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: Mandip Thapa

London Met ID: 19031343

College ID: NP01NT4A190136

Assignment Due Date: January 22, 2021

Assignment Submission Date: January 22, 2021

Word Count: 5260

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.

Table of content

Abstract

This coursework was completed successfully with lots of hard work. This report includes information about the cryptographic system. Research works were done about information security, cryptography, and various cryptographic algorithms. A brief explanation of the cryptographic algorithm, its history, and its types are done. Row Transposition cipher, Playfair cipher, and Caesar cipher are selected, their background is explained briefly and modification is done and a new cipher is made and named as Mandip-crypto cipher. This new cryptographic algorithm is tested by using five different examples. Finally, the evaluation of the new cryptographic algorithm is done and its application area is briefly explained.

This coursework was interesting and very helpful as it helped to gain different experiences and knowledge. This report can be used to gain information about the cryptographic algorithm and its types. This coursework assisted me in understanding the concept of cryptography and I was able to create a new cryptographic algorithm. I want to thank my teacher, module leader, friends, and college for guiding me towards the direction of completion of this coursework.

List of Figures

List of Tables

Introduction

Information security has been one of the basic needs in the computer world and its demand is increasing day by day because the computers and networks are being misused at a growing rate. Information security authorizes the company to protect digital information, physical information, important assets, and the main objective of Information security is to ensure confidentiality, integrity, and availability of the information for the organization (Cassetto, 2019). Application security, Cloud security, Cryptography, infrastructure security, Incident management and Vulnerability management are the types of information security and the group of technologies, policies, protocols, and practices are always required to secure the information of an organization and security is the journey, not the destination. The CIA stands for Confidentiality, Integrity, and Availability, which is the security model that has been designed for information security (ForcePoint, 2019).

Figure 1: The CIA Triad (Burnette, 2020).

The figure shown above is the CIA (Confidentiality, Integrity, and Availability) triad.

Confidentiality involves the protection of information, giving access to those users who are allowed to see it while preventing unauthorized users from accessing the data or important information, Integrity is another important aspect of information security that ensures the authenticity and accuracy of the data, and it is maintained by disallowing request to edit or change the information, Availability is the property that the information is accessible to the authorized users only and they can easily access or modify the information (Michael Goodrich, 2014).

Cryptography is a portion of information security that consists of the mathematical function used to disguise the information known as Encryption and the same method repeated to get back to the original information known as Decryption and the whole process of encryption and decryption uses a common mathematical function to generate a Key that has a vital role in Cryptography (Chhetri, 2019). The method of creating and applying codes to secure the data transmitted from various sources is also known as Cryptography. Cryptography is derived from the Greek words krypton that means hidden and graphein which means to write and involves creating and applying codes to secure messages (Michael E.Whitman, 2018). Cryptography is the process that ensures the secure transmission of information between the two groups and it aims to convert the information into a non-readable form with the help of an algorithm and key which is known to sender and receiver only (Umang Bhargava, 2017). Cryptographic techniques were used even in ancient times and the most used technique was symbol replacement which is the most basic form of cryptography and it was used in Egyptian and Mesopotamian civilization, the ancient cryptographic technique known was found in the tomb of an Egyptian noble which dates back 3,900 years (BinanceAcademy, 2018). Cryptography dates back to the history when Julius Caesar gave information to his generals and did not trust his messages so, every letter A was replaced with D, B with E, and so on through the alphabet, only the person that knew the rule could translate the information which was encrypted and to get this process of securing the information two types of the algorithm for cryptography were used, which are encryption and decryption algorithm (Chhetri, 2019).

Figure 2: Ancient Scytale Tool (SemanticScholar, 2017).

The figure shown above is of Ancient Scytale tool which was used in ancient period to securely transfer the messages in military and in the government. In 1466, the fathers of Cryptography, Leon Battista operated with polyalphabetic substitution and invent a cipher disk, in 1553, Giovan Battista Bellaso presented the plan of the passphrase as a key for encryption, and his polyalphabetic encryption process is later derived for another man who later used the technique known as Vigenere Cipher (Dooley, 2018). The figure of Vigenere Cipher is shown below.

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

Figure 3: The Vigenere Cipher (MichiganTech, 2018).

From 18th century to 20th century, the cryptographic system began to evolve and became more advanced with the advancement of technologies. In the First World War first time, electricity was used to encipher a message and the teletype one-time tape cipher was also introduced, the cipher wheel was also invented just before First World War and the Enigma machine was also developed by the Germans in 1918 but was used in Second World War. The US Navy also used different electric rotor cipher and convinced the US Army to apply the same invention so they could transmit information with each other. The figure shown below is of Enigma machine.

