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: Satvisha Panta

London Met ID: 23047457

College ID: NP01NT4A230133

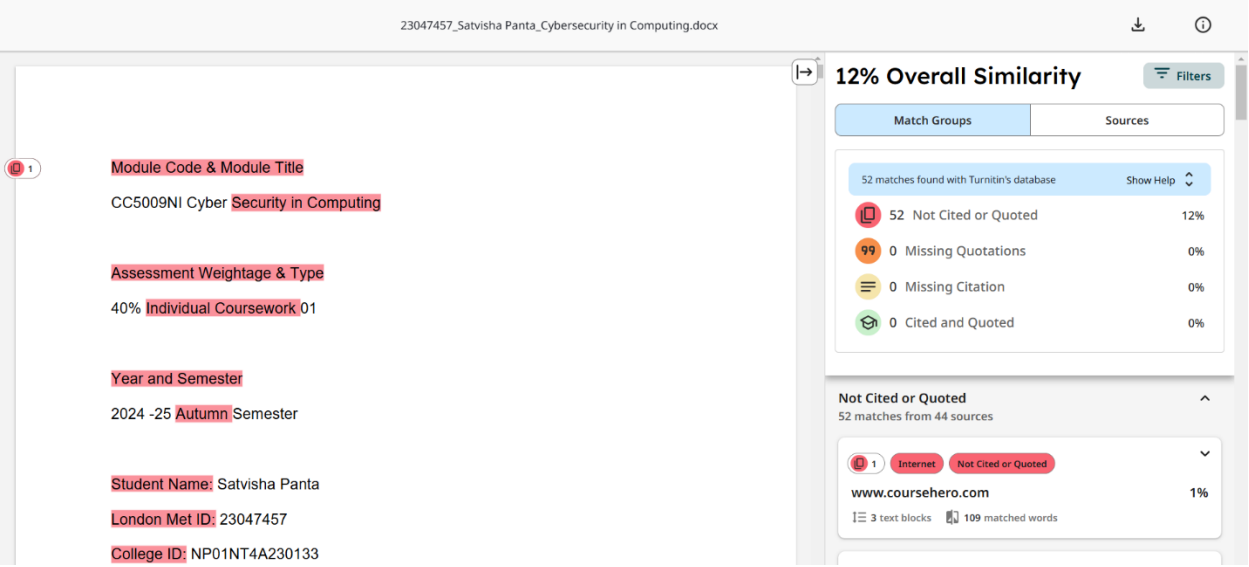
Assignment Due Date: 20th January 2025

Assignment Submission Date: 20th January 2025

Word Count (Where Required): 6495

I confirm that I understand my coursework needs to be submitted online via my Second Teacher 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.

Turnitin Report



Acknowledgement

I am happy to share this report on cryptography and how it has improved over time with a special focus on making the Caesar Cipher better. In this report, I have researched how cryptography started in ancient times and how it has developed into the advanced systems we use today. I have focused on the Caesar Cipher which is one of the oldest and simplest encryption methods and introduced a new way to make it stronger using techniques like Caesar shifts, left cyclic shifts, and XOR operations. These improvements help make data more secure and protect it from modern threats.

I would like to sincerely thank my teachers for their constant support, guidance, and encouragement throughout this project. Their valuable advice and feedback have helped me understand cryptography better and complete this report successfully. I truly appreciate the time and effort they put into teaching and helping me improve my work. I am also very thankful to Islington College for providing me with a great learning environment and useful resources that helped me a lot during my research.

Lastly, I want to express my gratitude to my friends, classmates and family for their encouragement and support. Their motivation helped me stay focused and complete this report. I truly appreciate their patience and belief in me throughout this journey.

Table of Contents

1. Introduction 1
1.1. Aim 1
1.2. Objectives 1
1.3. Fundamentals of Security 2
1.4. CIA triad and its role 2
1.4.1. Confidentiality 3
1.4.2. Integrity 4
1.4.3. Availability 5
1.5. Importance of CIA Triad 6
1.6. Cryptosystems 7
1.6.1. Components of Cryptosystem 8
1.6.2. Types of Cryptosystems 9
2. History of Cryptography 12
2.1. Hieroglyphs Cryptography 13
2.2. Caesar Cipher 14
2.3. Vigenere Cipher 14
2.4. Hebern rotating machine 15
2.5. Enigma machine 16
3. Development of a new Cryptographic Algorithm i.e. Caesar Cipher 17
3.1. Background and history of Caesar Cipher 17
3.1.1. Pros and Cons of Ceasar Cipher 17
3.2. Working Mechanism of Ceasar Cipher 18
3.2.1. Encryption Algorithm in Caesar Cipher and XOR. 18
3.2.2. Decryption Algorithm in Caesar Cipher 22

3.3. Improvement of Caeser Cipher according to my new algorithm..... 24
4. Flowchart 26
4.1. Flowchart of Encryption..... 26
4.2. Flowchart of Decryption 27
5. Test Cases..... 28
5.1. Testing 1 28
5.2. Testing 2 30
5.3. Testing 3 34
5.4. Testing 4 36
5.5. Testing 5 39
6. Conclusion 43
7. References..... 44

Table of Figures

Figure 1 Fundamentals of Security 2
Figure 2 CIA triad and its role 3
Figure 3 Confidentiality 4
Figure 4 Integrity 5
Figure 5 Availability 6
Figure 6 Importance of CIA Triad 7
Figure 7 Cryptosystems 8
Figure 8 Components of Cryptosystem 9
Figure 9 Symmetric-Key Encryption 10
Figure 10 Asymmetric-key encryption 11
Figure 11 History of Cryptography 12
Figure 12 Hieroglyphs Cryptography 13
Figure 13 Caesar Cipher 14
Figure 14 Vigenere Cipher 15
Figure 15 Hebern rotating machine 16
Figure 16 Enigma machine 16
Figure 17 Encryption flowchart 26
Figure 18 Decryption flowchart 27

Table of Tables

Table 1 Reference table for mathematical encryption i.e. Caesar Cipher and left cyclic shift..... 19
Table 2 Caesar Cipher with shift of 4 19
Table 3 The shifted value after Caesar Cipher..... 19
Table 4 Changing the encrypted text by left cyclic shift by 3 20
Table 5 Binary value of all alphabets for XOR..... 20
Table 6 Binary value of encrypted letter 21
Table 7 Binary result with XOR key 10001..... 21
Table 8 Letter formed by Binary value for encryption 22
Table 9 Binary value formed for decrypted letter..... 23
Table 10 Binary result with XOR key 10001 for decryption 23
Table 11 Decrypted Letter from binary value 23
Table 12 Reversing the left cyclic shift by 3 23
Table 13 Reversing the Caesar cipher..... 24
Table 14 Left cyclic shift by 3 for encryption for Testing 1..... 28
Table 15 Reversing the left cyclic shift for decryption of Testing 1..... 30
Table 16 Left cyclic shift by 3 for encryption for Testing 2..... 31
Table 17 Reversing the Left cyclic shift for decryption for Testing 2 33
Table 18 Left cyclic shift by 3 for encryption for Testing 3..... 34
Table 19 Reversing the Left cyclic shift for decryption for Testing 3 36
Table 20 Left cyclic shift by 3 for encryption for Testing 4..... 37
Table 21 Reversing the Left cyclic shift for decryption for Testing 4 38
Table 22 Left cyclic shift by 3 for encryption for Testing 5..... 40
Table 23 Reversing the Left cyclic shift for decryption for Testing 5 41

Abstract

Cryptography has always been important in keeping our sensitive information safe, especially in today's world of constant digital threats. In this report, there is the history of cryptography, starting with ancient techniques like hieroglyphic ciphers, Enigma machine and many more. Caesar Cipher is a simple but powerful encryption method which is an effective tool for encryption and where its simplicity leads to vulnerabilities in the face of more sophisticated attacks.

