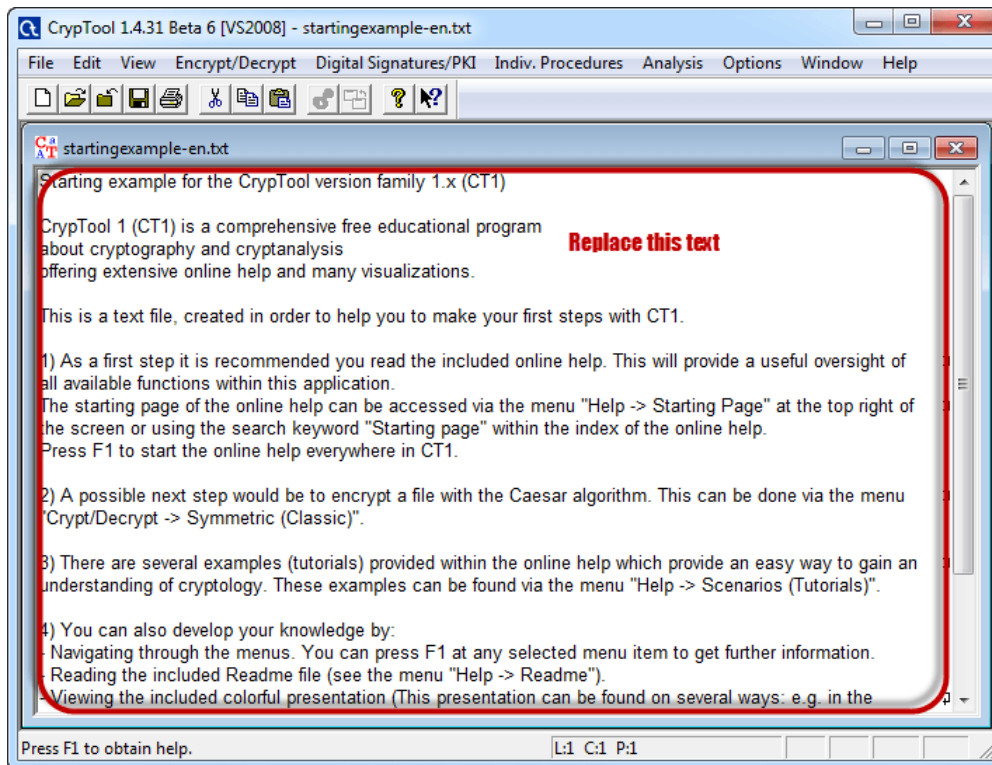


Figure 2: Cryptool 1 Window.

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

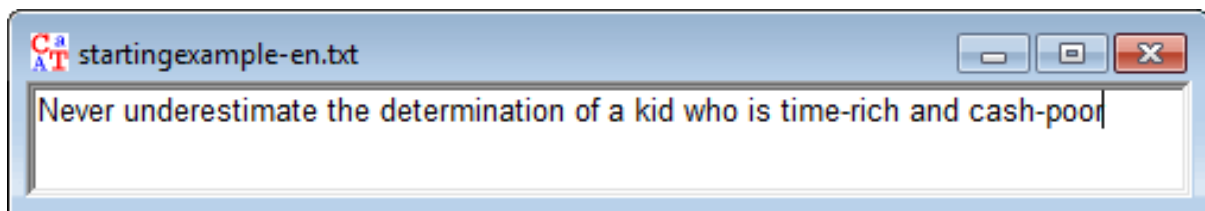


Figure 3: Text Window.

- Click on Encrypt/Decrypt menu as shown below in Figure 4.

