

**Cryptography (CTG)**

Year 1 (2020/21), Semester 2

**SCHOOL OF INFOCOMM TECHNOLOGY**

Diploma in Cyber Security & Digital Forensics

**ASSIGNMENT**

|  |  |
| --- | --- |
| **Tutorial Group:** | **P03** |
| **Tutor:** | **Lei SUN** |
| **Date of Submission:** |  |

| **Student Number** | **Student Name** | **Grade** |
| --- | --- | --- |
| **S10242282** | **Teo Keng Hwee Sherwyn** |  |
| **S10241971K** | **Huang Wen** |  |
| **S10243154** | **Yeung Kai Heng Keiran** |  |
| **S10242175** | **Ernest Lee** |  |

Table of Contents

[1. Introduction 3](#_Toc125481899)

[2. Morse Code 3](#_Toc125481900)

[2.1 Characteristics 3](#_Toc125481901)

[2.2 Detail Operations 4](#_Toc125481902)

[2.3 Purposes 4](#_Toc125481903)

[2.4 Strengths and Weaknesses 5](#_Toc125481904)

[2.4.1 Strengths 5](#_Toc125481905)

[2.4.2 Weaknesses 6](#_Toc125481906)

[2.5 Relevant Information 6](#_Toc125481907)

[3. Rivest Cipher 4 7](#_Toc125481908)

[3.1 Characteristics 7](#_Toc125481909)

[3.2 Detail Operations 7](#_Toc125481910)

[3.3 Purposes 12](#_Toc125481911)

[3.4 Strengths and Weaknesses 13](#_Toc125481912)

[3.4.1 Strength 13](#_Toc125481913)

[3.4.2 Weakness 13](#_Toc125481914)

[3.5 Relevant Information 13](#_Toc125481915)

[4. Conclusion 15](#_Toc125481916)

[References 16](#_Toc125481917)

CTG Assignment 2022

# Introduction

Cryptography is defined as the art of writing and solving codes. The most well-known use is to keep confidential information safe from unauthorized individuals. This is accomplished by concealing the original message, the plaintext, behind a ciphertext that appears illogical but follows a logical algorithm. Rivest Cipher 4 (RC4) would be an illustration of this. However, cryptography can also be used as a method of communication when security is not the main concern. This enables prompt and effective communication in situations where talking or writing is not feasible. This is best illustrated by the well-known Morse code.

# Morse Code

Dots and dashes, also known as dits and dahs, are standardized sequences of two different signal durations that are used in Morse code to represent text characters in communications. Samuel Morse, one of the telegraphy's creators, is honoured by having his invention bear his name.

## Characteristics

Known as dots and dashes, or dits and dahs, Morse code is a sort of classical cipher used in telecommunications to encode letters and numbers as regulated sequences of two different signal durations. Depending on the key used, punctuations can also be encoded as well. The 26 basic Latin letters, from A to Z, and the Arabic numerals, from 0 to 9, are all encoded in international morse code.

No distinction is made between capital and lowercase letters. A series of dits and dahs combine to make each Morse code symbol. The fundamental unit of time measurement in Morse code transmission is the dit duration. A dah lasts for three times as long as a dit does. Each dit or dah in an encoded character is followed by a gap, or period of silence, that lasts the length of the dit. A word's letters are separated from one another by a space that lasts for three dots, and words are separated by a space that lasts for seven dots. Words were separated by a gap equivalent to five dots until 1949.

Morse code can be memorized and transmitted in a way that can be perceived by humans, such as sound waves or visible light so that those who have studied it can decipher it for themselves. On-off keying of an information-carrying medium, such as electrical current, radio waves, visible light, or sound waves, is typically how Morse code is sent. When the dit or dah occurs, the current or wave is there; it is not present between dits and dahs.

The length of each symbol in Morse code is roughly inverse to how frequently the character it represents appears in English-language text, which increases the efficiency of encryption. Thus, the letter E, which is the most frequently used in English, has the shortest code, which is a single dit. The Morse code is often delivered at the greatest pace that the receiver is capable of deciphering because the Morse code elements are specified by proportion rather than precise time periods. The rate of Morse code transmission is measured in groups per minute, often known as words per minute.

Sometimes, when two parties want to communicate with each other using morse code but want to keep the content of their messages private as well, they can come up with their own morse code.

## Detail Operations

The way morse code work is by transmitting electrical signals over a wire laid between stations. In addition to helping invent the telegraph, the Morse code assigned a set of dots and dashes to each letter of the English alphabet and allowed for the simple transmission of complex messages across telegraph lines. To create the encrypted morse code, morse code turns each letter, number, and punctuation into the equivalent set of dits and dahs. The receiver will obtain the ciphertext and use the key to decrypt it in order to obtain the original message.

