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: Karsang Gurung

London Met ID: 19031333

College ID: NP01NT4A190138

Assignment Due Date: 22nd January, 2021

Assignment Submission Date: 22nd January, 2021

Word Count (Where Required): 4583

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

Foremost, I would like to express my sincere and deepest gratitude to my module leader Mr. Akchayat Bikram Dhoj Joshi for such an excellent opportunity to work on this project. I would also like to thank my tutor Mr, Suryansh Mathema for invaluable guidance throughout the whole work. Their enthusiasm, motivation and patience has helped me in the completion of this work. It was a great privilege to work on this project and I'm thankful to what they have offered.

I am very grateful to my parents and friends for their support, prayers and sacrifices. It wouldn't have been possible to complete this work in limited time without their assistance. I am very thankful for guiding me out despite of their busy schedules. I am very much overwhelmed by everyone's humbleness and gratefulness throughout the process of finalizing the project.

Abstract

Security helps to keep the asset of the company free from risks, threats and vulnerabilities. It is one of the main component, which helps an organization to achieve its aims and objectives. An employee or any personnel of an organization should always be familiar with cautious preventive measure to counter any security in the company.

Therefore, this project solely helps an individual to research and study about the history, importance, security measure and its counter measures. This work is all about researching about cryptography and its types. It encourages student to learn about how the risks, vulnerabilities and threats can be minimized.

Students are motivated to create their own cryptographic method of encrypting and decrypting texts which has had helped every individual to learn more about cryptography.

Contents

List of Figures

List of table

1. Introduction

Security is the defending of the data, systems and network from various malicious attacks or external damages. It can also be defined as the protection of the assets of an individual or enterprises from any kinds of damages or thefts. Here, the assets refer to the important documents, working software, applications and hardware components of the individual or enterprise.

With the increase in the number of computer users, the need of security for them is also increasing in the same pace. As, security is the protection of the IT assets and system from various malicious threats, it has become one of the basic need in day-to-day life. It controls the physical access to the hardware components and attacks through networks. Security helps to prevent the loss of assets of enterprises such as data, information, software and hardware components, which are the basic requirement for an enterprise to achieve its aims and objectives. (Fleeger, 2015)

In order to reduce the impact of all the risks and threats to the assets of an enterprise, IT risk assessment can be carried out in consecutive ways. IT risk assessment is the preventive measure to mitigate or reduce the risk to the minimum to avoid the impact of the loss caused to the organization. The steps followed in risk assessment are:

- Identification: First, the assets of organizations are identified and classified. They are identified according to their usage, usefulness, pros and cons in an organization. Usually, the assets consist of important data, files, media, software applications.
- Assessment: Once the assets are identified, the risks connected to those assets are determined. For instance, if the laptop is unprotected chances of getting attacks will be high. Similarly, risk is calculated and evaluated then distributed towards risk mitigation.
- Mitigation: Security measures are enforced in each asset and their risk. Research is done on how the threats and vulnerabilities can be reduced.
- Prevention: here, the circumstances causing risk are eliminated. Security controls are applied along with insurance measure. (Biscoe, 2020)

2. CIA Triad

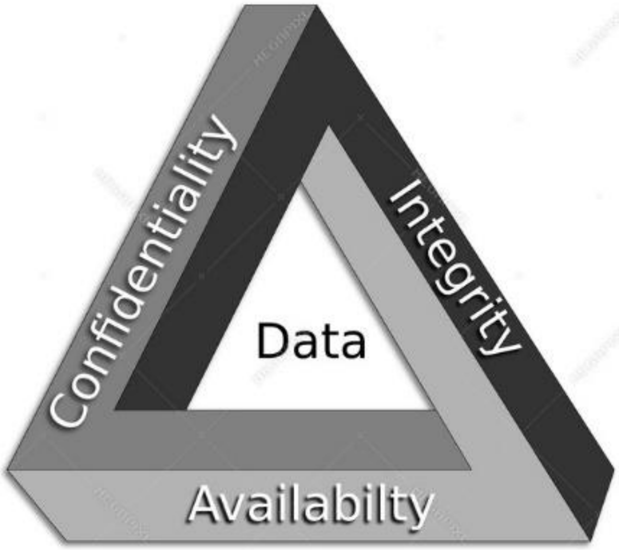

Figure 1: CIA Triad model

CIA triad is a model which implements policies for the security of IT assets of an organization. It stands for Confidentiality, Availability and Integrity. This triad is considered to be the foundation and objective of the security of an organization. If any one of these principles is contravened, then the company suffers casualty. Threats and vulnerabilities of an organization are evaluated on the basis of this model. Then, security measures are applied on the basis of the evaluation.

