



**Module Code & Module Title**

**CC5004NI Security in Computing**

**Assessment Weightage & Type**

**30% Individual Coursework**

**Year and Semester**

**2020 -21 Autumn**

**Student Name: Himanshu Pandey**

**London Met ID: 19031311**

**College ID: NP01NT4A190131**

**Assignment Due Date: 22nd Jan 2021**

**Assignment Submission Date: 22nd Jan 2021**

**Word Count (Where Required):**

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

**Contents**

[Introduction 3](#_Toc62151870)

[COMPUTER SECURITY 3](#_Toc62151871)

[CIA 3](#_Toc62151872)

[Confidentiality 4](#_Toc62151873)

[Availability 5](#_Toc62151874)

[Cryptography 5](#_Toc62151875)

[History of cryptography 6](#_Toc62151876)

[Symmetric and Asymmetric Encryption Systems 8](#_Toc62151877)

[Symmetric Encryption System 8](#_Toc62151878)

[Asymmetric Encryption System 9](#_Toc62151879)

[Task 2 10](#_Toc62151880)

[Caesar Cipher 10](#_Toc62151881)

[Mathematical Description 10](#_Toc62151882)

[Advantage and disadvantage of Caesar Cipher 10](#_Toc62151883)

[Advantage 11](#_Toc62151884)

[Disadvantage 11](#_Toc62151885)

[Task 3 11](#_Toc62151886)

[Modified Caesar cipher 11](#_Toc62151887)

[Flow chart 13](#_Toc62151888)

[Strength and Weakness of modified Caesar cipher 19](#_Toc62151889)

[Strength 19](#_Toc62151890)

[Weakness 19](#_Toc62151891)

[Application of new cipher 19](#_Toc62151892)

[Conclusion 20](#_Toc62151893)

[References 21](#_Toc62151894)

[Figure 1 the CIA triad 4](#_Toc62151947)

[Figure 2history of cryptography 7](#_Toc62151948)

[Figure 3 Symmetric encryption 8](#_Toc62151949)

[Figure 4Asymmetric Encryption 9](#_Toc62151950)

[Figure 5 encryption process 13](#_Toc62151951)

[Figure 6Decryption process 14](#_Toc62151952)

Abstract

This workshop is an individual assessment of computer security. This workshop is divided into five separate activities. This article discusses the history of cryptography along with the symmetrical and asymmetric cipher algorithm. Task 2 is about choosing a cryptographic algorithm as defined in the coursework. Task 3 is all about Caesar's cipher, and a new algorithm is about k key 5 and another alphabet value, and task 4 is all about checking a new algorithm of its own. The job is to test the new algorithm with its shortcomings and strengths.

# Introduction

# COMPUTER SECURITY

Computer security is defined as the process of securing the various IT assets and enterprises through IT procedures and is continuous in the ongoing process. In other words, it is known as the security and defense of organizational properties, which are essential documents for the organization of working software, applications and various hardware components such as network, device, data, server, etc. Because of the malicious attacks. And it also says that to protect public and business properties from malicious attacks. Attacker thinks differently and uses a number of tricks and strategies that the user does not know how to reveal sensitive data and business information. So, in order to monitor the malicious attack, the user should be aware of these attackers and pay more attention to them. (htt)

# CIA

CIA is referred to as Confidentiality, Honesty and Availability, which is designed to direct information protection for an entity or any business. Often this paradigm is also referred to as the AIC triad, which is referred to as Availability, Honesty and Confidentiality. These three elements are part of the triad. These elements are considered to be the most critical safety components.

