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: Suhrid Shrestha

London Met ID:23047343

College ID:NP01NT4A230038

Assignment Due Date: Dec 10, Tuesday, 2024

Assignment Submission Date: Dec 10, Tuesday, 2024

Word Count (Where Required):

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

Acknowledgement

Firstly, I would like to thank our module teacher, Suruchi Shrestha, for guiding us through this research project by correcting us and supporting us. The time that you have given us to go through this project is invaluable.

Also, I would like to thank my friends and colleagues for their slight support in giving me ideas about topics and how the report should be.

Finally, I would like to thank my family and friends for their unwavering support and understanding during this research. This project would not have been possible without their encouragement.

Abstract

This report delves into the intricacies of information security, emphasizing the significance of cryptographic methods to ensure confidentiality, integrity, and availability (CIA) of data. It begins by introducing the core principles of information security and the critical role the CIA triad plays in delivering quality and reliable security solutions. The concept of cryptography is explored, alongside its historical evolution and foundational terminologies, providing a solid framework for understanding modern encryption techniques. The report selects a specific cryptographic algorithm, analyzes its background, and demonstrates its practical application through an encryption and decryption example. The advantages and disadvantages of the algorithm are critically evaluated to provide insights into its strengths and limitations. Furthermore, the study proposes a modified encryption algorithm that integrates novel mathematical and logical enhancements to address existing vulnerabilities, enhance security, and optimize efficiency. This modified algorithm is presented with detailed explanations of its methodology, encryption, and decryption processes. Finally, a comprehensive flowchart is provided to visually represent the workings of the newly developed cryptographic system. The report aims to offer a structured and innovative approach to cryptography, contributing to the field of secure communication and data protection.

Contents

List of Tables

Table of Figures

1.Introduction

1.1. Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users through ransomware; or interrupting normal business processes.

An ideal cybersecurity approach should have multiple layers of protection across any potential access point or attack surface. This includes a protective layer for data, software, hardware and connected networks. In addition, all employees within an organization who have access to any of these endpoints should be trained on the proper compliance and security processes. Organizations also use tools such as unified threat management systems as another layer of protection against threats. These tools can detect, isolate and remediate potential threats and notify users if additional action is needed.

Cyberattacks can disrupt or immobilize their victims through various means, so creating a strong cybersecurity strategy is an integral part of any organization. Organizations should also have a disaster recovery plan in place so they can quickly recover in the event of a successful cyberattack.

1.1.2 Who needs cyber security?

It is a mistake to believe that you are of no interest to cyber attackers. Everyone who is connected to the Internet needs cyber security. This is because most cyber attacks are automated and aim to exploit common vulnerabilities rather than specific websites or organisations.

1.1.3. Network Security

Focuses on securing computer networks from unauthorized access, data breaches, and other network-based threats. It involves technologies such as Firewalls, Intrusion detection systems (IDS), Virtual private networks (VPNs), and Network segmentation. Guard your internal network against outside threats with increased network security. Sometimes we used to utilize free Wi-Fi in public areas such as cafes, Malls, etc. With this activity, 3rd Party starts tracking your Phone over the internet. If you are using any payment gateway, then your bank account can be Empty. So, avoid using Free Network because Free Network Doesn’t support Securities.

1.1.4. Data security

A subset of information security, data security combines many types of cybersecurity solutions to protect the confidentiality, integrity, and availability of digital assets at rest (i.e., while being stored) and in motion (i.e., while being transmitted).

1.1.5. Operational security

Operational security covers many types of cybersecurity processes and technology used to protect sensitive systems and data by establishing protocols for access and monitoring to detect unusual behaviour that could be a sign of malicious activity.

1.1.6. Cloud security

Cloud security focuses on protecting cloud-based assets and services, including applications, data, and infrastructure. Most cloud security is managed as a shared responsibility between organizations and cloud service providers. In this shared responsibility model, cloud service providers handle security for the cloud environment, and organizations secure what is in the cloud. Generally, the responsibilities are divided as shown below.

1.2 CIA Triad

The **CIA Triad** is a fundamental framework in information security.

