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: Anshumala Bhandari

London Met ID: 23047472

College ID: NP01NT4A230149

Assignment Due Date: 10th December, 2024

Assignment Submission Date: 10th December, 2024

Word Count (Where Required):2725

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.

1. Introduction

Security

Security is defined as the protection of systems, networks, and data from harmful activities such as cyber-attacks, theft, and unauthorized access. It's important for ensuring that sensitive information is kept safe from being altered, lost, or exposed to the wrong people. Effective security practices are important to maintain the confidentiality, integrity, and availability of information. For example, encryption ensures that sensitive data can only be accessed by authorized individuals, while firewalls protect networks from unauthorized access security is crucial for maintaining trust, especially in digital environments where threats are constantly evolving. (Cybersecurity & Infrastructure Security Agency (CISA), 2023).

CIA Triad and Its Role in Information Security

The **CIA Triad** is a essential concept in information security as it represents three core principles:

1. **Confidentiality**: It makes sure that sensitive information is accessible only to the people who have the proper authorization. It prevents unauthorized individuals from gaining access to confidential data.
2. **Integrity**: It ensures that the data must be accurate and unchanged. Integrity helps to prevent unauthorized modifications to data, to make sure that it remains trustworthy.
3. **Availability**: It Refers to making sure that information is accessible and usable by authorized individuals when needed. Availability makes sure that data is not lost or inaccessible, even when a cyber-attack occurs.

These three principles are essential because they help to establish how data should be protected and accessed, making them the foundation for effective information security strategies (IBM, 2023).

Cryptography

Cryptography is the practice of making communication secure by turning readable data into an unreadable format. This transformation is done through encryption algorithms, which only authorized parties can decrypt using a special key. Cryptography is essential in today's digital world for protecting sensitive information like passwords, credit card numbers, and private communications. It ensures that only those who have the proper key can access encrypted data, making it impossible for hackers to decipher without authorization. Cryptography is used widely in online banking, secure messaging, and data storage.

(TechTarget, 2023).

Key Terminologies in Cryptography

Here are some important terms in cryptography that help us understand how data protection works:

1. **Encryption**: The process of converting readable data into an unreadable format to protect it from unauthorized access.
2. **Decryption**: The opposite of encryption, It converts unreadable data back into a readable format using a secret key.
3. **Key**: A piece of information used in encryption or decryption to convert data into a secure form or back into a readable form.
4. **Cipher**: An algorithm used to perform encryption or decryption. It defines the process for transforming data.
5. **Hash Function**: A method of converting data into a fixed-size value (hash) that is used to verify the integrity of the data without revealing the original data.

These terms show how cryptography is used to maintain data security, especially in securing communications and preventing unauthorized access (National Institute of Standards and Technology (NIST), 2022).

The History of Cryptography

Cryptography has a long history that dates back to ancient civilizations. Cryptography was firstly used by the Egyptians around 1900 BCE, who used simple substitution ciphers to protect their messages. In the 20th century, cryptography gained widespread importance, especially during World War II, with devices like the German Enigma machine playing a important role in securing military communications.

Today, cryptography is essential in the digital world, ensuring the security of everything as it makes online shopping and email exchanges secure. The evolution of cryptography has helped to protect the privacy of individuals and organizations, and its role has grown as digital technologies have become advanced. From hand-written ciphers to modern-day encryption algorithms, cryptography continues to evolve to meet the demands of the digital age.

(Kahn, 1996).

Symmetric and Asymmetric Encryption

1. **Symmetric Encryption**: In symmetric encryption, the same key is used for both encryption and decryption. It's fast and efficient, making it ideal for encrypting large amounts of data. However, the major challenge is securely exchanging the key between parties. If an attacker finds out the key, they could decrypt the data. A popular example is **AES** (Advanced Encryption Standard)it is widely used to secure data in many systems (Schneier, 2015).
2. **Asymmetric Encryption**: Unlike symmetric encryption, asymmetric encryption uses two keys: a public key and a private key. The public key encrypts the data, while only the private key can decrypt it. This makes asymmetric encryption more secure because the private key never needs to be shared. While it is slower than symmetric encryption, it provides better security for applications like digital signatures and secure communication **RSA** is a commonly used example of asymmetric encryption Both types of encryption are essential for ensuring data

security. While symmetric encryption is faster and more efficient, asymmetric encryption offers better security for key exchanges and digital signatures (Stallings, 2006).