In this report there is the importance of the CIA Triad i.e. confidentiality, integrity, and availability when designing strong cryptographic systems. By combining proven cryptographic methods with the latest security advancements, this report highlights how innovation plays a crucial role in protecting our data in today's rapidly evolving digital world.

Finally after developing this classic method, in this report there is a new encryption algorithm that takes things a step further. By combining Caesar shifts, left cyclic shifts and XOR operations, this new system creates multiple layers of protection by making it much harder to break through with brute force or known-plaintext attacks. For this new algorithm there is the test which shows how it can securely encrypt and decrypt messages.

1. Introduction

Cryptography is the application and the science same as protecting messages that converts them into a form that cannot be understood by unauthorized individuals. The methods ensure that the information is kept secret and intact, as well as authentic and non-repudiated, at rest or during an event of transmission. As per Phil Zimmermann cryptography is 'Cryptography is the science of using mathematics to encrypt and decrypt data.' And as per Bruce Schneier 'Cryptography is the art and science of keeping messages secure.' (Adomey, 12/10/2016). It uses algorithms to transform plaintext data into ciphertext, making a typical message unreadable (Buxton, 2023).

A cipher can be defined as an algorithm that provides the process of encrypting or decrypting-a series of well-defined steps that can be followed as a form of procedure. The cryptosystem has the capability of implementing cryptographic techniques and their entire infrastructure to ensure service provisioning concerning information security. A cryptosystem or cipher system is also used for the same purpose (Adomey, 12/10/2016).

1.1. Aim

The aim of the objectives is to design, implement and test a new cryptographic algorithm that can provide better protection for data. This involves evaluation of existing methods, creation of a safe and efficient system, and verification of its effectiveness through tests.

1.2. Objectives

The objectives of this report are:

a. To design a modified cryptographic algorithm that enhances the security of the traditional Caesar cipher.
b. To enhance security awareness
c. To connect historical and modern methods
d. To provide a step-by-step explanation of the encryption and decryption processes.

1.3. Fundamentals of Security

Security is an essential part of our lives. Securing sensitive information has become necessary, and the fundamentals of security tell us how to secure that data against threats while making systems reliable and trustworthy. It is about core security principles: confidentiality which means keeping information secret, integrity which means not allowing tampering with data, and availability which means giving access to resources on-demand. Other principles are proving identities through authentication, controlling rights with authorization and ensuring accountability through non-rejection. By this we can build systems that protect our information and help secure us in a dynamic digital environment (Whitman, 2021).

Figure 1 Fundamentals of Security

1.4. CIA triad and its role

CIA stands for Confidentiality, Integrity, and Availability. The primary feature of the CIA Triad which is widely accepted for security systems development is to use as an identifier for locating weaknesses or vulnerabilities and methods of developing solutions (Becan, 2024).

Confidentiality, integrity, and availability of information are important for the smooth operation of any business. The CIA triad breaks these concepts into separate components to help security teams tackle each one effectively. Confidentiality ensures sensitive data is accessible only to authorized individuals, integrity maintains the accuracy and consistency of information and availability guarantees resources are accessible when needed. This division allows organizations to

develop targeted strategies for protecting information by addressing each concern individually while improving overall security (Becan, 2024).

Figure 2 CIA triad and its role

1.4.1. Confidentiality

Confidentiality means protection against unauthorized disclosure of sensitive information. Breaches happen purposely through some attacks like man-in-the-middle or human errors, such as sharing passwords or failing to encrypt data. Measures to protect confidentiality are training employees to minimize breaches, access control, data classification, and using multi-factor authentications. All employees associated in finance will access financial data, but most employees would not need to know them as they are from another department. It signifies strict access control that an organization can do in protecting sensitive information from within the organization. Even while giving access to confidential information, the employees should be under certain conditions and agreements so there is more less chance for breaches (Becan, 2024).

Figure 3 Confidentiality

1.4.2. Integrity

The fundamental principle of integrity is in ensuring that data remains authentic and accurate. In integrity reliability plays a very important role not only in creating trust but also in avoiding difficult consequences. For example, if there is information on the website of an organization regarding its senior managers or directors that is not true, it could have serious effects for the organization. Integrity can be broken in many was as either it can be broken maliciously through the intrusion of a hacker or even humans who may make mistakes while entering data. To secure integrity in every aspect, there are several techniques of hashing, digital signatures, and encryptions on the part of organizations. Non-denial would include such examples as where emails are signed digitally so that whatever transaction occurs, the sender or receiver cannot deny it thus adds to authenticate either or even both the communications and the data (Becan, 2024).

Figure 4 Integrity

1.4.3. Availability

Availability means that when required the critical information, systems, and services are made available to authorized employees. Disruption could come from various sources, for example, power outages, natural disasters, or cyberattacks, like denial-of-service (DoS) attacks or ransomware. During a power outage without a backup system, employees may lose access to important systems. Similarly, flood or other natural disasters and conditions can deny certain staff from accessing the office while restricting access to workstations and other critical tools and it may delay to their work. All this is made possible using terminated systems, backup servers, and disaster recovery plans that organizations can use to maintain availability. On the other hand one must keep updating and applying patches to known security holes that prevent some system malfunctioning or vulnerabilities among them. This assures the timely restoration of data and services, limiting downtime and hence maintaining continuous access during sudden occurrence events (Becan, 2024).

Figure 5 Availability

1.5. Importance of CIA Triad

The principle of CIA is important and by implementing such confidentiality, integrity, and availability principles into cybersecurity foundation it results in favourable returns for the organization:

Secure data - Cyber-attacks are becoming very advanced and ever more complex. Data protection through implementation of confidentiality, integrity, and availability so it safeguards against hacking scenarios that may bring data loss (Obrien, 2024).

Identifying weaknesses- By measuring the security features against the principles of CIA, threats, risks, and weaknesses that can be identified with relative help. Then the organization can then apply controls and software to mitigate such weaknesses (Obrien, 2024).

Regulatory Compliance - This security triad positions the organization to comply with relevant legal frameworks or by regulating concerning cybersecurity and data protection (Obrien, 2024).

Integrated Protection- This triad will ensure safety in every aspect, from cyber threats to harsh risk; it will keep the data safe against every type of potential risk. Without such protection, the organization would have an overemphasis on cybersecurity at the expense of the availability consequences (Obrien, 2024).