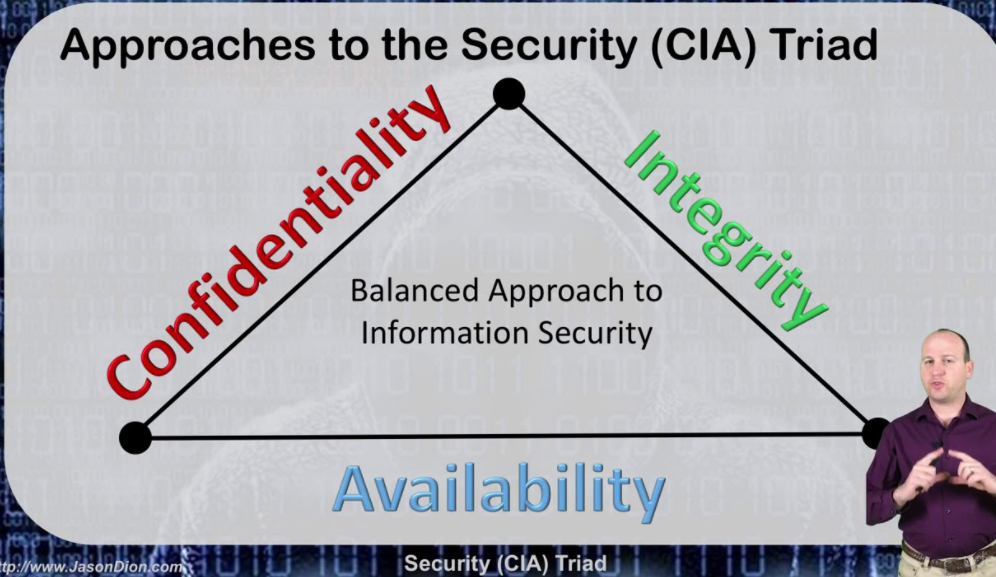
**

Figure 1 the CIA triad

# Confidentiality

Confidentiality means the protection of information or data from disclosure by an unauthorized person. It's the same thing as anonymity. Only an approved individual may gain access to sensitive data. If the unauthorized individual discloses the data, the breach of confidentiality shall be specified.

Example In a data file, confidentiality is protected or access is given to an authorized user, while the unauthorized person is prevented from accessing it. If Ram sends a message to Bobby and if the message contains a confidential message or valuable information or is a hidden message or a sensitive message and confidentiality states that the message can only be read by Bobby if the Trudy or the Middle Man catches the message and discloses it to others, it is considered to be a breach of confidentiality.

**Integrity**

Integrity requires ensuring that information is truthful and that information is not authorized and that information is true. If the unauthorized individual changes the data or records, the infringement is considered to be an integrity breach. It ensures the consistency, precision and reliability of the data over the entire life cycle. It requires the permission of the file and user controls.

Example: The hacker can intercept and change data before it is transmitted to the intended recipient and the measure to preserve the integrity of the information includes Encryption, Hashing, User Access Controls, Checksums, Version Control, Backups. If Ram sends a message to Bobby then in the centre, Trudy Man attacks the data and changes the data in it, it is a breach of honesty.

# Availability

Availability means that an information system is accessible to the approved user. Measures to secure timely and interrupted access to the system. Non-malicious and hardware failures, network latency problems and downtime of unscheduled applications are primary risks to availability.

Example, the message sent by Ram to Bob then the message should only be received by Bobby, which means that only an approved individual has access to the message. If the Trudy man in the center attacks a message or data, then if Trudy does not send a message to the approved individual, but is accessed by an unauthorized person, then this is a breach of Availability. (Mike, 2017)

# Cryptography

Cryptography is a process of creating an algorithm that is used only by the sender and the recipient, except that it hides information. Provides secure information in the presence of hostile third parties. Algorithm is used in encryption by a key to transform input (i.e. plain text) to encrypted output (i.e., text cipher). If the same key is used in the algorithm, it transforms the same level into the same code. (synopsys, 2021)

If the attacker cannot distinguish or specify the properties of the standard text or the key that obtained the code, the only algorithm is known to be the same. The intruder should not be able to recognise or evaluate the key, the code combination used by the key.

There are four terms of cryptography mentioned below:

• Plain text

Simple text or plain message is a readable text that can be read by anyone.

• Text of the cipher: Cipher is an algorithm that is applied to plain text to get a cipher text that is an unreadable result of a cryptography algorithm. The cipher text should be converted to plain text in order to understand the text, but the cipher text cannot be Understand the text, but the text of the cipher cannot be understood.

• Encryption of: It is a mechanism that renders its unreadable content until you have a decryption key by applying a mathematical function to a text.

• Decryption of: When Encryption has secured the file, decryption reverses the file by converting the encrypted text back to plain text. In decryption, two elements are required, which is the right the password and the accompanying decryption algorithm.

