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: 20h January, 2024

Assignment Submission Date: 19th January, 2024

Word Count (Where Required):4266

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.

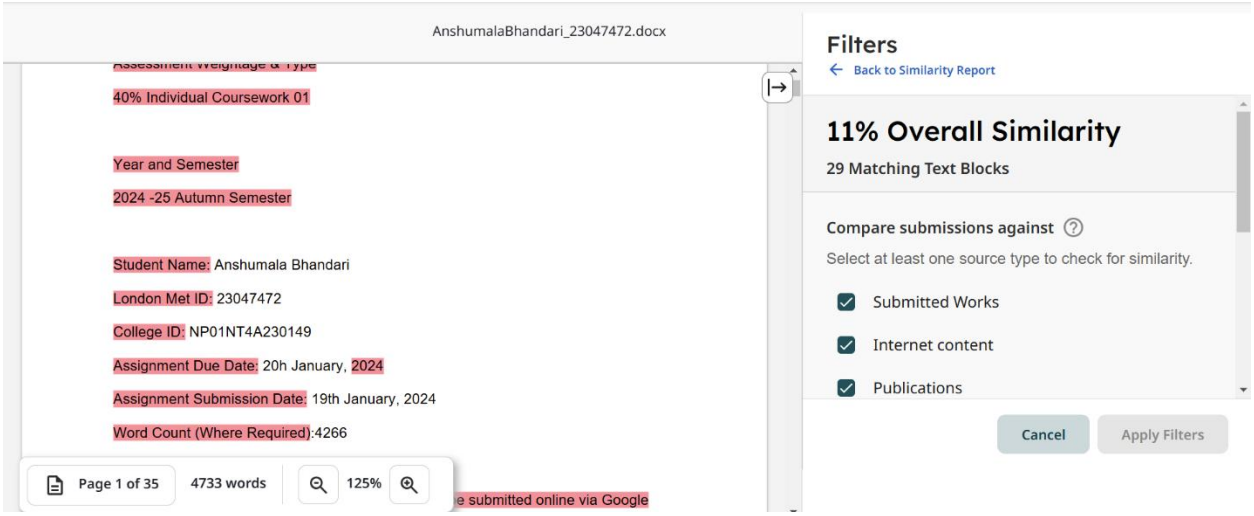
Acknowledgement

I fully express my gratitude that I have got the opportunity to work my way through this coursework. Those who supported me while completing this project on cryptography made this process a lot easier for me.

I am deeply thankful to my teacher for their guidance and valuable feedback they provided me throughout the project. Their knowledge and encouragement helped me understand the concepts of cryptography and implement them effectively.

I also would like to mention appreciation to my classmates and friends who guided me and my closed ones, who supported me and motivated me throughout the completion of this work.

Finally, I acknowledge the resources and references that have contributed hugely to the successful completion of this project. Thank you to everyone who made this journey informational and rewarding.


AnshumalaBhandari_23047472.docx
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: 20h January, 2024
Assignment Submission Date: 19th January, 2024
Word Count (Where Required):4266
Page 1 of 35
4733 words
125%
e submitted online via Google
Filters
Back to Similarity Report
11% Overall Similarity
29 Matching Text Blocks
Compare submissions against
Select at least one source type to check for similarity.
Submitted Works
Internet content
Publications
Cancel
Apply Filters

Abstract

The project has included a good understanding and exploration of cryptography, which is a method used to protect information by turning it into a code. As online security threats increase, learning how to secure data is important. This project focuses on encryption, which helps to protect data that is sensitive by making it encrypted and unreadable to users that are unauthorized.

The main problem solved in this project is understanding how encryption works and how it can be applied to secure messages. I tested different encryption methods, including a custom one, to see how they protect data.

In this project, I learned about basic encryption methods, created a simple encryption algorithm, and tested it to make sure it could keep data safe. After completing the project, I found that encryption is an effective way to protect information, but more advanced methods are needed for stronger security.

