LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2018-19 Autumn

Student Name: Abiral Joshi Shrestha

London Met ID: 17030696

College ID: NP01NT4A170008

Assignment Due Date: 4th February, 2019.

Assignment Submission Date: 3rd February, 2019.

Word Count (Where Required): 4218

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

Contents

Table of Figures

Abstract

The following report is the task assigned to us as an individual coursework in the module of 'Security in Computing'. It accounts for 30% of our overall grade for this module. The report includes the topic of security and cryptography along with a modified substitution algorithm. The report was with the help of research and study. The first portion of the report contains information regarding security, cryptography, the history of cryptography, symmetric encryption systems and asymmetric encryption systems. The information in this report was generated through books, journals, reliable websites, etc.

The final portion of the report contains the Modified Caesar Cipher. It discusses about the shortcomings of the traditional Caesar Cipher and tries to mitigate them. It contains information regarding the Caesar Cipher, the Modified Caesar Cipher, its working mechanism, encryption procedure and decryption procedure. It also contains the testing done to verify the working of the Cipher and evaluates its strengths and weaknesses. Finally, it is concluded that the new Modified Caesar Cipher is a much more reliable and secure encryption algorithm when compared to the traditional Caesar Cipher.

TASK 1 INTRODUCTION TO CRYPTOGRAPHIC SYSTEMS

1.1) Security

Security, in terms of computing and information technology, are the preventive measures applied in order to protect the components of a computer system from unauthorized access, modification, various malwares and harm. It includes the protection of the physical components, operational functions, network, information, etc. The concept of physical security deals with the protection of hardware, software, data and information from physical harms and mishaps, which could lead to serious loss or damage to an enterprise. It includes protection from factors like natural calamities, theft, vandalism, etc. Operational security deals with the protection of critical and specific pieces of information and employing measures to protect them. It is carried out to make sure that a system remains functional and accessible. Network security is an enterprise's strategies and tactics to ensure the security of its networking assets and data. It allows us to deal with the variety of threats and stop them from spreading into a given network. Information security is the protection of data and information from unauthorized access, use, alteration or threat to its confidentiality. It is important as it helps to keep our information protected and maintains the overall health of the computer system's overall health by preventing viruses and malwares from infecting the system and allowing programs to run smoothly (Rhody, n.d.).

Security measures detect and prevent attacks and also help in recovering from the attacks that do succeed. Carrying out a system analysis requires the user to understand how the security measures operate. The understanding of such measures allows for the creation of better measures (Bishop, 2002). This is necessary as enterprises are always susceptible to new threats and malwares every day, if proper measures are not carried out to protect the system from such new threats, the security of a system will be compromised.

1.2) CIA

(Anon., n.d.)

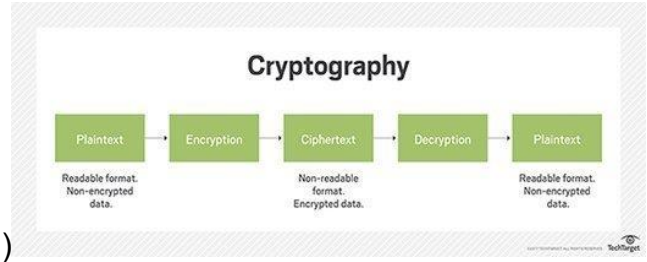
Figure 1 - The CIA Triad

CIA Triad is a model that elaborates the three main objectives which are needed to achieve information security. The objective are: Confidentiality, Integrity and Availability (Henderson, 2017). Confidentiality is the protection of disclosure of information to those individuals whom are not authorized. Integrity is the protection of data and information from being destroyed, altered or corrupted by unauthorized personnel. Availability is ensuring that the information is available to the authorized user at all times. The best way to ensure availability of information is to maintain all the hardware components and ensure operational security. But this somewhat causes a misbalance in the Triad cause if the security measures to ensure confidentiality and integrity are made highly secure, the availability of that information is decreased. Similarly, if the information is to be made highly available, the security measures have to be somewhat dropped which will in turn effect the confidentiality and integrity of the information. So, this model attempts to qualify risk as costs in monetary value, however it is often difficult to assign costs for various types of risks (Stapleton, 2014).

