LONDON
METROPOLITAN
UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2020 -21 Autumn

Student Name: Ishan Gurung

London Met ID:19031315

College ID: np01nt4a190139

Assignment Due Date: January 22, 2020

Assignment Submission Date:

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

Abstract

This coursework is the individual evaluation of security of computing. This coursework is divided into five different tasks. In this report, it has researched about the history of cryptography along with the symmetric and asymmetric cipher algorithm. Task 2 is about choosing cryptographic algorithm as given in the coursework. Task 3 is all about Caesar cipher and new algorithm is about it with the k key 5 and another alphabet value and task 4 is all about testing of own new algorithm. The task is evaluating the new algorithm by its weakness and strengths.

1. Introduction

COMPUTER SECURITY

Computer security is defined as the process of securing the different IT assets and enterprise through the IT procedures and it is continuous in ongoing procedure. Also, in other words, it is known as the protecting and defending organizational assets that are important document of an organization working software, application and various hardware component like Network, Computer, Data, Server etc. from the malicious attacks. And also says that to protect the individual and enterprise assets from the malicious attacks. Attacker thinks in a different way and uses different tricks and method that the user may not know to disclose the confidential data and business information. So, to control from the malicious attack the user should be aware of these attackers and should pay more attention when user is in internet or online. After only the user information on website gets security. (Aryal, n.d.)

CIA

CIA is termed as Confidentiality, Integrity and Availability which is designed to guide the information security with an organization or any company. Sometimes this model is also called as AIC triad which is termed as Availability, Integrity and Confidentiality. These three components are a triad element. These elements are considered as the most important safety components.

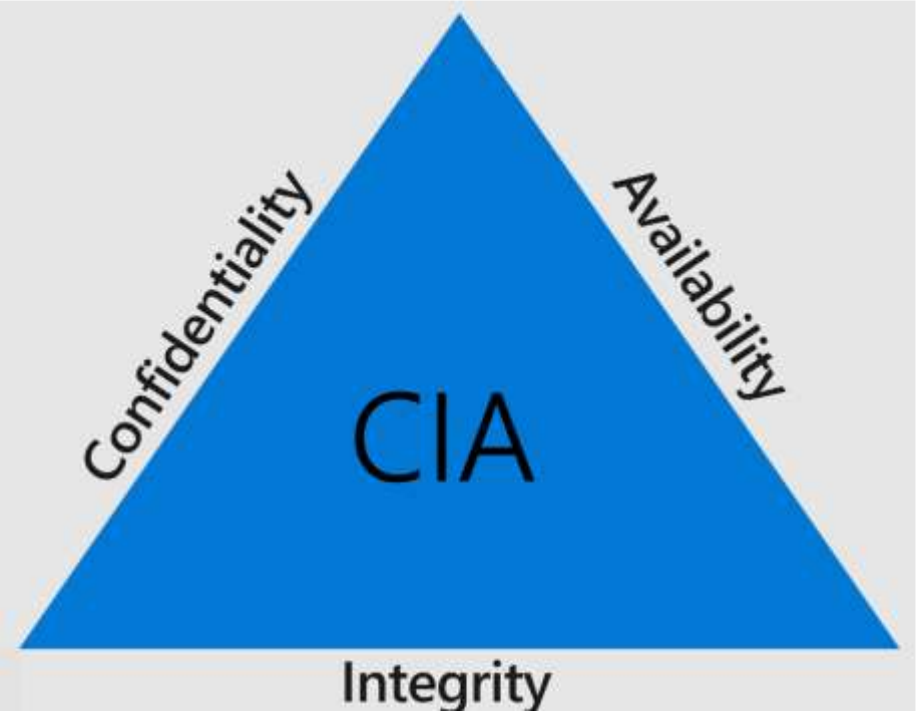


Figure 1 CIA triad

Confidentiality

Confidentiality means to protect the information or data from being accessed by the unauthorized person. It is equal to the privacy. In simple only authorize person can gain access to sensitive data. If the unauthorize person disclose the data the it is said the violation of confidentiality.

Example In computer file, confidentiality is maintained or give access to the authorized person, while unauthorized person is blocked from accessing it. If Alice is sending a message to bob and if the message has a confidential message or the important data or it is secret message or sensitive message and the confidentiality says that the message should only read by bob if the Trudy or middle man captures the message and disclosed to others then it is said to be violation to the confidentiality

Integrity

Integrity means the ensuring the authenticity of information and which information is not allowed and the information is genuine. If the unauthorized person changes the data or information then it said to be the violation of integrity. It maintains the consistency, accuracy and reliability of the data throughout the life cycle. It include file permission and user controls.