2.1 Confidentiality

Confidentiality refers to the privacy or secrecy of the data and information of an organization. It ensures that the data and information are only accessible by authorized person of the organization and not accessible to those who are not authorized to access the data and information. The confidentiality of the organization might be breached through various ways. Some of them are eavesdropping, malicious attacks, system escalation. Besides these, Human errors, carelessness and poor security controls can also lead to the violation of confidentiality. For instance, poor username and password, eavesdropping in physical presence, lack of encryption, theft etc. The counter measures to the violation of confidentiality can be utilization of Access Control Records (ACL), encryption of data, strong username and password proper authentication and access control.

2.2 Integrity

Integrity determines if the data, information and sources are trust worthy or not. It makes sure if the data and information has been manipulated and modified or not. It also ensures the reliability and accuracy of the data and information. The integrity of an organization can be violated directly through attack. The file, data, information might be tampered and modified. Beside the attack through network, human errors can also lead to the violation of integrity. Carelessness of employees might lead to the theft of data and information. Other errors such as coding errors, poor policies, and poor protectives measures might lead to the violation of integrity. The counter measures for this can be strong encryption of data. Audits, digital certificates and credentials, strong authentication and access controls.

2.3 Availability

Availability ensures that the data, information, files and other assets are accessible and available to all the authorized personnel of an organization who needs them. There are many factors that can lead to the violation of availability in an organization. Power failure, software failure, natural disasters, human errors can lead to the unavailability of the resources. Major factor i.e. attack on the system leads to the unavailability too. The countermeasures to such hindrances can be power backups, regular software patches, upgrading systems and disaster recovery plans. (Walkowski, 2019)

3. Cryptography

Cryptography is the method of maintaining the secrecy of data and information and protecting them. In simple words, Cryptography is the method of converting plain texts into cipher texts. The word ‘cryptography’ was derived from Greek words *“kryptos”* and *“graphos”.* The meaning of these two words were “secret” and “to write” respectively.

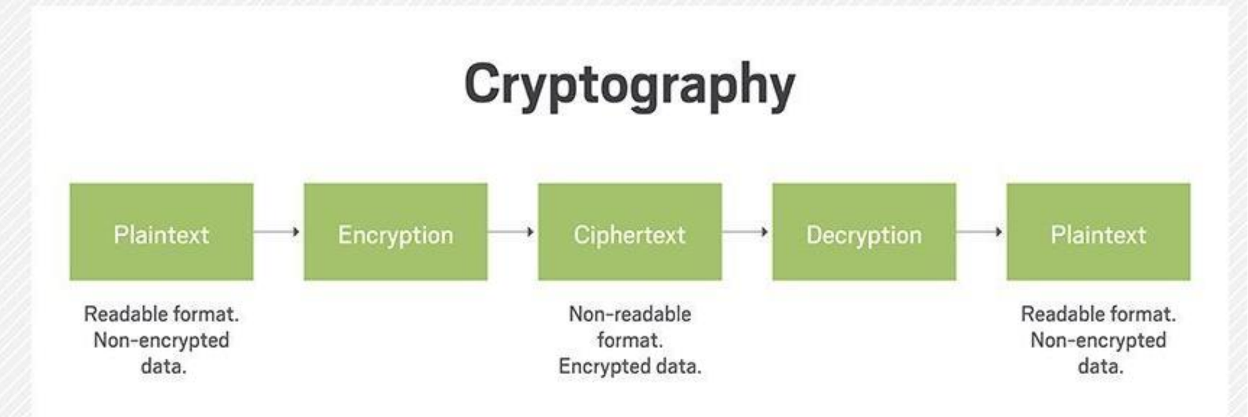
Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

Figure 2: Process of Cryptography

Cryptography involves the method of converting plain texts into cipher texts. This method is called encryption in which normal texts in simple words are converted into encrypted words known as cipher texts. Similarly, converting the cipher text to normal or plain text is called decryption. The encryption and decryption techniques have evolved a lot in the recent times. Use of numbers in the encryption process has made it very reliable way of encrypting the plain texts. (Munir, 2005)

3.1 History of Cryptography

Cryptography is believed to be originated from about 4000 years ago i.e. 2000 B.C. The first cryptographic methods were practised by Egyptians via Hieroglyph. Hieroglyph was a writing system that consisted of various elements with logograph that was only known to the messenger of the God and King.

Figure 3: Hieroglyph

In 100B.C, the very first known modern cipher was created. It was created by Julius Caesar. Thus, the cipher method was named on him as Caesar cipher. This cipher solely depends on the method of shifting letters of text by a certain number among which three was preferred the most. The ciphered text would be shifted back by the same number to get the original text again. (Rouse, n.d.)