This project is important because it helps to improve understanding of encryption and how it helps in securing and protecting data, which is critical in today's world where cyber threats are very common.

Table of Contents

Table Of Figures

List Of Tables

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 has made sure that sensitive data only gets 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** has been an essential idea in information security as it showcases three principles:

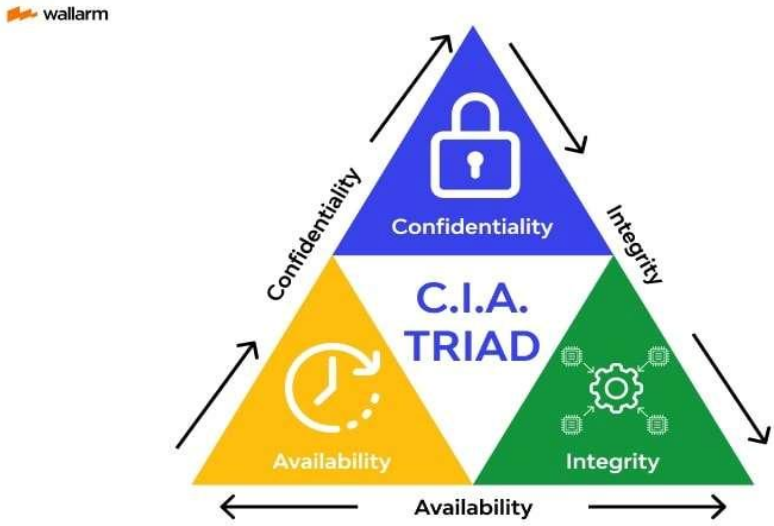


Figure 1:CIA Triad

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 can only be accessed and used by authorized individuals when it is 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 involves the practice of making communication secure by turning data that is readable into an unreadable format. This transformation is done through encryption algorithms, which only authorized parties can decrypt using a special key. Cryptography is very important essential in today's digital world for keeping sensitive information like passwords, credit card numbers, and private communications protected. It makes sure that only those who have the proper key can get the access to 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).

Figure 2:Cryptography

Key Terminologies in Cryptography

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

1. **Encryption**: The process of turning readable information into a scrambled format to prevent unauthorized access and keep it safe.
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 technique for turning data into a unique, fixed-size value (called a hash) that helps to check if the data has been altered, without showing the original information.

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's history has been very long even back to the 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 to both scramble and unscramble the data. It's quick and works well for encrypting large volumes of information. The main difficulty, though, is making sure that the key is exchanged safely. 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).