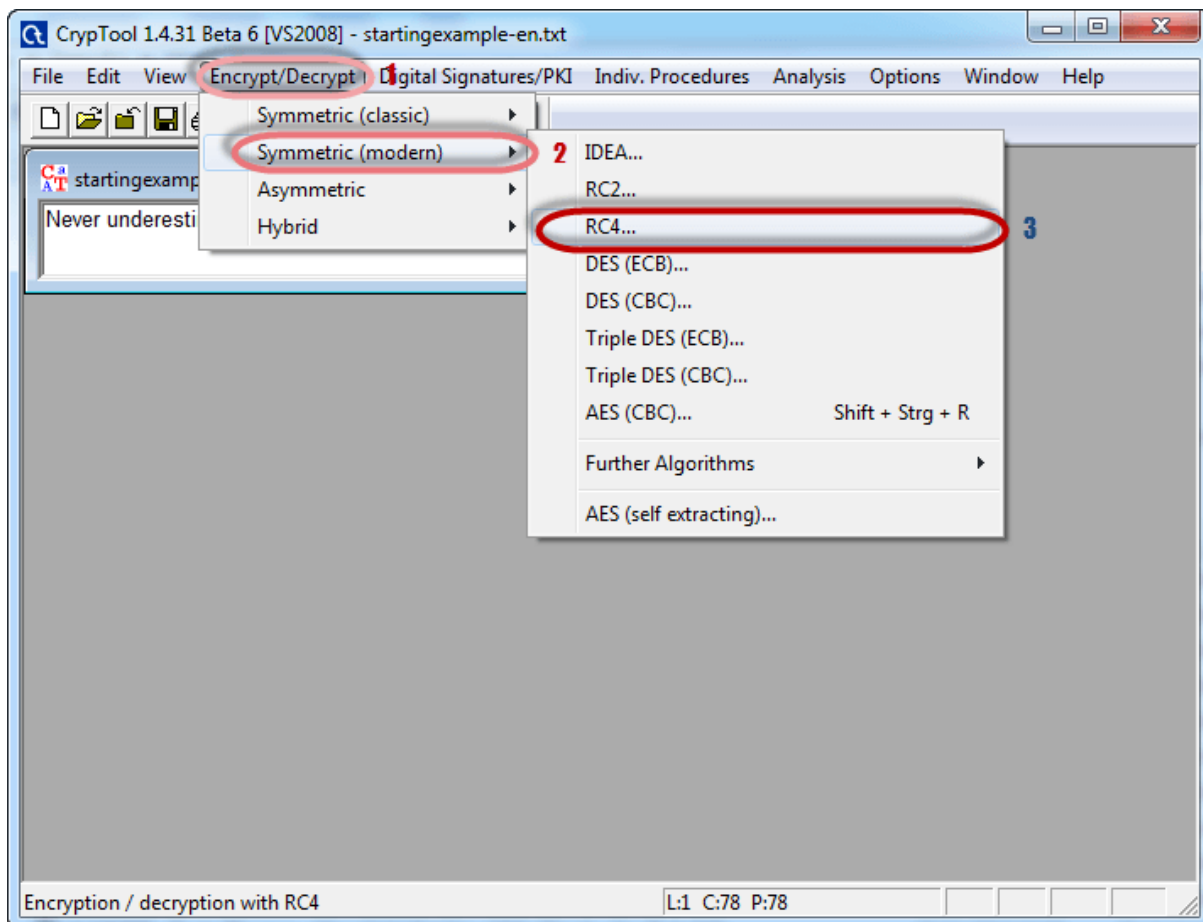


Figure 4: Encrypt/Decrypt Functions.