# History of cryptography

The misconception is that the art of cryptography is born with the art of writing. As a human being organized and active, they civilized themselves into classes, tribes and kingdoms. These ideas of cryptography allow people to interact secretly with a selective receiver who switches to a continuous production of cryptography. The origins of cryptography lies in the Roman and Egyptian civilizations. The first cryptography was traced through the use of "hieroglyphs." About 4000 years ago, Egyptians used hieroglyphics to communicate with letters. Figure shown is the figure of the hieroglyphics:

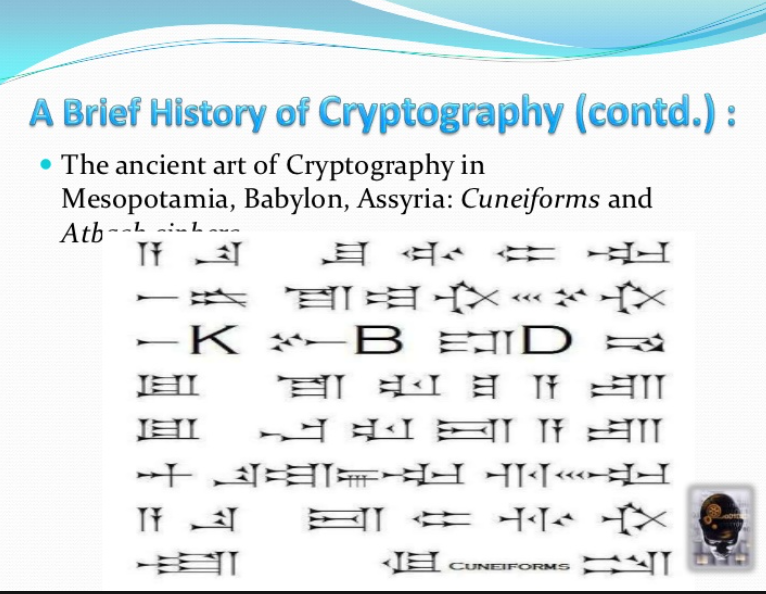


Figure 2history of cryptography

Scientists moved from 500-600 BC to single phase replacement cloths. This hieroglyph was used to replace the alphabet message with other alphabets with a hidden rule. This rule is very critical for sending a response from a message that has been activated.

The figure of Caesar's change is an example of a mono-alphabetic figure. It's easy to know that the encryption process is easy to crack. By juxtaposing, simply lower the alphabet and the beginning of the alphabet for each subsequent alphabet. To see and make sense of the message, it is decrypted in each iteration. If the message is understandable, the code is broken. Frequency analysis refers to the split of the mono-alphabetic number assigned to the Arabs around 1000 AD. This form is used in the letter in English.

Until the Middle Ages, the art and science of cryptography did not display any significant changes or development. However, in the present case, European governments are using encryption in one way or another. The founder of western cryptography is A Leon Battista Alberti, who has created a polyalphabetic substitution. This replacement has been established for the use of two copper disks intertwined. They've always had alphabet character. This disk has been turned to modify the encryption logic, and decrypts the study encryption by restricting the use of the frequency. (Anon, 2020)

There are a number of modifications to polyalphabetic substitution and it is especially attributed to vigenere, although Rubin has little to do with its development. Rubin identified the use of encryption persisted throughout the civil war, using bronze encrypted disks to the south and decoding the message to the north.

# Symmetric and Asymmetric Encryption Systems

# Symmetric Encryption System

Symmetric Encryption Method is a type of encryption that only involves encrypting and decrypting information in a secret key. It's old and it's easier to know the methodology. This device uses a hidden key that is a phrase, a series of letters, or a random number that is a mixture of plain text messages to modify the content in a specific way. To decode and encrypt all texts, sender and receiver the hidden key should be known.