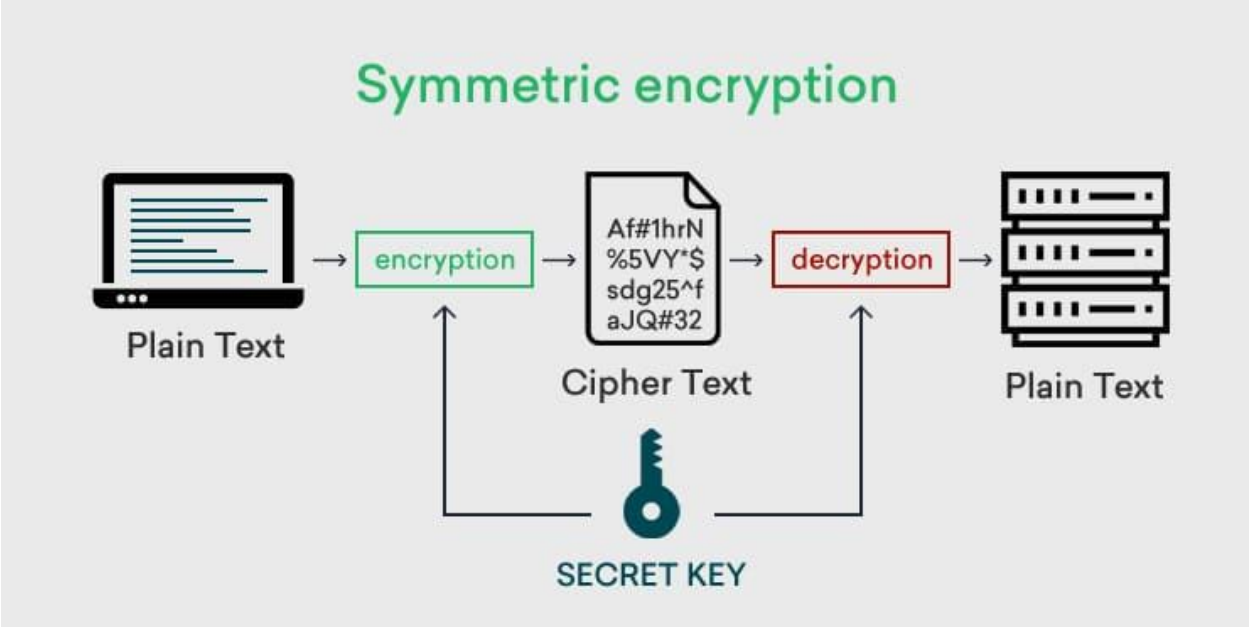


Figure 3:Symmetric Encryption

2. **Asymmetric Encryption**: Unlike symmetric encryption, asymmetric encryption includes 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 should not need 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 important for making sure that data is protected. While symmetric encryption is faster and more efficient, asymmetric encryption offers better security for key exchanges and digital signatures (Stallings, 2006).

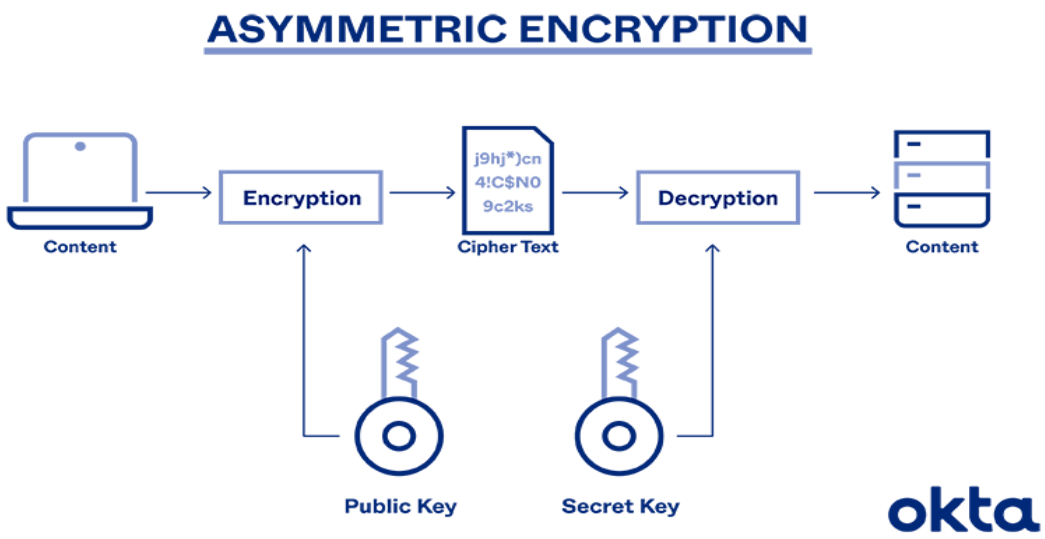


Figure 4:Asymmetric Encryption

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 used most of the time 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 earliest and simplest encryption methods in cryptography. It works by replacing each letter in the original message with another letter that is a set number of places down 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 shifting each letter of the message a certain number of places forward or backward in the alphabet. For instance, if the shift is 3, "A" becomes "D," "B" turns into "E," and so on. This process is repeated for every letter in the message, making it unreadable to anyone who doesn't know the shift number, which is called the "key" (Stallings, 2006).