The security of information was provided by physical and administrative documents before the widespread use of data processing equipment. With the introduction of computers, the need of automated tools for protecting files and other information stored on computers became mandatory. The rapid increase of information transmitted electronically led to the dependency of the confidentiality and integrity being

vulnerable to threats. To counteract against such threats, AAA (Authentication, Authorization and Accountability) must be implied. Authentication helps preventing of information from being accessed by unauthorized users. It is the process in which the user proves that he/she is the person he/she is claiming to be. Authorization helps us to maintain a level of access control based on the position and tasks of individual users as any other authorization beyond the normal tasks of users may lead to accidental or intentional flouting of the confidentiality, integrity and availability, even the information security itself. The final step of ensuring information security and CIA is accountability. It is the process of keeping record of what each users do while they are logged into the system as such records can be very valuable if any security issues occur (Nweke, 2017)

1.3) Cryptography



(Rouse, n.d.)

Figure 2 - Flowchart of basic cryptography

Cryptography can be defined as a method of protecting information and communications through the use of algorithms so that only those for whom the information is intended can read and process it. It is used to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher (Christof Paar, 2009). Cryptographic systems are used to provide privacy and authentication in communication systems. Cryptography can be used to increase the security of a network. Network security is one of the most critical components in information security. Along with other suitable communications protocols, cryptography can be applied to provide a high degree of protection in digital communication against intruders (Mukund R. Joshi, 2015).

1.4) Key terminologies in Cryptography

Some of the key terminologies of Cryptography are:

- Plaintext: It can be defined as the simple, unencrypted text that anyone can read.

- Cipher text: It can be defined as the encrypted plaintext.

- Encryption: It is the process of applying functions to a text that makes it unreadable unless the decryption key is applied.

- Decryption: It is the process changing the cipher text into plaintext using the decryption key.

- Public Key: It is the key that is accessible to anyone to encrypt the text.

- Private Key: It is the key that is only distributed to a specific entity, intended to decrypt the text. (Phillips, 2018).

1.5) History of Cryptography

People from ages have had two needs: to share information and to share it selectively. This led to the art of coding the message in such a manner that only those who were intended could have access to the information. The art of cryptography is thought to have been created alongside the art of writing. As times changed, people got organized into tribes, groups, etc. This led to the idea of battles, politics and warfare. This further fueled the need of people to communicate selectively (Anon., n.d.).

(Anon., n.d.) 

Figure 3 - Symbols used by Ancient Egyptians

The earliest examples of cryptography were found in the ancient civilizations of Egypt, Greece and Rome. As early as the 1900 B.C., ancient Egyptians used hieroglyphs when writing scribes in order to hide their meaning from those who did not now. The ancient Greeks used to wrap a tape around a stick and then write their messages on the wounded tape, meaning the writing would be meaningless when the tape was unwound. The intended receiver was required to have a stick of the same diameter in order to decipher the message. The ancient Romans utilized the idea of shifting letters by an agreed upon number and writing the message using letter shift. The receivers would then have to shift the letters back by the same number and the message would be deciphered. This method used by the Romans was called the Caesar Shift Cipher (M.Damico, 2009). These ancient methods of cryptography weren't very reliable as these methods of encryption could be broken simply. Yet, the science of cryptography didn't have any major changes until the Middle ages. By this time, most European governments were using cryptography techniques in one way or another. Leon Battista Alberti was known as "The Father of Western Cryptography" due to his development of polyalphabetic substitution and had made the most significant advancement in cryptography in at least five hundred years (Hill, 2003) .

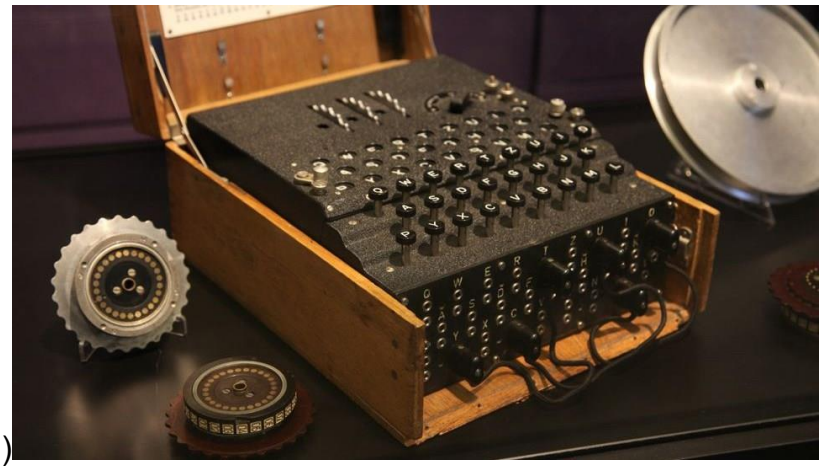
(Anon., n.d.) 