Figure 6 Importance of CIA Triad

1.6. Cryptosystems

Cryptosystems also known as cryptographic are dedicated to preserving data so that it can be accessed only by the proper key owner. They accomplish this through mathematical transformations captured within algorithms used to encode messages into formats that can be easily read. Cryptosystems are dependent on key security because that is what defines the processes under which messages are hidden from those who are unauthorized to decode them. An excellent key is required to keep the message safe after encryption (Goyal, 2024).

A cryptosystem can greatly depend on the efficiency with which these keys will be managed and kept secret. A weak key also known as a compromised key will leave the whole cryptosystem open to successful attacks. That is why the protection and management of such keys is essential for the continuity and secrecy of the information that is protected. Theoretically, this means that the security of the cryptosystem is said to be as strong as its keys (Goyal, 2024).

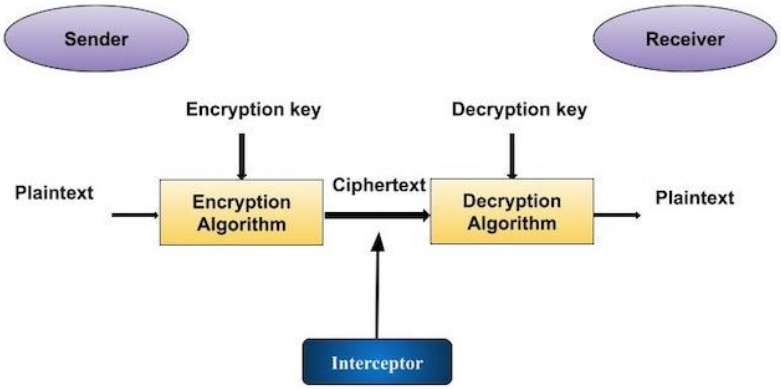


Figure 7 Cryptosystems

In this figure, the sender creates a message for receiver and in order to send the message confidentially cryptosystems are used. It uses the encryption algorithm to encrypt the message using a secret key. This ciphertext is then sent to the receiver. Now decryption algorithm is used for converting the ciphertext back to the original message (Goyal, 2024).

1.6.1. Components of Cryptosystem

- **Plaintext**: A plaintext is a readable message generated by the sender, which is input into the encryption algorithm (Goyal, 2024).
- **Encryption Algorithm**: A encryption algorithm is a method provided by the cryptosystem that generates an encryption key and converts plaintext into ciphertext (Goyal, 2024).
- **Encryption Key**: A encryption key is a random set of bits used to encrypt plaintext into ciphertext. This key is known to the sender (Goyal, 2024).
- **Ciphertext**: A ciphertext is an unreadable version of the plaintext, created by the encryption algorithm using the encryption key so that the unauthorized user cannot get access to it (Goyal, 2024).

- **Decryption Algorithm**: Decryption algorithm is the method that takes the encrypted text (ciphertext) and converts it back to the original message (Goyal, 2024).
- **Decryption Key**: A decryption key is a random set of bits used to decrypt ciphertext and recover the original message. This key is known to the receiver (Goyal, 2024).

Figure 8 Components of Cryptosystem

1.6.2. Types of Cryptosystems

There are two types of cryptosystems based on keys available in the system. They are Symmetric-Key Encryption and Asymmetric-Key Encryption.

1.6.2.1. Symmetric-Key Encryption

In symmetric-key encryption also known as symmetric cryptography, both the sender and receiver use the same key to encrypt and decrypt messages. This shared secret key makes sure that the information remains secure while being transmitted. The sender uses the key to convert a readable message into an unreadable format and the receiver uses the same key to turn the encrypted message back into its original form (Goyal, 2024).

This method of encryption is called "symmetric" because the same key is used for both the encryption and decryption processes. While this system is capable, it requires careful management of the key to prevent unauthorized access as anyone with the key can decrypt the message (Goyal, 2024).

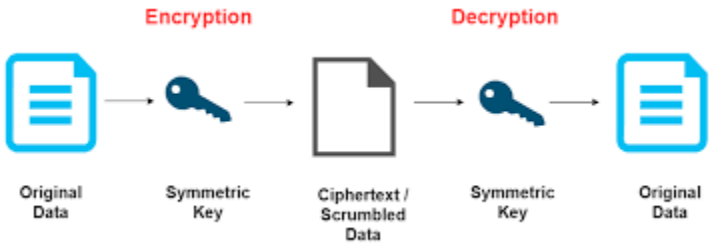


Figure 9 Symmetric-Key Encryption

1.6.2.2. Asymmetric-Key Encryption

In Asymmetric-key encryption also known as asymmetric cryptography two different but mathematically related keys are used that is a public key and a private key. The public key is shared freely and used by the sender to encrypt the message, while the private key, known only to the receiver, is used to decrypt it. This method ensures that even if the public key is interrupted, it is extremely difficult to derive the private key, making the communication secure (Goyal, 2024).

To make the process easier, digital certificates are used to transmit the public keys. Since public keys are typically very long and hard to remember, digital certificates provide a reliable and secure way of distributing them. The sender can use the receiver's public key to encrypt the message, and only the receiver, with their private key, can decrypt and read the message, ensuring both confidentiality and security in communication (Goyal, 2024).

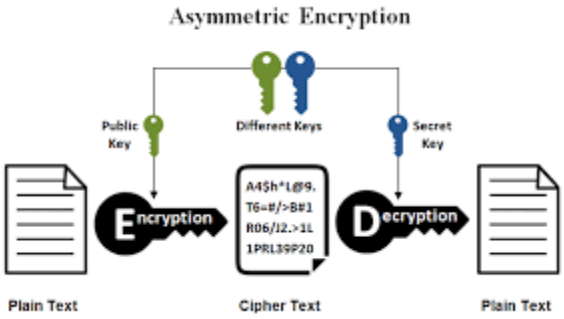


Figure 10 Asymmetric-key encryption

2. History of Cryptography

The term "cryptography" is derived from the Greek words "krypto," meaning hidden, and "graphene," writing. The basic aim of this is to conceal information so that it secures the communication or protects data (GeeksforGeeks, 2022).

An Egyptian tomb at about 1900 B.C. also contains the earliest evidence of cryptography. It contains a scribe, who used strange hieroglyphic symbols instead of normal, in the tomb of Khnumhotep II. As per research these strange might have symbols that were employed for hiding or disguising information so that others may not understand. It portrays a kind of an early civilization that had some secret writing techniques to preserve information, signifying one of historically prior examples of cryptography (Sidhpurwala, 2023).

The purpose of early cryptography wasn't to hide messages but to transform them into a form that seemed more respectable or prestigious. For example, an ancient Egyptian inscription used unusual symbols to modify its original text, making it the oldest known example of text transformation. Cryptography has been present in many early civilizations. In India, Kautalya's *Arthashastra* detailed the use of "secret writing" in espionage, demonstrating how cryptographic techniques were used for statecraft and intelligence in ancient times (Sidhpurwala, 2023).