Figure 4: German Enigma Machine (Cnet, 2018).

In Second World War, different types of cryptographic systems were used which were more advanced than the systems used in First World War. In 1937, the Japanese empire invented the Purple machine that was based on standards similar to the German Enigma and was used to encrypt various important information and in 1940 the code generated by the purple cipher was broken and a new machine was made which could quickly decode the Purple's cipher (Rohwer, 1999).

The figure shown below is the Purple machine used by the Japanese.

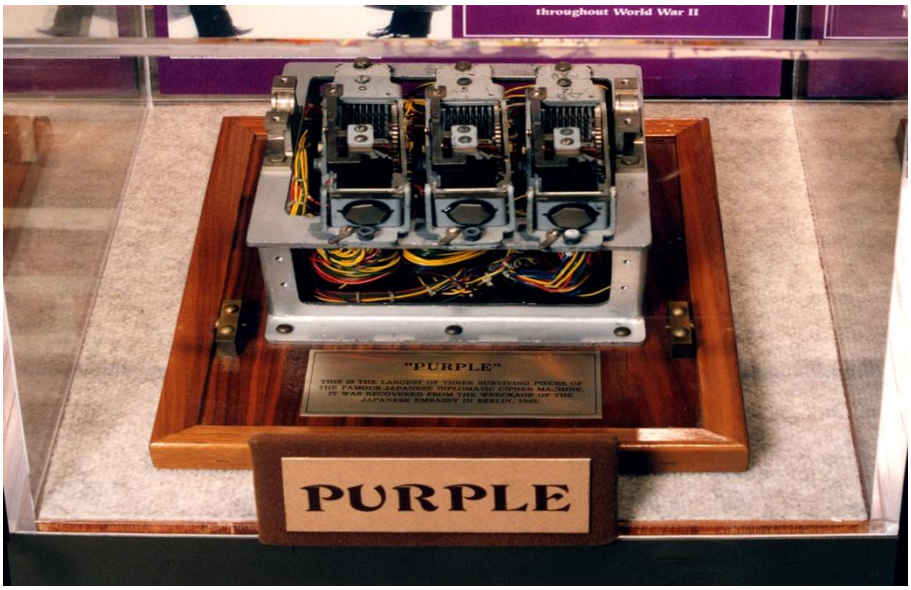

Figure 5: Purple Machine (Wonders&Marvels, 2005).

Even in the past people knew the great importance of information and data and the cryptographic system began to evolve with the advancement of technology. The mathematical function which is used for encryption and decryption is also known as a cryptographic algorithm and this function depends on a key value that is compulsory for the encryption process and decryption process. The two cryptographic algorithms used to encrypt and decrypt the information are Symmetric and Asymmetric encryption.

i. Symmetric Encryption

Symmetric encryption is a type of encryption that converts plaintext into ciphertext using the same cryptographic key for sender and receiver, symmetric encryption uses only one key for encryption and decryption (M.Shallal, 2016). In this encryption system, the sender and receiver must know the key which is used to encrypt and decrypt the information, the examples of symmetric encryption are: AES, DES, Blowfish, RC4, RC5, and RC6 (Chhetri, 2019).

The symmetric encryption algorithm is a lot faster than an asymmetric algorithm but the main disadvantage of symmetric encryption is that senders and receivers have access to the private key that is vulnerable and can be misused by other users (M. B. Yassein, 2017). The figure shown below is the symmetric encryption method.

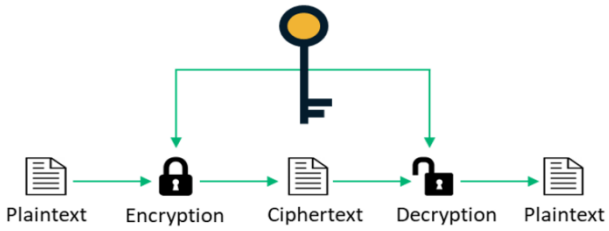

Figure 6: Symmetric Encryption (Sectigo, 2020).

ii. Asymmetric Encryption

Asymmetric encryption is an encryption method where the user intends to send information using a key, which is public to the receiver for encryption and the receiver, apply its private key to decrypt the message sent to them and it is very hard to break or reveal the secret key as the reason is its complexity in creating an algorithm (Chhetri, 2019). Asymmetric encryption is often used in communication channels, especially over the internet and some of its examples are RSA, ECC, ElGamal, and DSA (T.P.Innokentievich, 2017). The figure shown below is the asymmetric encryption method.