## Purposes

Morse code became a popularized means of communication in the 1890s. International Morse code today is most popular among amateur radio operators, where it is used as the pattern to key a transmitter on and off in the radio communications mode commonly referred to as "continuous wave" or "CW". The original amateur radio operators used Morse code exclusively, as voice-capable radio transmitters did not become commonly available until around 1920.

Morse code can also be used for communication where the user cannot speak. For example, Denton, who endured almost eight years of gruelling conditions as an American prisoner of war (POW) in North Vietnam in 1965, was forced by his captors to participate in a 1966 televised propaganda interview which was broadcast in the United States. While answering questions and feigning trouble with the blinding television lights, Denton blinked his eyes in Morse code, spelling the word "T-O-R-T-U-R-E" and confirming for the first time to U.S. Naval Intelligence that American POWs were being tortured. Another example would be that in aviation, pilots use radio navigation aids. To ensure that the stations the pilots are using are serviceable, the stations transmit a set of identification letters, usually a two-to-five-letter version of the station name, in Morse code.

Morse code has been employed as an assistive technology, helping people with a variety of disabilities to communicate. Morse can be sent by people with severe motion disabilities if they have some minimal motor control. In some cases, this means alternately blowing into and sucking on a plastic tube, "puff and sip" interface. People with severe motion disabilities in addition to sensory disabilities, such as deafness and blindness, can receive Morse through a skin buzzer. Products are available that allow a computer operating system to be controlled by Morse code, allowing the user access to the Internet and electronic mail.

## Strengths and Weaknesses

### Strengths

First off, using morse code is simple and inexpensive. No flashy, sophisticated hardware is required to encrypt or decrypt messages. Most of the time, just being proficient in it is sufficient to use it effectively. The best that can be done to assist people who are unfamiliar with the cryptography system to utilize it is to create a straightforward gadget that uses the least amount of computer power.

Additionally, transmission channels for messages encoded in morse code, like light, sound, and electrical pulse, are widely available and simple to use. Sending a morse code message can even be done by blinking your eyes. The usage of radios, flashlights and knocking are some of the more popular methods. Thus, even at greater distances, these mediums allow for nearly instantaneous transmission speeds that are difficult to obstruct. This makes it a great option for use in emergency communications, like an SOS signal, enabling the rescuer to act quickly and effectively.

### Weaknesses

Morse code has the drawback that it requires learning before use, not to mention the amount of practice required to utilize it well. This makes learning morse code incredibly time-consuming. Additionally, when encrypting lengthy messages, the ciphertext will be quite long, making its decipherment extremely laborious.

The encryption system lacks a lot of security. It is fairly simple to decipher the encryption using the globally standardized international morse code or by exploiting statistical properties because it was designed with communication in mind rather than security. As a result, it is untrustworthy for use in the encryption of sensitive data. Even if private, one-of-a-kind keys were used in place of the universal ones, they would still need to be exchanged through a secure channel, which would be somewhat inconvenient.

## Relevant Information

The timing reference and determining factor for message transmission speed is the length of the dit. Morse code speed is commonly expressed as "words per minute" (WPM). In standard, full-speed Morse, a dah is typically three times longer than a dit. One dit, three dahs, and seven dits are required to separate dits and dahs inside a character, letters within a word, and words themselves.

According to the Paris standard, the dot-and-dash timing required to convey the word "Paris" a specific number of times per minute represents the pace of Morse transmission. The word Paris is picked because, according to textbook timing, it is exactly 50 "dits". According to this standard, the time for one "dit" can be computed by the formula, *T* = 1200 / *W,* where *W* is the desired speed in words-per-minute, and *T* is one dit-time in milliseconds.

American morse code

A morse code system was created in the United States in the 1830s for electrical telegraphy by American artist and inventor Samuel F.B. Morse who is also known as the twin brother of the international morse code. Morse's partner and assistant, American scientist Alfred Lewis Vail, made more improvements to this version. It was quickly realized that the original Morse Code, which lacked codes for letters with diacritical markings, was insufficient for the transmission of a large amount of non-English text.

# Rivest Cipher 4

Rion Rivest created the Rivest Cipher 4 in 1987, which is known as RC4. Bit by bit, this stream cipher encrypts data. Out of all stream ciphers, it is also the one that is most frequently employed.