Example: A hacker may intercept data and modify it before sending it on to the intended recipient and the measure to maintain the integrity of information includes Encryption, Hashing, User Access Controls, Checksums, Version Control, Backups. If Alice sends a message to bob then Trudy man in the middle attacks the data and changes the data in it then it is the violation of the integrity.

Availability

Availability means to be available to the authorized user of an information system. It measures to protect timely and interrupted access to the system. The fundamental threats to availability are non-malicious and hardware failures, issues in network bandwidth issues and downtime of unscheduled software.

Example, the message sent by Alice to bob then the message should only receive by the bob it means that only authorized person can gets access to the message. If the Trudy man in the middle attacks the message or data then if Trudy doesn't send message to the authorized person bob but it is access in unauthorized person then it is the violation of Availability. (certMike, 2017-2019)

Cryptography

Cryptography is the process of developing algorithm which is only be used by the sender and receiver except them it hides information. It provides secure information in the presence of malicious third parties. Algorithm is used in the encryption a key to convert input (i.e., plain text) to encrypted output (i.e., text cipher). If in the algorithm it uses the same key then it turns the same level into the same code.

If the attacker cannot identify or determine the properties of the standard text or the key that received code the only algorithm is considered as same. Attacker should not be able to identify or to determine about the key, code combination which is used by the key. (synopsys, 2021)

There are four terms of cryptography which are listed below:

- Plain-text
  Plain text or a plain message is a readable which can be read by anyone.

- Cipher-text
  Cipher is an algorithm which is applied to plain text to get ciphertext which is unreadable output of an encryption algorithm. Cipher text should be converted into plain text to understand the text but the cipher text cannot be understandable.

- Encryption:
  It is the process rendering its unreadable content until you have decryption key by applying s mathematical function to a file.

- Decryption:
  When Encryption locked the file then the decryption reverses the file by turning cipher text back to plain text. Two elements are required in decryption which is the correct password and the corresponding decryption algorithm.

History of cryptography

There is the myth that the art of cryptography is born with the art of writing. As a human organized and the involved civilized themselves into groups, tribes and kingdoms. These ideas of cryptography help people to communicate secretly with a selective recipient which turns to continued development of cryptography. The root of cryptography lies in Roman and Egyptian civilization. The first traced cryptography by the use of “hieroglyphs”. About 4000 years ago, Egyptians uses hieroglyphics to communicate with message. The figure of hieroglyphics is shown figure:

Figure 2history of cryptography

Scientists had switched to single phase replacement cloths from 500-600 BC. This hieroglyphic has involved to replace the message of alphabet with other alphabets with a secret rule. This rule is great important to resending a message from a triggered message.

The figure of Caesar’s shift is an example of an monoalphabetic figure. It is easy to know about why encryption method is easy to break. By juxtaposing simply lower the alphabet and the beginning of alphabet with is each subsequent. To see the message and make sense, it is decrypted in each iteration. If the message is readable the code has been broken. Frequency analysis refers to break the monoalphabetic number which is attributed to the Arabs around 1000 AD. This method is used in the English letter.

Until the middle ages, the art and science of cryptography did not show major changes or progress. But at the present situation European governments uses encryption in one way or another. The father of western cryptography is A Leon Battista Alberti because he has developed polyalphabetic substitution. This substitution was developed to use two copper disks intertwined. Ever of them has alphabet character. This disc was turned to change encryption logic, it decrypts the encryption of analysis limiting the use of frequency.

Polyalphabetic substitution has the variety of change and is notable attributed to vigenere, although Rubin it has nothing to do with its creation. Rubin has identified the use of encryption continued during civil war, with the use South of bronze encryption discs, and although the north decoded the message. (Anon., 2020, p. tutorialpoint)

Symmetric and Asymmetric Encryption Systems

Symmetric Encryption System

Symmetric Encryption System is the types encryption which only involves in secret key to encrypt and decrypt information. It is old and better know a technique. This system uses a secret key which is a word, sequence of letter or a random number which is the mixture with the plain text of message to change the content in a specific way. To decrypt and encrypt all message, the sender and recipient should to known the secret key.