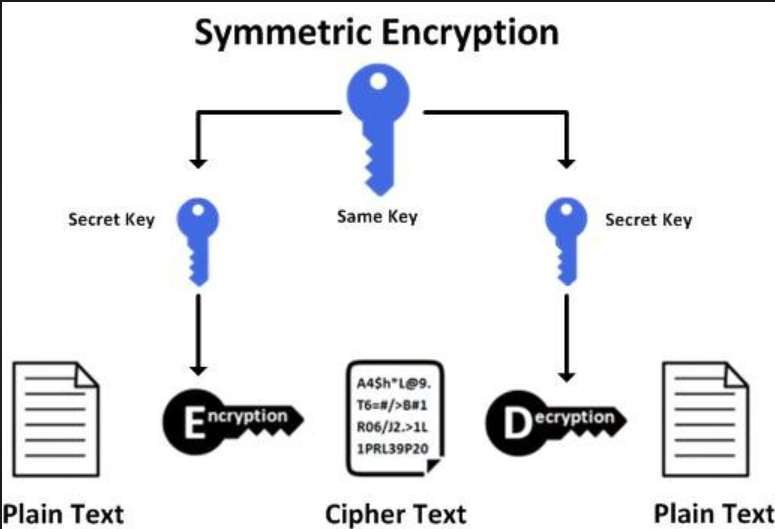


Figure 3 Symmetric encryption

# Asymmetric Encryption System

Asymmetric Encryption also applies to Public Key Encryption. This is a relatively new approach compared to symmetric encryption. That's because it means that the key is not misused by malicious people. It is crucial that anyone with a secret key can decrypt a message that uses two associated keys to increase protection. There is a public key that is free for anyone who sends a message, and the second private key is kept secret. Public key protection is available to the public and can be transmitted over the internet, so now public key security. During communication, the asymmetric key has more power to ensure the security of information.

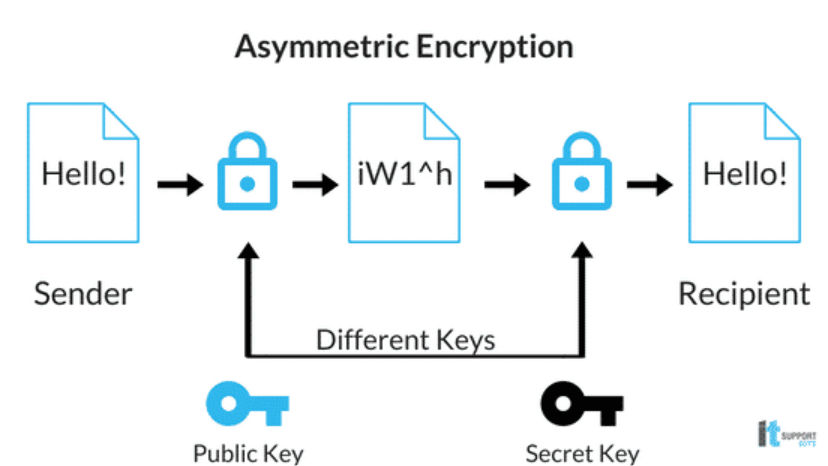


Figure 4Asymmetric Encryption

# Task 2

# Caesar Cipher

Caesar's cipher is the simplest and earliest known cipher. This is the sort of substitution cipher in which each plain text is transferred to a certain position in the alphabet. For eg, with the shift of 1, I would be replaced by shifted to J, S would be replaced or moved to T, and so on. This method, Caesar Cipher, was called Julius Caesar, the method used to communicate with the generals. (Anon, 2021)

Example

The example of Caesar's cipher requires encryption and decryption, and this example encrypts text with a change of 2.

|  |  |
| --- | --- |
| Plain text | Security in Computing |
| Cipher  text | Ugewtva kp eqorwvkpi |

# Mathematical Description

At first, converting all of our characters into numbers in which 'a' is set to 0, 'b' is set to 1 ......., and 'z' =25.now, using the emperor encoding function and (x) a suggestion, where x is the character that we encode, if:

(x) = (x+k) (modification 26)

Where k refers to the key used for each letter. The product of this function is the transformation of a number into a letter and its decryption function is as follows:

(x) = (x-k) (modification 26)

# Advantage and disadvantage of Caesar Cipher

# Advantage

• Caesar cipher is one of the simplest methods to use for encryption and can provide the information with the least amount of protection.

• Only shortcut keys are used through the process.

• If the device cannot use complex coding techniques, the Caesar cipher is one of the better solutions.

• Few computer resources are required.

# Disadvantage

• Uses a basic framework.

• Just offers the least protection to the details.