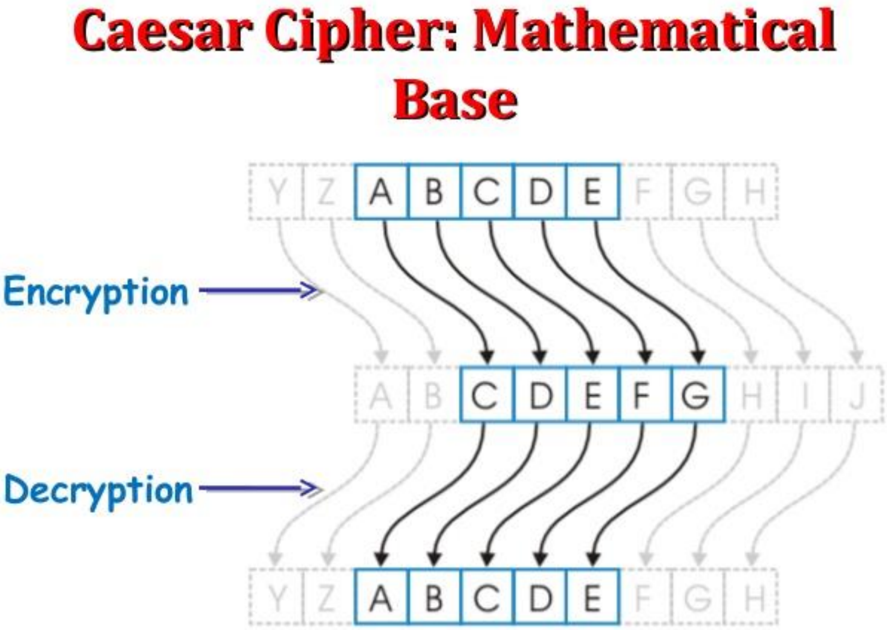

Figure 4: Caesar Cipher

After the 19th century, Cryptography evolved into mechanical and electromechanical form. They were used in world war I & II for military purposes. After that, mathematical algorithms were used in cryptography and more encryption methods have been made. Cryptography was used as the means of coding and invention of different technologies has brought effectiveness in the utilization of cryptography method. (Rouse, n.d.)

3.2 Importance of Cryptography

Cryptography has a vital role to play in present context of communication as it helps to maintain the privacy and secrecy of the data and messages. Not all the medium of communications are 100% secured. If they are attac.ked, the data and information might be accessible to the intruders. Even if the attackers get the access to the data and information, the encrypted data might not be readable to them.

Cryptography is an equipment that helps to maintain the secrecy of the texts and the potentiality to encrypt the data, information and maintain personal privacy. Cryptography has been a great help in all organizations. Most importantly, it has proven itself to solid in banking organizations where the official work are carried out via open switched networks. (Munir, 2005)

3.3 Objectives

As we all know, the main objective of cryptography is to provide confidentiality and secrecy. But along with that, the other objectives are:

- To provide integrity to the data
- To provide proper authentication
- To reject repudiation.

3.4 Types of Cryptography

For cryptography, mathematical function, also known as cryptographic algorithm is used in the encryption and decryption of texts. The algorithm is made of keys, which is made of number, word or phrase. One or more than one keys are used in the cryptography of a text. However, the effectiveness of encryption depends upon the keys and algorithm.

The cryptographic algorithms based on keys are given below:

3.4.1 Symmetric Cryptography

Symmetric cryptography is the cryptography technique in which only one key is shared for the encryption and decryption. The key is shared among the sender and the receiver to exchange information. Since, only one key is used in this cryptography, it is called symmetric cryptography.

