LONDON
METROPOLITAN
UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2023 -24 Autumn

Student Name: Kipa Shrestha

London Met ID: 22066682

College ID: np01nt4a220120

Assignment Due Date: Monday, 15th January 2024

Assignment Submission Date: Monday, 14th January 2024

Word Count (Where Required): 6820

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.

Abstract

The information security triad of confidentiality, integrity, and availability (CIA) helps in protecting an organization's privacy. The CIA also contributes to the security of common people's information. Various methods of cryptography help to encrypt confidential messages. Playfair cipher is one of the many cryptography algorithms. The top-secret data is encrypted using a substitution method by the Playfair cipher. Playfair cipher can be easily cracked by brute force attack, so a new algorithm named Extended Playfair Cipher is a more secure version of Playfair cipher. The Extended Playfair Cipher uses two 6*6 matrices to encrypt the secret information.

Table of Contents

Table of Figures

1. Introduction to Cryptographic Systems

1.1. CIA Triad

CIA also known as Confidentiality, Integrity, and Availability is a model designed to guide policies for information security within an organization. They are used for finding vulnerabilities and methods for creating solutions. When all three standards have been met, the security profile of the organization is stronger and better equipped to handle threat incidents (Fortinet, 2023).

The CIA Triad
IntelliPaat
Confidentiality
Integrity
Availability

Figure 1: CIA Triad (Intellipaat, 2023).

1.2. Introduction to Cryptography

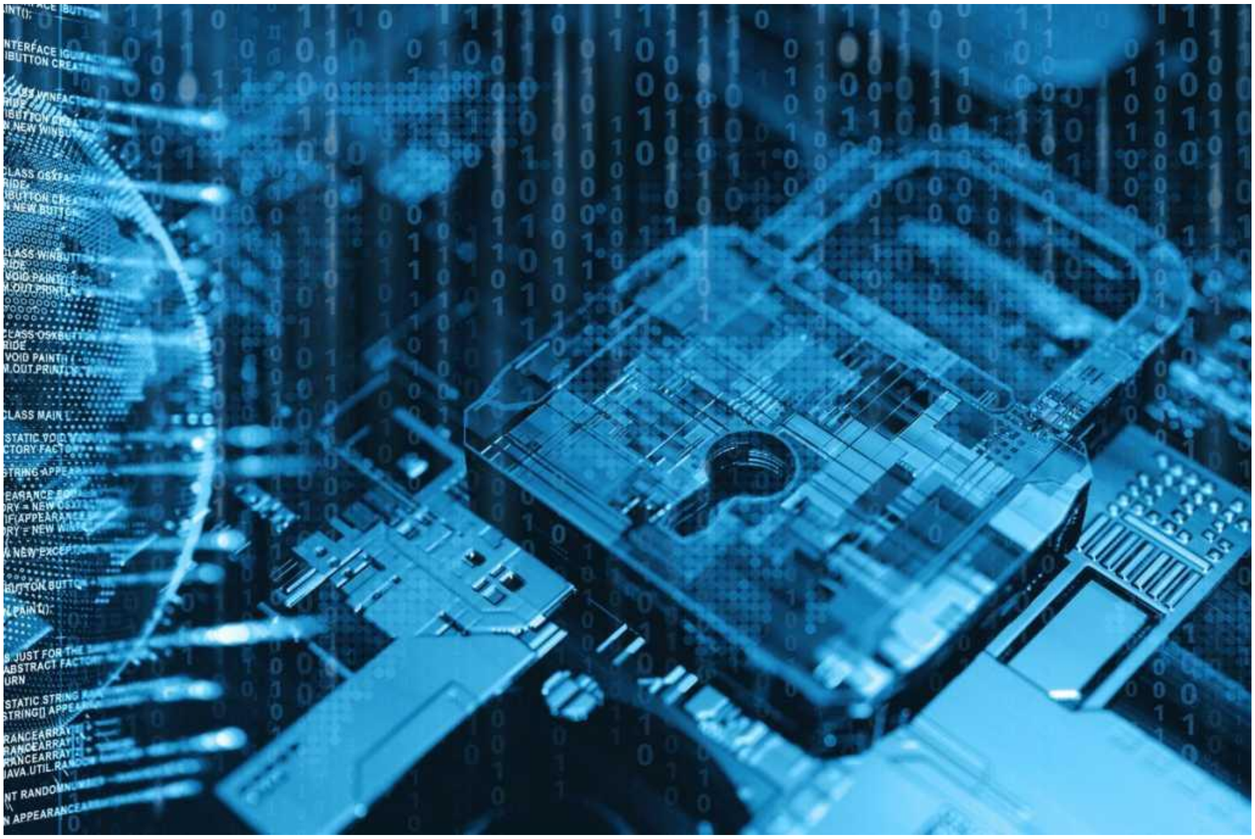

Figure 2: Cryptography (Fruhlinger, 2022).