Figure 11 History of Cryptography

2.1. Hieroglyphs Cryptography

The word cryptography can be followed from 1900 B.C.E in ancient Egypt during the Old Kingdom. Egyptians implemented a method of non-standard hieroglyphs as their one and only secret unique form of writing. These atypical symbols were understood to encode messages but not from the already understood hieroglyphics but also making such writing only understandable to a few individuals in which it used to be mainly the royal translators and within the royal court. They were trusted officials who transferred the confidential agenda of the king while in the same court. In all the possibilities the government may have wanted to keep sensitive information from those in authority from being accessed unauthorizedly, allowing only the informed and experts to decode messages (GeeksforGeeks, 2022).

Cryptography is a clear demonstration of how the ancient Egyptians recognized the necessity of communication security, especially regarding issues of government and state. It similarly shows the sort of cleverness of the creations in developing a system that would keep vital information from falling into the wrong hands. In ancient times, secret writing symbolized the importance of keeping information private and maintaining control which was valued for both confidentiality and social status. It is possibly the first recorded use of cryptographic methods and set the foundation for ancient and future civilizations to develop ways to encode and protect information (GeeksforGeeks, 2022).

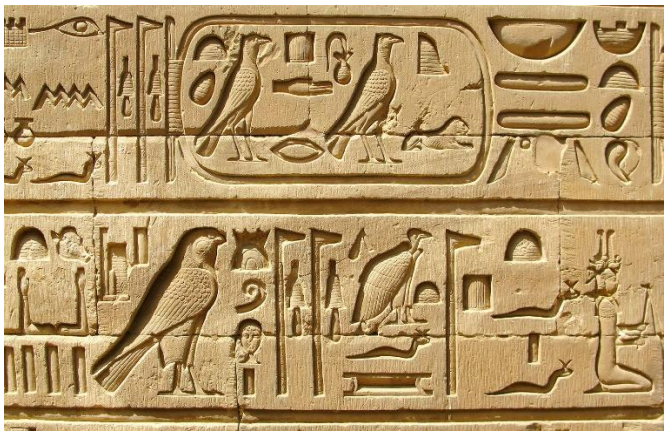


Figure 12 Hieroglyphs Cryptography

2.2. Caesar Cipher

The Greeks were the earliest inventors of ciphers, one of which is popular as the Caesar Cipher which is also known as Shift Cipher. This is one of the basic cryptographic techniques. According to this method, each letter in a message would be replaced by another letter a certain fixed number of positions shifted alongside in the alphabet. For example, with a shift the letters of three that is making the key as 3, the letter "A" becomes "D," "B" becomes "E," and more (GeeksforGeeks, 2022).

The Caesar Cipher was named after Julius Caesar, as he used it to communicate secrets between military generals. The only ones who would understand such an encoded message are those who could figure out its shift value. This is a simple technique but it was an advance in the history of cryptography as it showed how much difference shifting letters could make. As per recent time, it is something limited and very easily broken. It is also believed that it is the foundation for more new complicated methods of encryption. This cipher shows how the Greeks used creative methods to protect sensitive information, ensuring privacy and control during times when knowledge was a key asset for military and politician (GeeksforGeeks, 2022).

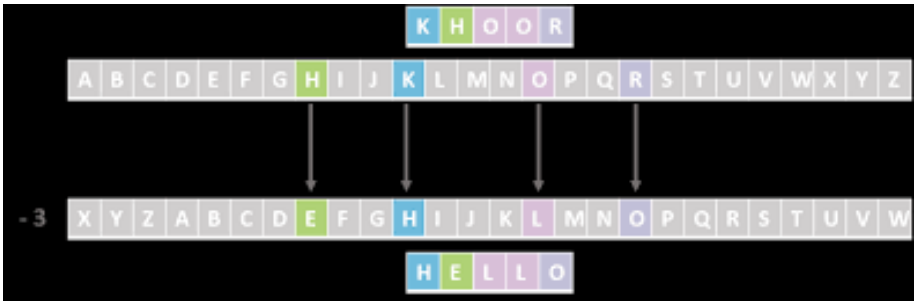


Figure 13 Caesar Cipher

2.3. Vigenere Cipher

During the 16th century, Blaise de Vigenere invented a cipher that was more highly developed than all forces before this cipher. This had a key word or phrase that

was continued throughout the message and each letter of the message would then be shifted using that of the key, according to mod 26. The cipher was more difficult to break than simpler ciphers like the Caesar Cipher as the key controls how much each letter of the message is shifted, with the shift varying depending on the key's letters, making it more complex to decipher without knowing the key. However, the cipher was vulnerable. It depended mostly on the privacy of the encryption key. If one could guess the key, then the cipher could easily be broken (GeeksforGeeks, 2022).

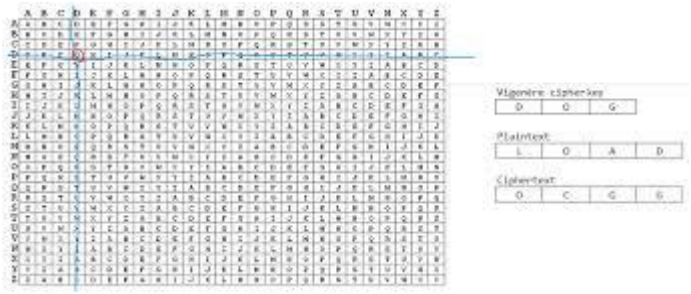


Figure 14 Vigenere Cipher

2.4. Hebern rotating machine

At the beginning of 19th century an inventor named Hebern came up with the Hebern rotating machine, a cryptographic apparatus. With the single rotor a secret key is listed on a rotating disc. The key had a substitution table to convert letters of the entering message into cipher text. Every time a key is pressed, the machine generates the output as encrypt text. But still, the system had some weakness. The code could be broken by analysing the frequencies of letters, showing how the cipher text appeared (GeeksforGeeks, 2022).

Figure 15 Hebern rotating machine

2.5. Enigma machine

During World War II, cryptography contributed heavily to the success of the Allied forces particularly with respect to the German Enigma machine. The German Enigma was the most advanced cipher machine through which Germans encrypted their messages. It incorporated multiple rotors by jumbling the letters in a complicated manner and making it impossible to crack. However, the first mathematicians to break this Enigma cipher were the Poles, whose expansion work was later taken on by British cryptanalysts. This enabled the Allies to listen into some of the crucial German messages, which were pivotal to them in winning the war. The ability to decode Enigma communications is considered one of the most significant achievements in cryptographic history that changed the outcome of the war on the Allies' side (GeeksforGeeks, 2022).

Figure 16 Enigma machine

3. Development of a new Cryptographic Algorithm i.e. Caesar Cipher

The Caesar Cipher is a simple encryption method where each letter in a message is shifted by a fixed number of positions in the alphabet. This technique was used by Julius Caesar to communicate secretly with military generals. Although it is easily broken today, the Caesar Cipher was a significant advancement in cryptography and laid the groundwork for more complex encryption methods (geeksforgeeks, 2024).

3.1. Background and history of Caesar Cipher

The Caesar cipher created by Julius Caesar was a simple encryption method used to protect military messages by shifting each letter by three positions. It was practical for Roman generals and scribes who could easily encode and decode messages. Over time it became a key example of substitution ciphers and laid the groundwork for more complex encryption methods. Today, it's mainly used in educational settings to demonstrate the basics of cryptography, though it's no longer secure in modern times.