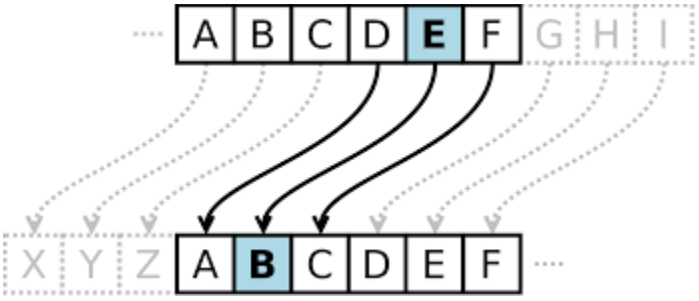


Figure 5:Caesar Cipher

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. One of the weaknesses of the Caesar Cipher is its vulnerability to brute-force attacks. Since there are only 25 possible shifts in a 26-letter alphabet, an attacker can quickly test all the possible shifts to decode 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).

To sum up, although the Caesar Cipher is a significant encryption technique from history, 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:

We are now using the **Caesar Cipher** which shifts by the number **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).

3. 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." The values of the alphabets start's from 1 to 26; a=1, b=2……z=26 (in this format)

A = 1	N = 14
B = 2	O = 15
C = 3	P = 16
D = 4	Q = 17
E = 5	R = 18
F = 6	S = 19
G = 7	T = 20

H = 8	U = 21
I = 9	V = 22
J = 10	W = 23
K = 11	X = 24
L = 12	Y = 25
M = 13	Z = 26

Table 1: Caesar Cipher Table

Encryption Process:

1. Calculate the Shift Key:

   -Each letter in "violet" is assigned its position in the alphabet:

   - 'v' is the 22nd letter.
   - '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
   Now we are using, modulo 26 to keep the shift within a smaller range: 83 divided by 26 leaves a remainder of 5.

2. **Apply the Shift:**

   -Shift each letter in "violet" by 5 positions in the alphabet:

   -'v':

- 22+5=27
- If the result is bigger than 26, subtract 26 to start over from a: 27>26 so, 27−26=1 Result: 'a'.

-'i':

- 9+5=14
- If the result is ≤ 26, no starting over is needed, 14≤26 So, keep it as it is. Result: 'n'.

-'o':

- 15+5=20
- 20≤26 So keeping it as it is. Result: 't'.

-'l':

- 12+5=17
- 17≤26, Result: 'q'.

-'e':

- 5+5=10
- 10≤26 , Result: 'j'.

-'t':

- 20+5=25
- 25≤26 , Result: 'y'.

-Encrypted Word: "antqjy".

Decryption Process:

1. Using the Same Key:

- The key is the shift of 5, as calculated during encryption.

2. **Apply the Reverse Shift:**

-Reverse the shift by moving each letter in "antqjy" backwards by 5 positions:

-'a':

- 1−5=−4
- If the result is less than 1, add 26 to Continue from 'z': −4<1 so, −4+26=22, Result: 'v'.

-'n':

- 14−5=9
- If the result is ≥ 1, Continuing from 'z': is not needed: 9≥1 so, keep it as it is, Result: 'i'

-'t':

- 20−5=15
- 15≥1, Result: 'o'.

-'q':

- 17−5=12
- 12≥1, Result: 'l'.

-'j':

- 10−5=5
- 5≥1, Result: 'e'.

-'y':

- 25−5=20

- 20≥1, Result: '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:

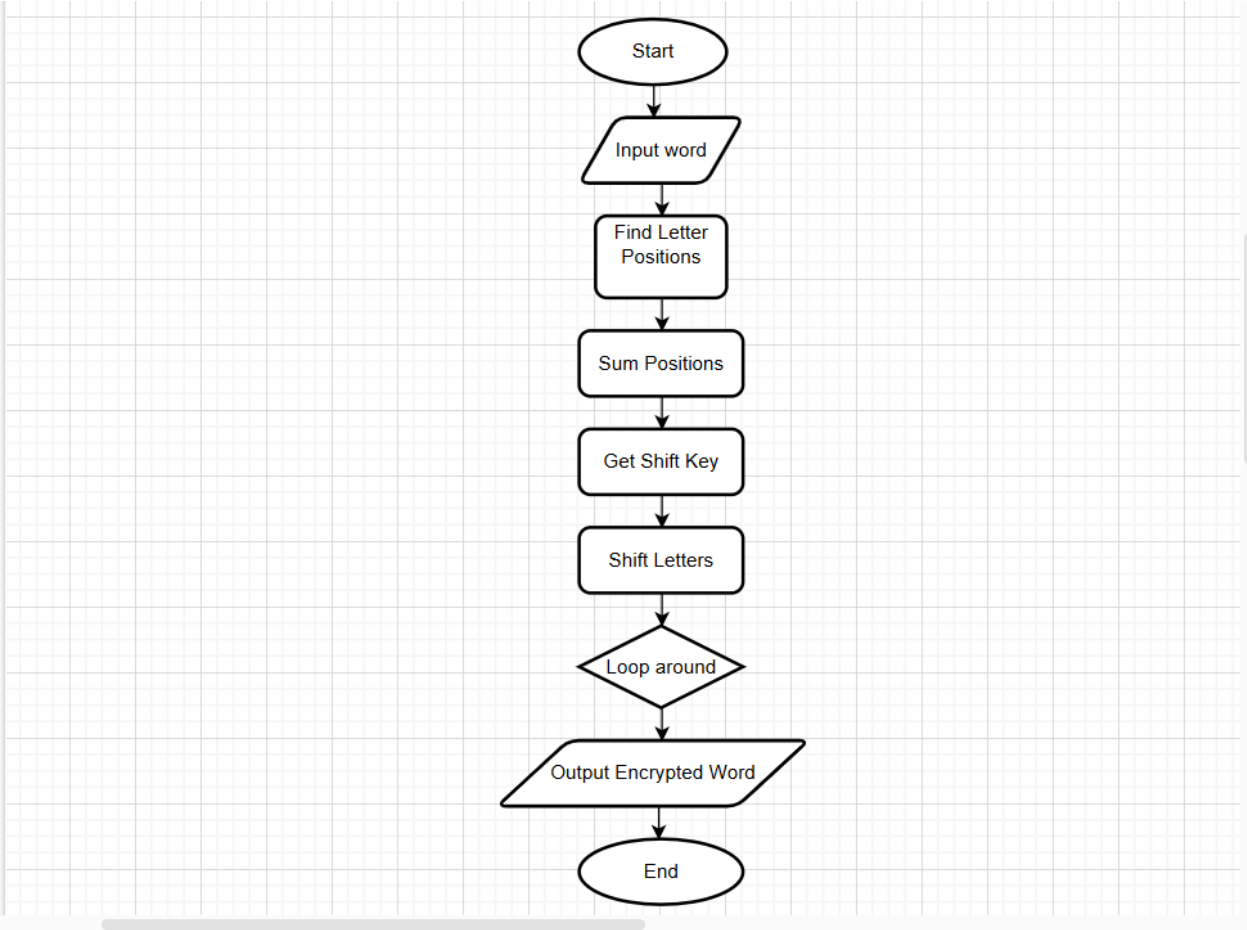


Figure 6:Flowchart for encryption process

For decryption Process:

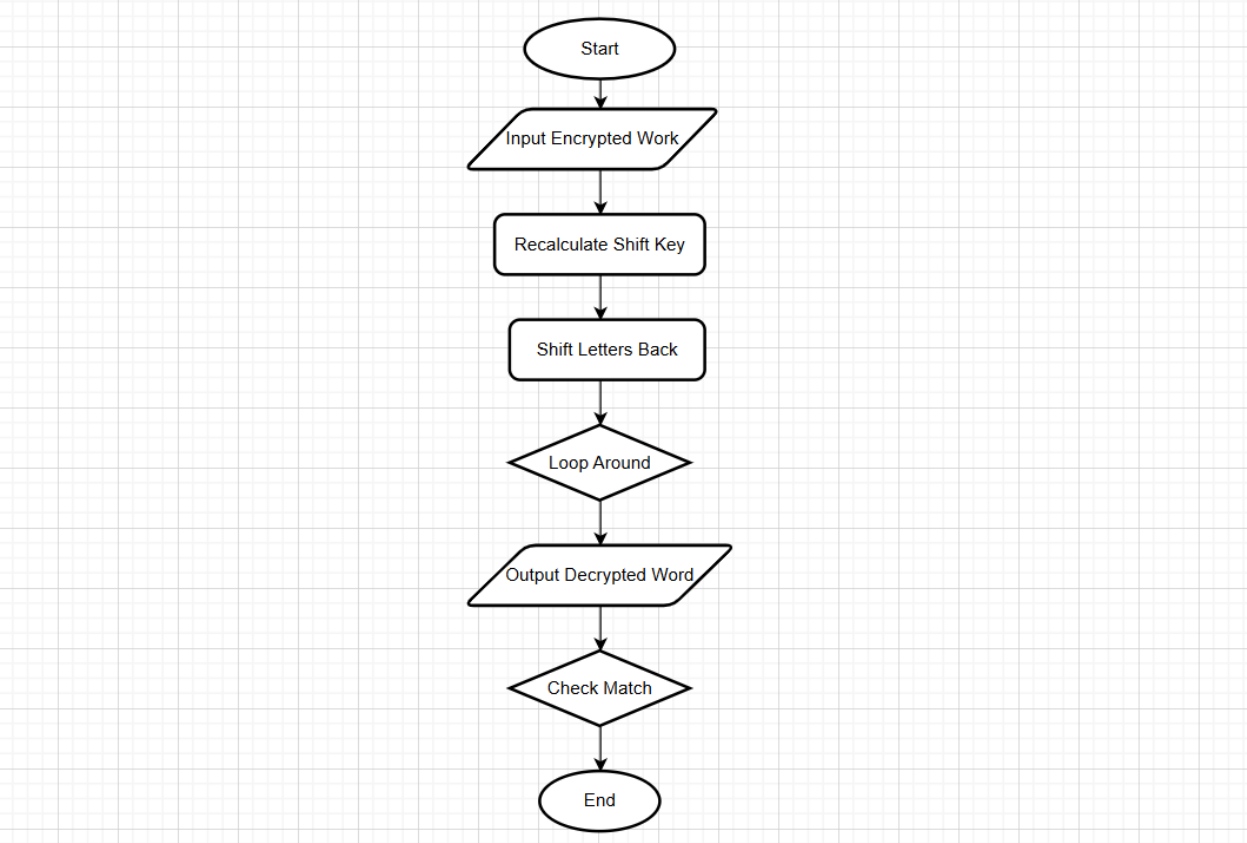


Figure 7:Flowchart for decryption process

4.Test Cases

Demonstrating the Working Steps of the Algorithm:

In this section I have demonstrated the working steps of the encryption and decryption algorithm created in **Task 03**. The algorithm has been tested with at least 5 examples of plaintext which are converted into ciphertext and then decrypted back to plaintext. Each example follows the algorithm's process of calculating the shift key, applying the shift for encryption, and reversing the shift for decryption.