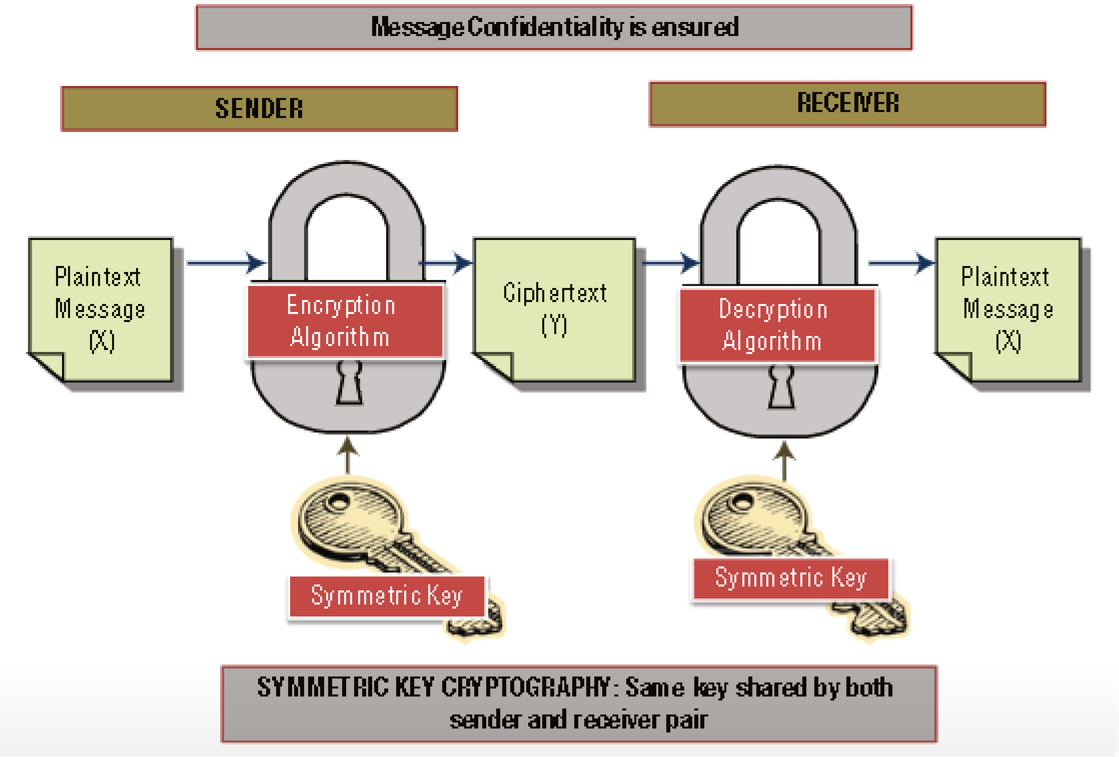

Figure 5: Symmetric Cryptography

In this cryptography, both sender and receiver for the encryption and decryption must know the single secret shared key. This cryptography method operates in two modes i.e. stream and block. In stream cipher, one byte is taken at a time to convert the plain text to cipher text. Whereas, in block cipher, 64 bits for the encryption. (Umesh Hodeghatta Rao, 2014)

3.4.2 Asymmetric Cryptography

Asymmetric Cryptography is the cryptography technique in which more than one keys are shared among the sender and the receiver for encryption and decryption. Usually, only two keys are shared among the sender and the receiver i.e. public and private key. The public key is used by anybody sending or receiving the text but private key is shared only with the receiver.

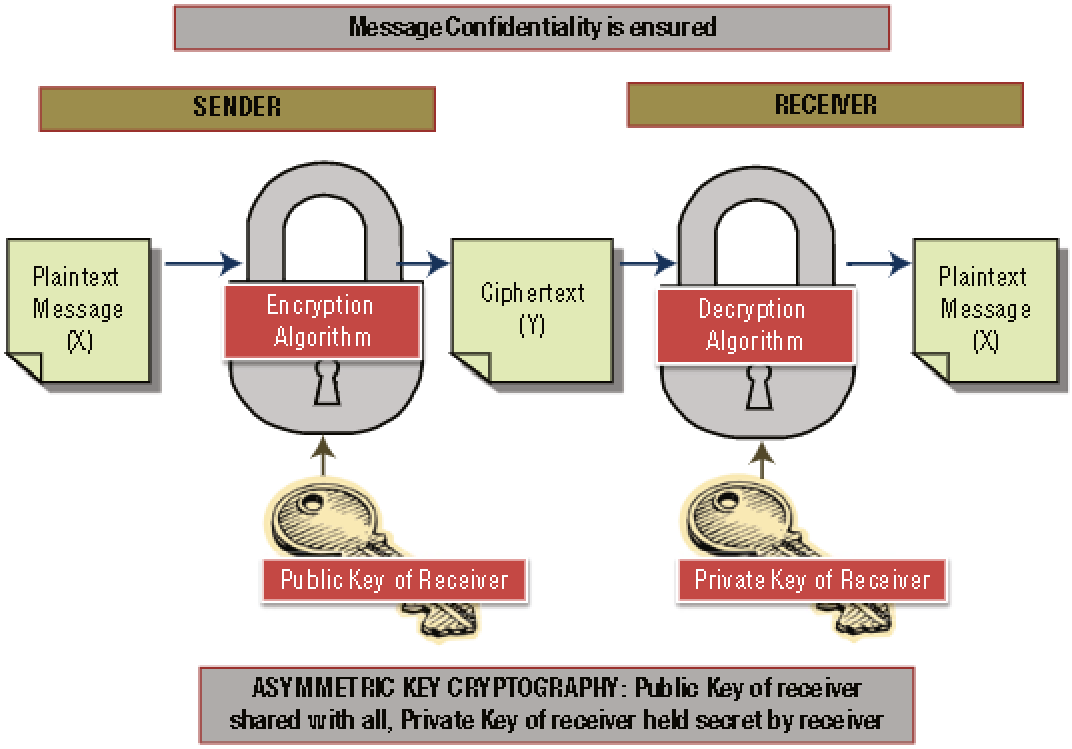

Figure 6: Asymmetric cryptography

Asymmetric cryptography is considered very safe as it uses two keys for the encryption and decryption. The keys are generated via generator whose algorithms are connected to each other mathematically making it easy to generate corresponding key quickly. (Umesh Hodeghatta Rao, 2014)

4. Caesar cipher

Caesar Cipher was invented by Julius Caesar in 100 B.C. for the military purpose. This Cipher is also known as shift cipher, as it uses the technique of shifting. This cipher is known to be the quickest and the simples technique of encryption. It uses the method where the letters to be ciphered are replaced by letters of certain number. This method of cryptography. This cryptography method works on the basis of transposition method and symmetric key algorithm. Since it works in the asymmetric key algorithm, it needs only one key for encryption and decryption. The decryption of text by this method is done just by reversing the encryption. (Andress, 2014)

An example for encryption and decryption using Caesar cipher is shown below. Here, the shift key is taken of three.