Cryptography is the process of hiding or coding data so that only the intended person may read it. In simple terms, it is the practice of coding information to ensure only the person whom a message was written for can read and process the information. Cryptography has been used to code messages for thousands of years. It is still used today in e-commerce, bank cards and computer passwords. The encryption and decryption of data are made possible by modern cryptography techniques, which include cyphers and algorithms like 128-bit and 256-bit encryption keys. Modern ciphers, such as the Advanced Encryption Standard (AES), is considered virtually unbreakable (Fortinet, 2023).

Figure 3: Importance of cryptography (Fortinet, 2023).

Cryptography is still essential for maintaining confidentiality, safeguarding users' data, and preventing hackers from obtaining private company information. Every day, people and organisations use cryptography to safeguard their privacy and maintain the confidentiality of their communications and data. By encrypting communicated messages with an algorithm and a key that is only known to the sender and receiver, cryptography maintains confidentiality. A common example of this is the messaging app WhatsApp, which encrypts user communications to prevent hacking or interception. Cryptography also secures browsing, such as with Virtual Private Networks (VPNs), which use encrypted tunnels, asymmetric encryption, and public and private shared keys (Fortinet, 2023).

1.3. Technical Terminologies

Encryption and Decryption:

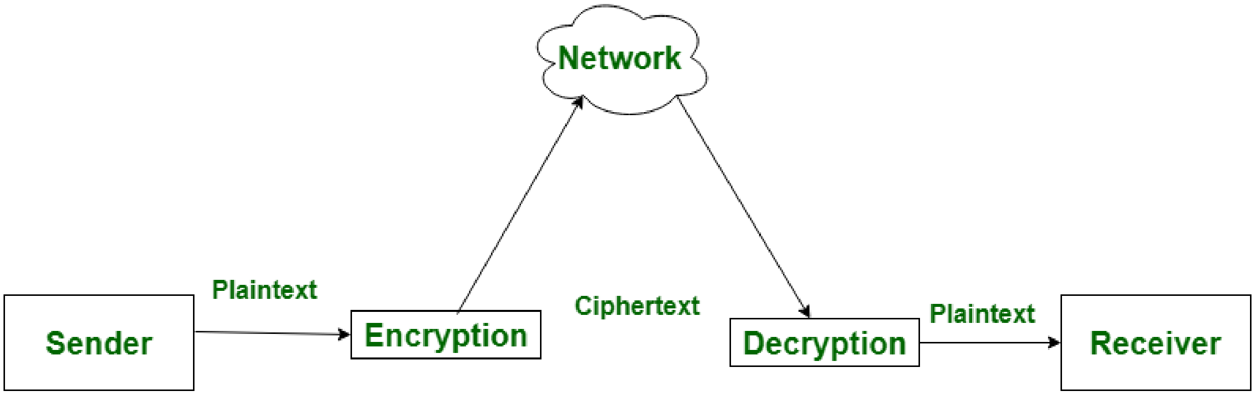

Figure 4: Encryption and Decryption (Geeksforgeeks, 2023).

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext). Any message can be encrypted with either secret key or public key. On the other hand, the process of converting a meaningless message (Ciphertext) back to its original form(plaintext) is known as decryption. The encrypted message can be decrypted with either secret key or private key (Geeksforgeeks, 2023).

Algorithm:

Algorithms are widely used throughout all areas of IT. An algorithm is typically used in mathematics, computer science, and computer programming to describe a brief process that resolves an ongoing issue. Algorithms are also used as specifications for performing data processing and play a major role in automated systems (Gillis, 2023).

Plain text:

Plain text is any text, text file, or document that only contains the text. Plain text supports ASCII characters, symbols, and spaces, but does not support any type of text formatting. Bold, Italic and Underlined styles are not allowed to use in plain text (Loshin, 2023).

Cipher text:

Ciphertext is an encrypted text which is transformed from plain text using various sorts of the algorithm. The ciphertext is an unreadable text. To gain information from the ciphertext, it must be decrypted using a key (Rosencrance, 2023).

1.4. Aim and Objectives:

Aims:

This coursework's main goal is to research, create, and test a novel cryptographic system to increase data protection and secure communication. Enhancing the security and integrity of data in various digital environments is the aim, which will be achieved by addressing the challenges in existing cryptographic algorithms.

Objectives:

- To investigate the history of cryptography, symmetric and asymmetric ciphers.
- To choose a relevant base cryptosystem for improvement.
- To formulate secure encryption and decryption algorithms.
- To assess the cryptographic system’s performance and vulnerabilities.
- To identify potential areas for the system’s effective utilization.