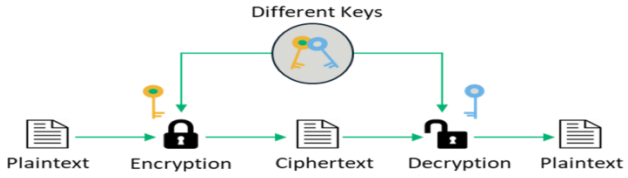

Figure 7: Asymmetric Encryption (Sectigo, 2020).

The main aim of this coursework is to conduct research, develop and test the new cryptographic system and its objectives are to research the cryptographic system and its history, develop a new cryptographic system, testing it and make a report about this.

Background

The new algorithm is developed by combining and modifying three different cryptographic algorithms which are Row Transposition Cipher, Playfair Cipher and Caesar Cipher.

Row Transposition Cipher

The row transposition cipher is a type of algorithm that uses an additional complicated theme by inputting the plaintext in a rectangle, row by row, and browse off the message column by column and the order of columns are permuted, later that will be the key to this cryptographic system. The example is shown below.

Plaintext: WE ARE GOING FOR PICNIC

Key: 4312567

Key	4	3	1	2	5	6	7
Plain Text	W	E	A	R	E	G	O
	I	N	G	F	O	R	P
	I	C	N	I	C	X	Y

Table 1: Row Transposition Cipher (Background)

Cipher text: AGN RFI ENC WII EOC GRX OPY

By rearranging the ciphertext in the above table as the order of columns, we can get the plain text.

Plaintext: WE ARE GOING FOR PICNIC.

The advantage of this cipher is that it is fast and maintains confidentiality and integrity and the disadvantage is that it is error-prone and can be assumed.

Playfair Cipher

The Playfair cipher is a manual symmetric encryption technique that was invented in 1854 by Charles Wheatstone which uses a block size of 2 to encrypt the data and based on the use of a 5 x 5 matrix of letters constructed using a key (Planetcalc, 2019). There are certain rules for this algorithm, which are:

i. If letter in plaintext are repeated in the same pair then it is separated with a filler letter such as “X”. For example: SALLOON would be SA LX LO ON.
ii. Plaintext letters that are in the same row in the matrix are restored with the letters in the right.
iii. Plaintext letters that are in the same column in the matrix are restored with the letters below.
iv. Plaintext letter that is in pair is restored by the letter, which lies in their respective row and column occupied by other plaintext letter.

The example of Playfair cipher is given below.

Plaintext: DANGER Key: ALERT

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

Table 2: Playfair Cipher (Baground)

Now,

DA = BE NG = UN ER = RT

So, the Ciphertext = BEUNRT

The decryption can be done by using above matrix as:

BE = DA UN = NG RT = ER

So, the plaintext is DANGER.

The advantage of the Playfair cipher is that it is fast and uses the substitution method that is difficult to predict. The disadvantage is that it can only encrypt a limited number of characters.

Caesar Cipher

Caesar cipher is one of the simplest, well-known, and oldest kinds of substitution method that is named after Julius Caesar, which replaces the letter of the alphabet with a letter that is 3 places ahead of it (Mishra, 2013). The algorithm for this cipher is given as:

For encryption:

C = (P+3) mod 26 (C = Ciphertext, P = Plaintext)

For decryption:

P = (C-3) mod 26

The example of this cipher is given below.

Plaintext: KEYBOARD

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
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 3: Caesar Cipher (Background)

So, Ciphertext = NHBERDUG

The decryption can be done by using above table.

NHBERDUG= KEYBOARD

Its advantage is that it is very fast to operate and requires few computing resources. Its disadvantage is that its algorithm is well known and there are only limited characters to try.

Development

Modification

The new algorithm containing two keys is developed by combining and modifying three different well-known cryptographic algorithms that are Row Transposition Cipher, Playfair Cipher and Caesar Cipher. The changes made in these algorithms are explained below.

Row Transposition Cipher

This cipher is modified by adding five more special characters (@, #, $, %, &) and they are used instead of regular alphabets. These special characters will be used in the blank space instead of the regular alphabets (X, Y, and Z) and the first key will be used here. Encryption and Decryption is done by using block size of 4. The example is given below.

Plaintext = EAT THE FRUIT

Key = 312

For encryption:

KEY	3	1	2
	E	A	T
	T	H	E
	F	R	U
	I	T	@

Table 4: Row Transposition Cipher (Modification)

Ciphertext: AHRT TEU@ ETFI

For decryption:

By rearranging the ciphertext in the above table as the order of columns, we can get the plain text.

Plaintext = EAT THE FRUIT

Playfair Cipher

The ciphertext of the Row Transposition Cipher would be the plain text for this cipher. The second key will be used in this method. The regular 5X5 matrix is modified as 6X5 matrix and the placement of plaintext is changed from row by row to column by column but the other rules are not changed. Extra five special characters (@, #, $, %, &) are used and encryption and decryption is done by using block size of 2. (#) is used if the letters are repeated in a pair or there is insufficient letter in a pair. The example is given below.