## Characteristics

RC4 is a stream cipher in cryptography that employs a symmetric key encryption technique. It is based on the Key Scheduling Algorithm (KSA) and Pseudo-Random Generation algorithm (PRGA), two fundamental mathematical ideas. Although RC4 is notable for its speed and simplicity in software, numerous security flaws have been found in it, making it insecure. It is particularly vulnerable when related or non-random keys are utilized, or when the output keystream's beginning is not discarded. Insecure protocols like WEP have been created as a result of particularly problematic RC4 uses.

As of 2015, there is conjecture that some state cryptologic organizations may be able to crack the TLS protocol's use of RC4 encryption. RFC 7465, published by the IETF, forbids the use of RC4 in TLS; Mozilla and Microsoft have also made suggestions to this effect. RC4 has been strengthened in several ways, most notably by Spritz, RC4A, VMPC, and RC4+.

## Detail Operations

1. User enters plaintext and a secret key.
2. The encryption engine will then use the secret key entered and create a keystream using the KSA (Key scheduling algorithm) and PRGA (Pseudo-random generation) algorithm.
3. Plaintext is then XORed byte by byte using the keystream created to generate the encrypted text.

More detailed version:

1. User enters plaintext and a secret key.
2. Uses an S array of length 256 where S[0]=0 and S[255] =255
3. The key entered would then be encoded using the ASCII table.
   * Key: HI W
   * Encoded with ASCII table: 72 73 32 87
4. The encoded key is then repeated to fill the key array of length 256
   * K[0] = 72
   * K[3] = 87
   * K[7] = 87
5. Key scheduling – to get the key
   * J=0
   * For I = 0 to 255 carry out
   * J=J+ S[I] +T[I] mod 256
   * Swap S[I] and S[J]

For example:

Key: 1 2 3 4

Key-array = [ 1 2 3 4 1 2 3 4]

Plaintext: 1 3 4 5

S-Array length: 8

S-Array: [ 0 1 2 3 4 5 6 7]

J=0

For I =0 to 7, carry out

J=J+ S[I]+K[I]mod8

Swap S[I] AND S[J]

---------------------------------------------------------------

First iteration:

When I = 0

J=0+S[0]+K[0]mod8

J = 0+0+1mod8

J=1

Swap S[0] and S[1]

S-Array = [ 1 0 2 3 4 5 6 7 ]

Second iteration:

When I =1

J=1+0+2mod8

J=3

Swap S[1] and S[3]

S-Array=[ 1 3 2 0 4 5 6 7 ]

Third iteration

When I = 2

J=3+2+3mod8

J=0

Swap S[2] and S[0]

S-Array = [ 2 3 1 0 4 5 6 7 ]

Continue until the length of the s array has been reached, in this case, 7

Then, using the S array generated when I = 7, for the key stream generation

Eg: S -Array = [ 2 3 4 0 6 1 5 7 ]

1. Keystream generation (Pseudo - Random generation)
   * I = J = 0
   * For I = I + 1 to the length of the plaintext
   * J = J + S[I] mod 256
   * Swap S[I] and S[J]
   * T= S[I] +S[J] mod256
   * Keystream = S[T]

Example:

I = J = 0

For I = I + 1 to the length of the plaintext

J= J +S[I] mod 8

Swap S[I] and S[J]

T= S[I] + S[J] mod8

Keystream = S[T]

(using S-Array = [ 2 3 1 0 4 5 6 7] and plaintext of [ 1 3 4 5 ])

First iteration

When I =1

J=J+S[1]mod8

J=0+3

J=3

Swap S[1] and S[3]

S-Array = [ 2 0 1 3 4 5 6 7 ]

T=S[1] + S[3]mod8

T= 0 + 3

T=3

Keystream = S[3]

Keystream = 3

Second iteration

When I =2

J = 3 + 1 mod 8

J = 4

Swap S[2] and S[4]

S-Array = [ 2 0 4 3 1 5 6 7 ]

T= 4+1

T = 5

Keystream = S[5]

Keystream = 5

Third iteration

When I = 3

J = 4 + 3 mod 8

J = 7

Swap S[3] and S[7]

S-array = [ 2 0 4 7 1 5 6 3]

T = 7 + 3 mod 8

T = 2

Keystream = S[2]

Keystream = 4

Repeat this process until the length of the plaintext has been reached, in this case: 7.