This report explains cryptography, its history, and how it is used to secure data. It starts with a simple overview of cryptography's evolution, followed by a discussion of the two main encryption methods: symmetric and asymmetric encryption. Finally, it includes the development, testing, and evaluation of a new cryptographic algorithm, focusing on its practical applications.

1.2Aim

The aim of this coursework is to gain a deeper understanding of cryptography, its role in securing digital information, and the different encryption methods that are commonly used to protect sensitive data in modern systems.

1.3 Objectives

1. To explore the history of cryptography and how it has evolved over time.
2. To examine the two main types of encryption methods, symmetric and asymmetric encryption, and understand their advantages and limitations.
3. To design and develop a simple cryptographic algorithm to encrypt and decrypt data securely.
4. To test the performance of the newly developed algorithm and evaluate its effectiveness in real-world applications like data security and digital communication.

2. Background

Background on Caesar Cipher

The Caesar Cipher is one of the simplest and oldest encryption techniques used in cryptography. It is a type of substitution cipher, where each letter in the plaintext is shifted by a fixed number of positions in the alphabet. This method is named after Julius Caesar, who reportedly used it to protect his personal messages (Kahn, 1996). Although it is a very basic encryption technique, it played a significant role in the early history of cryptography, serving as a foundation for more complex algorithms used today (Schneier, 2015).

The Caesar Cipher works by replacing each letter of the plaintext with a letter a fixed number of positions down or up the alphabet. For example, if the shift is 3, then "A" becomes "D," "B" becomes "E," and so on. The same process is applied to every letter of the message, making the text unreadable to anyone who does not know the shift value, which is called the "key" (Stallings, 2006).

Advantages of the Caesar Cipher

The Caesar Cipher has several advantages, including its simplicity and ease of use. It is fast and requires minimal system resources, making it ideal to use in environments where efficiency is important (TechTarget, 2023). And it is also straightforward to implement in a variety of programming languages, which makes it accessible even to beginners in cryptography (Stallings, 2006).

Disadvantages of the Caesar Cipher

Despite its historical importance, the Caesar Cipher has significant weaknesses. The most notable con is its vulnerability to brute-force attacks. Since there are only 25 possible shifts (in an alphabet of 26 letters), an attacker can easily try all possible shifts to decrypt the message. Additionally, because the cipher is based on a simple substitution method, it is prone to frequency analysis, where patterns in the ciphertext can be analyzed to determine the shift value and break the encryption (Schneier, 2015).

In conclusion, while the Caesar Cipher is an important historical encryption method, it is not secure by modern standards and is rarely used for protecting sensitive information today. However, its simplicity makes it a valuable tool for understanding the basic principles of encryption (Kahn, 1996).

An example to Encrypt and Decrypt a message using Caesar Cipher:

Let's use the **Caesar Cipher** with a shift of **3** to encrypt and decrypt the message "ORANGE."

1. **Encryption Process:**

   Plaintext: "ORANGE"

   Shift Value: 3

   Encryption: Each letter is shifted three positions forward in the alphabet.

   - O → R
   - R → U
   - A → D
   - N → Q
   - G → J
   - E → H

   Ciphertext: "RUDQJH"

   So, the word "ORANGE" is encrypted using the Caesar Cipher with a shift of 3 and it becomes **"RUDQJH"**.

2. **Decryption Process:**

   Ciphertext: "RUDQJH"

   Shift Value: 3

Decryption: To decrypt, each letter is shifted three positions backward in the alphabet.

- R → O
- U → R
- D → A
- Q → N
- J → G
- H → E

Plaintext: "ORANGE"

Thus, the decrypted message is **"ORANGE"**.

This example explains how the Caesar Cipher works using a shift of 3 on the word "ORANGE" (Stallings, 2006).

2. Development

Modifications that can be made in Caesar Cipher:

To improve the security of the Caesar Cipher, several modifications can be made. One effective approach is using **polyalphabetic substitution**, where multiple alphabets are used instead of a single one. This method is seen in the **Vigenère Cipher**, It helps to prevent frequency analysis because the same letter in the plaintext maps to different letters in the ciphertext based on a repeating key (CaesarCipher.net, 2024). Another modification is combining substitution with permutation. For example, modern algorithms like **AES** use **substitution-permutation networks** to add layers of complexity, making the encryption stronger. This approach rearranges and substitutes characters systematically, making it harder to identify the patterns.Adding a **random key** and **encryption process** is also essential. It avoids predictable patterns, which are a common vulnerability in simple ciphers like Caesar. Techniques from classical cryptography, such as the mechanical complexity of the **Enigma machine**, can also inspire more secure designs ((NIST), 2024).