Figure 4- Enigma Machine

By the Second World War, mechanical and electromechanical cipher machines were in wide use but were such machines were impractical, manual systems were continued to be used. The Nazi Germans made heavy use of an electromechanical rotor

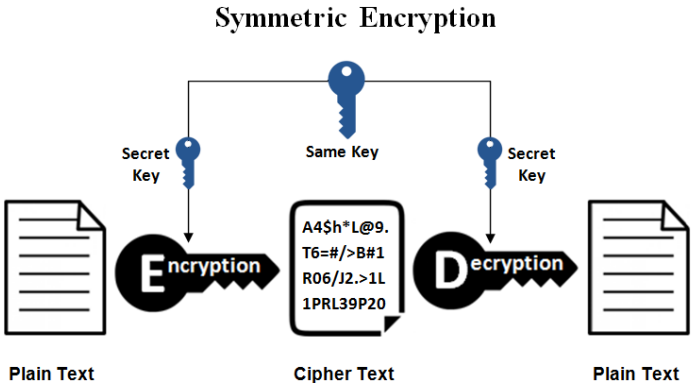
called Enigma for writing secret messages. However, in December 1932, Marian Rejewski, deduced the detailed structure of the Enigma. This was considered to be the greatest breakthrough in cryptanalysis in more than ten decades. The secrets of Enigma decryption allowed Poland to keep track of the German Army's advancements. However, the breakage of the German Enigma Cipher was never to be revealed as it would give the defeated Germans to claim that they were not fairly beaten (Hill, 2003).

The development of digital computers and electronics made it possible to create much more complex ciphers. Modern computers allowed for the encryption of any kind of data. However, the use of computers has also aided in the advancement of cryptanalysis. The era of modern cryptography began in the mid-1970s. IBM designed the algorithm that became the Federal Data Encryption Standard, Whitfield Diffie and Martin Hellman published their key agreement algorithm and Martin Gardner published the RSA algorithm in his Scientific American column. Ever since then, cryptography has become a widely use strategy in communications, computer networks and computer security. During the 1980s and 1990s, cryptography emerged from its role as technology used by the government to protect its communications to a necessary underpinning of Internet traffic. However, enterprises efforts to develop and use cryptography were prevented by government export control regulations. But during the late 1990s, the US government held an attitude that was hardly believable to the rest of the world. But the rise of open source software to the Europeans and the evidence of US Communications intelligence came as a reason to force a change (Landau, 2007).

Prior to the 20th century, cryptography was mainly concerned with linguistic and lexicographic patterns. Later, the emphasis shifted to the extensive use of mathematics, including aspects of information theory, computational complexity, statistics, combinators, abstract, algebra, number theory, and finite mathematics. Until June of 1976, symmetric key cryptography was the only kind of encryption known to the public. In the same year, Whitefield Diffie and Martin Hellman proposed the notion of asymmetric cryptography. It was describes as "the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance" by historian David Kahn. In 1978, Ronald Rivest along with Adi Shamir and Len Adleman invented the RSA. In the year 1997, it

became publicly known that asymmetric key cryptography was the invention of James H. Ellis and that both the Hellman and RSA algorithms had been developed by Malcom J. Williamson and Clifford Cocks (Ahmed Al-Vahed, 2011).

1.6) Symmetric encryption systems



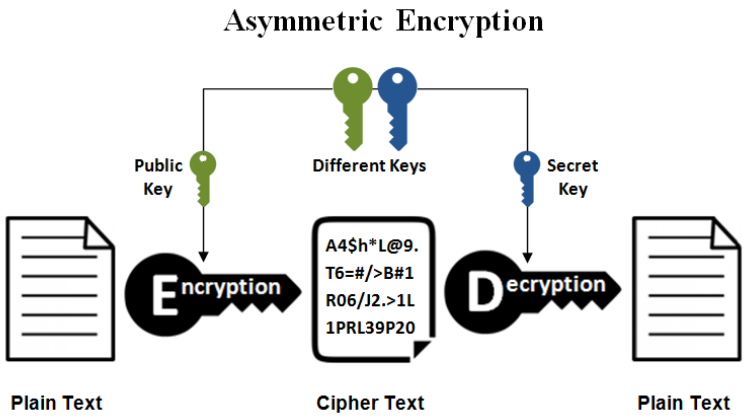
(Anon., n.d.)

