LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5009NI Cyber Security in Computing

Assessment Weightage & Type

40% Individual Coursework 01

Year and Semester

2024 -25 Autumn Semester

Student Name: Samrat Regmi

London Met ID: 23047407

College ID: np01nt4a230112

Assignment Due Date: 10 December 2024

Assignment Submission Date: 10 December, 2024

Word Count (Where Required):

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Contents

Table of figures

Table of tables:

1. Introduction to cryptography:

Cryptography is the method of safeguarding communication and information by encoding messages so that only the intended recipient can read or interpret them. Cryptography transforms message into unreadable format that can only be decrypted by intended user. Even though, modern cryptography has grown significantly over time, the general idea remains same. It focuses on four main principles i.e. Confidentiality, Integrity, Non-repudiation and Authentication. (beal, 2024) It combines various disciplines like engineering, computer science and mathematics to create complex code.

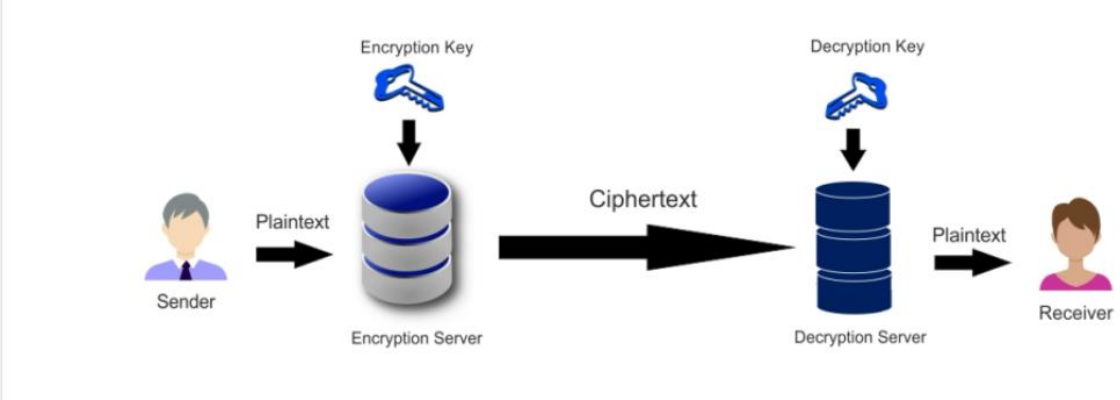

Figure 1: Mechanism of cryptography

(linn, 2023)

1.1 Key Terminologies used in cryptography:

Private key: A key that is used to encrypt and decrypt data.

Plain text: It is original, unencrypted message that you want to protect through encryption. This is the text in readable format.

Cipher text: The text which is obtained after applying encryption to plain text using a cipher. It is encoded message in unreadable format.

Encryption: It is the process of encrypting plain text using cipher. Only those persons who has access can decipher can access the original plaintext information.

Decryption: It is the process of converting plain text into cipher text. A key is generated during encryption process so that the reader can decipher the encrypted text.

1.2 History of cryptography:

Cryptography has progressed from basic ciphers in earlier times to sophisticated encryption methods today, fueled by technological advancements and human creativity. In ancient times, cryptography was employed as a method of communication between military leaders during wartime. Around 50 BC, Julius Caesar created his own cipher, which involved shifting each letter of a message by a set number of positions down the alphabet. (Feder, 2023) In 1500s, this Italian scholar Giovan Battista Bellaso invented the seed of encryption key. This key would be shared between two individuals, and with it they would be able to send messages to each other without secret third parties being able to eavesdrop. The actress Hedy Lamarr, during World War II, assisted in the development of a radio communication system that would avoid enemy detection, which would go on to be the basis for things like Wi-Fi and Bluetooth. By the 1970s, the digital industry was growing rapidly, and cryptography became a priority for major companies. IBM formed a crypto group to develop block cipher to protect IBM customer data. Today AES is the most widely used encryption method, using linked public and private keys to secure data. (Beal, 2024)