Plaintext: MANGO

Key: FRUIT

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

Table 5: Playfair Cipher (Modification)

Encryption:

MA = UP NG = EO O# = %M

Ciphertext: UP EO %M

Decryption:

UP = MA

EO = NG

%M = O#

Plaintext = MANGO

Caesar Cipher

Caesar cipher uses the shift of three characters and it is modified as shift of 5 characters with the addition of 5 more special characters which are: @ (27), # (28), $(29), % (30) and & (31). For decryption we use anti shift of 5 characters. The new algorithm for this cipher is:

For encryption:

C = (P+K) mod 31

For decryption:

P = (C-K) mod 31

The example of this modification is given below:

For encryption:

Plaintext: ORANGE$

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

Table 6: Caesar Cipher (Modification)

Ciphertext: TWFSLJC

For decryption:

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

Plaintext = ORANGE$

By combining all three modifications of these ciphers a new cipher is made that is named as Mandip-crypto Cipher. The modifications of those algorithms were necessary to improve the encryption and decryption technique. It was also necessary to make it more secure, very difficult, and which cannot be easily predicted. The new methodology which has been implied is the use of special characters instead of regular alphabet letters and both the transposition technique and substitution technique are used to make this new algorithm more secure. The encryption and decryption steps are given below.

Encryption and Decryption Methods

Encryption steps for Mandip-crypto Cipher are:

i. The plaintext should be placed in Row Transposition Cipher table using first key (Key1).
ii. The output should be generated by using the table that has block size of 4 and place the character (@, #, $, %, &) if blank space is left in the table.
iii. The 6X5 matrix should be created by using second key (Key2).
iv. The output that is generated in step (ii) should be encrypted by using the above matrix with block size of 2 and place the character (#) where letter repeats.
v. The output of Step (iv) should be substitute by using shift of 5 characters in modified Caesar Cipher.
vi. The output of Step (v) is the required ciphertext.

Decryption steps for Mandip-crypto Cipher are:

i. The Ciphertext should be substitute by using anti-shift of 5 characters in modified Caesar Cipher.
ii. The 6X5 matrix should be created by using second key (Key2).
iii. The output of Step (i) should be decrypted by using the above matrix with block size of 2.
iv. The character (#) should be removed from the output of step (iii) if present and it should be combined in block size of 4.
v. The Row Transposition Cipher table is created using output of step (iv) and first key (Key1).
vi. The output of step (v) should be combined and that is the required Plaintext.

Flowchart

The flowchart of Mandip-crypto Cipher is given below.