• It gives a good idea to decode the whole message by the frequency of the letter pattern. (rsarock03, 2008)

# Task 3

# Modified Caesar cipher

The modified César cipher is an extension of the César cipher. The attacker can easily examine the cipher of Caesar so that a fresh idea has been put in place to confuse the cipher of Caesar and strengthen the attacker's security to decrypt the information. Caesar's encryption improves the character by placing or by shifting the algorithm. In this article, there is a new method in which the key size is defined by one and the alphabet index is tested first if the alphabet index is proportional, then the value is increased by one or the index is odd, and then the value is increased by one. If an effort was made to decode the encoding code, it would not be easy to decrypt the document.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Text | | 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 |
| Ke  y | | B | |  | A |  | D | | C | F | E | H | G | J | | I | L | |  | K | N | | M | | P | O | | R | Q | | T |  | S |  | V |  | U | | X | | W | | Z | Y | |
|  | | | | |  | |  | |  |  |  | |  |  | |  |  | | |  | | |  | |  |  | |  |  | |  |  |  | |  | |  | | | |  |  | |  | |
| 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 | |
| 0 | 1 | | 2 | | 3 | | 4 | | 5 | 6 | 7 | 8 | 9 | 1  0 | | 1  1 |  | 1  2 | | 1  3 | |  | 1  4 |  | 1  5 | 1  6 | | 1  7 | 1  8 | | 1  9 |  | 2  0 | | 2  1 | |  | 2  2 | |  | 2  3 | 2  4 | | 2  5 | |

Encryption Algorithm

Step 1: Take plain text in the input.

Step 2: First, the alphabet index is tested whether it is increased by one or the other or if the key is reduced by one.

Step3: Encrypt your text.

Algorithm Decryption

Step 1: Input, take the text of the code.

Step 2: First, the alphabet index is checked whether the alphabet index is proportional, then the alphabet index is increased by one or the other or the main value is reduced by one.