1.5. History of Cryptography

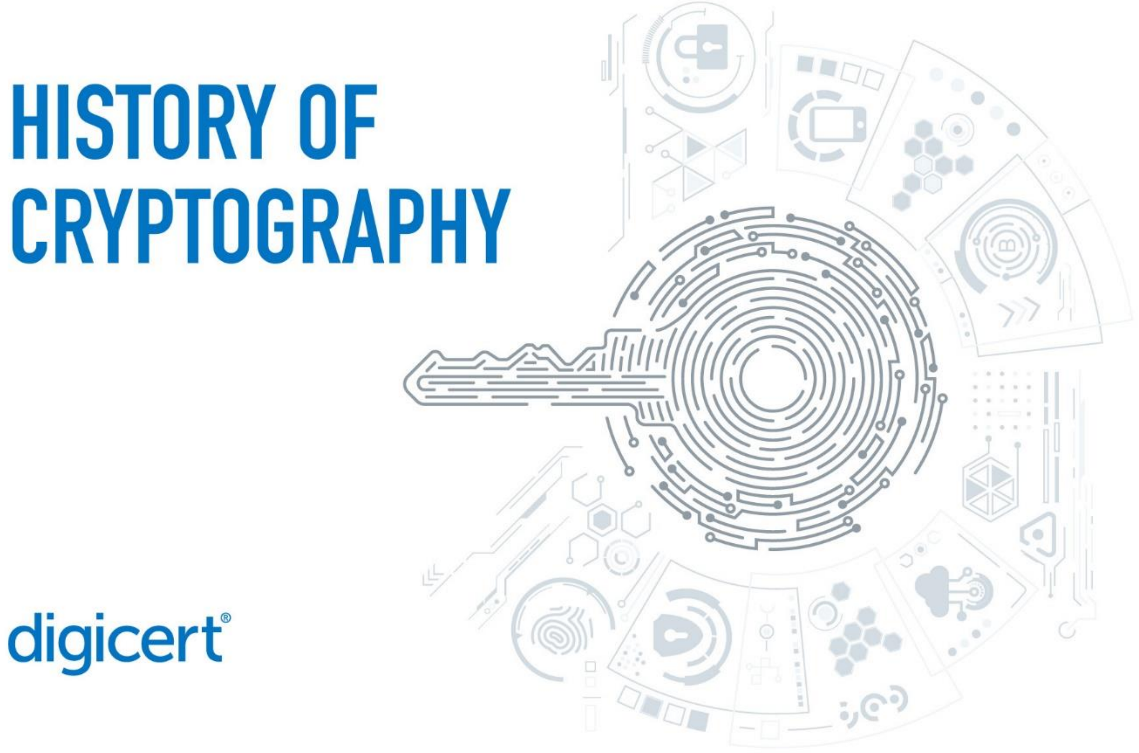

Figure 5: History of Cryptography (Digicert, 2023).

The word cryptography comes from the Greek words “kryptos” meaning hidden, and “graphien” meaning to write. This “hidden writing” has been advancing for thousands of years. The first known evidence of cryptography was found in an inscription carved around 1900 BC in the main chamber of the Egyptian nobleman Khnumhotep II's tomb. In 1500 BC, a Mesopotamian scribe used cryptography to hide a glaze formula for pottery. This is the first example of cryptography being used to hide sensitive data. Cryptography has been used in practically every significant early civilization, according to available data. Kautilya, also known as Chanakya, wrote the ancient text "Arthashashtra," describing how spies were assigned missions in "secret writing" in early India. The ancient Greeks were known to use ciphers (an algorithm used for encryption or decryption), to transform a message (Tutorials point, 2023).

In 100 BC, Julius Caesar shared secret messages with his army generals during a battle by using a form of encryption. The Caesar Cypher is one of the most well-known uses of cryptography. Alternatively referred to as a substitution cypher, the cypher text is created by replacing each character in the plain text with a different character (Sidhpurwala, 2023).

In the 16th century, the Vigenère Cipher came to be. This technique uses a series of interconnected Caesar cyphers based on a keyword's letters to encrypt alphabetic text. This is known as polyalphabetic substitution. While it was first described by Giovan Battista Bellaso in 1553, Blaise de Vigènere got the credit in the 19th century. Despite being more secure than the Caesar cypher and having been used by numerous individuals, Friedrich Kasiski cracked the Vigènere cypher in 1863 (Sidhpurwala, 2023).

The Hebern rotating machine, invented in 1917 by Edward Hebern in Illinois, came next. Combining the electrical and mechanical components of an electric typewriter with the mechanical parts of a regular typewriter, this machine was the first to use electrical circuits in a cipher device. Connected through a scrambler, the machine included a disk with electrical contacts on either side (called as a rotor). Wires were used to connect each letter to another letter on the opposite side in random fashion, also known as a single substitution alphabet (Sidhpurwala, 2023).