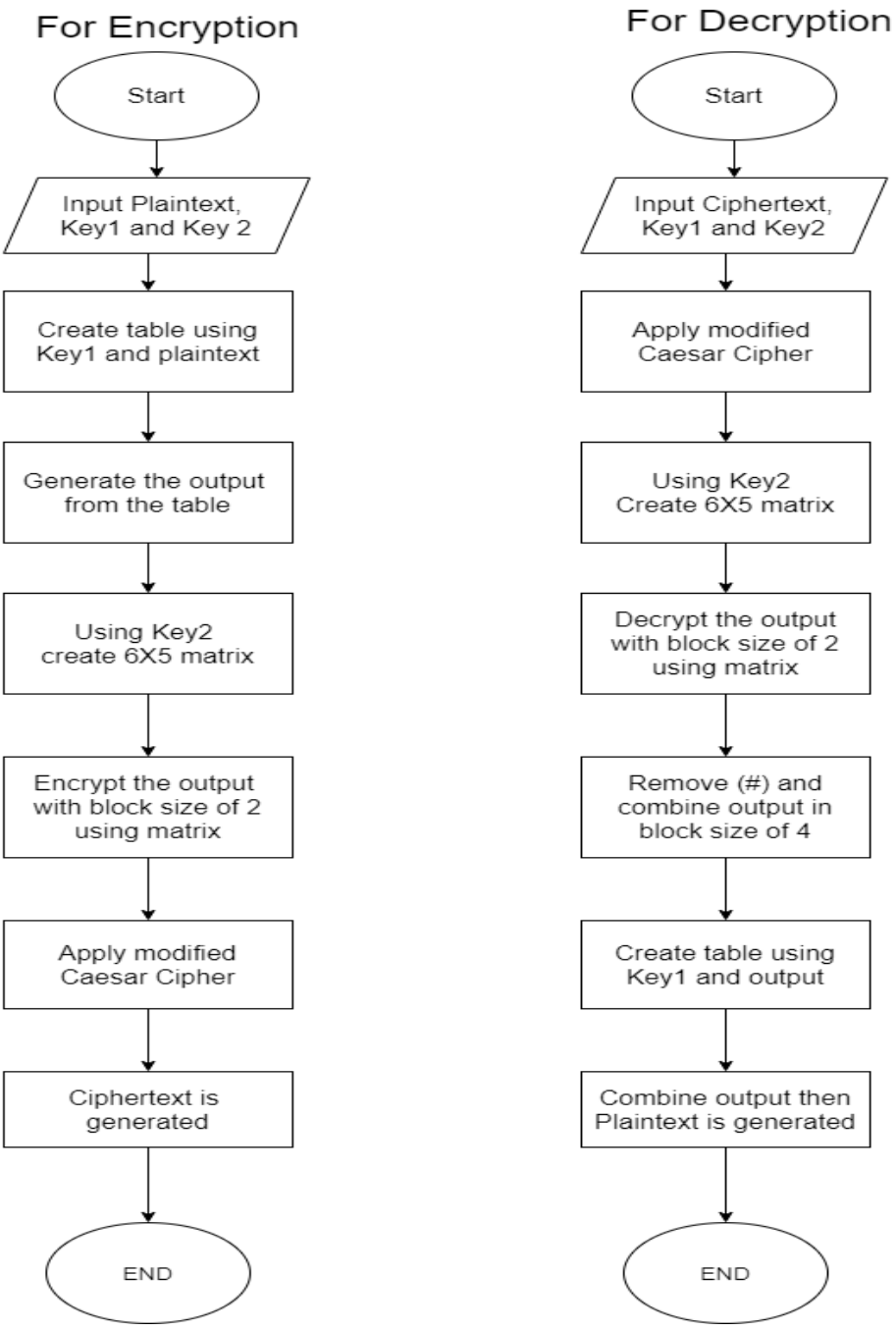

Figure 8: The flowchart of Mandip-crypto Cipher

Testing

First Example:

Plaintext = LETS MOVE TO THE FRONT

Key1 = 53124

Key2 = INFOSEC

For Encryption

The plaintext should be placed in table using first key (Key1).

Input = LETS MOVE TO THE FORNT

Key	5	3	1	2	4
	L	E	T	S	M
	O	V	E	T	O
	T	H	E	F	R
	O	N	T	@	#

Output = TEET STF@ EVHN MOR# LOTO

Create 6X5 matrix using Key2 and encrypt the above output with block size of 2.

Input = TE ET ST F@ EV HN MO R# LO TO

I	C	K	T	Z
N	A	L	U	@
F	B	M	V	#
O	D	P	W	$
S	G	Q	X	%
E	H	R	Y	&

Output = IY YI XI #N YF EA FP &M NP IW

Substitute the above output by using shift of 5 characters.

Input = IY YI XI #N YF EA FP &M NP IW

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

Output = N% %N $N BS %K JF KU ER SU N#

So, Ciphertext = N%%N$NBS%KJFKUERSUN#

For Decryption

Ciphertext = N%%N$NBS%KJFKUERSUN#

Key1 = 53124

Key2 = INFOSEC

Substitute the Ciphertext by using anti shift of 5 characters.

Input = N%%N$NBS%KJFKUERSUN#

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

Output = IYYIXI#NYFEAFP&MNPIW

Create 6X5 matrix using Key2 and decrypt the above output with block size of 2.

Input = IY YI XI #N YF EA FP &M NP IW

I	C	K	T	Z
N	A	L	U	@
F	B	M	V	#
O	D	P	W	$
S	G	Q	X	%
E	H	R	Y	&

Output = TE ET ST F@ EV HN MO R# LO TO

Decrypt the above output by using Key1 with block size of 4.

Input = TEET STF@ EVHN MOR# LOTO

Key	5	3	1	2	4
	L	E	T	S	M
	O	V	E	T	O
	T	H	E	F	R
	O	N	T	@	#

Output = LETSMOVETOTHEFRONT@#

Remove (@, #)

So, Plaintext = LETS MOVE TO THE FRONT

Second Example:

Plaintext = CLASS HAS BEEN POSTPONED

Key1 = 625143

Key2 = BENCH

For Encryption

The plaintext should be placed in table using first key (Key1).

Input = CLASS HAS BEEN POSTPONED

Key	6	2	5	1	4	3
	C	L	A	S	S	H
	A	S	B	E	E	N
	P	O	S	T	P	O
	N	E	D	@	#	$

Output = SET@ LSOE HNO$ SEP# ABSD CAPN

Create 6X5 matrix using Key2 and encrypt the above output with block size of 2.