Stage 3: Decode the text

# Flow chart

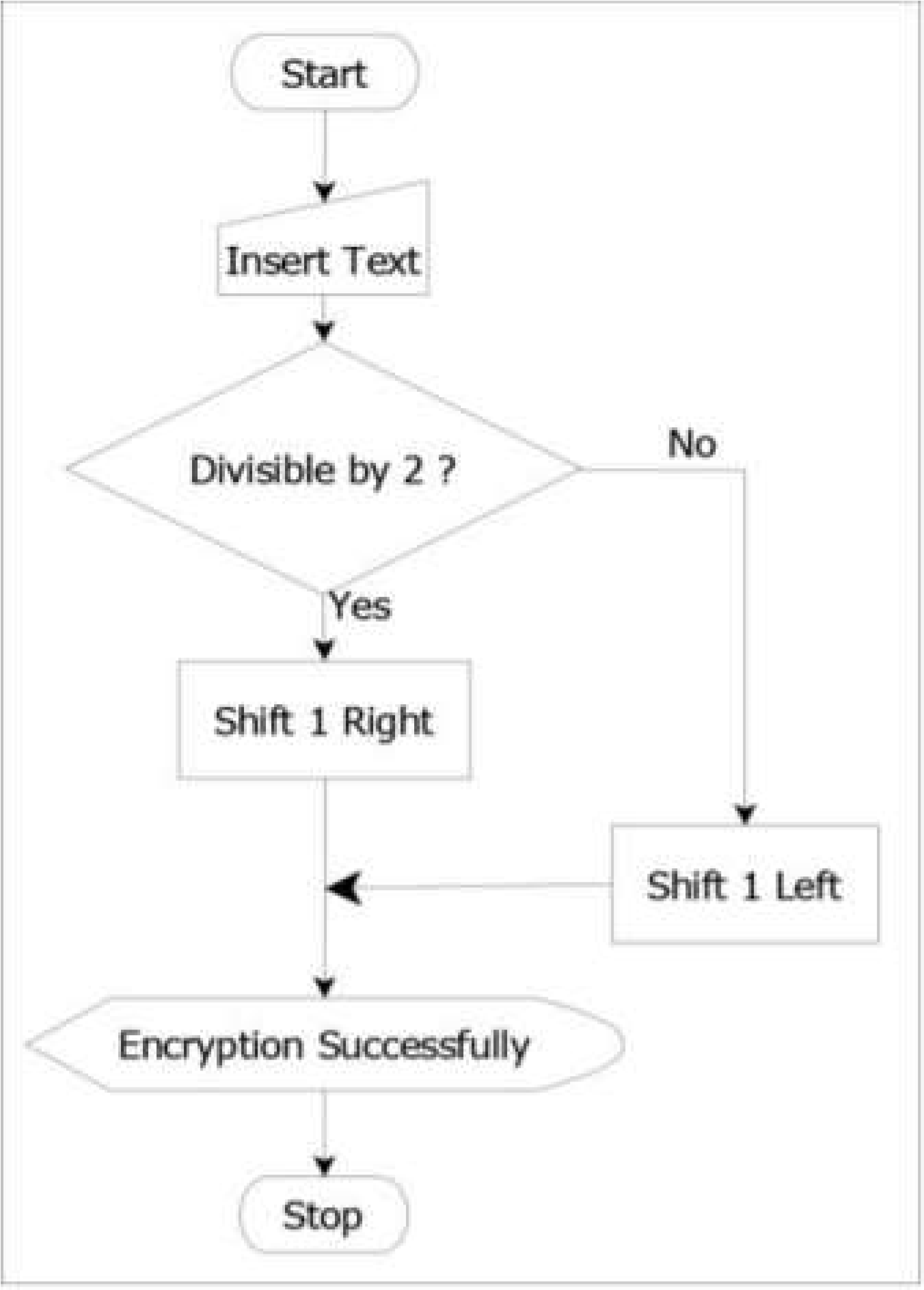


Figure 5 encryption process

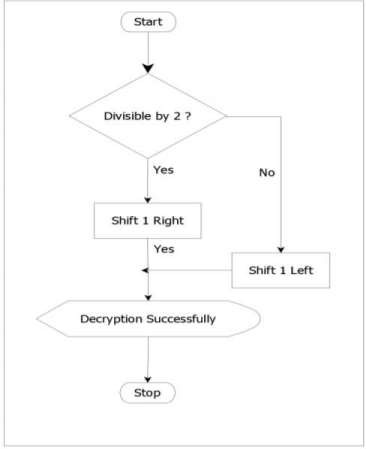


Figure 6Decryption process

Task 4

Testing

Test 1:

Encryption

C= (P+1) mod 26 if P is even then add one or zero than add one Else C=(P-1) mod 26 if P is odd than subtract one.

Decryption

P=(C-1) if C is odd than Subtract one

Else P= (C+1) if C is even or zero than add one

Encrypting plain text “TASK”

T= (P-1) mod 26= 18= S

A= (P+1) mod 26= 1= B

S= (P+1) mod 26= 1= T

K= (P+1) mod 26= 11= L

Hence, the cipher text is “SBTL”;

Decrypting back to plain text;

S= (C+1) mod 26= 19= T

B= (C+1) mod 26= 0=A

T= (C-1) mod 26= 18=S L= (C-1) mod 26= 18=K

Hence the plain text is “TASK”

Test 2

Encryption

C= (P+1) mod 26 if P is even or zero than add one

Else C= (P-1) mod 26 if P is odd than subtract one

Decryption

P=(C-1) if C is odd than Subtract one

Else P= (C+1) if C is even or zero than add one

Encrypting plain text “HELLO”;

H= (P-1) mod 26= 3= G

E= (P+1) mod 26= 10= F

L= (P-1) mod 26= 1= K

L= (P-1) mod 26= 19= K

O=(P+1) mod 26= 19= P

Hence, the cipher text is “GFKKP”;

Decrypting back to plain text;

G= (P+1) mod 26= 7= H F= (P-1) mod 26= 4=E

K= (P+1) mod 26= 11=L

K= (P+1) mod 26= 11=L

P= (P-1) mod 26= 14=O

Hence the plain text is “HELLO”.

Test 3:

Encryption

C= (P+1) mod 26 if P is even then add one or zero than add one Else C=(P-1) mod 26 if P is odd than subtract one.

Decryption

P=(C-1) if C is odd than Subtract one

Else P= (C+1) if C is even or zero than add one

Encrypting plain text “PORK”;

P= (P-1) mod 26= 14= O

O= (P+1) mod 26= 10= P

R= (P-1) mod 26= 16= Q K= (P+1) mod 26= 19= L

Hence, the cipher text is “OPQL”; Decrypting back to plain text;

O= (P+1) mod 26= 15= P

P= (P-1) mod 26= 14=O

Q= (P+1) mod 26= 17=R

L= (P-1) mod 26= 10=K

Hence the plain text is “PORK”.