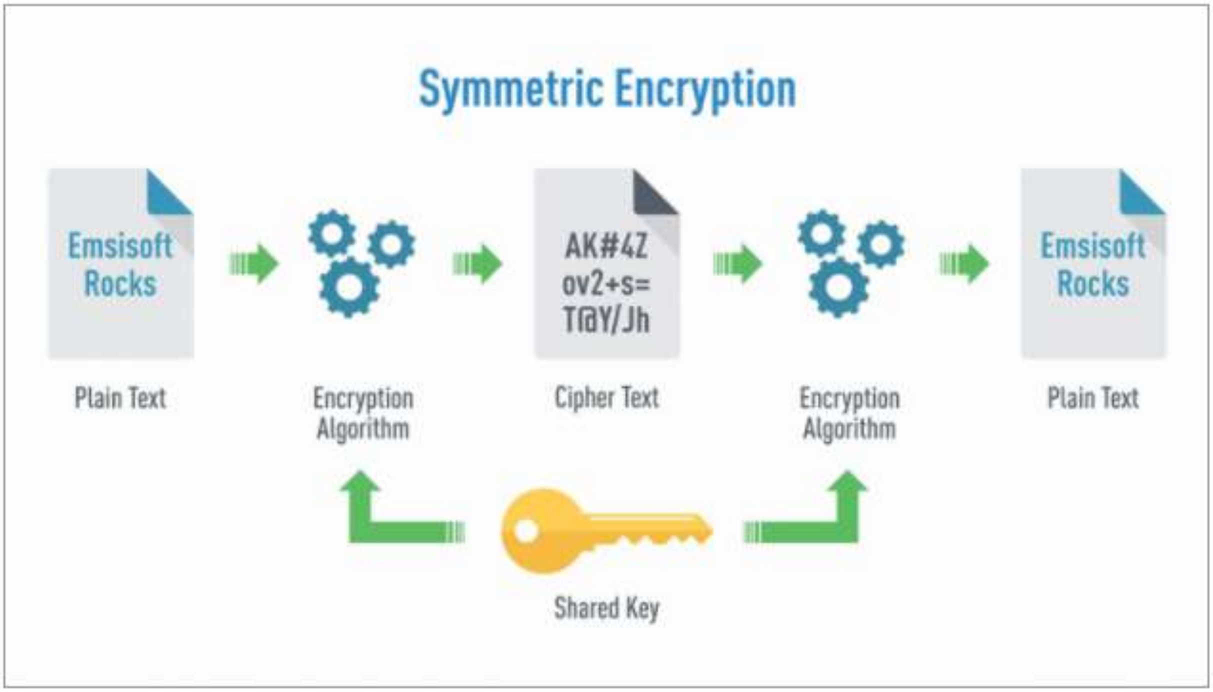


Figure 3 symmetric encryption

Asymmetric Encryption System

Asymmetric Encryption System also refers to Public key encryption. This is the relatively new method it compared to symmetric encryption. It is because it ensures the malicious people do not misuse the key. It is an important Anyone with a secret key can decrypt the message by which it uses two associated keys to increase security. There is a public key which is free to anyone who send a message and the second private is kept secret. Public key security is a publicly accessible and can be transmitted over internet so now public key security. During communication the asymmetric key has more power to ensure to the security of information.

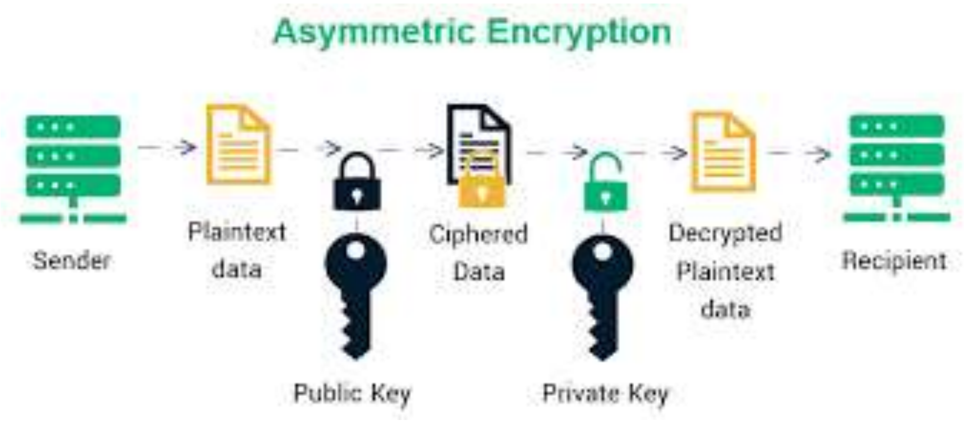


Figure 4 figure of asymmetric encryption

Task 2

Caesar Cipher

Caesar cipher is the simplest and earliest known cipher. This is the type of substitution cipher in which in each plain text is shifted to certain place in the alphabet. For example, with the shift of 1, I would be replaced of shifted to J, S would be replaced or shifted to T and its so on. This method Caesar Cipher was named Julius Caesar which method is used to communicate with generals. (Anon., 2017) (Anon., 2021)