3.1.1. Pros and Cons of Ceasar Cipher

Advantages:

- It is simple to implement, making it great for beginners.
- It can be physically implemented with rotating disks or a scytale, useful in certain situations.
- It requires minimal pre-shared information.
- It can be modified for enhanced security, such as by using multiple shifts or keywords.

Disadvantages:

- It is vulnerable to modern decryption methods.
- It is easy to crack with known-plaintext attacks.

- There are limited number of keys makes it susceptible to brute-force attacks.
- It is not suitable for encrypting long texts.

3.2. Working Mechanism of Ceasar Cipher

The Caesar Cipher is one of the simplest ways to create a secret code. It works by shifting the letters of the alphabet by a fixed number. For example, in Ceasar Cipher it is chosen to be shifted by 3, the letter "A" becomes "D," "B" becomes "E," and so on. When it reaches the end of the alphabet, it wraps around, so "X" becomes "A," "Y" becomes "B," and "Z" becomes "C."

Let's say if we want to encrypt the word "HELLO" with a shift of 3. Each letter in "HELLO" gets replaced with the letter that is three steps ahead in the alphabet. So "H" becomes "K," "E" becomes "H," "L" becomes "O," and "O" becomes "R." The encrypted message would be "KHOOR." It's like a secret way of writing that only someone who knows the shift can understand.

If we want to decode the message, we just reverse the process. Shift the letters back by the same number. For example, "KHOOR" shifted back by 3 would become "HELLO" again. It's a simple system.

The Caesar Cipher is named after Julius Caesar, who used it to send secret messages to his army. It's simple and fun to use but not very secure because it's easy to figure out the shift if you try all the possibilities.

3.2.1. Encryption Algorithm in Caesar Cipher and XOR.

Step 1: Input the plaintext message.

Step 2: Shift the plaintext message by 4, if the letter goes past Z then start again at A.

Step 3: Shift the encrypted text again by 3 in the text using left cyclic shift.

Step 4: Change each letter into its binary value. (e.g., A = 00000, B = 00001, etc.)

Step 5: Perform a logical XOR operation on the binary values from the encrypted letter with the binary value (10001).

Step 6: Change the resulting binary values back into letters using the same table in reverse.

Step 7: Combine all the letters and make one encrypted message.

Example:

Taking this table as reference in my encryption.

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

Table 1 Reference table for mathematical encryption i.e. Caesar Cipher and left cyclic shift

- Input the plaintext.
  Plaintext: SATVISHA
- Apply a Caesar cipher with a shift of 4.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Table 2 Caesar Cipher with shift of 4

- Keeping the shifted value.

S=19+4 23=W	A=1+4 5=E	T=20+4 24=X	V=22+4 26=Z	I=9+4 13=M	S=19+4 23=W	H=8+4 12=L	A=1+4 5=E

Table 3 The shifted value after Caesar Cipher

- S → W, A → E, T → X, V →Z, I → M, S → W, H → L, A → E
  Result: WEXZMWLE

- Changing the encrypted text by left cyclic shift by 3 again.

W	E	X	Z	M	W	L	E
Z	M	W	L	E	W	E	X

Table 4 Changing the encrypted text by left cyclic shift by 3

Result: ZMWLEWEX

- Now by using XOR i.e. logical operation encrypt the already encrypted text to make it stronger.

Alphabet	**Binary value**	**Alphabet**	**Binary value**
A	00000	Q	10000
B	00001	R	10001
C	00010	S	10010
D	00011	T	10011
E	00100	U	10100
F	00101	V	10101
G	00110	W	10110
H	00111	X	10111
I	01000	Y	11000
J	01001	Z	11001
K	01010	Space	11010
L	01011	!	11011
M	01100	.	11100
N	01101	?	11101
O	01110	*	11110
P	01111	£	11111

Table 5 Binary value of all alphabets for XOR

Encrypted Letter	Binary value
Z	11001
M	01100
W	10110
L	01011
E	00100
W	10110
E	00100
X	10111

Table 6 Binary value of encrypted letter

Binary value of encrypted letter	XOR value	Result
11001	10001	01000
01100	10001	11101
10110	10001	00111
01011	10001	11010
00100	10001	10101
10110	10001	00111
00100	10001	10101
10111	10001	00110

Table 7 Binary result with XOR key 10001

Binary value	Letter formed by binary value
01000	I
11101	?
00111	H
11010	Space
10101	V
00111	H
10101	V
00110	G

Table 8 Letter formed by Binary value for encryption

Result: I?H VHVG

- Final Encrypted Text: I?H VHVG

3.2.2. Decryption Algorithm in Caesar Cipher

Step 1: Input the encrypted text.

Step 2: Convert each letter into its binary value (e.g., A = 00000, B = 00001, etc.).

Step 3: Perform a logical XOR operation on the binary values from the encrypted text with the binary value (10001).

Step 4: Change the resulting binary values back into letters using the reverse of the binary table.

Step 5: Shift the letters back by 3 (reverse it by left cyclic shift).

Step 6: Shift the letters back by 4 (reverse the first Caesar cipher shift).

Step 7: Combine all the letters to get the original plaintext message.

Example:

- Input the encrypted word.
- To reverse the XOR operation, we apply XOR again with the same key (10001) because XOR is its own inverse.

Letter of decrypted word	**Binary value**
I	01000
?	11101
H	00111
Space	11010
V	10101
H	00111
V	10101

G	00110

Table 9 Binary value formed for decrypted letter

Binary value of decrypted letter	XOR value	Result
01000	10001	11001
11101	10001	01100
00111	10001	10110
11010	10001	01011
10101	10001	00100
00111	10001	10110
10101	10001	00100
00110	10001	10111

Table 10 Binary result with XOR key 10001 for decryption

Binary value	Decrypted Letter
11001	Z
01100	M
10110	W
01011	L
00100	E
10110	W
00100	E
10111	X

Table 11 Decrypted Letter from binary value

Result: ZMWLEWEX

- To reverse the left cyclic shift by 3, we apply a right cyclic shift by 3 as it is the reverse of the encrypted.

Z	M	W	L	E	W	E	X
W	E	X	Z	M	W	L	E

Table 12 Reversing the left cyclic shift by 3

Result: WEXZMWLE

- To reverse the Caesar cipher where we have shifted the letter by 4, we shift each letter backward by 4.

W=23-4 19=S	E=5-4 1=A	X=24-4 20=T	Z=26-4 22=V	M=13-4 9=I	W=23-4 19=S	L=12-4 8=H	E=5-4 1=A

Table 13 Reversing the Caesar cipher

Result: SATVISHA

- Final Decrypted Text: SATVISHA

3.3. Improvement of Caeser Cipher according to my new algorithm

1. Added Layers of Security

- In this report there is combinations of Caesar shifts, left cyclic shifts, and XOR operations for stronger encryption as a result each layer makes it harder for attackers to break through the system.