Example 1

Plaintext: "garden"

Shift Key Calculation:

- Positions: g = 7, a = 1, r = 18, d = 4, e = 5, n = 14
- Sum: 7 + 1 + 18 + 4 + 5 + 14 = 49
- Modulo 26: 49 % 26 = 23

Encryption:

- g = d, a = x, r = o, d = a, e = b, n = k
- **Ciphertext:** "dxoabk"

Decryption:

- d = g, x = a, o = r, a = d, b = e, k = n
- **Decrypted Text:** "garden"

Example 2

Plaintext: "cipher"

Shift Key Calculation:

- Positions: c = 3, i = 9, p = 16, h = 8, e = 5, r = 18
- Sum: 3 + 9 + 16 + 8 + 5 + 18 = 59
- Modulo 26: 59 % 26 = 7

Encryption:

- c = j, i = p, p = w, h = o, e = l, r = y
- **Ciphertext:** "jpwoly"

Decryption:

- j = c, p = i, w = p, o = h, l = e, y = r
- **Decrypted Text:** "cipher"

Example 3

Plaintext: "apple"

Shift Key Calculation:

- Positions: a = 1, p = 16, p = 16, l = 12, e = 5
- Sum: 1 + 16 + 16 + 12 + 5 = 50
- Modulo 26: 50 % 26 = 24

Encryption:

- a = y, p = n, p = n, l = j, e = c
- **Ciphertext:** "ynnjc"

Decryption:

- y = a, n = p, n = p, j = l, c = e
- **Decrypted Text:** "apple"

Example 4

Plaintext: "secure"

Shift Key Calculation:

- Positions: s = 19, e = 5, c = 3, u = 21, r = 18, e = 5
- Sum: 19 + 5 + 3 + 21 + 18 + 5 = 71
- Modulo 26: 71 % 26 = 19

Encryption:

- s = l, e = x, c = v, u = n, r = k, e = x
- **Ciphertext:** "lxvnkx"

Decryption:

- l = s, x = e, v = c, n = u, k = r, x = e
- **Decrypted Text:** "secure"

Example 5

Plaintext: "planet"

Shift Key Calculation:

- Positions: p = 16, l = 12, a = 1, n = 14, e = 5, t = 20
- Sum:16 + 12 + 1 + 14 + 5 + 20 = 68
- Modulo 26: 68 % 26 = 16

Encryption:

- p = f, l = b, a = q, n = d, e = u, t = j
- **Ciphertext:** "fbqduj"

Decryption:

- F = p, b = l, q = a, d = n, u = e, j = t
- **Decrypted Text:** "planet"

5. Critical Evaluation of the new Cryptographic Algorithm

Analysis of Strengths and Weaknesses of the Cryptographic Algorithm

This section focus is on the evaluation of the encryption algorithm developed in Task 03. This section analyzes how well it performs and identifies its strong points and limitations. By examining its strengths and weaknesses, we can understand its reliability, usability, and areas that need improvement.

Strengths

Here are five key strengths of the algorithm:

1. **Simple to Understand and Implement:** The algorithm is straightforward which makes it easy for beginners to understand and use it without needing advanced cryptographic knowledge.
2. **Reversible Process**: The encryption is fully reversible using the same key, which makes sure that the original text can always be recovered accurately.
3. **Dynamic Key Calculation**: The shift key is calculated based on the text itself, making it unique to each input and harder to predict.
4. **Works with Any Alphabet-Based Text**: The algorithm can handle any text made of letters, as it is not limited by specific word lengths or fixed patterns.
5. **Lightweight and Fast**: Due to its simplicity, the algorithm performs quickly and doesn't require significant computational resources.

Weaknesses

Here are five weaknesses of the algorithm:

1. **Predictable Key Range**: The use of modulo 26 to calculate the shift key limits the range to 1–26, which could make brute force attacks easier.

2. **No Resistance to Frequency Analysis**: Since it doesn't hide the letter frequency of the original text, the algorithm is weak against to attacks that can analyze letter patterns.
3. **Fixed Alphabet Set**: It only works with letters and does not work for special characters, numbers, or spaces, which reduces its practicality for broader applications.
4. **Not Secure Against Modern Standards**: The algorithm lacks complex encryption techniques like multi-layer ciphers, making it unsuitable for protecting sensitive data.
5. **Key Sharing is Insecure**: The shift key is derived from the plaintext which means an attacker who knows the process can easily recreate it which makes the key security weak.