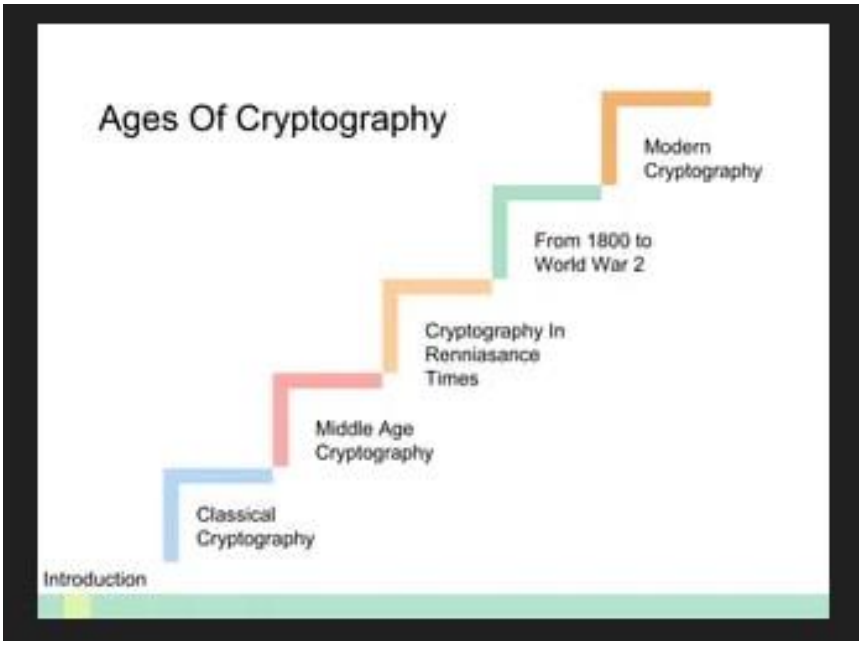

Figure 2: History of cryptography

1.3 Types of Cryptography:

There are two main types of cryptography. Both keys are used to encrypt and decrypt data which are sent and received.

1. **Symmetric cryptography:**

   Symmetric key cryptography utilizes one key to encrypt or decrypt data. Sender and receiver use the same secret key in symmetric cryptography to encrypt and decrypt the message. Symmetric Key cryptography is quick and easiest but the issue is that the sender and receiver need to share keys securely in some way.

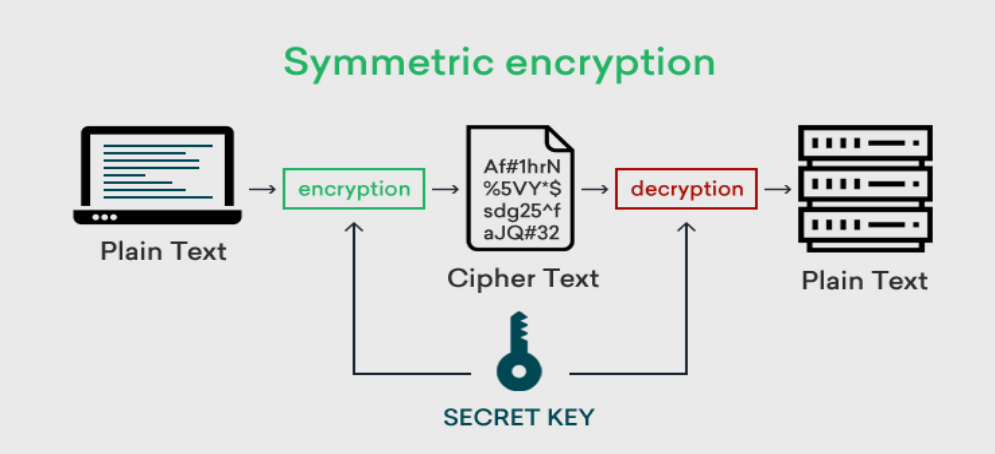

Figure 3: Symmetric Encryption

2. **Asymmetric cryptography:**

In asymmetric cryptography a pair of keys is used to encrypt and decrypt information. It relies on a single private key and a single public key. The sender's public key is used to encrypt the message, while the receiver's private key is used to decrypt it. The intended receiver is the only one who can decrypt the message because they are the only ones with the private key. Public key cryptography allows secure key exchange over an untrusted network without needing to share a secret key. This is because the public key is only used for encryption, not decryption.