Example

The example of Caesar cipher is involved the encryption and decryption and in this example the text will encrypt with shift of 2.

Plain text	Security in Computing
Cipher text	Ugewtva kp eqorwvkpi

Mathematical Description

At first, translating all our character into number, in which ‘a’ is set as 0, ‘b’ is set as 1 ……., and ‘z’ =25.now, using the emperor encoding function and (x) proposal, where x is character which we are encoding, if:

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

Where, k refers to the key applied to each letter. The result of this function is the translating a number into a letter and its decryption function is:

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

Advantage and disadvantage of Caesar Cipher

Advantage

- Caesar cipher is one of the easiest methods to use for encryption and can provide the least amount of security to the information.
- Through out the process it uses only shortcut keys.
- When the system cannot use complex coding techniques then Caesar cipher is one of the best methods.
- It needs few computing resources.

Disadvantage

- It uses of simple structure.
- It only provides least security to information.
- It gives the good idea to decode the whole message by the frequency of the letter pattern. (Anon., 2017)

Task 3

Modified Caesar cipher

Modified Caesar cipher is an extension of the Caesar cipher. Caesar cipher can be easily analyzed by the attacker so the new concept was made to complicate the Caesar Cipher and increase security for the attacker to decrypt the information. Caesar encryption increase the character by the position or shifted by its algorithm. In this report, there is a new method in which key size is defined by one and the alphabet index is checked first if the alphabet index is proportional, then the value is increased by one or the index is odd, then the value is increased by one. It would not be easy to decrypt the text, if an attempt was made to decrypt the encoding code.

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
Key	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

Table 1key of alphabets

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	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2 Mapping table of alphabet

Encryption Algorithm

Step 1: In input, take a plain text.

Step 2: At first the alphabet index is checked if it is even then it is increased by one or other or decreased the key by one.