-Confidentiality ensures that information is accessible only to authorized individuals or systems, protecting sensitive data from unauthorized access or disclosure through methods like encryption, access controls, and secure network configurations.

-Integrity guarantees that data remains accurate, consistent, and unaltered, employing techniques such as hashing, digital signatures, and checksums to detect and prevent unauthorized modifications or corruption.

-Availability ensures that authorized users have timely and reliable access to information and systems, even during disruptions, through strategies like redundancy, regular backups, load balancing, and DDoS protection. Together, these principles form the cornerstone of protecting information systems and maintaining trust in their operations.

1.2.1 Importance of CIA Triad

Each letter in the CIA triad represents a foundational principle in cybersecurity. The importance of the security model speaks for itself: Confidentiality, integrity and availability are considered the three most important concepts in infosec. Considering these three principles together within the triad framework guides the development of security policies for organizations. When evaluating needs and use cases for potential new products and technologies, the triad helps organizations ask focused questions about how value is being provided in those three key areas. Benefits of CIA Triad:

- **Data security and privacy:** The most obvious benefit is ensuring preparedness in the face of today's sophisticated cyberattacks and other unauthorized attempts to access, steal or manipulate valuable data.
- **Compliance:** Ensuring the confidentiality, integrity and availability of sensitive information means regulations and legal frameworks that exist to safeguard this information are followed.
- **Proactive risk prevention:** When applied correctly, the triad creates an environment where security risks are proactively prevented. Existing vulnerabilities are identified and mitigated to prevent future threats.
- **Comprehensiveness:** The three components mean that security teams aren't just concerned with thwarting attackers, but they're also ensuring the veracity and availability of their data. For example, when a large volume of data is needed for analysis, following the CIA triad means the data is available and accessible when needed.

1.3 What is Cryptography? (Evolution and History)

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce.

1.3.1 Evolution

The history of cryptology spans several distinct eras, each marked by significant advancements and innovations. Before 1500, cryptology was often considered a form of magic. The ancient Greeks and Romans developed early techniques, such as the Caesar cipher, to protect communications. During the Middle Ages, the Arab world made substantial contributions, including the development of frequency analysis, which became a foundational tool for breaking ciphers. Monastic scholars and poets in Europe also experimented with cryptographic methods, blending their work with art and intellect.

From 1500 to 1776, cryptology evolved into a more structured practice with the rise of "black chambers," secret offices dedicated to intercepting and deciphering correspondence. Notable events included Bacon and Shakespeare's cryptographic experiments and the use of ciphers in political intrigues, such as the plot involving Mary, Queen of Scots. This period also saw the development of nomenclators and increasingly complex substitution ciphers.

Cryptography played a pivotal role during the American Revolution, where secret writing and espionage became critical tools in warfare. Both British and American forces used cipher systems to secure their communications. After the revolution, cryptographic methods continued to advance, reflecting the growing importance of secure communication in diplomacy and statecraft.

During the American Civil War (1861–1865), cryptography was employed by both Union and Confederate forces. Techniques included encoding battlefield messages, and efforts to break the Vigenère cipher gained prominence. The war underscored the strategic value of cryptology in military operations.

World War I (1914–1919) marked a turning point with significant cryptographic breakthroughs. The British intelligence group Room 40 played a crucial role in decoding German messages, while the United States established MI-8, its first code-breaking unit. Trench codes were widely used, and new ciphers like the ADFGVX were introduced. These advancements laid the groundwork for modern cryptology, which would come into its own during subsequent conflicts and in the age of computing. *(JF Dooley - History of Computing, 2018 – Springer)*

1.3.2 Formation of Cryptography

The formation of cryptography is rooted in the need for secure communication throughout history, evolving alongside societal and technological advancements. Initially, cryptography focused on encryption and secrecy to protect messages against unauthorized access. Ancient methods like substitution ciphers, such as the Caesar cipher, laid the foundation for symmetric encryption, where both sender and receiver use the same key.