In World War I and World War II, cryptography played a vital role. German engineer Arthur Scheribus built the Enigma Machine in 1918. The Nazi German military employed it frequently by the time of World War II. The machine produced ciphertext by spinning three or more rotors at different speeds to scramble the 26-letter alphabet. The Enigma Machine was ultimately cracked by Poland, which led the British to create the Bombe, a device that helped to identify the wheel order of the Enigma machine and the rotors' initial settings. Up until now, most cryptography applications have been related to warfare. That all changed, though, when organisations realised how profitable it might be to use cryptography to protect customer data from competitors (Sidhpurwala, 2023).

In the 1970s, IBM created the block cipher, Lucifer. It uses an algorithm that works with blocks, which are fixed-length groups of bits. Block ciphers use symmetric-key algorithms, which encrypt plaintext with the same cryptographic keys and decrypt it with other ones.

By combining substitution and transposition encryption, Lucifer created the Data Encryption Standard (DES), which is in use today (Digicert, 2023).

1.6. Symmetric and asymmetric ciphers:

1.6.1. Symmetric ciphers:

In symmetric ciphers, the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another. Some of the common algorithms of symmetric cryptography are Blowfish, AES, RC4, DES, RCS, and RC6. Moreover, the most widely used algorithm are AES-128, AES-192, and AES-256 (Geeksforgeeks, 2023).

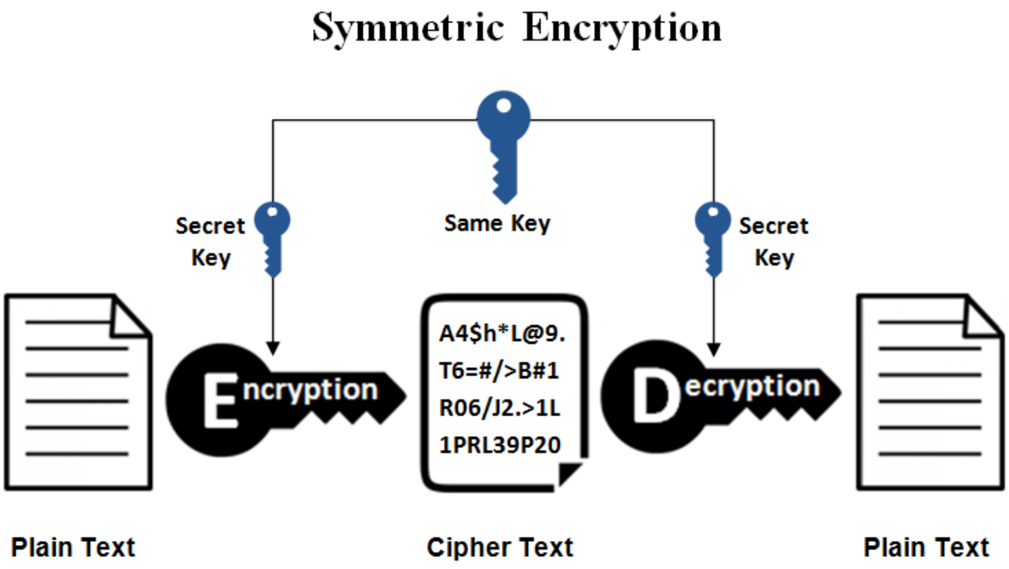

Figure 6: Symmetric Encryption (Ssl2Buy, 2023).

The advantages of symmetric cryptography are:

- Symmetric cryptography is extremely secured if encrypted by using 256-bit key length.
- Symmetric cryptography is faster in encryption and decryption rather than other algorithms (AAT, 2022).

The disadvantages of symmetric cryptography are:

- As a single key is used for encryption and decryption, it should be kept secure at both ends.
- As the number of keys depends on the number of communicating parties, the key stack in larger networks will be more which affects the maintenance (1000 Projects, 2012).

1.6.2. Asymmetric ciphers:

Whereas asymmetric ciphers are based on public and private key encryption techniques. It uses two different keys to encrypt and decrypt the message. It is more secure than the symmetric ciphers but is much slower. Many protocols rely on asymmetric cryptography. Some of these protocols are transport layer security (TLS) and secure socket layer (SSL) protocols, which make HTTPS possible (Geeksforgeeks, 2023).