Application Area of the Cryptographic Algorithm

This encryption algorithm, due to its simple nature and ease of implementation, can be used in various basic applications. However, it is more suitable for environments where high-level security is not important but where data privacy or confidentiality is still needed. Here are some areas where it can be applied:

1. **Educational Purposes**: This algorithm is good for teaching beginners about encryption. It helps students and learners understand the fundamental concepts of how data can be securely encoded and decoded.
2. **Basic Communication Systems**: The algorithm can be used in small-scale or internal communication systems (like emails or messages within a group) where high security is not a major concern but privacy is still needed.
3. **Simple File Encryption**: For non-sensitive files or documents, this algorithm could provide a basic layer of encryption to protect data. It could be useful in personal settings or among small teams.

4. **Fun or Creative Projects**: It can be applied in games or puzzles, where the goal is to encode and decode simple messages. This would make it enjoyable and interactive for users without demanding high levels of security.
5. **Non-Sensitive Data Storage**: The algorithm could be used to encrypt files that don't contain highly sensitive information, like personal notes, non-financial documents, or casual communication.

6. Conclusion

In this project, I have learned about the importance of cryptography in keeping information safe. It starts by understanding the basic concepts of the CIA Triad which are:- confidentiality, integrity, and availability. These are very key elements to protect sensitive data and to make sure it stays accurate and accessible.

This report explores two types of ecryption: symmetric and asymmetric. Symmetric encryption uses the same key to both encrypt and decrypt, while asymmetric uses two keys. Both are used in many online services to protect personal data.

I also looked at the Caesar Cipher, a simple encryption technique, and improved it by creating my own method. This method used a word as the key to shift letters differently, making it more secure than the basic Caesar Cipher.

Testing the algorithm showed it could encrypt and decrypt messages, proving that it worked well for basic encryption. While it's not as secure as modern methods, the project gave can give a better understanding of how encryption helps to keep data safe.

In conclusion, this project helped me understand how cryptography works and how it protects information in the real world.

7. Bibliography

Khan Academy, 2024. *Introduction to encryption.* [Online] Available at: https://www.khanacademy.org/computing/computer-science/cryptography [Accessed 10 December 2024].

(NIST), N. I. o. S. a. T., 2024. *Advanced Encryption Standard (AES),* Gaithersburg: National Institute of Standards and Technology.

CaesarCipher.net, 2024. *Overcoming Caesar Cipher's Security Challenges.* [Online] Available at: https://caesarcipher.net/overcoming-caesar-ciphers-security-challenges/ [Accessed 9 December 2024].

Cybersecurity & Infrastructure Security Agency (CISA), 2023. *Cybersecurity Overview.* [Online]
Available at: https://www.cisa.gov/cybersecurity[Accessed 8 December 2024].

Encyclopedia Britannica, Inc., 2024. *Caesar cipher.* [Online] Available at: https://www.britannica.com/topic/Caesar-cipher
[Accessed 9 December 2024].

IBM, 2023. *What is the CIA triad?.* [Online] Available at: https://www.ibm.com/topics/cia-triad
[Accessed 8 December 2024].

Kahn, D., 1996. *The Comprehensive History of Secret Communication from Ancient Times to the Internet.* revised ed. New York: Scribner.

National Institute of Standards and Technology (NIST), 2022. *FIPS PUB 180-4: Secure Hash Standard (SHS).* [Online] Available at: https://www.nist.gov/publications/fips-publication-180-4-secure-hash-standard-shs
[Accessed 8 December 2024].

Schneier, B., 2015. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Second ed. New York: Wiley.

Stallings, W., 2006. *Cryptography and Network Security: Principles and Practice.* 4th ed. USA: Prentice Hall.

Stallings, W., 2017. *Cryptography and Network Security: Principles and Practice (7th edition).* 7th ed. Boston, MA: Pearson Education.

TechTarget, 2023. *Cryptography definition.* [Online] Available at: https://www.techtarget.com/definition/cryptography
[Accessed 8 December 2024].