Plain letters	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
Ciphered letters	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: Index

Let us, take a plain word ‘Bike’

For encryption,

B = 1	I = 8
C = (1 + 3) mod 26	C = (8 + 3) mod 26
= 4	= 11
= e	= l
K = 10	E = 4
C = (10 + 3) mod 26	C = (4 + 3) mod 26
=13	= 7
=n	= h

Hence, using the shift of key three, the ciphered text obtained for word ‘bike’ is ‘elnh’

Now, further deciphering the text :

For decryption,

E = 4

C = (4 - 3) mod 26

= 1

= B

N = 13

C = (13 - 3) mod 26

=10

=k

I = 11

C = (11 - 3) mod 26

= 8

= i

H = 7

C = (7 - 3) mod 26

= 4

= e

Hence, The text obtained after deciphering is ‘bike’

4.1 Advantages of Caesar cipher

The advantages of Caesar cipher are given below:

- The algorithm of this cipher is very simple and easy
- Users without much knowledge about coding and cryptography can also be familiar with this cipher
- Due to the use of only one shared key, it is quite simple and easy to send and receive messages
- Any application or device is not required to decipher this encryption, which keeps the cost to minimum.
- No complex mathematical algorithms are used in it, making it simple. (Anon., 2017)

4.2 Disadvantages of Caesar cipher

The disadvantages of Caesar cipher are:

- As, it is the easiest and simplest cryptographic method, it is easy and simple to decipher too.
- Since no mathematical algorithms are used, it is very easy to decipher the texts by everyone.
- It only has 26 probabilities, which makes it limited to less ways to encrypt the text.
- This technique of cryptography is guessable by people without the knowledge of cryptography too.
- This technique bears a huge risk as only one key is shared among the receiver and sender. (zachvdg, 2020)

5. New Cryptographic Algorithm

Here, a new cryptographic algorithm is required to be made from Caesar cipher. The name. This cipher has been named as Odd-Even cipher (OEC) due to the algorithms used in it. This cipher is similar to the authentic cipher technique of Julius Caesar. Few changes like addition of shift key has been made.

The method used by Caesar cipher was:

$C = (p + k) \bmod 26$

Where,

C = ciphered text

P = plain text

K = shift key

And,

$D = (p - k) \bmod 26$

Where,

D = Deciphered text

P = plain text

K = shift key

For this modified version of the cipher, both the encryption and decryption has their own algorithm, which will be discussed below.

In this method of cipher, if the value of the alphabet is odd in number then it is increased by two and if the alphabet is even then it is decreased by two (Goyal, 2013).

Let us explain the method in an example.

Plain letters	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
Ciphered letters	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

For the encryption,

E = ((p+2) + k) mod 26 // if the value of p is odd

E = ((p-2) + k) mod 26 // if the value of p is even

Similarly, For the decryption

D = ((p+2) - k) mod 26 // if the value of p is odd

D = ((p-2) - k) mod 26 // if the value of p is even

For instance, the word to be ciphered is ‘’cup”

For encryption,

C = 2-2 = 0

E = (0 + 3) mod 26

= 3

= D

U = 20-2 = 18

E = (18 + 3) mod 26

= 21

= v

P = 15+2

E = (17 + 3) mod 26

= 20

= U

The ciphered text for ‘cup’ is’dvu’

Now for decryption,

D = 3+2 = 5

D = (5 - 3) mod 26

= 2

= C

U = 20-2

D = (18 - 3) mod 26

= 15

= P

V = 21+2 = 23

D = (23 - 3) mod 26

= 20

= U

Hence, The deciphered text for ‘dvu’ is ‘cup’

The word taken as instance as has been ciphered and then again deciphered successfully. Here, if the plain text was odd the value was increased by 2 and if the plain text was even, the value was decreased by 2. Increasing and decreasing the value of plain text is the modification given to the Caesar cipher.