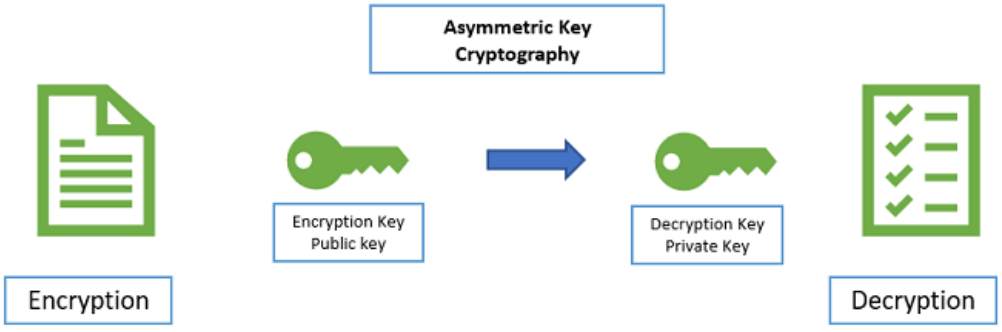

Figure 4: Asymmetric encryption

1.4 Aims and Objective

Aim

- The goal of this project is to create an improved version of the classic Caesar cipher by introducing a more diverse character set.

Objective

- To Enhance Caesar Cipher
- To implement new Mathematical Framework
- To compare new and old cipher performance

2. Introduction to Caesar cipher:

Caesar cipher was first introduced in the year 58 BCE by Julius Cesar. It is one of simplest and oldest methods of encrypting messages. The Caesar cipher is based on shifting each letter of plaintext message by a certain number of letter which is also said key. (Wickramasinghe, 2024) For example, with a shift of two, letter ‘A’ becomes ‘C’, ‘B’ becomes ‘D’ and so on. (Andress, 2014) The Cipher text can be decrypted by applying same number of shifts in opposite direction. This type of encryption is also known as substitution cypher due to substitution of one letter for another. The algorithm of Caesar cipher can be expressed as:

$$C = (P+K) \bmod 26$$

Where **P** = Plaintext letter, **C** = cipher text letter and **K** = range

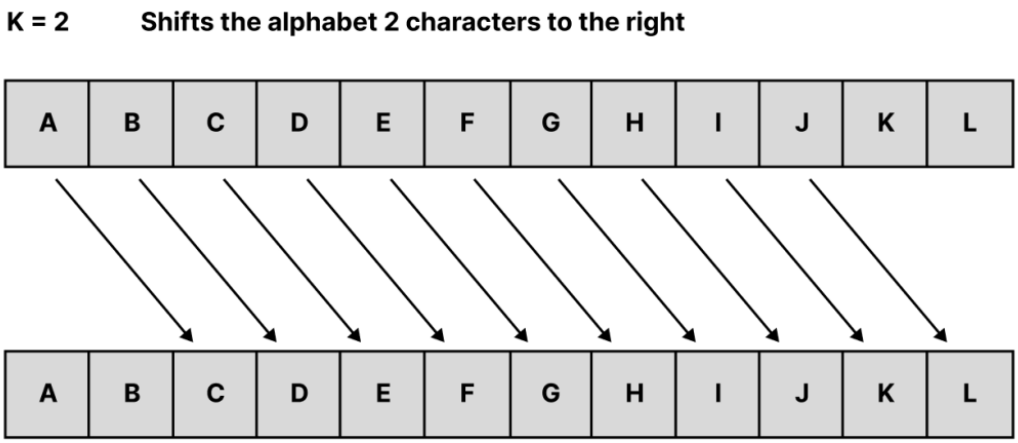

Figure 5: Caesar cipher with shift 2

2.1 Advantages of Caesar cipher:

- It is very easy for new users to implement
- Due to simplicity, encryption and decryption can be done quickly.
- Requires only a small set of information

2.2 Disadvantages of Caesar cipher:

- It is not secure as compared to modern decryption methods.
- It is not suitable for long text encryption as it is easy to crack.
- Doesn't fulfil security triad i.e. Confidentiality, integrity and availability.