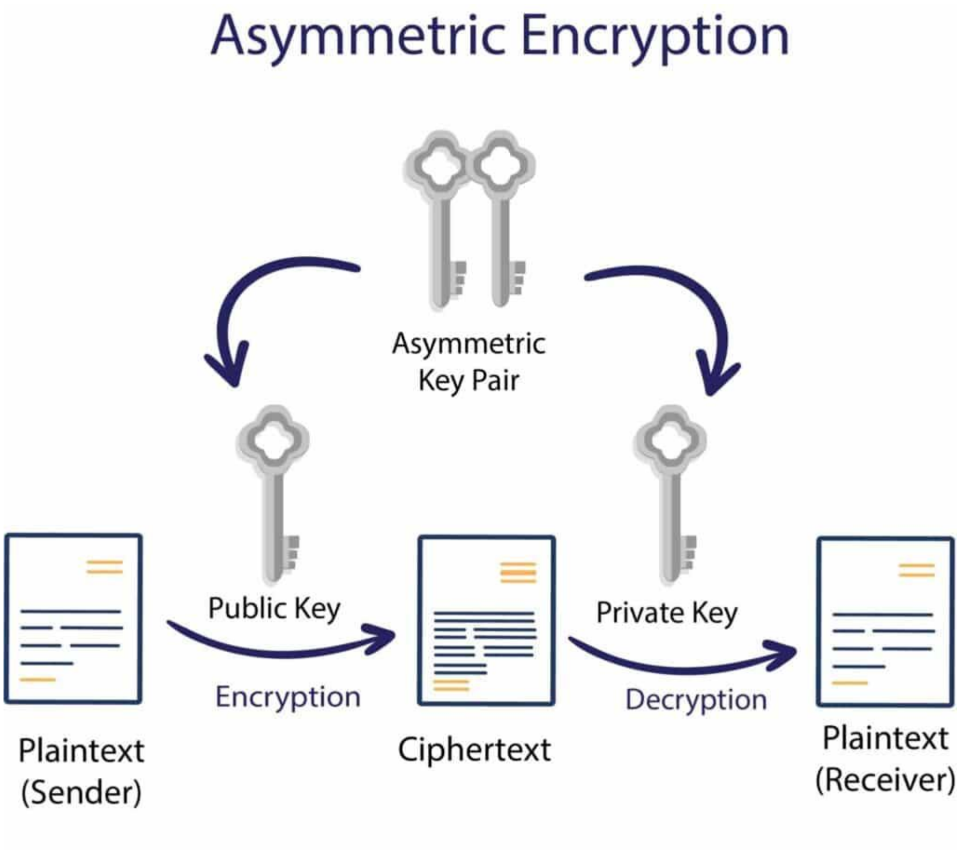

Figure 7: Asymmetric Encryption (Encryption Consulting, 2023).

The advantages of Asymmetric cryptography are:

- The private key is not transferred through the secure channel for the encryption to be successful.
- There is a possibility of an electronic signature (evangelos, 2017).

The disadvantages of Asymmetric cryptography are:

- In asymmetric cryptography, there is more use of resources rather than symmetric cryptography.
- As, asymmetric uses two keys, a lot of time is consumed for the encryption as well as decryption process (Brush, 2023).

2. Background of the Playfair Cipher

Charles Wheatstone created the Playfair cipher in 1854. In the 18th century, the Playfair cipher was heavily used by Lord Playfair. Playfair cipher was based on the polyalphabetic cipher. There is the only use of 26 letters that can be easily cracked. Playfair cipher arranges the plaintext in a table based on a key value. There are two stages of Playfair cipher, encryption, and decryption. Hence Playfair cipher is a symmetrical key algorithm then the two stages are the same. The alphabet in the Playfair cipher is assembled in a 5 *5 matrix (Simmons, 2023).

Some of the rules for Playfair cipher are:

a. It is important to delete all the spaces and symbols in the plain text, only the alphabet is allowed to use.
b. The alphabet is arranged in a 5*5 matrix. The key alphabet is arranged firstly, and it is being followed by the remaining letter without any repetition of an alphabet.
c. J and I are supposed as same like I/J.
d. If the plain text is odd in number, then add Z at the end of the letter.
e. The plaintext which is supposed to encrypt is written in pair form.
f. If there are repeated letters in plain text, then add filler (X, Y, Z) in them.

For encryption,

a. If there are the same letter in the same row, then it is replaced with the letter on the right circularly.
b. If there are the same letter in same column, then it is replaced by the letter below circularly.
c. If neither of the previous two rules is true, create a rectangle on the grid with the two letters at its corners. Replace each letter of the diagram with the letter on the corner of the rectangle that is on the same row.

For decryption,

a. If there are the same letter in the same row, then it is replaced with the letter on the left circularly.

b. If there are the same letter in the same column, then it is replaced with the letter upward circularly.

c. If two letters are not in the same row or key column, the first letter is replaced by the letter at the intersection of the first letter line with the second letter column. The second letter is replaced by the letter at the fourth vertex of a square or rectangle formed by the 3 letters used (Intellipaat, 2023).

Example:

Plaintext: Cipher

Key: PLAYFAIR

Step 01: 5 * 5 matrix is created.

- The blue colour indicates the key for encryption and decryption.

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Step 02. Pair the Plaintext and if there is an odd letter at the end insert Z as filler.

CI PH ER

For encryption,

Step 01: Now start to encrypt the pair of letters accordingly.