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

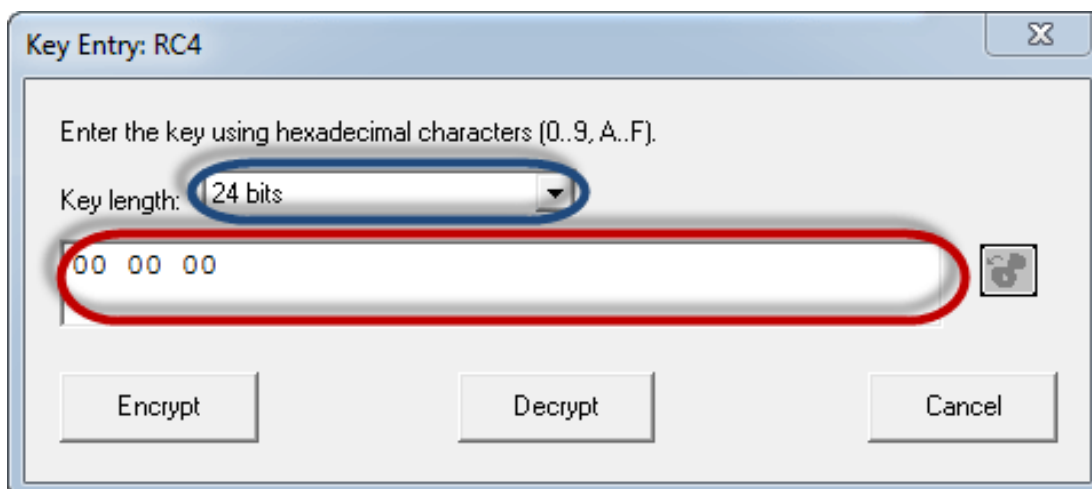


Figure 5: Selecting encryption bits.

- Select 24 bits as the encryption key
- Set the value to 00 00 00
- Click on the Encrypt button
- You will get the stream cipher as shown in Figure 6 below

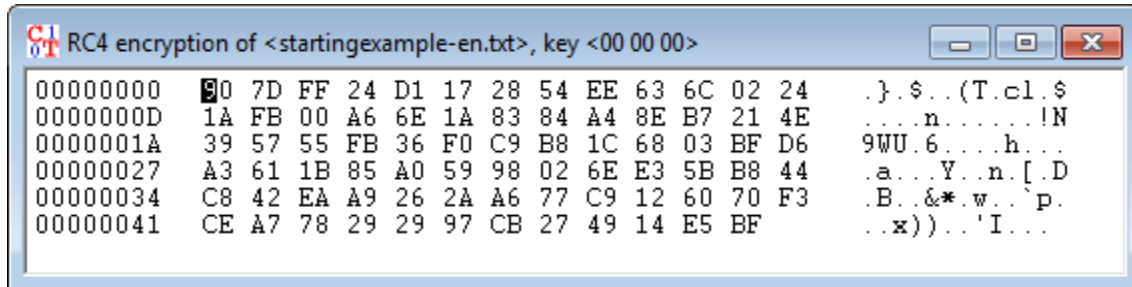


Figure 6: Stream Cipher.

Attacking the stream cipher

- Click on Analysis menu as shown below in Figure 7.