As communication expanded with the advent of electronic systems, the objectives of cryptography diversified to include confidentiality, integrity, and authentication. Modern cryptography introduced asymmetric encryption, exemplified by the RSA algorithm, enabling secure key exchanges and digital signatures. The use of mathematical principles, such as modular arithmetic and discrete logarithms, further enhanced cryptographic strength.

Cryptography evolved to address emerging challenges, such as e-commerce and digital communication, by providing secure payment protocols and digital signatures that hold legal validity. Recent developments, including elliptic curve cryptography and quantum-resistant algorithms, continue to shape cryptography to meet the demands of an interconnected world. *(H Delfs, H Knebl, - 2002 – Springer)*

1.4 Types of cryptography

1.4.1 Symmetric Cryptography

Symmetric cryptography, also known as secret-key cryptography, relies on a single key shared between the sender and the receiver for both encryption and decryption. This approach is efficient and fast, making it ideal for encrypting large volumes of data, such as in file storage or real-time communication. Popular algorithms include the Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES. Symmetric cryptography is commonly used in applications like VPNs, disk encryption, and secure file transfers.

1.4.2 Asymmetric Cryptography

Asymmetric cryptography, or public-key cryptography, employs a pair of keys: a public key for encryption and a private key for decryption. This key pair eliminates the need for a shared secret, as the public key can be freely distributed while the private key remains secure. Algorithms such as RSA, ElGamal, and Elliptic Curve Cryptography (ECC) are foundational to asymmetric methods. Asymmetric cryptography is widely used in digital signatures, secure key exchange protocols, and email encryption.

2. Caesar Cipher Text (Selected Algorithm)

The earliest known and the simplest use of substitution cipher was by Julius Caesar. The Caesar Cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

2.1 History of Caesar Cipher Text

The Caesar Cipher is one of the earliest and simplest known encryption techniques in history, named after the Roman general and statesman Julius Caesar. It was primarily used during his military campaigns around 58-50 BCE to secure sensitive communications. Caesar reportedly used this cipher to send encrypted messages to his commanders, ensuring that even if the messages were intercepted by enemies, the contents would remain incomprehensible.

The cipher works by shifting each letter in the plaintext by a fixed number of positions in the alphabet. For example, with a shift of 3, the letter "A" becomes "D," "B" becomes "E," and so on. Julius Caesar is said to have used a shift of three for his communications, though the specific shift can vary, depending on the user.

Despite its historical significance, the Caesar Cipher is highly insecure by modern standards. Its simplicity means it can be easily broken using techniques like frequency analysis, where patterns in the text are analyzed to reveal the encryption key. However, during Caesar's time, it served its purpose effectively, as literacy was limited, and the concept of cryptographic analysis was unknown.

The Caesar Cipher laid the foundation for more sophisticated encryption methods. Over time, it evolved into more complex techniques, such as the substitution ciphers used in the Middle Ages. Today, it remains a popular teaching tool in cryptography, introducing beginners to the fundamental principles of encryption and decryption.

2.2 How Caesar Cipher works?

The Caesar cipher is a type of substitution cipher that replaces each letter in the plaintext with another letter located a fixed number of positions forward or backward in the alphabet. In this example, a forward shift of 3 is applied, meaning 'A' is transformed into 'D,' 'B' into 'E,' and so on. While this straightforward method is simple to use and easy to grasp, it offers minimal security. The table below show the conversion of every alphabet to cipher.

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
D	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

Table 1 of Plaintext to Cipher Text

2.3 Example of Caesar Cipher Text

For example, we take a word, BURGER.

‘BURGER’ is the plaintext message that we now need to convert to cipher text. So, to encrypt, we have to shift each of the alphabet in that word to 3 letters further.

B→E

U→X

R→U

G→J

E→H

R→U

After shifting, we have the cipher text ‘EXUJHU’ which is the encrypted message.

Now, the cipher text is ‘EXUJHU’. So, to decrypt the message we need to shift the letter 3 alphabets backwards.

E→B

X→U

U→R

J→G

H→E

U→R

After shifting we have the decrypted message ‘BURGER’.

2.3. Advantages of Caesar Cipher

-Easy to implement and use thus, making suitable for beginners to learn about encryption.
-Can be physically implemented, such as with a set of rotating disks or a set of cards, known as a scytale, which can be useful in certain situations.
-Requires only a small set of pre-shared information.