2. Bigger Key space

- Instead of just one shift value, the algorithm uses multiple keys with different lengths and values which creates more possible combinations, making brute-force attacks nearly impossible.

3. Better Protection Against Known-Plaintext Attacks

- The layered approach scrambles the connection between the original message and the encrypted one so even if attackers know part of the message, they can’t easily figure out the rest.

4. Stronger Security Overall

- It solves common weaknesses like predictability and limited keys in the original Caesar Cipher. The added layers make it much more reliable while keeping it simple.

5. Modern Use

- It can work in real-time systems or low-power devices that need secure communication and has potential to combine with other encryption methods for even more security.

4. Flowchart

4.1. Flowchart of Encryption

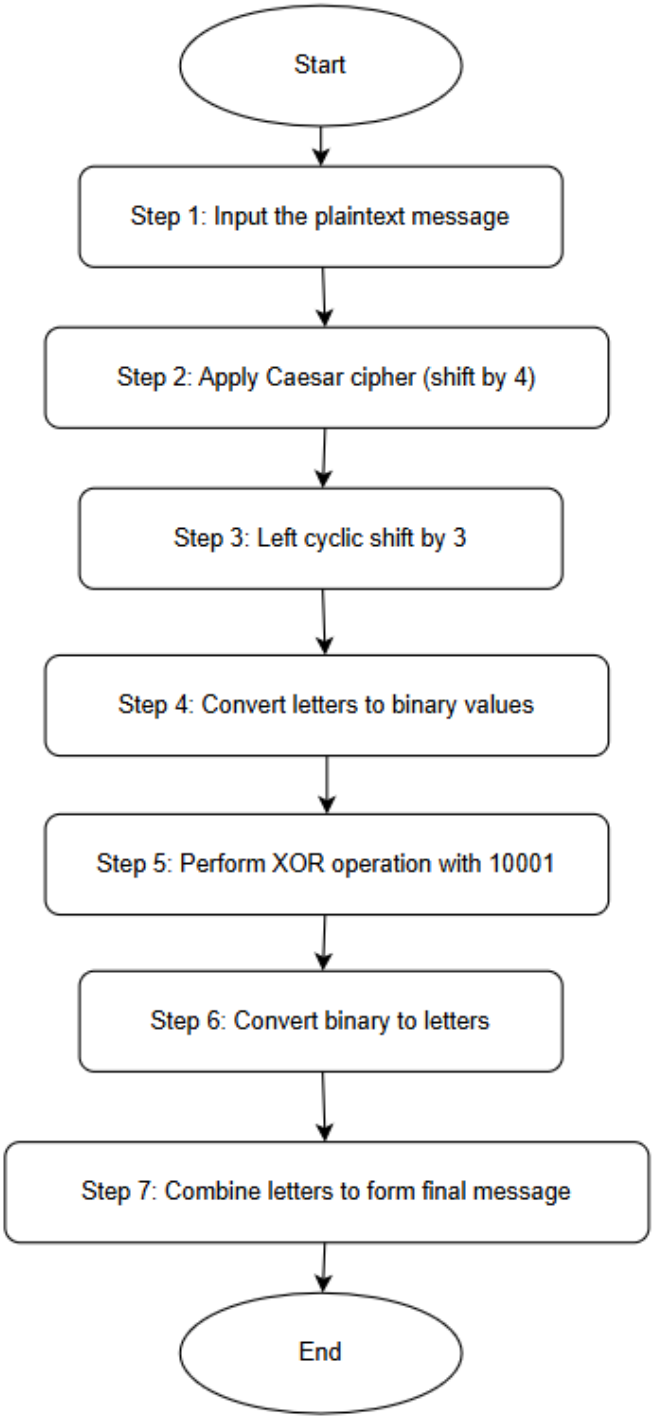


Figure 17 Encryption flowchart

4.2. Flowchart of Decryption

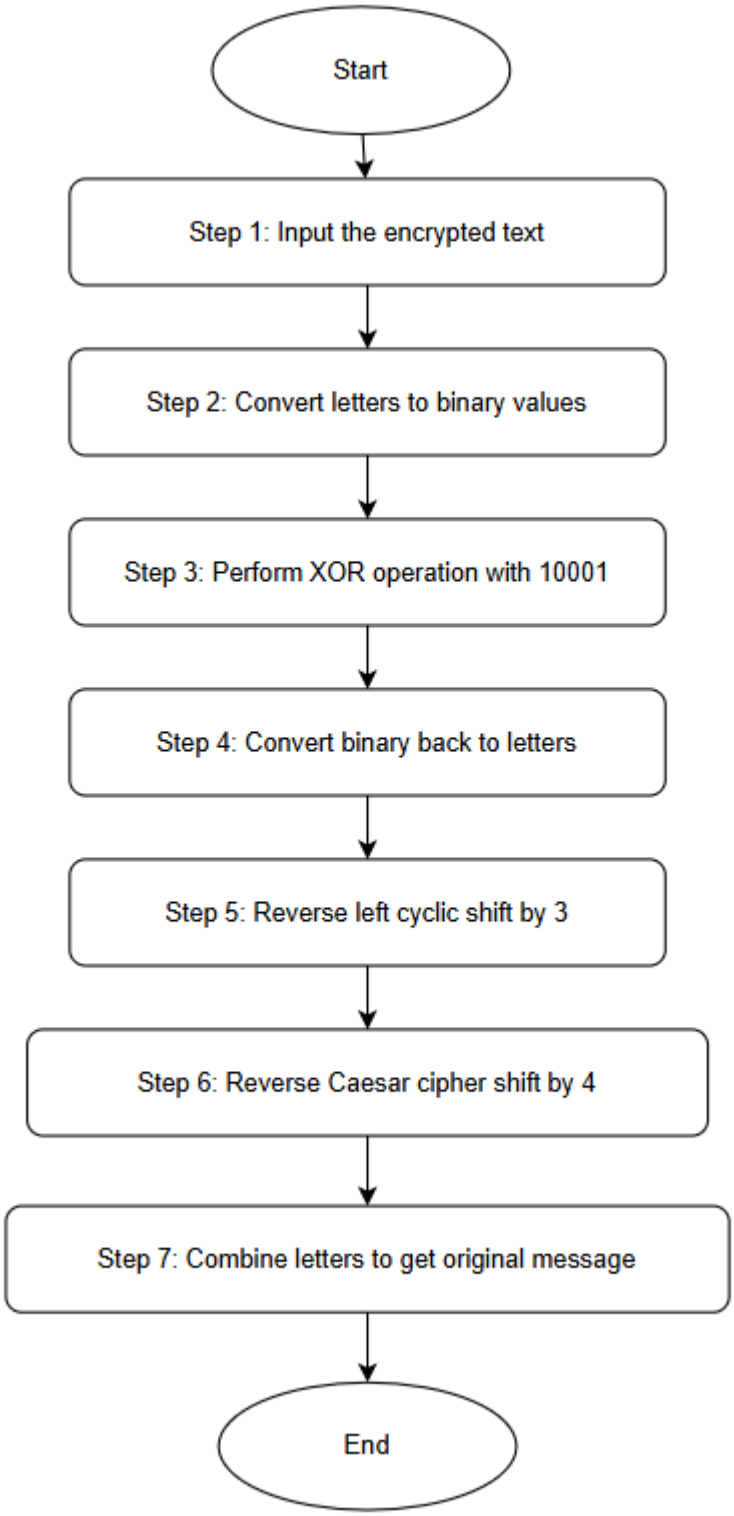


Figure 18 Decryption flowchart

5. Test Cases

5.1. Testing 1

Encrypting Word: TIME

Step 1: Apply a Caesar Cipher with a Shift of 4

T = X

T = 20

20 + 4 = 24 = X

I = M

I = 9

9 + 4 = 13 = M

M = Q

M = 13

13 + 4 = 17 = Q

E = I

E = 5

5 + 4 = 9 = I

Result after Caesar cipher= XMQI

Step 2: Left Cyclic Shift by 3

Original	X	M	Q	I
Shifted	I	X	M	Q

Table 14 Left cyclic shift by 3 for encryption for Testing 1

Result after the cyclic shift= IXMQ

Step 3: XOR Encryption

Now, using the binary XOR operation for further encryption.

I = 8 Binary: 01000

X = 24 Binary: 10111

M = 12 Binary: 01100

Q = 16 Binary: 10000

Performing XOR operation with 10001 for all the letters:

01000 XOR 10001 = 11001 = Z

10111 XOR 10001 = 00110 = G

01100 XOR 10001 = 11101 = ?

10000 XOR 10001 = 00001 = B

Result after XOR encryption= ZG?B

The final encrypted text for "TIME" is “ZG?B”

Decrypting Word: ZG?B

Step 1: Reverse XOR Encryption

Using the same XOR key (10001 in binary) on each letter.

Z = 25 Binary: 11001

G = 6 Binary: 00110

? = 29 Binary: 11101

B = 1 Binary: 00001

Performing XOR again with 10001 for all the letters:

11001 XOR 10001 = 01000 = I

00110 XOR 10001 = 10111 = X

11101 XOR 10001 = 01100 = M

00001 XOR 10001 = 10000 = Q

Result after reversing XOR: IXMQ

Step 2: Reversing the Left Cyclic Shift

Original	I	X	M	Q
Shifted	X	M	Q	I

Table 15 Reversing the left cyclic shift for decryption of Testing 1

Result after reversing the cyclic shift: XMQI

Step 3: Reversing Caesar Cipher

X = T

X = 24

24 - 4 = 20 = T

M = I

M = 13

13 - 4 = 9 = I

Q = M

Q = 17

17 - 4 = 13 = M

I = E

I = 9

9 - 4 = 5 = E

Result after reversing the Caesar cipher: TIME

The final decrypted text for " ZG?B " is “TIME”

5.2. Testing 2

Encrypted Word: FLIES