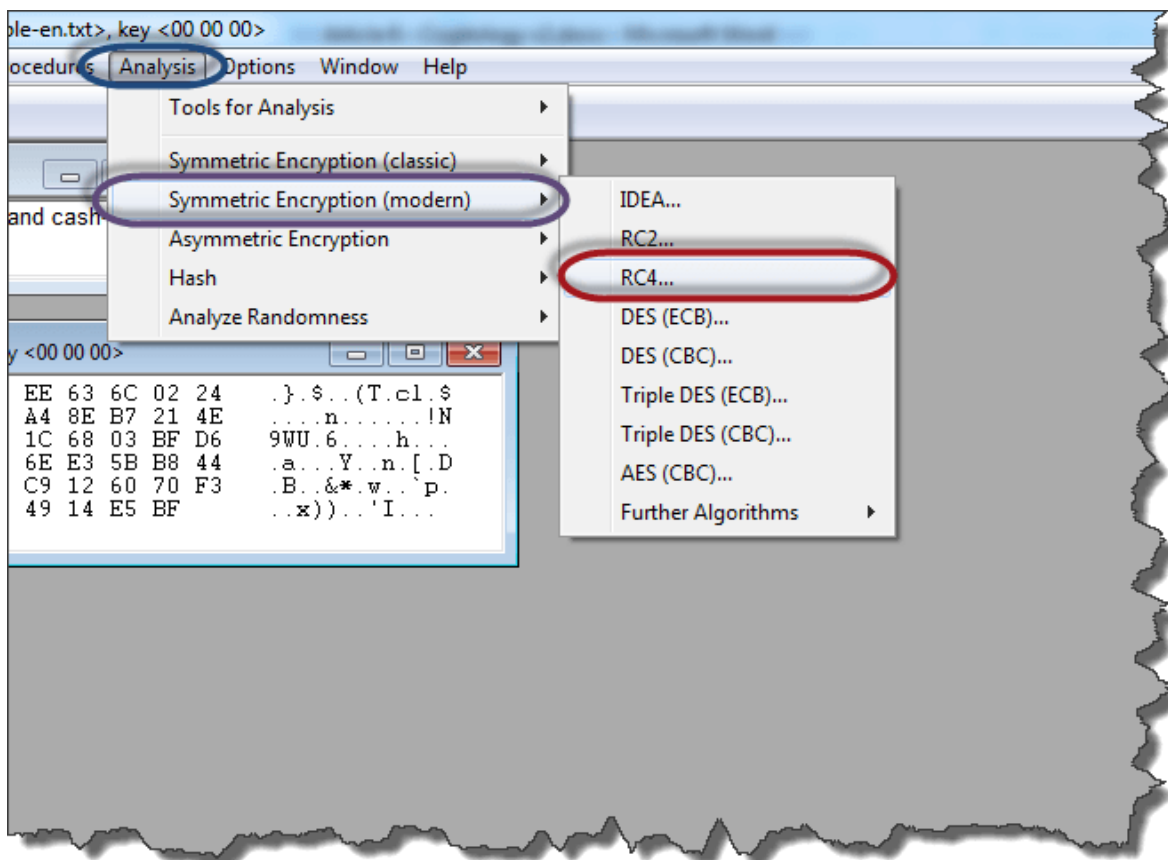


Figure 7: Analysis Menu.

- Point to Symmetric Encryption (modern) then select RC4 as shown above in Figure 7.

- You will get the window as shown in Figure 8 below

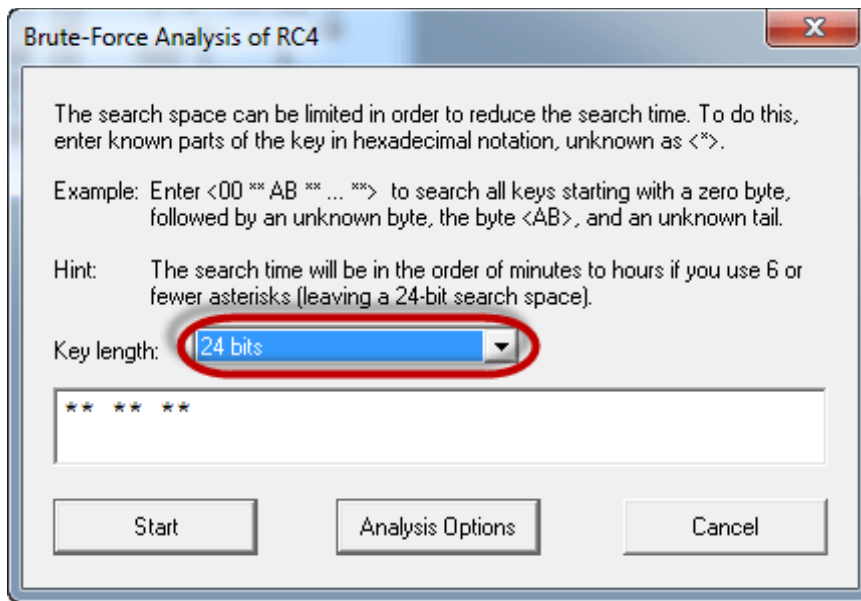


Figure 8: Brute-Force Analysis.