Which means to repeat the process one more time to get a Keystream of [ 2 5 4 7]

To encrypt:

PT = [ 1 3 4 5]

KS = [ 2 5 4 7]

CT = PT XOR KS

1. Change both PT AND KS to binary digits.
   * PT=0001 0011 0100 0101
   * KS=0010 0101 0100 0111
2. PT XOR KS (Compare the PT and KS bit by bit ,1 and 0 gives 1 , 1 and 1 gives 0 , 0 and 0 gives 0)
   * CT = 0011 0110 0000 0010
   * CT=3 6 0 2

To decrypt:

CT = [ 3 6 0 2]

KS = [ 2 5 4 7]

PT = CT XOR KS

1. Change both CT AND KS to binary digits.
   * CT=0011 0110 0000 0010
   * KS=0010 0101 0100 0111
2. CT XOR KS
   * PT = 0001 0011 0100 0101
   * PT = 1 3 4 5

## Purposes

RC4 was invented by Ron Rivest in 1987. At first, it was developed as a proprietary algorithm for RSA. RC4 was generally faster and required less computational resources to encrypt large data compared to other encryption algorithms at that time. This gave RSA a huge advantage over other companies such as IBM and Motorola. RC4 was used in Wireless Networks, Virtual Private Networks, Secure Socket Layer and RSA products.

However, in 1994, RC4’s algorithm was leaked onto the internet allowing cryptanalysis to study the algorithm which resulted in finding many vulnerabilities and weaknesses. This resulted in RC4 being deprecated and was recommended not to be used for future applications.

Today, RC4 is rarely used by companies and is only used to maintain legacy systems that still uses it. For example, some older wireless network devices may still use RC4 for encryption of data. RC4 will allow these devices to continue to communicate with each other securely.

## Strengths and Weaknesses

### Strength

Because of its mathematical simplicity, RC4's encryption speed is very quick, making it a high-performance cipher. This also enables it to function quickly and simply with enormous streams of data. RC4 stream ciphers also do not require any additional RAM. As a result, the cryptography system's implementation is straightforward.

### Weakness

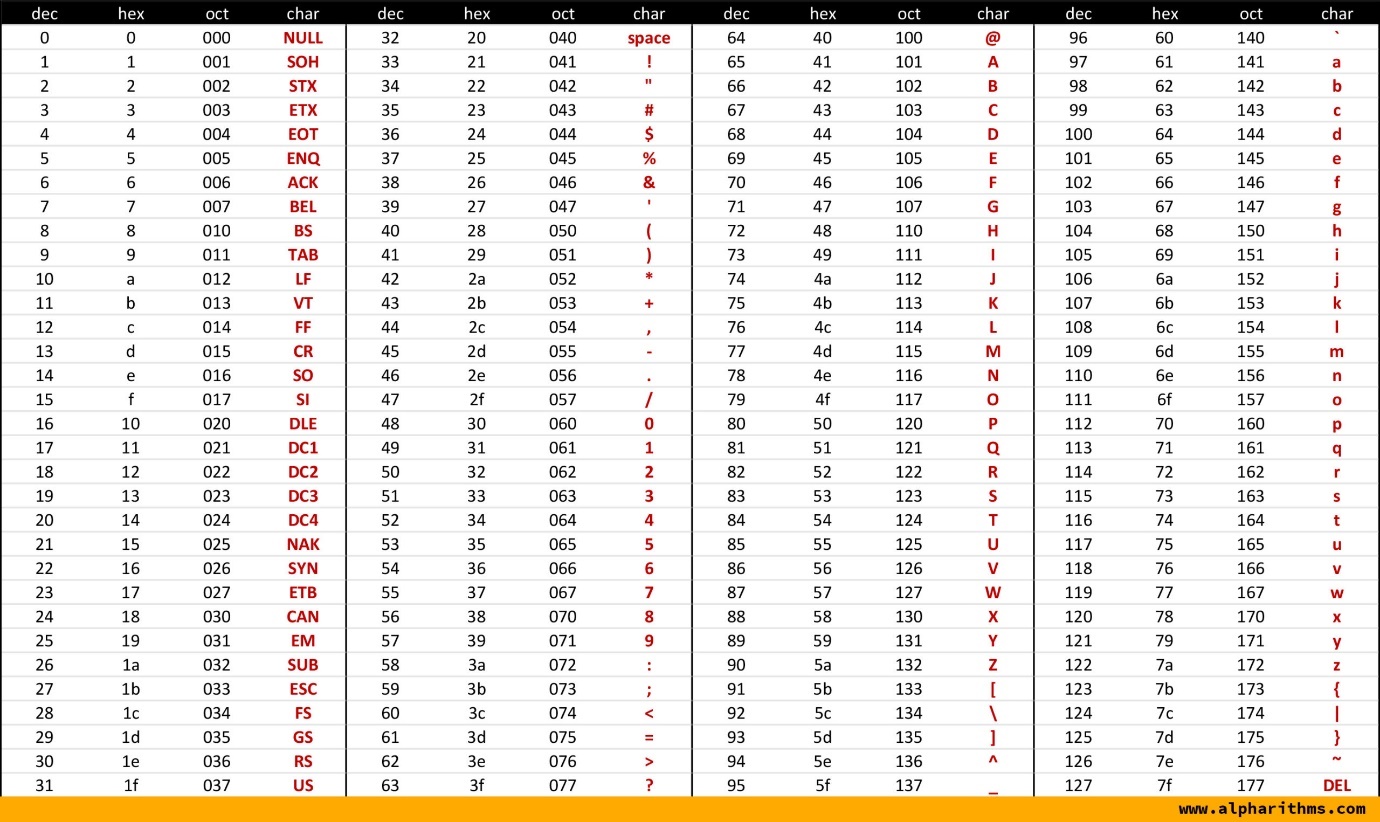
RC4 does not have authentication, making it vulnerable to attacks such as MITM (Men in the middle). It is also weak to bit flipping attack (flipping the binary bit to its opposite, changing the ciphertext). Additionally, it is not suitable for small stream of data as it is too niche. Furthermore, the key for encryption/decryption cannot be used repeatedly as the hacker can decrypt the ciphertext easily once he obtains the key, and it needs a secure platform to give the key to the receiver, to prevent hackers from getting hold of the key. Lastly, it allows remote attackers to exploit the vulnerabilities to obtain private information, making it extremely insecure.