❖ The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to the rules of the Encryption process,

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

- CI is ciphered as DR.

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

- PH is ciphered as AE.

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

- ER is ciphered as GI.

The ciphertext is generated as DR AE GI.

For decryption,

Step 01: Now start to decrypt the pair of letters accordingly,

- The purple colour indicates ciphertext, and the green colour indicates plaintext.

According to the rules of the Decryption process,

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

- DR is deciphered as CI.

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

- AE is deciphered as PH.

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

- GI is deciphered as ER.

Finally, the decrypted message is CI PH ER.

2.1. Advantages of Playfair Cipher

- It is much harder to crack because using the methodology of the frequency analysis used to break simple substitutions ciphers (25*25) = 625 digitals instead of 25 difficult monographs.
- The process for encryption and decryption is relatively easy as compared to other algorithms. Moreover, Playfair cipher consumes less time.

2.2. Disadvantages of Playfair Cipher

- The main disadvantage of Playfair Cipher is as it is a symmetric cipher the key that is used in encryption and decryption are the same.
- If the Plaintext is understood, then it becomes easier for hackers to crack the message (Geeksforgeeks, 2023).

3. Development of New Cipher

This extended play fair algorithm is based on the use of a 6 * 6 matrix of letters created using a keyword. The matrix is created by filling in the keyword's letters vertically. The remaining space in the matrix is then filled in with the remaining letters in alphabetical order and the numbers from 0 to 9. The digits 0 to 9 can be arranged in ascending order below the alphabet Z cells. To prevent confusion for the user during deciphering, we have placed both I and J in two separate cells rather than counting them as one letter in this case. The user can easily and quickly encrypt alphanumeric data since this method allows plain text containing alphanumeric values.

The main aim is to modify the Playfair Cipher into an Extended Playfair Cipher because the Playfair Cipher consists of only a few letters. Moreover, there is no way to encrypt the numeric value in the common Playfair Cipher. The extended Playfair Cipher overcomes all these defects that are present in Playfair Cipher. This was the objective to change the Playfair Cipher.

Some of the rules of Extended Playfair Cipher are:

a. Firstly, the alphabet is arranged into a 6*6 matrix. The alphabet is placed vertically, and the given key is to be implemented at the start.
b. Don’t repeat the keyword in the matrix.
c. The plain text which is supposed to encrypt is written in a pair forms. Like ab, cd, ef and so on.
d. If there are repeated letters in plaintext or an odd while pairing the plaintext, add fillers (Y, Z) between them.

For encryption:

a. If both letters are in the same column, different column, or different row, then replace the letters on the right circularly according to the position of letters. Like if A is in the 1st position, then it will replace the step right and if B is in the 2nd position, then it will replace the two-step right.

b. If both letters are in the same row, then replace the letter with three steps down circularly.

For decryption:

a. If both letters are in the same column, different columns different rows, then replace the first letter five-step right, and second letter four-step right circularly.
b. If both letters are in the same row, then replace the letter three step downward circularly.

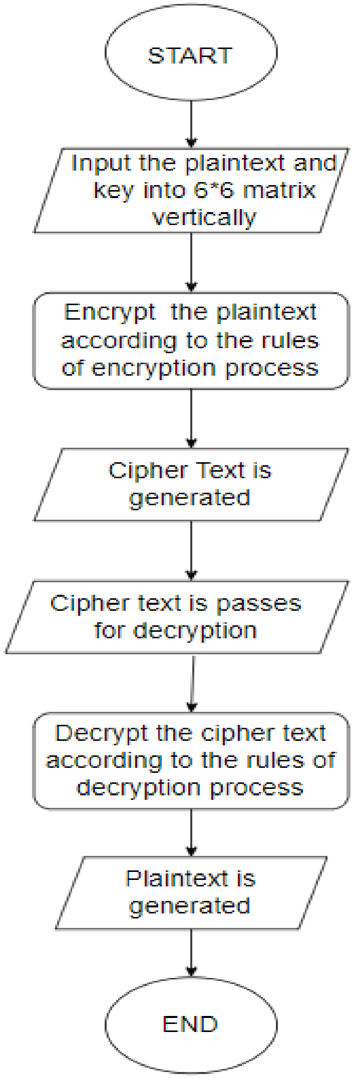
START
Input the plaintext and key into 6*6 matrix vertically
Encrypt the plaintext according to the rules of encryption process
Cipher Text is generated
Cipher text is passes for decryption
Decrypt the cipher text according to the rules of decryption process
Plaintext is generated
END

Figure 8: Flow chart of Extended Playfair Cipher.

4. Testing

4.1. Test 1

Key: Security

Plain text: HANSOHEE

Step 01. Two 6*6 matrix is created, and key are inserted vertically.

- The blue colour represents the key.

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

Step 02: Create a pair of plain text in two letters and if there is a repeated letter and single of double letter insert filler in them.