Figure 5 - Basic Working of Symmetric Algorithm

Symmetric encryption systems are algorithms for cryptography that use only one key to encrypt and decrypt the data. The key is to be distributed before transmission between the sender and the receiver, which is also the main disadvantage of such systems. The key used for such encryption plays an important role as the strength of the symmetric encryption system depends on the size of the key used. For an instance, the same encryption using a longer key is harder to break than the one encrypted using a smaller key. Some examples of symmetric encryption systems are RC2, DES, 3DES, RC6, Blowfish, AES, etc. (Kader, 2008). DES (Data Encryption Standard) is a symmetric encryption system which uses block size of 64 bits and a key size of 56 bits, which was developed by IBM in 1977. It operates on blocks of equal size and uses both permutations and substitutions in the algorithm. It uses 16 rounds of transportation and substitution to encrypt each group of plaintext letters and output each round by round. This system was vulnerable to a brute-force attack, so DES was no longer invulnerable to attacks. 3DES (Triple DES) is the same as the DES operation. It uses three 64 bit keys and the final length of the key is 192 bits. The procedure of encryption is the same as in the DES, but

the process is repeated thrice. The message is encrypted with the first key, then decrypted with the second key and finally encrypted again with the third key. AES (Advanced Encryption Standard) is a symmetric block cipher that has block size 128 bits and cipher keys of 128,192 and 256 bits. Here, the encryption algorithm is divided into three categories – transportation, substitution and transposition. It uses a round function that is to be compared to 4 different byte oriented transformations. Number of rounds is dependent on the length of the key. The requirement is 10 rounds for 128 bit, 12 rounds for 192 bit and 14 rounds for 256 bit keys. Blowfish is the symmetric key encryption that uses a 64 bit key size and a variable key length from 32 to 448 bits. It is based on a 16 round cipher network that implies large key size. Since the key size is larger, it is comparatively harder to break the code in this algorithm (Ritu Tripathi, 2014).

1.7) Asymmetric encryption systems



(Anon., n.d.)

Figure 6 - Basic Working of Asymmetric Encryption

Symmetric encryption systems were vulnerable in two aspects – key exchange and trust as the symmetric key could be used to identify the other party, so this system required communicating party to be trustable and reliable. Also, it was also a problem with the use of the key as it required both the communicating entities to keep the key a secret. However, with the growing popularity of the Internet, it was impractical for both parties to always have knowledge of each other. This made it difficult to confirm communication in a secure and authenticated way (Thorsteinson, 2003).

In order to deal with these short comings of the symmetric encryption system, asymmetric encryption system was developed. Asymmetric encryption systems are algorithms for cryptography that use two keys to encrypt a plain text. They involve large mathematical calculation so, the time complexities are considerably high (Wai, 2015). The public key is used for encryption while the private key is used for decryption. Only specific receivers know the private key while the public key is distributed to everyone in the communication system. The main advantage of asymmetric encryption to symmetric encryption is that the problem of distributing the key of encryption is solved. Such encryption allows the use of digital signatures. This allows the receiver to verify that message is from a particular sender. It also helps to detect whether or not the message was altered while in transmission. Some examples of asymmetric encryption systems are – RSA (Rivest Shamir Adleman), Elliptic curve, Digital signatures, etc. (Neha Garg, 2014).

TASK 2 BACKGROUND

2.1) Background

I have selected the Caesar Cipher as my cryptographic algorithm. It is one of the oldest and most well-known algorithms in cryptography. It is a substitution cipher type that carries out encryption by exchanging characters in plaintext into one character in the cipher text. The working principle of the algorithm is to shift all characters in plaintext with a common shift value in order to obtain the cipher text (Boni Oktaviana, 2016). When using the Caesar Cipher, it is necessary for both parties, the sender and the receiver, to have the 'key' for the cipher in order to pass the encrypted message from one person to another. This 'key' is critical as it allows the sender to encrypt the message while also allowing the receiver to decrypt the message. The key can be defined as the number of characters shifted to create the cipher (Anon., n.d.).

The earliest well known use of such a substitution cipher was used for military purpose in Julius Caesar's *Gallic Wars*. The message that was encrypted was sent by Julius Caesar to Marcus Tullius Cicero, a Roman philosopher, who was thinking of surrendering at the time. In the message, Julius Caesar replaced Roman letters with Greek letters. This substitution made the message unreadable to the enemy. After this, it is believed that Julius Caesar used secret writing frequently. In one of his most famous substitution techniques, he simply replaced each letter with the letter three places down in the alphabets. This process of substitution later came to be known as the Caesar cipher or the Caesar shift cipher. Although there is a misconception that the letters for the cipher can be shifted only three places, the number of characters shifted is not permanently set. So, it is possible to generate 25 different cipher keys (Singh, 2001).