2.4 Disadvantages of Caesar Cipher

-It is not secure against modern decryption methods.
-Vulnerable to known-plaintext attacks, where an attacker has access to both the encrypted and unencrypted versions of the same messages.
-The small number of possible keys means that an attacker can easily try all possible keys until the correct one is found, making it vulnerable to a brute force attack.
-It is not suitable for long text encryption as it would be easy to crack.
-It is not suitable for secure communication as it is easily broken.
-Does not provide confidentiality, integrity, and authenticity in a message.

3.Newly Modified Cryptography Method

In this coursework, I have used a substitution symmetric algorithm which is names as ‘XOR Caesar Crypt’. This method includes reversed caesar cipher. The XOR Caesar Crypt Algorithm is an innovative encryption technique that blends classical cryptographic methods with modern computational processes to achieve a multi-layered approach to data security. This algorithm leverages the simplicity and elegance of the Caesar Cipher, while enhancing it with modern transformations like ASCII encoding, binary manipulation, and XOR operations. The result is a dynamic and robust encryption process designed to resist common cryptanalysis techniques.

At its core, the XOR Caesar Crypt enhances the simplicity of the Caesar Cipher by introducing layers of complexity that transform the plaintext into an encrypted form through a series of structured steps. The use of reversible transformations, numerical representations, and bitwise operations ensures that the encryption process is dynamic and highly resistant to conventional cryptanalysis techniques.

This algorithm is designed to provide versatility and adaptability, making it suitable for various applications, from lightweight encryption tasks to educational demonstrations of cryptographic principles. By blending classical inspiration with modern innovation, the XOR Caesar Crypt represents a creative advancement in the field of encryption.

3.1 Changes made in this new algorithm

i. Reversed Caesar Cipher

In this algorithm, we use reversed Caesar cipher in the beginning instead of forward Caesar Cipher. This adds an extra layer of obfuscation by reversing the order of characters in the plaintext before encryption.

ii. Decimal Conversion

Converts the binary output of XOR back into decimal values, making the data more readable or easier to process in subsequent steps.

iii. Final Caesar Cipher with Dynamic Shift

Reintroduced Caesar Cipher, but this time used a dynamic shift value derived from the previous XOR-to-decimal step. This ensures the shift is unpredictable and unique to each message, making the cipher harder to crack.

iv. Introduced dynamic and multi-step shifting rather than a fixed key.

3.2 XOR Caesar Crypt Algorithm

Encryption:

Here is a step by step process of XOR Caesar Crypt algorithm:

We take a word for example that is ‘BURGER’.

Step 1: First, we shift the letters of the word by 3 places backwards. (Reversed Caesar Cipher). We get, ‘YRODBO’.

B→Y

U→R

R→O

G→D

E→B

R→O

Step 2: Then, we apply ascii code to the new text. We get,

Y→89

R→82

O→79

D→68

B→66

O→79

Step 3: Now, We convert these ascii codes into binary numbers. We get,

Y→89→ 01011001

R→82→ 01010010

O→79→ 01001111

D→68→ 01000100 00001101

B→66→ 01000010

O→79→ 01001111

Step 4: Now, we apply XOR operations to these binary numbers.

We get, 00001101

Step 5: Now, we again convert this binary to decimal.

We get, 13.

Step 6: Now, we shift the Reversed Caesar Cipher text by 13. We get, 'LEBQOB'

Y shifted by +13 → (24 + 13) % 26 = 37 % 26 = 11 → L

R shifted by +13 → (17 + 13) % 26 = 30 % 26 = 4 → E

O shifted by +13 → (14 + 13) % 26 = 27 % 26 = 1 → B

D shifted by +13 → (3 + 13) % 26 = 16 % 26 = 16 → Q

B shifted by +13 → (1 + 13) % 26 = 14 % 26 = 14 → O

O shifted by +13 → (14 + 13) % 26 = 27 % 26 = 1 → B

So, The Encrypted message of plaintext “BURGER” is “LEBQOB”.