Step 1: Apply a Caesar Cipher with a Shift of 4

F = J

F = 6

6 + 4 = 10 = J

L = P

L = 12

12 + 4 = 16 = P

I = M

I = 9

9 + 4 = 13 = M

E = I

E = 5

5 + 4 = 9 = I

S = W

S = 19

19 + 4 = 23 = W

Result after Caesar cipher= JPMIW

Step 2: Left Cyclic Shift by 3

Original	J	P	M	I	W
Shifted	I	W	J	P	M

Table 16 Left cyclic shift by 3 for encryption for Testing 2

Result after the cyclic shift= IWJPM

Step 3: XOR Encryption

Now, using the binary XOR operation for further encryption.

I = 8 Binary: 01000

W = 22 Binary: 10110

J = 9 Binary: 01001

P = 15 Binary: 01111

M = 12 Binary: 01100

Performing XOR operation with 10001 for all the letters:

01000 XOR 10001 = 11001 = Z

10110 XOR 10001 = 00111 = H

01001 XOR 10001 = 11000 = Y

01111 XOR 10001 = 11110 = *

01100 XOR 10001 = 11101 = ?

Result after XOR encryption= ZHY*?

The final encrypted text for "FLIES" is “ZHY*?”

Decrypting Word: ZHY*?

Step 1: Reverse XOR Encryption

Using the same XOR key (10001 in binary) on each letter.

Z = 25 Binary: 11001

H = 7 Binary: 00111

Y = 24 Binary: 11000

* = 30 Binary: 11110

? = 29 Binary: 11101

Performing XOR again with 10001 for all the letters:

11001 XOR 10001 = 01000 = I

00111 XOR 10001 = 10110 = W

11000 XOR 10001 = 01001 = J

11110 XOR 10001 = 01111 = P

11101 XOR 10001 = 01100 = M

Result after reversing XOR: "IWJPM"

Step 2: Reversing the Left Cyclic Shift

Original	I	W	J	P	M
Shifted	J	P	M	I	W

Table 17 Reversing the Left cyclic shift for decryption for Testing 2

Result after reversing the cyclic shift: "JPMIW"

Step 3: Reversing Caesar Cipher

J = F

J = 10

10 - 4 = 6 = F

P = L

P = 16

16 - 4 = 12 = L

M = I

M = 13

13 - 4 = 9 = I

I = E

I = 9

9 - 4 = 5 = E

W = S

W = 23

23 - 4 = 19 = S

Result after reversing the Caesar cipher: FILES

The final decrypted text for " ZHY*? " is “FILES”

5.3. Testing 3

Encrypted Word: WHEN

Step 1: Apply a Caesar Cipher with a Shift of 4

W = J

W = 23

23 + 4 = 27 = A

H = L

H = 8

8 + 4 = 12 = L

E = I

E = 5

5 + 4 = 9 = I

N = R

N = 14

14 + 4 = 18 = R

Result after Caesar cipher= ALIR

Step 2: Left Cyclic Shift by 3

Original	A	L	I	R
Shifted	R	A	L	I

Table 18 Left cyclic shift by 3 for encryption for Testing 3

Result after the cyclic shift= RALI

Step 3: XOR Encryption

Now, using the binary XOR operation for further encryption.

R = 17 Binary: 10001

A = 0 Binary: 00000

L = 11 Binary: 01011

I = 8 Binary: 01000

Performing XOR operation with 10001 for all the letters:

10001 XOR 10001 = 00000 = A

00000 XOR 10001 = 10001 = R

01011 XOR 10001 = 11010 = space

01000 XOR 10001 = 11001 = Z

Result after XOR encryption= AR Z

The final encrypted text for "WHEN" is “AR Z”

Decrypting Word: AR Z

Step 1: Reverse XOR Encryption

Using the same XOR key (10001 in binary) on each letter.