Step:3 Encrypt the text

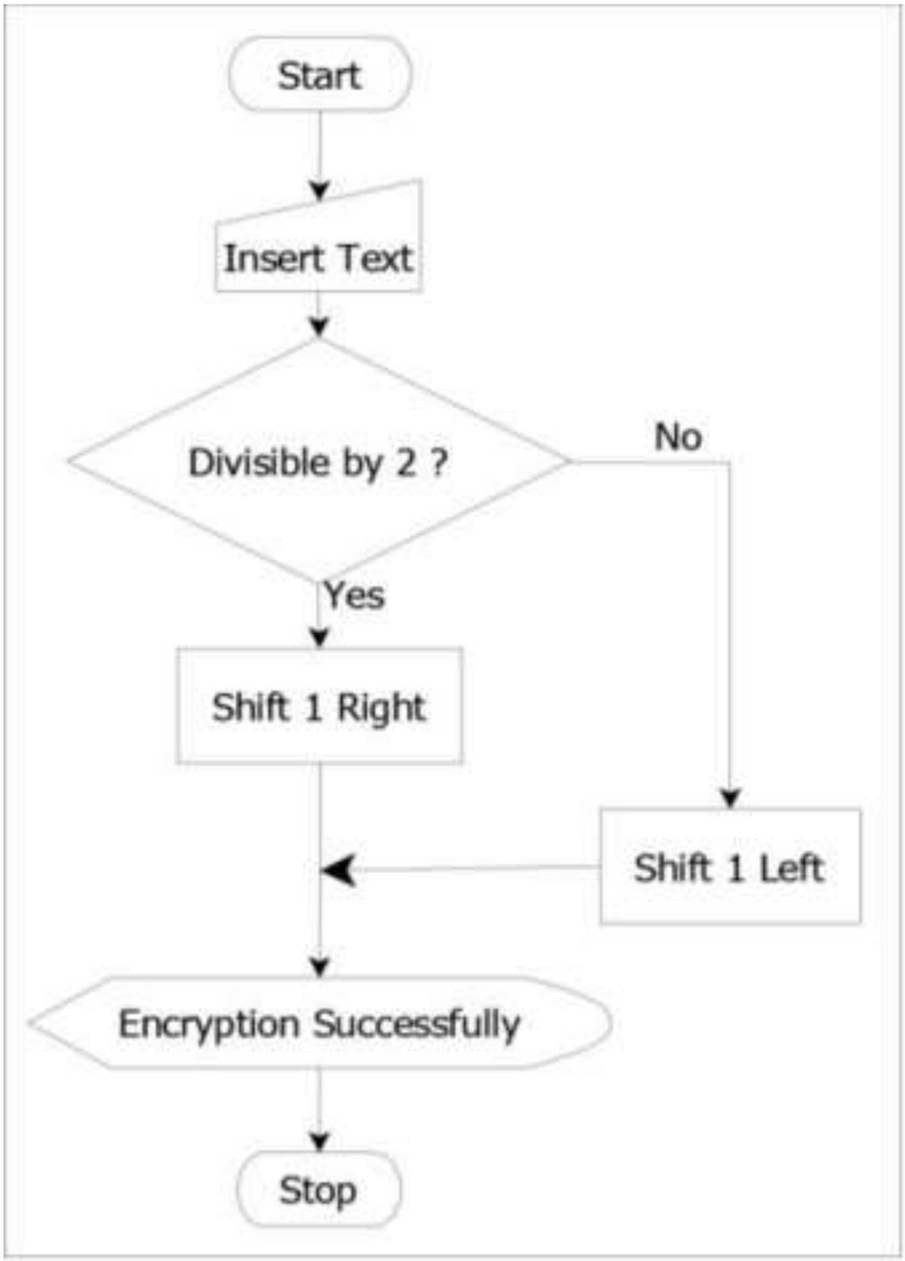
Decryption algorithm

Step 1: in input, take the code text.

Step 2: At first the alphabet index is checked if the alphabet index is proportional then it is increased by one or other or decreased the key value by one.

Step 3: decrypt the text

Flow chart



.