TASK 4

Encryption

C= (P+1) mod 26 if P is even or zero than add one

Else C= (P-1) mod 26 if P is odd than subtract one Decryption

P=(C-1) if C is odd than Subtract one

Else P= (C+1) if C is even or zero than add one

Encrypting plain text “WORLD”;

W= (P+1) mod 26= 3= X

O= (P+1) mod 26= 10= P

R= (P-1) mod 26= 16= Q

L= (P-1) mod 26= 10= K

D= (P-1) mod 26= 2= C

Hence, the cipher text is “XPQKC”; Decrypting back to plain text;

X= (P-1) mod 26= 22= W

P= (P-1) mod 26= 14=O

Q= (P+1) mod 26= 17=R

K= (P+1) mod 26= 11=L

C= (P+1) mod 26= 3=D

Hence the plain text is “WORLD”.

Encryption

C= (P+1) mod 26 if P is even or zero than add one Else C= (P-1) mod 26 if P is odd than subtract one Decryption P=(C-1) if C is odd than Subtract one

Else P= (C+1) if C is even or zero than add one

Encrypting plain text “WORLD”;

W= (P+1) mod 26= 3= X

O= (P+1) mod 26= 10= P

R= (P-1) mod 26= 16= Q

K= (P+1) mod 26= 19= L

Hence, the cipher text is “XPQKC”; Decrypting back to plain text;

X= (P-1) mod 26= 22= W

P= (P-1) mod 26= 14=O

Q= (P+1) mod 26= 17=R

L= (P-1) mod 26= 10=K

Hence the plain text is “WORK”.

# Strength and Weakness of modified Caesar cipher

# Strength

Data confidentiality is a very critical feature of Caesar's cipher. Key generation plays an important role in digit design. The article shown above is a changed emperor code which is a substitute. Nowadays, the use of the Internet and the network is growing rapidly so that it needs to protect data sent to different networks using different services. The different encryption method is used to provide network security. In this report, the Caesar cipher coding technique is used for security purposes in which different encryption methods are used which have their own unique method. It can be further enhanced if more than one algorithm is used to provide data security. To create a more secure environment, future work explores the concept and uses a data algorithm combination to store and retrieve data.

# Weakness

• It can be easily broken.

• The length of both plain text and cipher text is equivalent.

• More time is needed to encrypt and decrypt the information.

# Application of new cipher

• It can be used for testing purposes.

• It can be used to hide the details.

• You can use it to encrypt your password.

• It can be used to change the cryptographic algorithm.

# Conclusion

The specific task set in this coursework has been accomplished in several respects. This coursework allows me to have the requisite knowledge and information about the cryptographic system. The cryptographic scheme enables safe interaction in the presence of malicious third parties. Encryption uses an algorithm and a key to encrypt the output by converting input (i.e. plain text) (i.e., cipher text). If the same key is used, it transforms text at the same level into the same message. It is all about selecting the cryptographic algorithm.

In Task 2, in which the Caesar cipher is selected in this article. It is one of the earliest known and simplest ciphers in which, as a form of substitution cipher, each input letter (i.e. plain text) is transferred to a certain number of locations in the alphabet. Shifting the plain text by 2 then A would be moved to C, for instance, B would be transferred to D and so on.

In Task 3, it's all about creating a new encryption and decryption algorithm method of choice for us. As in Task 2, the Caesar cipher is described, so the new algorithm is about the Caesar cipher.

Task 4 deals with the testing of our own new algorithm with five different texts.

This report therefore discusses how to create a new cryptography algorithm, and this coursework also provides more knowledge of the cryptographic algorithm.

# References

(n.d.). Retrieved from https://www.edureka.co/blog/what-is-computer-security/#:~:text=What%20is%20computer%20security%3F%201%20Information%20security%20is,computer%20systems%2C%20which%20communicate%20over%20the%20computer%20networks

Anon. (2020). Retrieved from https://www.tutorialspoint.com/cryptography/origin\_of\_cryptography.htm

Anon. (2021). Retrieved from https://economictimes.indiatimes.com/definition/ciphertext

Mike. (2017). *CIA*. Retrieved from https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/

rsarock03. (2008, aug 18). Retrieved from cryptomath.wordpress.com/2008/08/18/caesar-cipher-pros-and-cons/

synopsys. (2021). Retrieved from cryptography: https://www.synopsys.com/glossary/what-is-cryptography.html