5.1 Flow chart for encryption

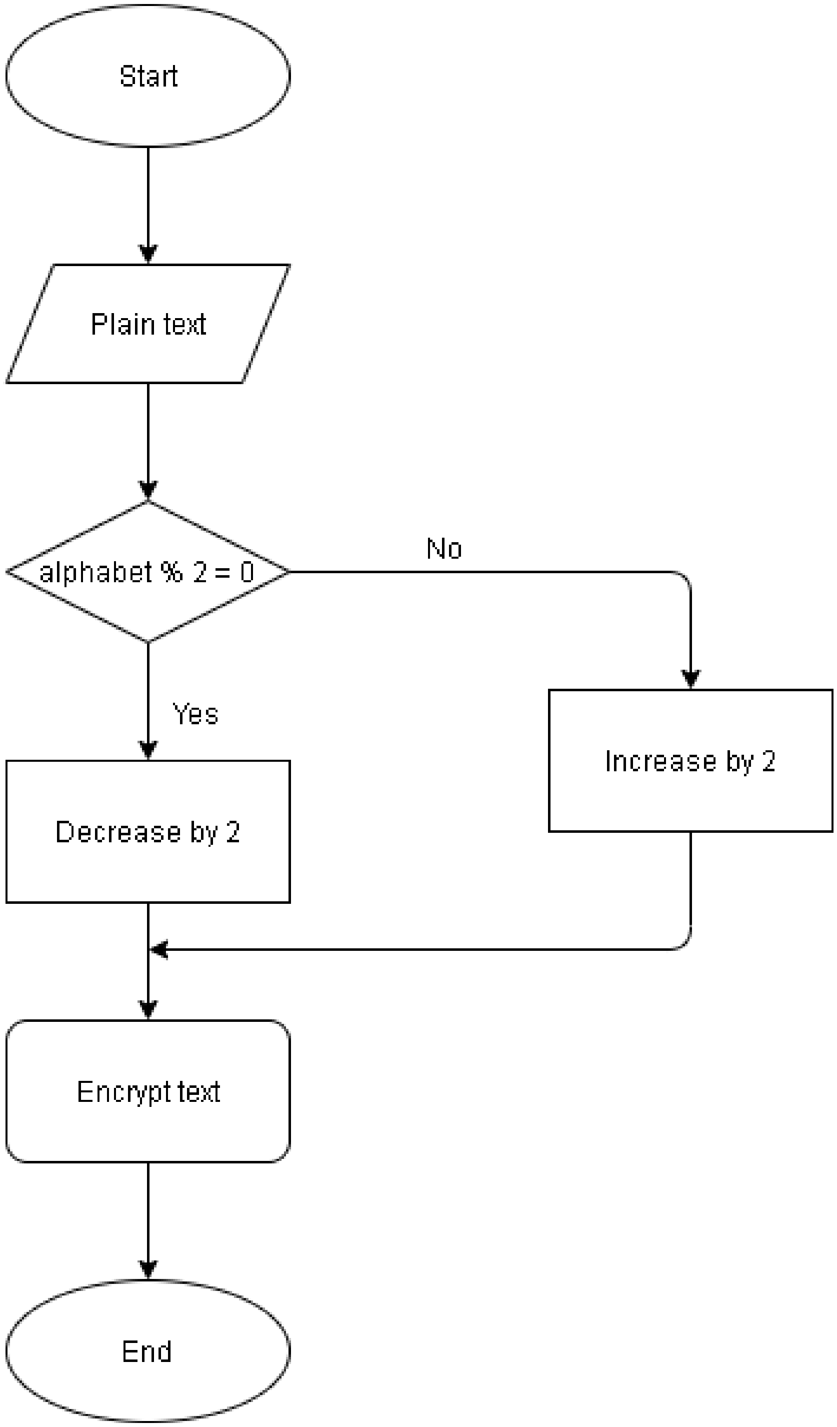

Figure 7: Encryption flowchart

5.2 Flowchart for decryption.

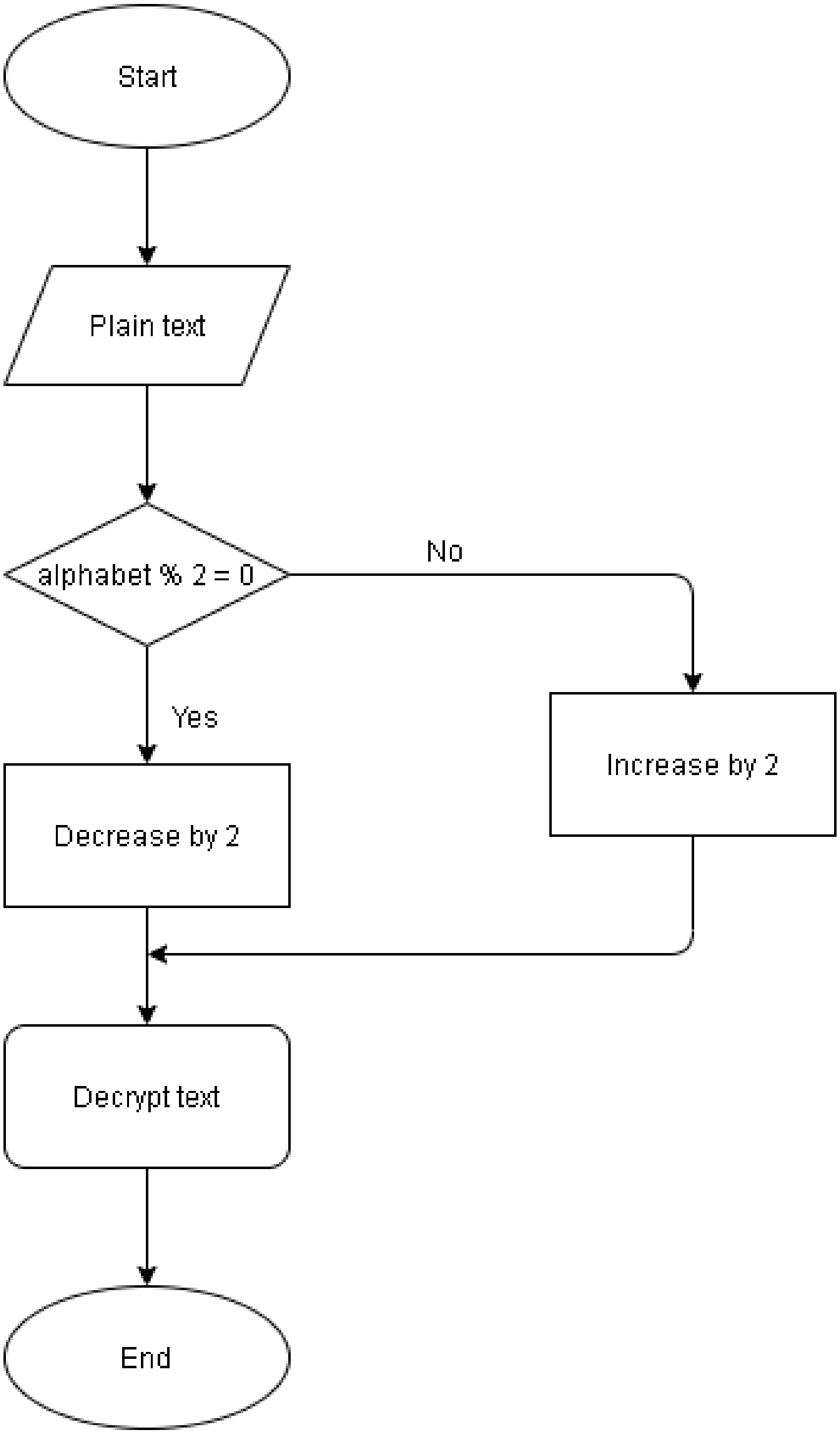

Figure 8: Decryption flowchart

6. Algorithm

6.1 Algorithm for encryption

Step 1: Plain text is entered

Step 2: alphabet is checked if it is odd or even

Step 3: plaintext value is increased by 2 if it is odd

Step 4: plain text values is decreased by 2 if it is odd

Step 5: Encryption method is applied

Step 6: Ciphered text is obtained

6.2 Algorithm for decryption

Step 1: Plain text is entered

Step 2: alphabet is checked if it is odd or even

Step 3: plaintext value is increased by 2 if it is odd

Step 4: plain text values is decreased by 2 if it is odd

Step 5: decryption method is applied

Step 6: deciphered text is obtained

7. Testing

Plain letters	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
value	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	26

- If the value of alphabets of plain text is odd, then it is increased by value 2.
- If the value of alphabets of plain text is even, the it is decreased by value 2.

7.1 Test 1