Figure 5 encryption process

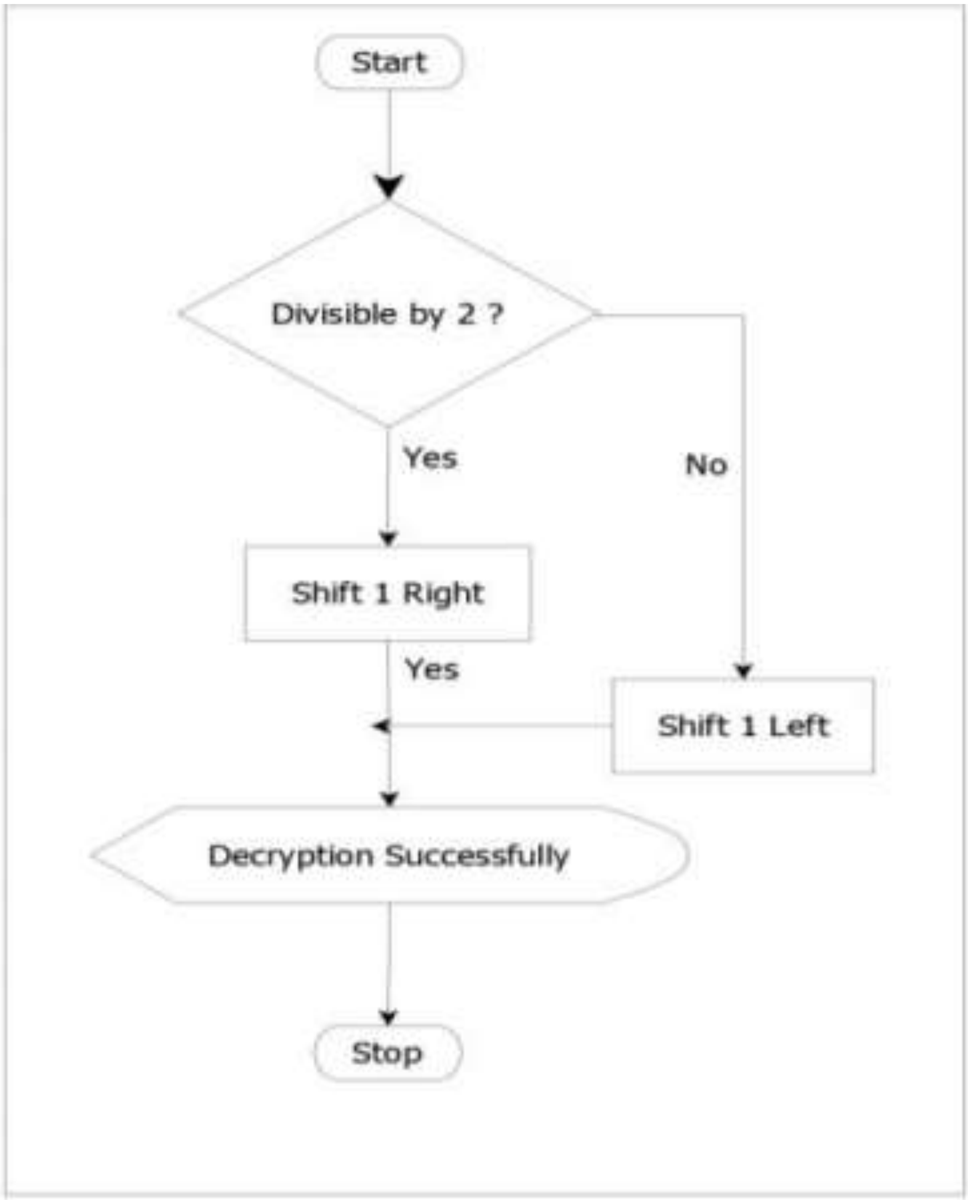


Figure 6 decryption process

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”.

TASK 5

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

In Caesar cipher data security is very important aspect. Key generation plays an important role in designing of the digits. The shown above article is a modified emperor code which is a replacement figure. Nowadays use of internet and the network is growing rapidly so it needs to protect data sent on different network using on different services. Different Encryption method is used to provide security for the network. In this report, Caesar cipher's coding technique is used for security in which different encryption method are used which has its own unique way. It can be further enhanced if more than one algorithm is applied to the data to provide security to the data. To create a more secure environment future work explore the concept and apply the combination of data algorithm for data storage and retrieval.

Weakness

- It can be easily breakable.
- The length of both plain text and cipher text are equal.
- It takes more time to encrypt and decrypt the information.

Application of new cipher

- It can be used for research purpose.
- It can be used for hiding the information.
- It can be used to encrypt the password.
- It can be used for modifying cryptographic algorithm.

Conclusion

The different task which is set in this coursework was completed through many ways. This coursework helps me provide the necessary knowledge and information about the cryptographic system. Cryptography system provides to secure communication in the presence of malicious third parties. Encryption uses an algorithm and a key to convert input (i.e., plain text) to encrypt output (i.e., cipher text). If the same key is used then it turns the same level text into the same code.

In task B, it is all about choosing the cryptographic algorithm in which Caesar cipher is chosen in this report. It is one of the earliest known and simplest ciphers in which it is a type of substitution cipher in which each letter of input (i.e., plain text) is shifted to certain number of places in the alphabet. For example, shifting the plain text by 2 then A would be shifted to C, B would be shifted to D and so on.

In task 3, it is all about creating new method of encryption and decryption algorithm on us on choice. As in task 2, it is described about the Caesar cipher so the new algorithm is about the Caesar cipher.

In the task 4, it is about testing of a new algorithm of our own of five different text.

Thus, this report discusses on how to make new algorithm of cryptography and also this coursework gives more knowledge about the cryptographic algorithm.

References

Anon., 2017 . *techopedia.* [Online]
Available at: https://www.techopedia.com/definition/6311/caesar-cipher

Anon., 2017. *techopedia.* [Online]
Available at: https://www.techopedia.com/definition/6311/caesar cipher

Anon., 2020. *tutorialpiont.* [Online]
Available at: https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm

Anon., 2021. *The economic Times.* [Online]
Available at: https://economictimes.indiatimes.com/definition/ciphertext

Aryal, M., n.d. [Online]
Available at: https://ictframe.com/what-is-computer-security-what-are-the-types-of-computer-security-threat/
[Accessed 2073].

certMike, 2017-2019. *www.certmike.com.* [Online]
Available at: https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-

triad/#:~:text=The%20CIA%20Triad%20of%20confidentiality,core%20underpinning%20of%20information%20security.&text=Availability%20means%20that%20authorized%20users,and%20the%20resour

synopsys, 2021. *www.synopsys.com.* [Online]
Available at: https://www.synopsys.com/glossary/what-is-cryptography.html