HA NS OH EZ

For Encryption,

Step 01: Now start to encrypt the pair of letters accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher encryption process,

- HA = OP

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

- NS = QU

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

- OH = VL

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

- EZ = R2

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

Therefore, the cipher text is OP QU VL R2.

For Decryption,

Step 01: Now start to decrypt the ciphertext accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher decryption process,

- OP = HA

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

- QU = NS

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

- VL = OH

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

- EZ = R2

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

Therefore, the plain text is HA NS OH EZ.

4.2. Test 2

Key: MONSTER

Plaintext: BANG2005

Step 01. Two 6*6 matrix is created, and key are inserted vertically.

- The blue colour represents the key.

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

Step 02: Create a pair of plain text in two letters and if there is a repeated letter and single of double letter insert filler in them.

BA NG 20 05

For Encryption,

Step 01: Now start to encrypt the pair of letters accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher encryption process,

- BA = IQ

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

- NG = BY

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

- 20 = 8N

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

- 05 = 6A

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

Therefore, the cipher text is IQ BY 8N 6A.

For Decryption,

Step 01: Now start to decrypt the ciphertext accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher decryption process,

- IQ = BA

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

- BY = NG

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

- 8N = 20

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

- 6A = 05

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

Therefore, the plain text is BA NG 20 05.

4.3. Test 3

Key: SUN

Plaintext: SWIFT

Step 01. Two 6*6 matrix is created, and key are inserted vertically.

- The blue colour represents the key.

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

Step 02: Create a pair of plain text in two letters and if there is a repeated letter and single of double letter insert filler in them.

SW IF TZ

For Encryption,

Step 01: Now start to encrypt the pair of letters accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher encryption process,

- SW = D8

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

- IF = PT

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

- TZ = 0U

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

Therefore, the cipher text is D8 PT 0U.

For Decryption,

Step 01: Now start to decrypt the ciphertext accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher decryption process,

- D8 = SW

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

- PT = IF

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

- 0U = TZ

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

Therefore, the plain text is SW IF TZ.

4.4. Test 4

Key: MARVEL

Plaintext: AVENGER6

Step 01. Two 6*6 matrix is created, and key are inserted vertically.

- The blue colour represents the key.

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

Step 02: Create a pair of plain text in two letters and if there is a repeated letter and single of double letter insert filler in them.

AV EN GE R6

For Encryption,

Step 01: Now start to encrypt the pair of letters accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher encryption process,

- AV = CN

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

- EN = G1

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

- GE = CA

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

- R6 = L9

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

Therefore, the cipher text is CN G1 CA L9.

For Decryption,

Step 01: Now start to decrypt the ciphertext accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher decryption process,

- CN = AV

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

- G1 = EN

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

- CA = GE

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

- L9 = R6

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

Therefore, the plain text is AV EN GE R6.

4.5. Test 5

Key: MOVIE

Plaintext: FROZEN

Step 01. Two 6*6 matrix is created, and key are inserted vertically.

- The blue colour represents the key.

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

Step 02: Create a pair of plain text in two letters and if there is a repeated letter and single of double letter insert filler in them.

FR OZ EN

For Encryption,

Step 01: Now start to encrypt the pair of letters accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher encryption process,

- FR = N4

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

- OZ = E2

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

- EN = G1

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

Therefore, the cipher text is N4 E2 G1.

For Decryption,

Step 01: Now start to decrypt the ciphertext accordingly.

- The purple colour indicates plaintext, and the green colour indicates ciphertext.

According to rules of the Extended Playfair Cipher decryption process,

- N4 = FR

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

- E2 = OZ

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

- G1 = EN

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

Therefore, the plain text is FR OZ EN.

5. Evaluation of Extended Playfair Cipher

5.1. Strength of Extended Playfair Cipher

- ❖ The Extended Playfair cipher uses two 6*6 matrix which makes it difficult to assume the encrypted messages.
- ❖ Extended Playfair cipher can encrypt and decrypt the numeric values.
- ❖ The plain text containing contact numbers, date of birth, house numbers and other numerical values can be easily and efficiently encrypted.
- ❖ The encryption and decryption rules are different in extended Playfair cipher as compared to normal Playfair cipher.

5.2. Weakness of Extended Playfair Cipher

- ❖ The key uses for encryption and decryption are the same.
- ❖ While encryption same key can be repeated for the same word occasionally.
- ❖ The encryption and decryption process consumes lots of time.
- ❖ Long sentences cannot be encrypted because it may cause an error.

The application areas of extended Playfair Cipher are:

- ❖ To Encrypt the ATM PIN code.
- ❖ It can be used in an organization to encrypt the valuable information of customers. In a hospital, it is used to encrypt the patients' details.
- ❖ School can use extended Playfair cipher to encrypt the student id and symbol number.