## Relevant Information

Stream cipher is an encryption technique which encrypts the plaintext bit by bit to produce a ciphertext.

* Used in Secure Socket Layer (SSL)
* Transport Layer Security
* IEEE 802.11 wireless LAN standard
* Wi-Fi Security Protocol WEP (Wireless Equivalent Protocol)

Ascii, which stands for American Standard Code for Information Interchange, is a character encoding standard for electronic communication. It converts letters, numbers, control characters, and other symbols to decimal or hexadecimal numbers according to the table below.



XOR

XOR, also known as exclusive or, is a logical operator that is true only if its argument is different.

For example:

1 XOR 2

We convert 1 and 2 into binary values first.

1 à 0001

2 à 0010

The first 2 binary digits of both values is the same, hence the first 2 binary digit of the output will be 0(false). Whereas the last 2 binary values of both digits are different, the last 2 digits of the outcome will be 1(true).

0001 XOR 0010 = 0011

Convert the outcome to denary.

0011 à 3

1 XOR 2 = 3

# Conclusion

In summary, both international morse code and RC4 have benefits and drawbacks. The simplicity and application of Morse code are its strengths. However, due to its ease of deciphering and intercepting, it is mostly employed for communication. The benefits of RC4 are its fast encryption speed and ease of use. However, it has several serious flaws, including a lack of authentication and a vulnerability to bit-flipping attacks. As a result, it is inappropriate for data protection and must be used in tandem with other types of encryption technologies. This paper makes it quite evident that cryptography has a promising future. Cryptography has advanced significantly between the debut of international morse code in 1851 and the development of RC4 in 1987. Cryptography has changed in the past 136 years from being something that even young children could learn with practice to something that, while still simple and unsafe in the field of security, only a specialist with specialized knowledge could expect to understand. Who knows where cryptography will go next? It has advanced beyond data transmission to data protection. There will undoubtedly be extremely sophisticated algorithms developed in the future that significantly outperform our current ones in complexity, as well as maybe novel, creative applications for cryptography. It goes without saying that cryptography is critical to modern society and will be for a long time. In this discipline, there is still plenty to learn and explore.

# 

# References

History.com Editors. (2022, August 12). *Morse Code & the Telegraph*. HISTORY. <https://www.history.com/topics/inventions/telegraph>

*International Morse Code*. (n.d.). Morse Code World. <https://morsecode.world/international/morse2.html>

King, E. (2019, June 2). *Morse code revolutionized communications 175 years ago*. Washington Post. <https://www.washingtonpost.com/health/morse-code-revolutionized-communications-175-years-ago/2019/05/31/08f1a2c0-7cd1-11e9-8ede-f4abf521ef17_story.html>

West, Z. (2022, June 16). *ASCII Table: Printable Reference & Guide*. Αlphαrithms. <https://www.alpharithms.com/ascii-table-512119/>

*Morse Code - New World Encyclopedia*. (n.d.). <https://www.newworldencyclopedia.org/entry/Morse_Code>