The plain text to be encrypted and decrypted is ‘palm’

For encryption,

P = 15+2 = 17
E = (17 + 3) mod 26
= 20
= U

L = 11+2 = 13

E = (13 + 3) mod 26

= 16

= Q

A = 0-2 = -2
E = (-2 + 3) mod 26
= 1
= B

M = 12-2 = 10

E = (10 + 3) mod 26

= 13

= N

The encrypted form of the word ‘PALM’ is ‘UBQN’

For decryption,

U = 20-2 = 18

D = (18 - 3) mod 26

= 15

= P

Q = 16-2 = 14

D = (14 - 3) mod 26

= 11

= L

B = 1+2 = 3

D = (3 - 3) mod 26

= 0

= A

N = 13+2 = 15

D = (15 - 3) mod 26

= 12

= M

Hence, the decrypted form of the word ‘UBQN’ is ‘PALM’

7.2 Test 2

The plain text to be encrypted and decrypted is ‘CALM’

For encryption,

C = 2-2 = 0
E = (0 + 3) mod 26
= 3
= D

A = 0-2 = -2
E = (-2 + 3) mod 26
= 1
= B

L = 11+2 = 13
E = (13 + 3) mod 26
= 16
= Q

M = 12-2 = 10
E = (10 + 3) mod 26
= 13
= N

The encrypted form of the word ‘CALM’ is ‘DBQN’

For decryption,

D = 3 + 2 = 5
D = (5 - 3) mod 26
= 2
= C

B = 1+2 = 3
D = (3 - 3) mod 26
= 0
= A

Q = 16-2 = 14
D = (14 - 3) mod 26
= 11
= L

N = 13+2 = 15
D = (15 - 3) mod 26
= 12
= M

The decrypted form of the word ‘DBQN’ is ‘CALM’

7.3 Test 3

The plain text to be encrypted and decrypted is ‘CAT’