An example of the encryption and decryption of the Caesar Cipher is provided below:

2.2) Encryption

Using the Caesar Cipher, to encrypt the plaintext 'ISLINGTON' using shift key 3:

Plaintext: ISLINGTON

I	S	L	I	N	G	T	O	N
L	V	O	L	Q	J	W	R	Q

Cipher Text: LVOLQJWRQ

Hence, the encryption of the plaintext ‘ISLINGTON’ using Caesar Cipher and shift key 3 is ‘LVOLQJWRQ’.

2.3) Decryption

Using the Caesar Cipher, to decrypt the cipher text ‘LVOLQJWRQ’ using shift key 3:

Encrypted Text: LVOLQJWRQ

L	V	O	L	Q	J	W	R	Q
I	S	L	I	N	G	T	O	N

Decrypted Text: ISLINGTON

Hence, the decryption of the encryption ‘LVOLQJWRQ’ is ‘ISLINGTON’.

2.4) Advantages of Caesar Cipher

- One of the easiest methods in cryptography to use and understand.
- Single short key is used for the entire process.
- Can be used even in the system which cannot use complicated coding techniques.
- Very few computing resources are required (Anon., n.d.).

2.5) Disadvantages of Caesar Cipher

- It uses a very simple structure.
- It provides only minimum level of security to the information.
- The pattern and the frequency of letters can act as a clue to decipher the message (Anon., n.d.).

TASK 3 DEVELOPMENT

In the Caesar cipher, the plaintext is encrypted simply by shifting the characters by a number of positions. This made sense when the cipher was newly developed and most people were mostly not clever enough to decipher the encryption. But in the modern age, the Caesar cipher can be easily decrypted by modern computer systems and basic guess work. The pattern and tendency of replacement of characters can easily hint at the value of the key, comprising the entire message and encryption.

Modified Caesar Cipher

To avoid such vulnerability in the Caesar cipher, I have proposed a heavily modified and more complex variation to the Caesar cipher. For this Modified Caesar Cipher, the value of the key is set and fixed to one. The new method works on the basis of the index of the alphabets. The index of the alphabet is checked, if it is odd the value of the key is increased by one meaning that the alphabet is replaced by a letter one step further up the alphabets. Else, if the index of the alphabet is even, the value of the key is decreased by one meaning that the alphabet is replaced by a letter one step down the alphabet. Similarly, for numeric values, if the number is odd, its value is increased by one, else decrease by 1.

Table 1. Index of the upper case alphabets

Letter	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
Index	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

Table 2. Index of lower case alphabets

Letter	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

Index	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

Table 3. Keys for uppercase alphabets

Letter	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 4. Keys for lowercase alphabets

Letter	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 5. Keys for numbers

Number	1	2	3	4	5	6	7	8	9	0
Key	2	1	4	3	6	5	8	7	0	9

This new Cryptographic Algorithm is named Modified Caesar Cipher.

3.1) Working mechanism of the Modified Caesar Cipher

The working mechanism of the Caesar Cipher was that the letters were shifted, by a selected number, down the alphabets. Such encryption soon became vulnerable as the pattern and tendency of the cipher text would hint at the value of the key, thus compromising the entire encryption. The modification proposed removes such vulnerabilities while also making the encryption and decryption process a little more complex, such that it doesn't hint at the solution of the encryption.

3.2) New Encryption algorithm

1. Plain text is taken for input.

2. The index of the alphabet or the number is checked, if it is odd the value of the key is increased by one, if it is even the value of the key is decreased by one.

3. Obtain the cipher text.

3.3) New Decryption algorithm

1. Cipher text is taken as input.
2. The index of the alphabet or the number is checked, if it is odd the value is decreased by one, else it is increased.
3. Obtain the plain text.