These changes make the cipher more secure than the traditional methods while maintaining efficiency.

A new encryption and decryption algorithm inspired by the Caesar Cipher. This algorithm introduces a new pattern using the word "violet."

Encryption Process:

Let's take the word violet.

Create the Shift Key:

Instead of using a fixed number for the shift, the algorithm uses a dynamic shift based on the sum of the positions of the letters in the word.

For "violet":

'v' is the 22nd letter of the alphabet.

'i' is the 9th letter.

'o' is the 15th letter.

'l' is the 12th letter.

'e' is the 5th letter.

't' is the 20th letter.

Sum of positions: 22 + 9 + 15 + 12 + 5 + 20 = 83.

Use modulo 26 to keep the shift within a smaller range: 83 divided by 26 leaves a remainder of 5.

Apply the Shift:

Now, shift each letter of "violet" by 5 positions in the alphabet:

'v' → 'a' (22 + 5 = 27 → loop around: 27 - 26 = 1 → 'a')

'i' → 'n' (9 + 5 = 14 → 'n')

'o' → 't' (15 + 5 = 20 → 't')

'l' → 'q' (12 + 5 = 17 → 'q')

'e' → 'j' (5 + 5 = 10 → 'j')

't' → 'y' (20 + 5 = 25 → 'y')

Encrypted Word: "antqjy"

Decryption Process:

decrypt the encrypted word "antqjy":

Using the Same Key: The key is the shift of 5, calculated before

Applying the Reverse Shift:

Reversing the shift by moving each letter backwards by 5 positions:

'a' → 'v' (1 - 5 = -4 → loop around: -4 + 26 = 22 → 'v')

'n' → 'i' (14 - 5 = 9 → 'i')

't' → 'o' (20 - 5 = 15 → 'o')

'q' → 'l' (17 - 5 = 12 → 'l')

'j' → 'e' (10 - 5 = 5 → 'e')

'y' → 't' (25 - 5 = 20 → 't')

Decrypted Word: "violet"

This encryption method is better than the traditional Caesar Cipher as it introduces a variable shift, which makes it harder to break using simple frequency analysis. Instead of using a fixed number (like the classic Caesar shift of 3), this algorithm calculates a dynamic shift based on the positions of the letters in the word itself.

The shift for each word is unique, based on the sum of the positions of the letters in that word. This makes the algorithm more flexible and less predictable. The use of modulo 26 makes sure that the shift stays within the bounds of the alphabet, even when the sum is larger than 26.

Encryption: The shift is calculated based on the sum of the letter positions in the word. Each letter is shifted forward by the corresponding value.

Decryption: The reverse shift is applied to get the original word.

This method creates a more complex encryption than the traditional Caesar Cipher while keeping the process simpler to execute.

The name for my new cryptographic algorithm is **"Violet Shift Cipher"**.

Why was the modification necessary?

The modification was necessary because traditional encryption methods like the Caesar Cipher are too simple and can be easily broken. One way to break them is through frequency analysis, where an attacker looks at how often certain letters show up in the encrypted message. Since the Caesar Cipher uses a fixed shift, it's easy for an attacker to figure out the pattern and break the code (Encyclopedia Britannica, Inc., 2024).

To make the encryption more secure and harder to predict, this new method uses a dynamic shift. Instead of using the same fixed number to shift the letters, the shift is based on the letters in the word itself. This makes each encryption different, even if the same word is used, and it’s much harder for someone to crack the code (Khan Academy, 2024).

By changing the encryption process to use a unique shift for each word, we make it much stronger than the traditional Caesar Cipher (Stallings, 2017).

The New Methodology Implied

The new methodology for this cryptographic algorithm introduces a dynamic shift system instead of a fixed one, inspired by the Caesar Cipher. Here’s how it works:

1. **Dynamic Key Generation**:
    - Traditional methods like the Caesar Cipher rely on a constant shift (e.g., +3 for all letters). While the new method calculates the shift based on the sum of the positional values of the letters in the word being encrypted.
    - Example: For the word "violet," the sum of the letter positions (v=22, i=9, o=15, etc.) it generates a unique shift key.
2. **Uniqueness for Every Input**:
    - Since the shift key depends on the letters of the input word, every word has its own unique encryption, even if the same word is used repeatedly.
3. **Improved Security**:

- By eliminating the predictability of a constant shift, this way makes it much harder for attackers to decode messages using traditional methods like frequency analysis.
- The unique key generation for each word prevents attackers from finding out patterns within the repeated text.