For encryption,

C = 2-2 = 0

E = (0 + 3) mod 26

= 3

= D

A = 0-2 = -2

E = (-2 + 3) mod 26

= 1

= B

T = 19+2 = 21

E = (21 + 3) mod 26

= 24

= Y

The encrypted form of the word ‘CAT’ is ‘DBY’

For decryption,

D = 3 + 2 = 5

D = (5 - 3) mod 26

= 2

= C

B = 1+2 = 3

D = (3 - 3) mod 26

= 0

= A

Y = 24-2 = 22

D = (22 - 3) mod 26

= 19

= T

The decrypted form of the word ‘DBY’ is ‘CAT’

7.4 Test 4

The plain text to be encrypted and decrypted is 'HAT'

For encryption,

H = 7+2 = 9

E = (9 + 3) mod 26

= 12

= M

A = 0-2 = -2

E = (-2 + 3) mod 26

= 1

= B

T = 19+2 = 21

E = (21 + 3) mod 26

= 24

= Y

The encrypted form of the word 'CAT' is 'MBY'

For decryption,

M = 12-2 = 10

D = (10 - 3) mod 26

= 7

= H

B = 1+2 = 3

D = (3 - 3) mod 26

= 0

= A

Y = 24-2 = 22

D = (22 - 3) mod 26

= 19

= T

The decrypted form of the word 'MBY' is 'HAT'

7.5 Test 5

The plain text to be encrypted and decrypted is ‘CAT’

For encryption,

C = 2-2 = 0

E = (0 + 3) mod 26

= 3

= D

A = 0-2 = -2

E = (-2 + 3) mod 26

= 1

= B

P = 15+2 = 17

E = (17 + 3) mod 26

= 20

= U

The encrypted form of the word ‘CAP’ is ‘DBU’

For decryption,

D = 3 + 2 = 5

D = (5 - 3) mod 26

= 2

= C

B = 1+2 = 3

D = (3 - 3) mod 26

= 0

= A

U = 20-2 = 18

D = (18 - 3) mod 26

= 15

= P

The decrypted form of the word ‘DBU’ is ‘CAP’

8. Critical evaluation

The modification of Caesar cipher has been done. Perhaps, this modification of Caesar cipher is different than the authentic one but it will surely be of some use somewhere in the future. Despite, the flaws and weakness of this encryption, this has been upgraded to advance form than the previous one. Here are some of the pros and cons of this cryptography.

8.1 Strength

The strengths of Odd-Even Cipher are:

- It can easily be brought to use without knowledge of mathematical logarithms too.
- It is very simple and easy technique of encryption and decryption
- lowercase doesn’t cause any affect in the cryptography system
- it also encrypts messages containing spaces
- small scale organisations will have lots of benefits from this cryptography method.
- The original authentic method of Caesar cipher will not work as the cipher has been upgraded to next level.

8.2 Weakness

As long as the cryptography has strength it will also have its own weakness. Some of the weakness of the modified Odd-Even Cipher (OEC) are:

- Due to the use of only one shared key, problems may arise if the key is lost from either one party.
- This cipher technique is not suitable to large scale organization to secure their files and data.
- It is very time consuming as each and every word has to be ciphered.
- This technique does not decrypt the special characters and numbers in the text.
- No mechanical or electronic devices needs to be used in this technique, hence, it might lead to lots of errors while working with this encryption.

9. Conclusion

Security plays a vital role in an organization to achieve their goals and objectives. Security of the assets of the organizations are the most vulnerable things to risk. If the assets of an organization are affected by threats, it might have big and negative on the organization itself. Therefore, in order to maintain the wellness of the organization, security in an organization is the most important thing.

One of the most valuable thing that ensures the security and safety of organization is Cryptography. Cryptography involves the process of making the assets of organization secure. In addition, Caesar cipher is one of them that keeps the secrecy and privacy of the information of an organization.

This project was all about study and research of different security measures along with Cryptography methods. But most importantly, this project was about creating a new cryptographic method with the modification of old one which is done inside the project itself. A cryptographic method by modification of Caesar cipher has been made with the research needed for it.

10. References

Andress, J., 2014. *The Basics of Information Security(Second edition).* s.l.:s.n.

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

Biscoe, C., 2020. [Online] Available at: https://www.itgovernance.co.uk/blog/7-steps-to-a-successful-iso-27001-risk-assessment

Fleeger, C. P., 2015. *Security in computing.* s.l.:s.n.

Goyal, K., 2013. International Journal of Computer Applications. *Modified Caesar Cipher for Better Security Enhancement,* Volume 73.

Munir, W., 2005. *Cryptography,* s.l.: s.n.

Rouse, M., n.d. *TechTarget.* [Online] Available at: https://searchsecurity.techtarget.com/definition/cryptography

Umesh Hodeghatta Rao, U. N., 2014. *The {InfoSec} Handbook.* s.l.:s.n.

Walkowski, D., 2019. CIA triad. 9 July.

zachvdg, 2020. *Cryptogramcenter.* [Online] Available at: https://cryptogramcenter.com/caesar-cipher-not-secure/