Input = SE T@ LS OE HN O$ SE P# AB SD CA PN

B	D	M	T	Z
E	F	O	U	@
N	G	P	V	#
C	I	Q	W	$
H	K	R	X	%
A	L	S	Y	&

Output = AO ZU SY UF AC @Q AO VN BE LM BH VG

Substitute the above output by using shift of 5 characters.

Input = AO ZU SY UF AC @Q AO VN BE LM BH VG

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

Output = FT &Z X% ZK FH AV FT @S GJ QR GM @L

So, Ciphertext = FT&ZX%ZKFHAVFT@SGJQRGM@L

For Decryption

Ciphertext = FT&ZX%ZKFHAVFT@SGJQRGM@L

Key1 = 625143

Key2 = BENCH

Substitute the Ciphertext by using anti shift of 5 characters.

Input = FT&ZX%ZKFHAVFT@SGJQRGM@L

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

Output = AOZUSYUFAC@QAOVNBELMBHVG

Create 6X5 matrix using Key2 and decrypt the above output with block size of 2.

Input = AO ZU SY UF AC @Q AO VN BE LM BH VG

B	D	M	T	Z
E	F	O	U	@
N	G	P	V	#
C	I	Q	W	$
H	K	R	X	%
A	L	S	Y	&

Output = SE T@ LS OE HN O$ SE P# AB SD CA PN

Decrypt the above output by using Key1 with block size of 4.

Input = SET@ LSOE HNO$ SEP# ABSD CAPN

Key	6	2	5	1	4	3
	C	L	A	S	S	H
	A	S	B	E	E	N
	P	O	S	T	P	O
	N	E	D	@	#	$

Output: CLASSHASBEENPOSTPONED@#$

Remove (@, #, $)

So, Plaintext = CLASS HAS BEEN POSTPONED

Third Example:

Plaintext = THERE IS AMBUSH AHEAD

Key1 = 53214

Key2 = EXPLODE

For Encryption

The plaintext should be placed in table using first key (Key1).

Input = THERE IS AMBUSH AHEAD

Key	5	3	2	1	4
	T	H	E	R	E
	I	S	A	M	B
	U	S	H	A	H
	E	A	D	@	#

Output = RMA@ EAHD HSSA EBH# TIUE

Create 6X5 matrix using Key2 and encrypt the above output with block size of 2.

Input = RM A@ EA HD HS SA EB H# TI UE

E	A	I	S	Z
X	B	K	T	@
P	C	M	U	#
L	F	N	V	$
O	G	Q	W	%
D	H	R	Y	&

Output = IN ZB AI RH YA ZI AX &C KS PS

Substitute the above output by using shift of 5 characters.

Input = IN ZB AI RH YA ZI AX &C KS PS

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

Output = NS &G FN WM %F &N F$ CH PX UX

So, Ciphertext = NS&GFNWM%F&NF$CHPXUX

For Decryption

Ciphertext = NS&GFNWM%F&NF$CHPXUX

Key1 = 53214

Key2 = EXPLODE

Substitute the Ciphertext by using anti shift of 5 characters.

Input = NS&GFNWM%F&NF$CHPXUX

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

Output = INZBAIRHYAZIAX&CKSPS

Create 6X5 matrix using Key2 and decrypt the above output with block size of 2.

Input = IN ZB AI RH YA ZI AX &C KS PS

E	A	I	S	Z
X	B	K	T	@
P	C	M	U	#
L	F	N	V	$
O	G	Q	W	%
D	H	R	Y	&

Output = RM A@ EA HD HS SA EB H# TI UE

Decrypt the above output by using Key1 with block size of 4.

Input = RMA@ EAHD HSSA EBH# TIUE

Key	5	3	2	1	4
	T	H	E	R	E
	I	S	A	M	B
	U	S	H	A	H
	E	A	D	@	#

Output = THEREISAMBUSHAHEAD@#

Remove (@, #)

So, Plaintext = THERE IS AMBUSH AHEAD

Fourth Example:

Plaintext = YOUR BILL IS TEN$

Key1 = 4213

Key 2 = MONEY

For Encryption

The plaintext should be placed in table using first key (Key1).

Input = YOUR BILL IS TEN$

Key	4	2	1	3
	Y	O	U	R
	B	I	L	L
	I	S	T	E
	N	$	@	#

Output = ULT@ OIS$ RLE# YBIN

Create 6X5 matrix using Key2 and encrypt the above output with block size of 2.

Input = UL T@ OI S$ RL E# YB IN

M	B	I	S	Z
O	C	K	T	@
N	D	L	U	#
E	F	P	V	$
Y	G	Q	W	%
A	H	R	X	&

Output = #U @O KM ZV IP $N GM ML

Substitute the above output by using shift of 5 characters.