Decryption:

Step 1: Apply decryption of -13 Caesar cipher. Which we got bye XOR operations and converted to decimal.

L: (11 - 13 + 26) % 26 = 24 → Y

E: (4 - 13 + 26) % 26 = 17 → R

B: (1 - 13 + 26) % 26 = 14 → O

Q: (16 - 13 + 26) % 26 = 3 → D

O: (14 - 13 + 26) % 26 = 1 → B

B: (1 - 13 + 26) % 26 = 14 → O

Step 2: Again, Use Caesar cipher and shift 3 places.

The letter Y shifted forward by 3 becomes B.

The letter R shifted forward by 3 becomes U.

The letter O shifted forward by 3 becomes R.

The letter D shifted forward by 3 becomes G.

The letter B shifted forward by 3 becomes E.

The letter O shifted forward by 3 becomes R.

So, we get the decrypted message “BURGER”.

4. Flow Chart

4.1 Encryption Flowchart

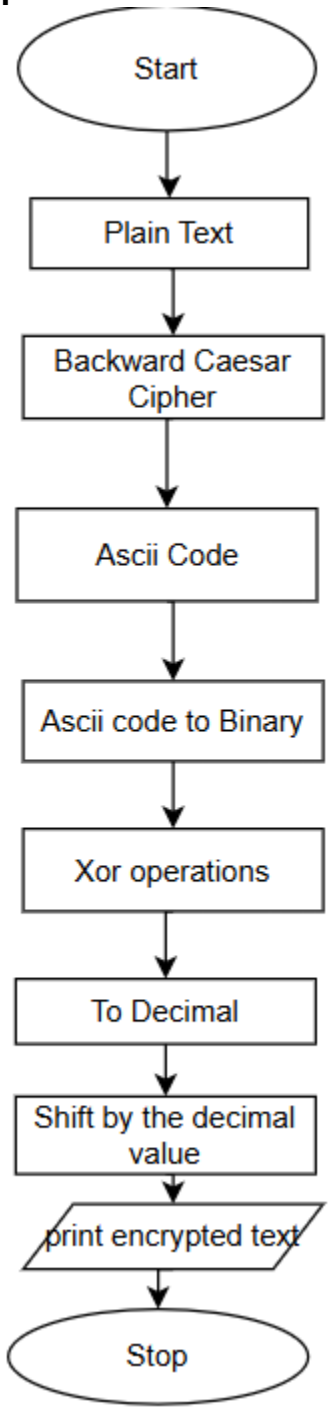

Figure 1 Encryption flowchart

4.2 Decryption Flowchart

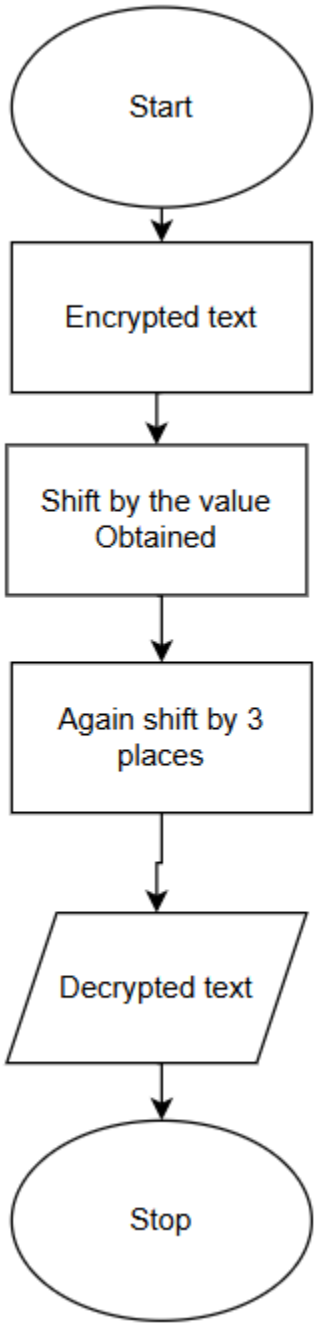

Figure 2 Decryption Folwchart