3. Development of new Caesar cipher:

For my new Ceaser cipher it contains more letters. Previously it contained alphabetical letter from a-z. For my new cipher, A = 0, B= 1, C= 2 …… '.' = 26, '_' = 27, '&' = 28, '* '= 29, '+' = 30, '- '= 31 and contained a certain shift. Now, I am introducing the shift

according to the characters. The characters are classified into 3 groups and are assigned with different shifts each.

Now, the mathematical equation for encryption is C = (x.a + k) mod 32. Where x = Position of the alphabet, K is the shift value and a is the multiplicative key we decide. For the decryption process D = a^{-1} * (y – k) mod 32. Where a^{-1} is modulus inverse of 32. K is shift value and y is position of ciphertext.

A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9	K 10	L 11	M 12	N 13	O 14	P 15
Q 16	R 17	S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25	. 26	_ 27	& 28	* 29	+ 30	- 31

Table 1 Variables:

For my new development I am assigning different shift for each variable. I am categorizing variable into 4 different groups.

3.1 Group 1: Shift 2

Variables included in this group are:

A, G, H, K, O, S, W, V, _, +

A 0	G 6	H 7	K 10	O 14
S 18	W 22	V 21	_ 27	+ 30

Table 2: Characters having shift 2

3.2 Group 2: Shift 5

Variables included in this group are:

B, D, F, J, N, Q, R, X, Y, &

B 1	D 3	F 5	J 9	N 13
Q 16	R 17	X 23	Y 24	& 28

Table 3: Characters having shift 5

3.3 Group 3: Shift 7

Variable included in this group are:

C, E, I, L, M, P, T, U, Z, * , ., -

C 2	E 4	I 8	L 11	M 12	P 15
T 19	U 20	Z 25	* 29	. 26	- 31

Table 4: Characters having shift 7

Now the shift will occur according to the variable. If character is in the set of shift 2, apply a shift of 2. If character is in the set of shift 5, apply a shift of 5 and if the character is in the set of shift 7, apply a shift of 7.

Mathematical equation for encryption:

$C = (x*a + k) \bmod 32.$

Where, k = shift key

Mathematical equation for decryption:

$D = a^{-1} * (y – k) \bmod 32$

Algorithm for Encryption:

Step 1: Decide the plaintext you want to decrypt.

Step 2: For each plaintext, determine its position x in character set.

Step 3: Find the corresponding shift k based on the character's group.

Step 4: Use the encryption formula **C = (x*a + k) mod 32** to compute the ciphertext character

Step 4: Replace plaintext character with resulting cipher text character.

Algorithm for Decryption:

Step 1: For each character determine the position from character set.

Step 2: Identify shift based on characters' group.

Step 3: Compute a^{-1}, the modular inverse using the formula:

Step 4: Apply the decryption formula **D = a^{-1} * (y – k) mod 32** to computer plaintext character.

Step 5: Replace the cipher text character with resulting plain text character.

4.Bibliography

Andress, J., 2014. Chapter 5 - Cryptography. In: J. Andress, ed. *The Basics of Information Security (Second Edition).* s.l.:s.n., pp. 69-88.

beal, V., 2024. *webopedia.* [Online]
Available at: https://www.webopedia.com/definitions/cryptography/
[Accessed 8 12 2024].

Beal, V., 2024. *webopedia.* [Online]
Available at: https://www.webopedia.com/definitions/cryptography/
[Accessed 8 12 2024].

Feder, M., 2023. *University of Phoenix.* [Online]
Available at: https://www.phoenix.edu/blog/what-is-cryptography.html
[Accessed 8 12 2024].

linn, r., 2023. *Headend Techs.* [Online]
Available at: https://headendinfo.com/what-is-cryptography/
[Accessed 9 12 2024].

Wickramasinghe, S., 2024. *Spunk Blogs.* [Online]
Available at: https://www.splunk.com/en_us/blog/learn/caesar-cipher.html
[Accessed 9 12 2024].