Input = #U @O KM ZV IP $N GM ML

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

Output = BZ AT PR &@ NU CS LR RQ

So, Ciphertext = BZATPR&@NUCSLRRQ

For Decryption

Ciphertext = BZATPR&@NUCSLRRQ

Key1 = 4213

Key2 = MONEY

Substitute the Ciphertext by using anti shift of 5 characters.

Input = BZATPR&@NUCSLRRQ

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

Output = #U@OKMZVIP$NGMML

Create 6X5 matrix using Key2 and decrypt the above output with block size of 2.

Input = #U @O KM ZV IP $N GM ML

M	B	I	S	Z
O	C	K	T	@
N	D	L	U	#
E	F	P	V	$
Y	G	Q	W	%
A	H	R	X	&

Output = UL T@ OI S$ RL E# YB IN

Decrypt the above output by using Key1 with block size of 4.

Input = ULT@ OIS$ RLE# YBIN

Key	4	2	1	3
	Y	O	U	R
	B	I	L	L
	I	S	T	E
	N	$	@	#

Output = YOURBILLISTEN$@#

Remove (@, #)

So, Plaintext = YOUR BILL IS TEN$

Fifth Example:

Plaintext = RATE IS TEN%

Key1 = 312

Key2 = FINE

For Encryption

The plaintext should be placed in table using first key (Key1).

Input = RATE IS TEN%

Key	3	1	2
	R	A	T
	E	I	S
	T	E	N
	%	@	#

Output = AIE@ TSN# RET%

Create 6X5 matrix using Key2 and encrypt the above output with block size of 2 and place the character (#) where letter repeats.

Input = AI E@ TS N# RE T%

F	C	M	T	Z
I	D	O	U	@
N	G	P	V	#
E	H	Q	W	$
A	K	R	X	%
B	L	S	Y	&

Output = BN $I MY GN AQ ZX

Substitute the above output by using shift of 5 characters.

Input = BN $I MY GN AQ ZX

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

Output = GS CN R% LS FV &$

So, Ciphertext = GSCNR%LSFV&$

For Decryption

Ciphertext = GSCNR%LSFV&$

Key1 = 312

Key2 = FINE

Substitute the Ciphertext by using anti shift of 5 characters.

Input = GSCNR%LSFV&$

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

Output = BN$IMYGNAQZX

Create 6X5 matrix using Key2 and decrypt the above output with block size of 2.

Input = BN $I MY GN AQ ZX

F	C	M	T	Z
I	D	O	U	@
N	G	P	V	#
E	H	Q	W	$
A	K	R	X	%
B	L	S	Y	&

Output = AI E@ TS N# RE T%

Decrypt the above output by using Key1 with block size of 4.

Input = AIE@ TSN# RET%

Key	3	1	2
	R	A	T
	E	I	S
	T	E	N
	%	@	#

Output = RATEISTEN%@#

Remove (@, #)

So, Plaintext = RATE IS TEN%

Evaluation

The newly created cryptographic algorithm is more secure and it must be critically evaluated to know about its strengths and weaknesses. In today's time, no cryptographic algorithms are totally secure. There are some strength and weakness of this new cryptographic algorithm which are as follows:

Strengths:

i. It contains transposition and substitution technique.
ii. The ciphertext length is larger than that of plaintext and contains two different types of keys that makes difficult to predict.
iii. It contains special characters (@, #, $, % and &).
iv. As it is symmetric cipher it is fast.

Weakness:

i. It contains alphabets and some special characters only.
ii. It contains minor modifications and it can be known.
iii. This cipher is not case sensitive so, it is not totally secure.
iv. Only limited special characters are used.

The application area of the new cryptographic algorithm will be for encrypting passwords and transmitting secure data or information. It can also be used in different organizations to encrypt their important data as it provides confidentiality, integrity, and availability of the data.

Conclusion

In the end, the assigned tasks were completed and for the completion of this task, research was conducted about Information security, Cryptography, and its history and background. Cryptography is the process of securing the data or information against adversarial attacks and symmetric and asymmetric cipher are the two kinds of the cryptographic algorithm. Row transposition cipher, Playfair cipher, and Caesar cipher were selected and modification was done and a new cipher was made and named as Mandip-crypto Cipher. To make sure that this new cryptographic algorithm works perfectly five tests of encryption and decryption of information are conducted. The evaluation of this new cryptographic algorithm is also conducted. The application area of the new cryptographic algorithm will be for encrypting passwords and transmitting secured information for different purposes.