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

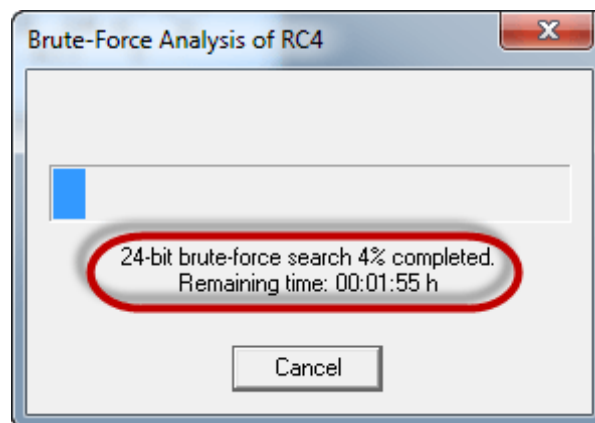


Figure 9: Brute-Force Analysis Progress.

- 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.

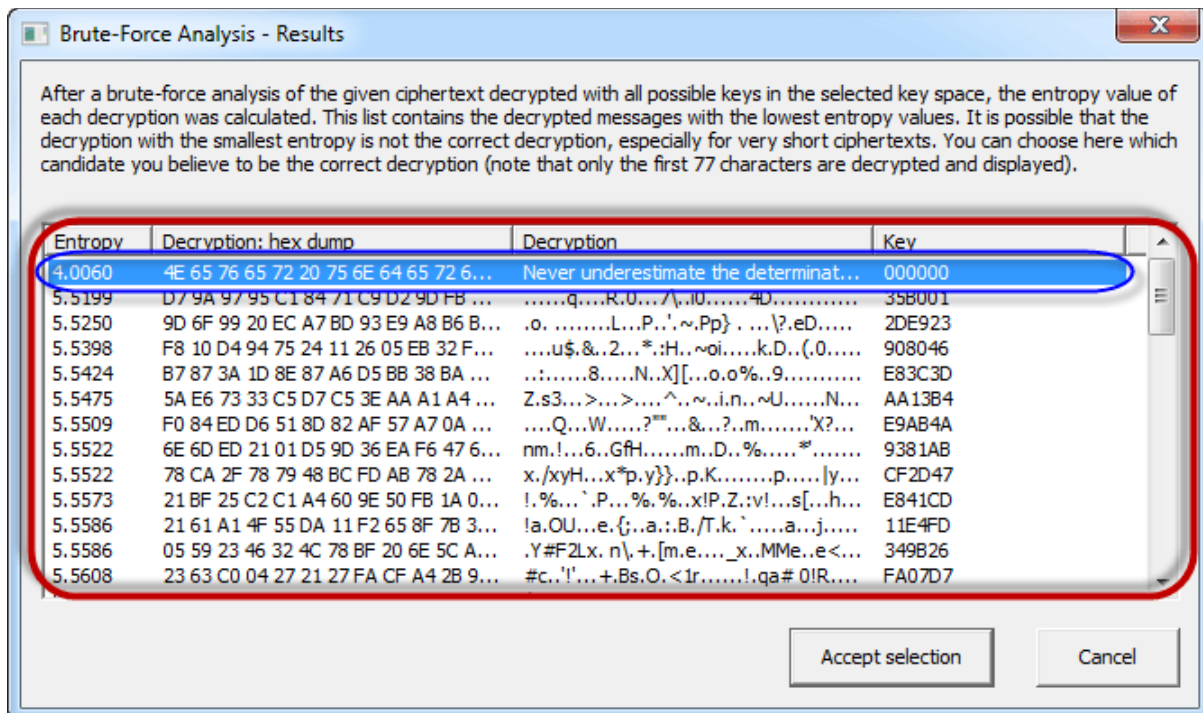


Figure 10: Brute-Force Analysis Results.

- 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

Conclusion

- Cryptography is the science of encrypting and decrypting messages.
- A cipher-text is a message that has been transformed into a non human readable format.
- Decrypting is reversing a cipher-text into its original form.
- Cryptanalysis is the art of decrypting cipheer-text without the knowledge of the key used to encrypt them.
- Cryptology combines the techniques of both cryptography and cryptanalyst.

Credit: The Lab exercises is adapted from Guru 99.