6. Conclusion

Privacy is one of the most important aspects of a person. People or organisations employ numerous security measures to increase privacy security. To maintain consistent security CIA triad is implemented. Along with the CIA, various sorts of cryptography are also used. Numerous algorithms are used in cryptography to secure messages. The Playfair cipher is just one algorithm among several. A 5*5 matrix is used by the Playfair Cipher to encrypt and decrypt the messages. With the help of a brute force attack, it is easily cracked because it encrypts data using a straightforward matrix. The weaknesses of the original Playfair cipher are fixed in the new version, called the Extended Playfair Cipher. For example, mathematical operations could not decipher the little letters used in the Playfair cipher; in comparison, the Extended Playfair cypher eliminates all these issues and is more secure. The extended Playfair cipher can be used in various fields in a bank, it is used to encrypt ATM pin, in a hospital it is used to encrypt a patient's details, in an organisation it is used to encrypt a client’s messages, and many more locations.

References

1000 Projects, 2012. *1000projects.org.* [Online]
Available at: https://1000projects.org/advantages-and-disadvantages-of-symmetric-cryptography.html
[Accessed 3 December 2023].

AAT, 2022. *allabouttesting.ord.* [Online]
Available at: https://allabouttesting.org/information-security-symmetric-cryptography/
[Accessed 3 December 2023].

Brush, K., 2023. *techtarget.com.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography
[Accessed 3 December 2023].

Digicert, 2023. *digicert.com.* [Online]
Available at: https://www.digicert.com/blog/the-history-of-cryptography
[Accessed 3 December 2023].

Encryption Consulting, 2023. *encryptionconsulting.com.* [Online]
Available at: https://www.encryptionconsulting.com/education-center/symmetric-vs-asymmetric-encryption/
[Accessed 10 December 2023].

evangelos, K., 2017. *electrodummies.* [Online]
Available at: https://www.electrodummies.net/en/asymmetric-encryption/
[Accessed 3 December 2023].

Fortinet, 2023. *fortinet.* [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/what-is-cryptography#:~:text=The%20Importance%20of%20Cryptography&text=Cryptography%20ensures%20confidentiality%20by%20encrypting,cannot%20be%20hacked%20or%20intercepted.
[Accessed 3 December 2023].

Fortinet, 2023. *fortinet.com.* [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,the%20development%20of%20security%20systems.
[Accessed 5 December 2023].

Fruhlinger, J., 2022. *csoonline.com.* [Online]
Available at: https://csoonline.com/article/569921/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html
[Accessed 3 December 2023].

Geeksforgeeks, 2023. *geeksforgeeks.org.* [Online]
Available at: https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/
[Accessed 3 December 2023].

Geeksforgeeks, 2023. *geeksforgeeks.org.* [Online]
Available at: https://www.geeksforgeeks.org/difference-between-symmetric-and-asymmetric-key-encryption/
[Accessed 3 December 2023].

Geeksforgeeks, 2023. *geeksforgeeks.org.* [Online]
Available at: https://www.geeksforgeeks.org/playfair-cipher-with-examples/
[Accessed 25 December 2023].

Gillis, A. S., 2023. *techtarget.com.* [Online]
Available at: https://www.techtarget.com/whatis/definition/algorithm
[Accessed 3 December 2023].

Intellipaat, 2023. *intellipaat.com.* [Online]
Available at: https://intellipaat.com/blog/playfair-cipher/
[Accessed 20 December 2023].

Intellipaat, 2023. *intellipaat.com.* [Online]
Available at: https://intellipaat.com/blog/the-cia-triad/
[Accessed 5 December 2023].

Loshin, P., 2023. *techtarget.com.* [Online]
Available at:
https://www.techtarget.com/searchsecurity/definition/plaintext#:~:text=In%20cryptography%2C%20plaintext%20is%20usually,algorithms%20is%20not%20always%20plaintext.
[Accessed 3 December 2023].

Rosencrance, L., 2023. *techtarget.com.* [Online]
Available at:
https://www.techtarget.com/whatis/definition/ciphertext#:~:text=Ciphertext%20is%20encrypted%20text%20transformed,the%20ciphertext%20back%20into%20plaintext.
[Accessed 3 December 2023].

Sidhpurwala, H., 2023. *redhat.com.* [Online]
Available at: https://www.redhat.com/en/blog/brief-history-cryptography
[Accessed 3 December 2023].

Simmons, G. J., 2023. *britannica.com.* [Online]
Available at: https://www.britannica.com/topic/Playfair-cipher
[Accessed 15 December 2023].

Ssl2Buy, 2023. *ssl2buy.com.* [Online]
Available at: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-

are-differences
[Accessed 10 December 2023].

Tutorials point, 2023. *tutorialpoint.com.* [Online]
Available at: https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm
[Accessed 3 December 2023].