3.4) Flowcharts

3.4.1) Encryption

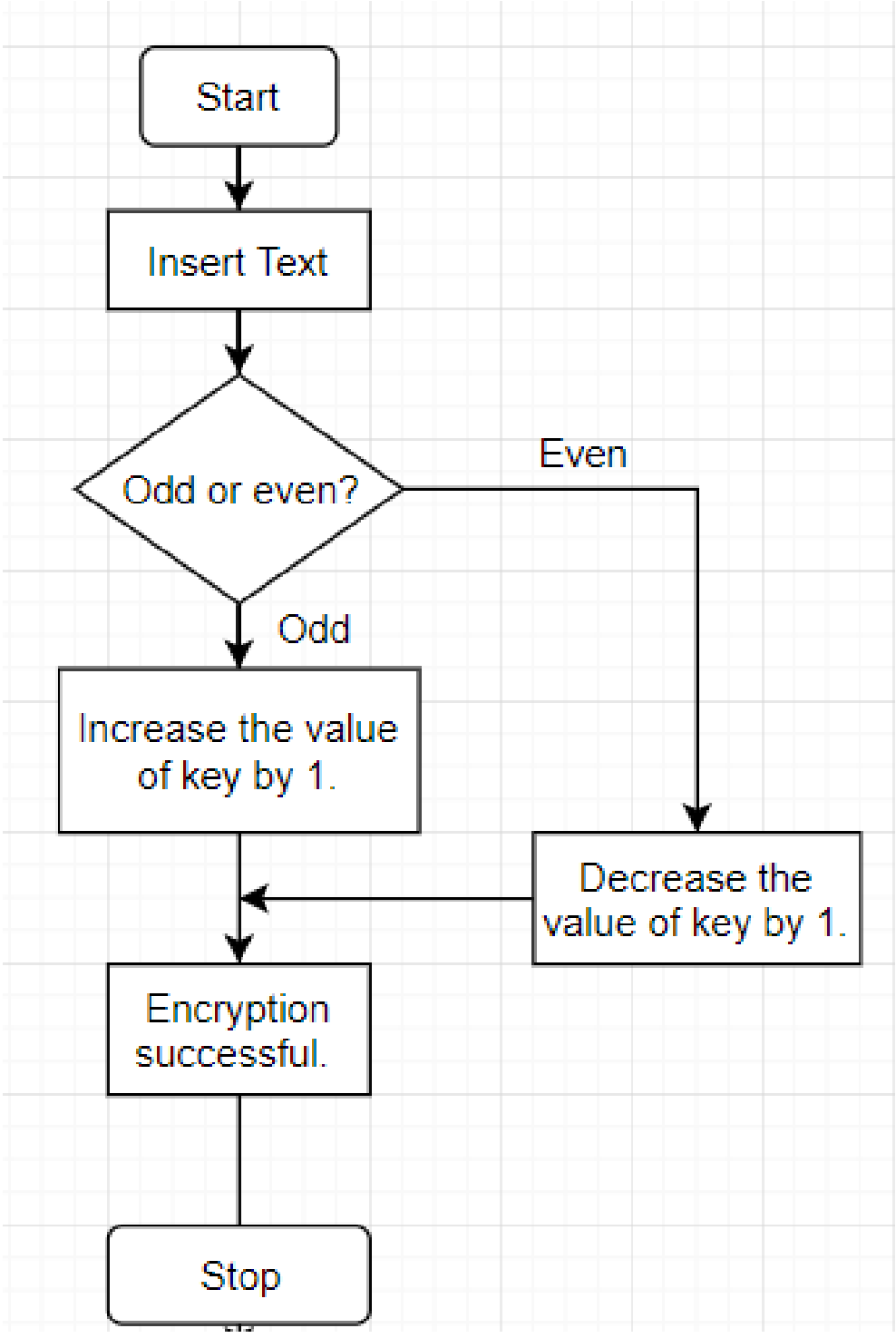


Figure 7 Flowchart for Encryption

3.4.2) Decryption

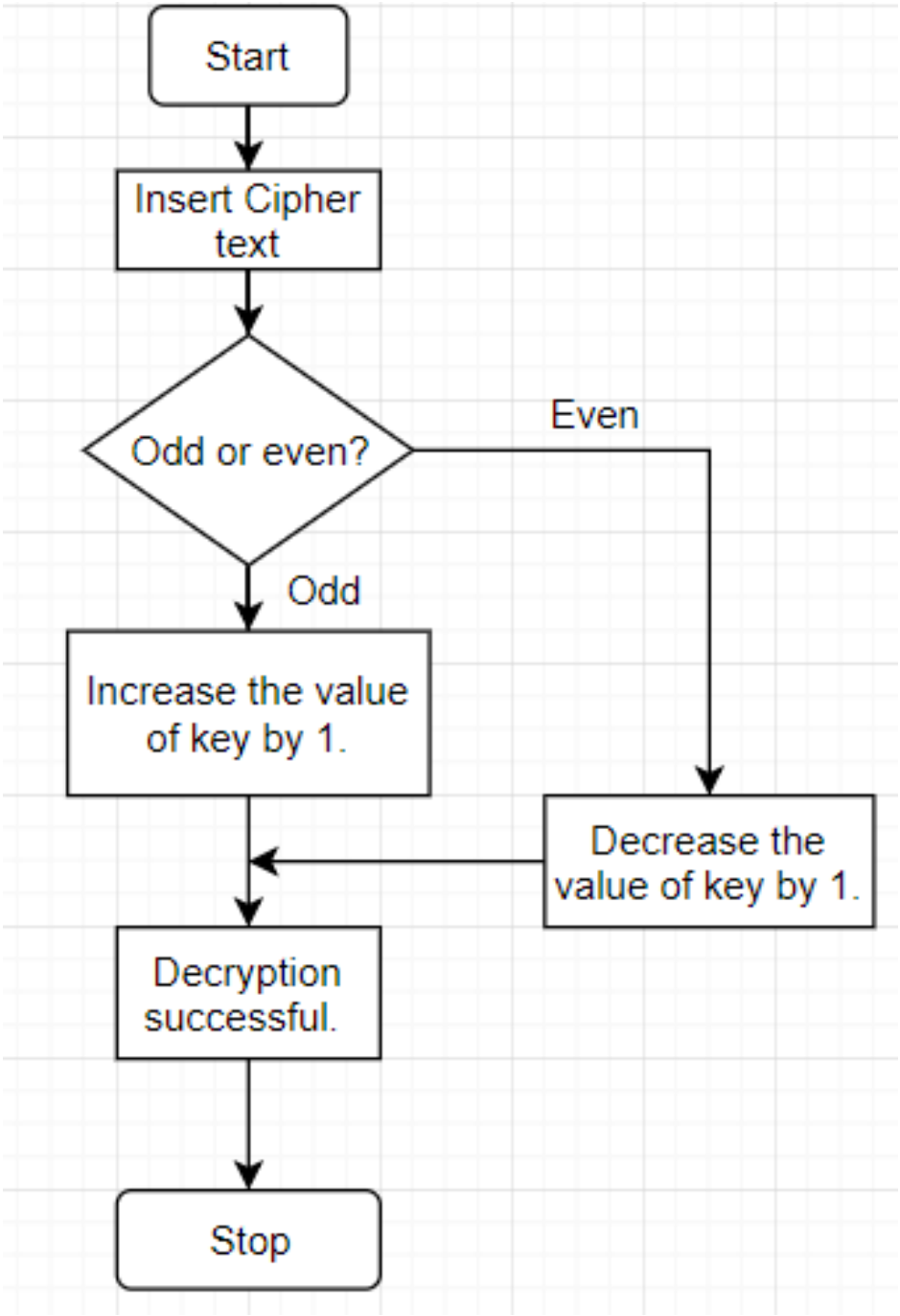


Figure 8 Flowchart for Decryption

Task 4 TESTING

Here are some examples of the encryption and decryption of the Modified Caesar Cipher.

Example 1

i) Encryption

Encrypt the message 'ISLINGTON'.

I	S	L	I	N	G	T	O	N
J	T	K	J	M	H	S	P	M

ii) Decryption

Decrypt the cipher text 'JTKJMHSPM'.

J	T	K	J	M	H	S	P	M
I	S	L	I	N	G	T	O	N

Example 2

i) Encryption

Encrypt the numerical message '2019'.

2	0	1	9
1	9	2	0

ii) Decryption

Decrypt the encrypted numerical '1920'.

1	9	2	0
2	0	1	9

Example 3

i) Encryption

Encrypt the message 'NEPAL1723'.

N	E	P	A	L	1	7	4	3
M	F	O	B	K	2	8	3	4

ii) Decryption

Decrypt the cipher text ‘MFOBK2834’.

M	F	O	B	K	2	8	3	4
N	E	P	A	L	1	7	4	3

TASK 5 EVALUATION

As we all are well aware, all cryptographic algorithms have the own strengths and flaws. To understand the strengths and weaknesses of the Modified Caesar Cipher, testing was carried out.

5.1) Strengths of the Modified Caesar Cipher

- It uses various keys and doesn't hint at the key for decryption like the Caesar Cipher.
- It is easier to understand and implement when compared to other cryptographic algorithms.
- It can be used to encrypt important messages between multiple people.
- The Modified Caesar Cipher is far more complex compared to the Caesar Cipher, so it can be relied on more.
- Although it is complex when compared to the Caesar Cipher, it doesn't implement complex mathematics.

5.2) Weaknesses of the Modified Caesar Cipher

- The cryptographic algorithm cannot be used to encrypt symbols.
- Although the Modified Caesar Cipher is intricate compared to the Caesar Cipher, it is still vulnerable to decryption by modern computer systems.
- For the numbers 0 and 9, the condition applies is a somewhat inconsistent when compared to the other numbers.
- The encryption and decryption process may become time consuming depending on the capabilities of the system and the user.
- The working mechanism of the algorithm limits the application area of the algorithm.