References

BinanceAcademy. (2018) *History of Cryptography* [Online]. Available from: https://academy.binance.com/en/articles/history-of-cryptography [Accessed January 2021].

Burnette, M. (2020) *Three Tenets of Information Security* [Online]. Available from: https://www.lbmc.com/blog/three-tenets-of-information-security/ [Accessed January 2021].

Cassetto, O. (2019) *Information security (InfoSec): The Complete Guide* [Online]. Available from: https://www.exabeam.com/information-security/information-security/ [Accessed January 2021].

Chhetri, B. (2019) Crypto-System: A Modified Ceaser Cipher. In *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*. New Delhi, 2019. IEEE.

Cnet. (2018) *Enigma: Up close with a Nazi cipher machine* [Online]. Available from: https://www.cnet.com/news/enigma-up-close-with-a-nazi-cypher-machine-bombe-bletchley-park/ [Accessed January 2021].

Dooley, J.F. (2018) *History of Cryptography and Cryptanalysis*. 1st ed. Springer.

ForcePoint. (2019) *The CIA triad* [Online]. Available from: https://www.forcepoint.com/cyber-edu/cia-triad [Accessed January 2021].

M. B. Yassein, S.A.E.Q.W.M.a.Y.K. (2017) Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *2017 International Conference on Engineering and Technology*. Antalya, 2017. IEEE.

M.Shallal, Q. (2016) A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal of Computer Applications*, 147, p.43.

Michael E.Whitman, H.J.M. (2018) *Principles of Information Security*. 6th ed. Course Technology.

Michael Goodrich, R.T. (2014) *Introduction to Computer Security*. 1st ed. Pearson Education Limited.

MichiganTech. (2018) *The Vigenère Cipher Encryption and Decryption* [Online]. Available from: https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html [Accessed January 2021].

Mishra, A. (2013) ENHANCING SECURITY OF CAESAR CIPHER USING DIFFERENT. *International Journal of Research in Engineering and Technology*, 2, pp.327-32.

Planetcalc. (2019) *Playfair cipher* [Online]. Available from: https://planetcalc.com/7751/ [Accessed January 2021].

Rohwer, J. (1999) Signal intelligence and World War II: The unfolding story. *The Journal of Military History*, 63(4), pp.939-51.

Sectigo. (2020) *Infosec insights* [Online]. Available from: https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/ [Accessed January 2021].

SemanticScholar. (2017) *Trends of cryptography stepping from ancient to modern* [Online]. Available from: https://www.semanticscholar.org/paper/Trends-of-cryptography-stepping-from-ancient-to-Rathidevi-Yaminipriya/17481af3e1fd60287dcf9e921af44febc61c6b52 [Accessed January 2021].

T.P.Innokentievich, M.V.V. (2017) The Evaluation of the cryptographic strength of asymmetric encryption algorithms. In *2017 Second Russia and Pacific Conference on Computer Technology and Applications*. Vladivostok, 2017. IEEE.

Umang Bhargava, A.S. (2017) A new algorithm combining substitution & transposition cipher techniques for secure communication. In *2017 International Conference on Trends in Electronics and Informatics (ICEI)*., 2017. IEEE.

Wonders&Marvels. (2005) *Secrets Abroad: A History of the Japanese Purple Machine* [Online]. Available from: https://www.wondersandmarvels.com/2013/02/secrets-abroad-a-history-of-the-japanese-purple-machine.html [Accessed January 2021].

Appendix

CIA Triad:

Confidentiality:

Confidentiality ensures that sensitive information is accessed only by an authorized or known person and kept away from those who are not authorized to possess them. Unique frameworks protect the confidentiality and safeguard data from malicious intruders.

Integrity:

Integrity ensures that information is in a format that is true and correct to its original purposes. The receiver of the information must have the information the creator intended him to have. The information can be edited by authorized persons only and remains in its original state when at rest.

Availability:

Availability ensures that information and resources are available to those who need them. It is implemented using methods such as hardware maintenance, software patching, and network optimization. Processes such as redundancy, failover, RAID, and high-availability clusters are used to mitigate serious consequences when hardware issues do occur.

Cryptographic System in real time scenario:

In today's time, many attacks are done to retrieve the information or secret data of many organizations and users. To reduce these types of attacks and secure our data and information cryptographic system plays a vital role. The cryptographic system maintains the CIA triad for the data and information. There are various kinds of uses of cryptographic systems.

They are used in ATMs of the banks for the secure service. In ATMs, our pin code is taken by the machine and it is highly encrypted which makes secure transactions. In social media also the cryptographic system is used for the encryption of the passwords and messages sent by the users. It is also used in mobile networks to E-mail services. In today's time, our digital assets and information are very important, and cryptographic system plays a vital role to protect it.