4. **Backward Compatibility:**
    - This method is based on the simple Caesar Cipher but includes extra features to make it more secure against hacking attempts.

The Encryption Algorithm

Step 1: Write down the word to encrypt.

Step 2: Identify the position of each letter in the alphabet (A=1, B=2, ..., Z=26).

Step 3: Add up the letter positions to get the total.

Step 4: Divide the total by 26 and note the remainder; this is the shift key.

Step 5: Shift each letter forward by the shift key number.

Step 6: If a letter goes past "Z," restart at "A."

Step 7: Write down each new shifted letter.

Step 8: Check if the new word is correct.

Step 9: Make sure every letter was shifted correctly.

Step 10: Finalize the encrypted word.

The Decryption Algorithm

Step 1: Start with the encrypted word.

Step 2: Identify the same shift key used for encryption.

Step 3: Calculate the total of the original letter positions.

Step 4: Divide by 26 and find the remainder for the shift key.

Step 5: Shift each encrypted letter backward by the shift key number.

Step 6: If a letter goes before "A," loop back to "Z."

Step 7: Write the original letter after shifting back.

Step 8: Double-check the shifted letters.

Step 9: Ensure the decrypted word matches the original word.

Step 10: Finalize the decrypted word.

Flowchart

For encryption process:

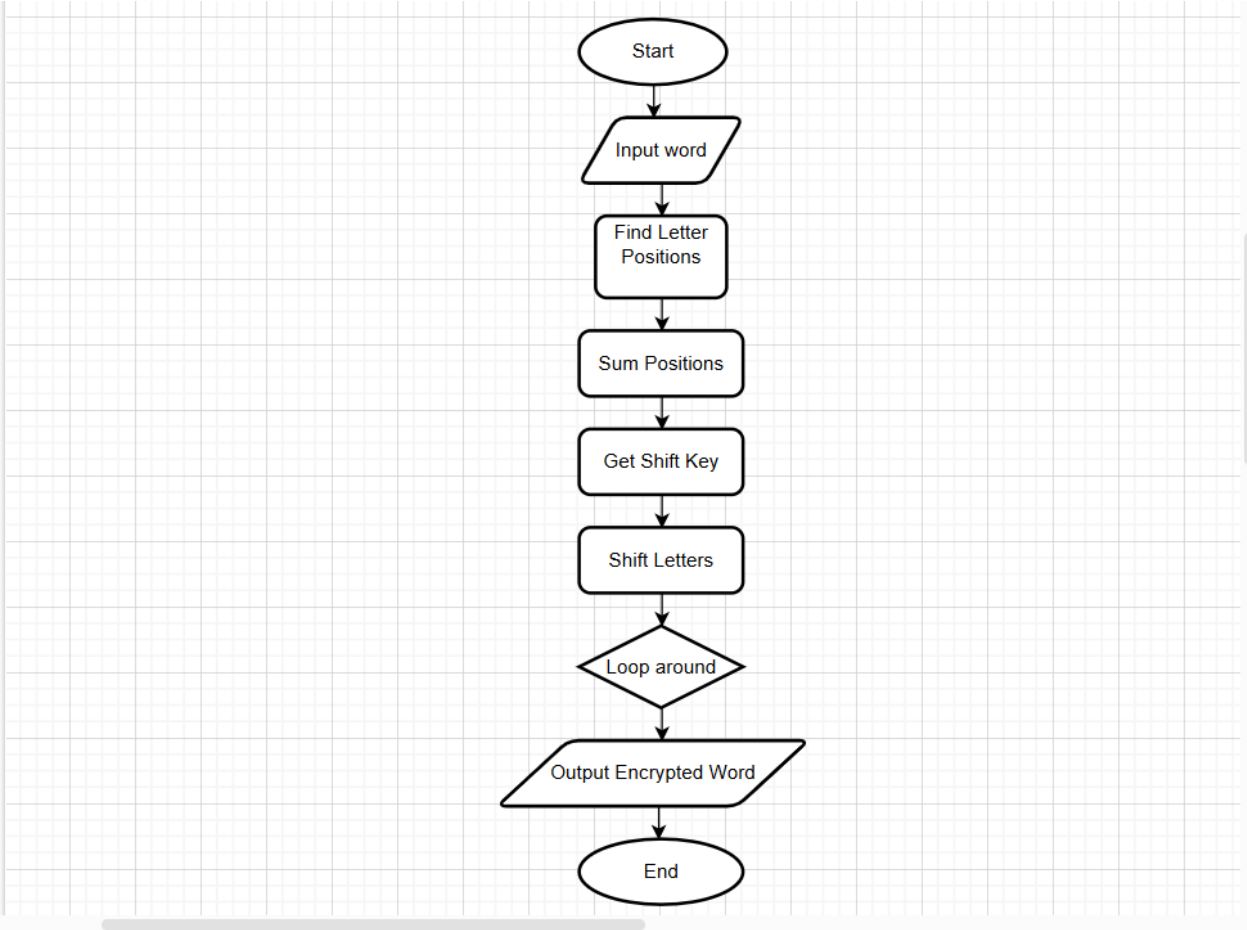

Figure 1:Flowchart for encryption process

For decryption Process:

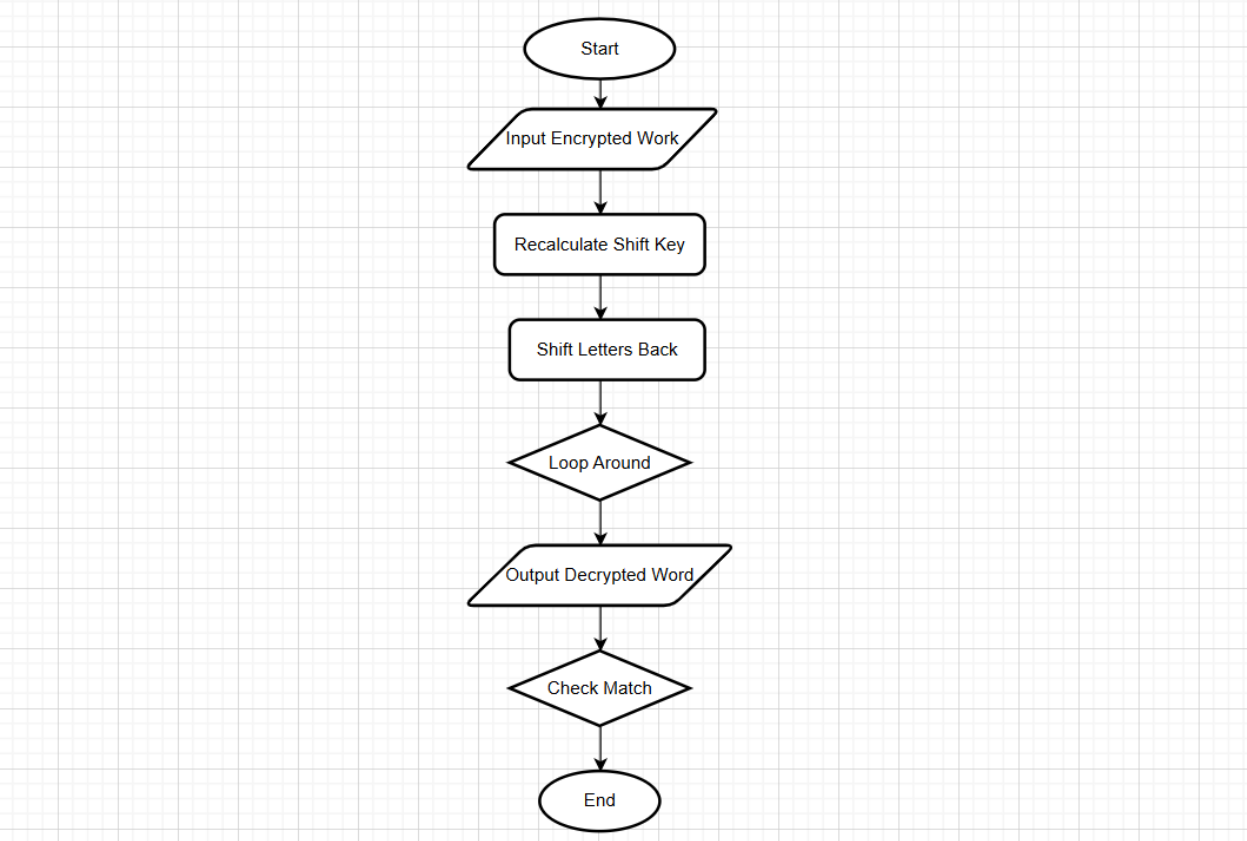

Figure 2:Flowchart for decryption process