A = 0 Binary: 00000

R = 17 Binary: 10001

space = 26 Binary: 11010

Z = 26 Binary: 11001

Performing XOR again with 10001 for all the letters:

00000 XOR 10001 = 10001 = R

10001 XOR 10001 = 00000 = A

11010 XOR 10001 = 01011 = L

11001 XOR 10001 = 01000 = I

Result after reversing XOR: "RALI"

Step 2: Reversing the Left Cyclic Shift

Original	R	A	L	I
Shifted	A	L	I	R

Table 19 Reversing the Left cyclic shift for decryption for Testing 3

Result after reversing the cyclic shift: "ALIR"

Step 3: Reversing Caesar Cipher

A = W

A = 27 (or 1)

27 - 4 = 23 = W

L = H

L = 12

12 - 4 = 8 = H

I = E

I = 9

9 - 4 = 5 = E

R = N

R = 18

18 - 4 = 14 = N

Result after reversing the Caesar cipher: WHEN

The final decrypted text for " AR Z" is “WHEN”

5.4. Testing 4

Encrypted Word: YOU

Step 1: Apply a Caesar Cipher with a Shift of 4

Y = C

Y = 25

25 + 4 = 29 = C

O = S

O = 15

15 + 4 = 19 = S

U = Y

U = 21

21 + 4 = 25 = Y

Result after Caesar cipher= CSY

Step 2: Left Cyclic Shift by 3

Original	C	S	Y
Shifted	C	S	Y

Table 20 Left cyclic shift by 3 for encryption for Testing 4

Result after the cyclic shift= CSY

Step 3: XOR Encryption

Now, using the binary XOR operation for further encryption.

C = 2 Binary: 00010

S = 18 Binary: 10010

Y = 24 Binary: 11000

Performing XOR operation with 10001 for all the letters:

00010 XOR 10001 = 10011 = T

10010 XOR 10001 = 00011 = D

11000 XOR 10001 = 01001 = J

Result after XOR encryption= TDJ

The final encrypted text for "YOU" is “TDJ”

Decrypting Word: TDJ

Step 1: Reverse XOR Encryption

Using the same XOR key (10001 in binary) on each letter.

T = 19 Binary: 10011

D = 3 Binary: 00011

J = 9 Binary: 01001

Performing XOR again with 10001 for all the letters:

10011 XOR 10001 = 00010 = C

00011 XOR 10001 = 10010 = S

01001 XOR 10001 = 11000 = Y

Result after reversing XOR: "CSY"

Step 2: Reversing the Left Cyclic Shift

Original	C	S	Y
Shifted	C	S	Y

Table 21 Reversing the Left cyclic shift for decryption for Testing 4

Result after reversing the cyclic shift: "CSY"

Step 3: Reversing Caesar Cipher

C = Y

C = 29 (or 3)

29 - 4 = 25 = Y

S = O

S = 19

19 - 4 = 15 = O

Y = U

Y = 25

25 - 4 = 21 = U

Result after reversing the Caesar cipher: YOU

The final decrypted text for "TDJ" is “YOU”

5.5. Testing 5

Encrypted Word: PLAY

Step 1: Apply a Caesar Cipher with a Shift of 4

P = T

P = 16

16 + 4 = 20 = T

L = P

L = 12

12 + 4 = 16 = P

A = E

A = 1

1 + 4 = 5 = E

Y = C

Y = 25

25 + 4 = 29 = C

Result after Caesar cipher= TPEC

Step 2: Left Cyclic Shift by 3

Original	T	P	E	C
Shifted	C	T	P	E

Table 22 Left cyclic shift by 3 for encryption for Testing 5

Result after the cyclic shift= CTPE

Step 3: XOR Encryption

Now, using the binary XOR operation for further encryption.

C = 2 Binary: 00010

T = 19 Binary: 10011

P = 15 Binary: 01111

E = 4 Binary: 00100

Performing XOR operation with 10001 for all the letters:

00010 XOR 10001 = 10011 = T

10011 XOR 10001 = 00011 = D

01111 XOR 10001 = 11110 = *

00100 XOR 10001 = 10101 = V

Result after XOR encryption= TD*V

The final encrypted text for "PLAY" is “TD*V”

Decrypting Word: TD*V

Step 1: Reverse XOR Encryption

Using the same XOR key (10001 in binary) on each letter.

T = 19 Binary: 10011

D = 3 Binary: 00011

* = 30 Binary: 11110

V = 21 Binary: 10101

Performing XOR again with 10001 for all the letters:

10011 XOR 10001 = 00010 = C

00011 XOR 10001 = 10011 = T

11110 XOR 10001 = 01111 = P

10101 XOR 10001 = 00100 = E

Result after reversing XOR: "CTPE"

Step 2: Reversing the Left Cyclic Shift

Original	C	T	P	E
Shifted	T	P	E	C

Table 23 Reversing the Left cyclic shift for decryption for Testing 5

Result after reversing the cyclic shift: "TPEC"

Step 3: Reversing Caesar Cipher

T = P

T = 20

20 - 4 = 16 = P

P = L

P = 16

16 - 4 = 12 = L

E = A

E = 5

5 - 4 = 1 = A

C = Y

C = 29 (or 3)

29 - 4 = 25 = Y

Result after reversing the Caesar cipher: PLAY

The final decrypted text for "TD*V" is “PLAY”

6. Conclusion

This coursework discusses the critical role cryptography plays in protecting sensitive information, finding its evolution from ancient methods to the advanced systems we use today. Caesar Cipher which is a simple yet historically significant encryption technique was revolutionary in its time but had major flaws like predictability and vulnerability to attacks which make it unreliable for modern cybersecurity needs.

To address these issues, the coursework introduces a new algorithm that builds on the Caesar Cipher by adding extra layers of security. This improved method combines Caesar shifts, left cyclic shifts, and XOR operations to create a much stronger encryption system. It's designed to defend against common threats like brute force and pattern recognition while still being user-friendly. Tests showed that the new algorithm works well, successfully protecting data while maintaining the core principles of cryptography: confidentiality, integrity, and availability.

At last, the study suggests ways to enhance this algorithm even further with flow-chart. It could be adapted for real-time applications, combined with asymmetric encryption techniques or applied to secure communication protocols. By combining simple, foundational ideas with modern improvements, this research highlights how cryptography can evolve to meet today's digital security challenges.

7. References

Adomey, M. K. (12/10/2016). *Introduction to Cryptography .*

Becan, K. (2024, November 18). *CIA Triad*. Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,and%20methods%20for%20creating%20solutions.

Buxton, O. (2023, November 27). *norton*. Retrieved from norton: https://us.norton.com/blog/emerging-threats/cryptography

GeeksforGeeks. (2022, October 06). Retrieved from GeeksforGeeks: https://www.geeksforgeeks.org/history-of-cryptography/

geeksforgeeks. (2024, June 27). Retrieved from geeksforgeeks: https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

Goyal, A. (2024, March 27). *code360 by codingninjas*. Retrieved from code360 by codingninjas: https://www.naukri.com/code360/library/what-do-you-mean-by-cryptosystem

Obrien, B. (2024). *YourShortlist*. Retrieved from YourShortlist: https://yourshortlist.com/the-importance-of-the-cia-triad-to-cybersecurity/

Sidhpurwala, H. (2023, January 12). *RedHat*. Retrieved from RedHat: https://www.redhat.com/en/blog/brief-history-cryptography#:~:text=The%20first%20known%20evidence%20of,place%20of%20more%20ordinary%20ones.

Whitman, M. E. (2021). *Principles of Information Security.* Boston, Massachusetts: Cengage Learning.