5.3) Application Areas

The Modified Caesar Cipher can be used in many areas as a better substitution cipher when compared to the Caesar Cipher. It can be used in small investment business that are not in threat of large scale attacks and also those that cannot afford to implement a proper security management system. It can also be used in those communication systems which do not involve modern computing systems such as postal services and

can be used to maintain confidentiality between two parties. It can also be used the educational field to help the students who study cryptography.

Conclusion

From the findings seen in the report, we can conclude that information security is a big issue. From ancient times, people had to find solutions to encrypt messages so that unintended people would not be able to understand it. In modern times, ancient traditional techniques have disappeared and modern techniques for communication over modern computing devices have been developed. This led to the idea of CIA. CIA is a concept that protects the confidentiality, integrity and availability of information.

Also, we studied the Caesar Cipher and considering that it could easily be decrypted as the frequency and tendency of letters used for substitution could hint that the decryption key, concluded that the algorithm was quite weak. So, through basic modifications in the encryption and decryption process, a new cryptographic algorithm was created and named, Modified Caesar Cipher. It new algorithm mitigated some of the shortcomings of the traditional Caesar Cipher.

References

Ahmed Al-Vahed, H. S., 2011. An overview of modern cryptography. *World Applied Programming,* pp. 55-61.

Anon., n.d. *Caesar Cipher.* [Online]

Available at: https://www.techopedia.com/definition/6311/caesar-cipher

[Accessed 5 January 2019].

Anon., n.d. *CIA Triad.* [Online]
Available at: https://www.informationsecuritybuzz.com/isbuzz-expert-panel/cia-triad-and-new-emerging-technologies-big-data-and-iot/

Anon., n.d. *Classical Cryptography.* [Online]
Available at: https://www.emaze.com/@AOZTQZLI

Anon., n.d. *Origin of Cryptography.* [Online]
Available at: https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm

Anon., n.d. *Practical Cryptography.* [Online]
Available at: http://practicalcryptography.com/ciphers/caesar-cipher/
[Accessed 5 1 2019].

Anon., n.d. *Symmetric vs Asymmetric Encryption.* [Online]
Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Anon., n.d. *Symmetric vs. Asymmetric Encryption.* [Online]
Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences

Anon., n.d. *The Enigma Machine.* [Online]
Available at: http://ct.excelwa.org/social-studies/the-enigma-machine/

Bishop, M., 2002. *Computer Security Art and Science.* s.l.:Addison Wesley.

Boni Oktaviana, A. P. U. S., 2016. Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography. *IOSR Journal of Computer Engineering,* 18(4), pp. 26-27.

Christof Paar, J. P., 2009. *Understanding Cryptography.* s.l.:Springer-Verlag Berlin Heidelberg.

Henderson, A., 2017. Information Technology. *The CIA Triad.*

Hill, T., 2003. *The Cryptographer.* s.l.:Faber and Faber.

Kader, H. A., 2008. Performance Evaluation of Symmetric Encryption Algorithms. *International Journal of Computer Science and Network Security.*

Landau, S., 2007. The Export of Cryptography in the 20th Century.

M.Damico, T., 2009. A Brief History of Cryptography. pp. 1-1.

Mukund R. Joshi, R. A. K., 2015. Network Security with Cryptography. *International Journal of Computer Science and Mobile Computing,* pp. 201-204.

Neha Garg, P. Y., 2014. Comparison of Asymmetric Algorithms in Cryptography. *International Journal of Computer Science and Mobile Computing,* pp. 1190-1196.

Nweke, L. O., 2017. Using CIA and AAA models to Explain Cybersecurity Activities. *PM World Journal.*

Phillips, G., 2018. *Basic Encryption Terms You Should Know.* [Online]
Available at: https://www.makeuseof.com/tag/encryption-terms/

Rhody, K., n.d. *The Importance of Computer Security.* [Online]
Available at: https://www.onsharp.com/the-importance-of-computer-security/

Ritu Tripathi, S. A., 2014. International Journal of Advance Foundation and Research in Computer. *Comparative Study of Symmetric and Asymmetric Cryptography Techniques,* pp. 71-73.

Rouse, M., 2014. *CIA Triad.* [Online]
Available at: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

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

Singh, S., 2001. Caesar Shift Cipher. In: *The Code Book.* s.l.:s.n.

Stapleton, J., 2014. *Security without Obscurity.* s.l.:s.n.

Thorsteinson, P., 2003. *NET Security and Cryptography.* s.l.:s.n.

Wai, M. S., 2015. *Study on Symmetric and Asymmetric Cryptographic Techniques.* s.l., s.n.