Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Faculty of Sciences and Engineering
Semester: (Spring, Year:2023), B.Sc. in CSE (Day)

K/S/A Test - 01
Cipher Implementation

Course title: Computer and Cyber Security
Course Code: CSE 323 **Section:** 202 D2

Students Details

Name	ID
Md.Rajin Saleh	202002069

Submission Date : 15-05-2023
Course Teacher's Name: Mr. Palash Roy

[For teachers use only: Don't write anything inside this box]

Lab Project Status	
Marks:	**Signature:**
Comments:	**Date:**

Contents

Chapter 1

Introduction

1.1 Introduction

In this project, we implemented and compared classical cipher techniques for securing communication. Classical ciphers are encryption methods that have been used historically to encode messages. We focused on two main categories of classical ciphers: substitution ciphers and transposition ciphers. Within each category, we implemented specific techniques to understand how each method works and compare their ability to provide security.

1. Substitution Ciphers: Substitution ciphers are encryption methods that replace plaintext letters with corresponding ciphertext letters. The four substitution ciphers we implemented are Additive Cipher, Multiplicative Cipher, Affine Cipher, and Autokey Cipher. Each of these techniques uses a different mathematical operation to encrypt the plaintext.
    - Additive Cipher: uses modular addition to encrypt plaintext.
    - Multiplicative Cipher: uses modular multiplication to encrypt plaintext.
    - Affine Cipher: combines both Additive and Multiplicative Cipher techniques.
    - Autokey Cipher: uses the plaintext itself as the encryption key.
2. Transposition Ciphers: Transposition ciphers are encryption methods that rearrange the order of plaintext letters to create a new ciphertext. The two transposition ciphers we implemented are Rail Fence and Row Transposition Cipher. Each of these techniques rearranges the plaintext letters in a different way.
    - Rail Fence Cipher: rearranges the plaintext letters diagonally across a grid.
    - Row Transposition Cipher: rearranges the plaintext letters in a specific order.

The purpose of this project was to gain practical experience in implementing classical cipher techniques and understand their effectiveness in providing security for communication. Through this project, we aimed to understand the encryption process of each technique, their strengths and limitations, and how they compare to each other.

1.2 Design Goals/Objectives

In this project, objectives are about -

- To gain practical experience in implementing classical cipher techniques and compare their security capabilities.
- to explore the encryption and decryption process of each technique, their strengths and weaknesses, and how they compared to each other.
- To understand the importance of key management in ensuring secure communication.
- To improve coding and problem-solving skills using web programming languages..

Chapter 2

Design/Development/Implementation of the Project

2.1 Solution Methodology

The overall methodology of the project involves implementing classical cipher techniques to secure communication. The project is divided into two main sections: Substitution Cipher and Transposition Cipher.

- The Substitution Cipher section includes the following classical cipher techniques: Additive Cipher, Multiplicative Cipher, Affine Cipher, Autokey Cipher, and Vigenere Cipher. Users can enter plaintext and a key value or key values to encrypt the plaintext using one of these techniques. The encrypted ciphertext and the decrypted plaintext can also be viewed on the web page.
- The Transposition Cipher section includes the following classical cipher techniques: Rail Fence Cipher and Row Transposition Cipher. Users can enter plaintext, the number of rails, and a key value to encrypt the plaintext using one of these techniques. The encrypted ciphertext and the decrypted plaintext can also be viewed on the web page.

The web application is built using HTML, CSS, and JavaScript. The HTML and CSS are used to create the user interface, while JavaScript is used to handle the logic of encrypting and decrypting the plaintext. The project has three web pages: Home page, Substitution Cipher page, Transposition Cipher page. The Home page displays the title of the project and a link to the Substitution Cipher page. The Substitution Cipher page displays the various classical cipher techniques available for substitution cipher encryption, as well as input fields for the plaintext and key value or key values. The Transposition Cipher page displays the various classical cipher techniques available for transposition cipher encryption, as well as input fields for the plaintext, number of rails, and key value. Overall, the project aims to demonstrate the implementation and comparison of classical cipher techniques for securing communication.

2.2 Algorithmic Description

Here's an algorithmic description of the solution methodology for the classical cipher techniques implemented in the project:

1. Substitution Cipher:
    - Additive Cipher:
        (a) Take plaintext input and a key value.
        (b) Convert the plaintext to all uppercase letters.
        (c) For each character in the plaintext, add the key value to its ASCII code and take the modulus with 26 to obtain the corresponding ciphertext character.
        (d) Append each ciphertext character to a new string.
        (e) Return the ciphertext.
    - Multiplicative Cipher:
        (a) Take plaintext input and a key value.
        (b) Convert the plaintext to all uppercase letters.
        (c) For each character in the plaintext, add the key value to its ASCII code and take the modulus with 26 to obtain the corresponding ciphertext character.
        (d) Append each ciphertext character to a new string.
        (e) Return the ciphertext.
    - Affine Cipher:
        (a) Take plaintext input and two key values: a and b.
        (b) Convert the plaintext to all uppercase letters.
        (c) For each character in the plaintext, apply the following formula: (a * (ASCII code of character) + b) mod 26.
        (d) Obtain the corresponding ciphertext character from the result of step c.
        (e) Append each ciphertext character to a new string.
        (f) Return the ciphertext.
    - Vigenere Cipher:
        (a) Take the plaintext input and a keyword.
        (b) Convert both the plaintext and keyword to uppercase letters.
        (c) Repeat the keyword to match the length of the plaintext.
        (d) For each letter in the plaintext and its corresponding letter in the keyword:
            – Assign numerical values to the letters (A=0, B=1, C=2, and so on).
            – Add the numerical values of the plaintext and keyword letters together.
            – Take the modulus of the sum with 26 to get the ciphertext letter's numerical value.
            – Convert the numerical value back to a letter.

(e) Append each ciphertext character to a new string.
(f) Concatenate the ciphertext letters to obtain the final encrypted message.

2. Transposition Cipher:

- Rail Fence Cipher::
  (a) Take plaintext input and the number of rails for the fence.
  (b) Create a matrix with dimensions of the number of rails and the length of the plaintext.
  (c) Place the plaintext characters diagonally on the matrix following the rail pattern.
  (d) Read the ciphertext by appending the characters row by row.
  (e) Return the ciphertext.
- Row Transposition Cipher::
  (a) Take plaintext input and a key value.
  (b) Convert the plaintext to all uppercase letters.
  (c) Create a matrix with dimensions of the key value and the length of the plaintext.
  (d) Place the plaintext characters column-wise in the matrix, filling each column from top to bottom.
  (e) Sort the columns of the matrix according to the key value.
  (f) Read the ciphertext by appending the characters row by row.
  (g) Return the ciphertext.

To decrypt the ciphertext, the same steps are followed, but instead of adding the numerical values, you subtract them. The resulting numerical values are then converted back to letters to obtain the original plaintext.

Chapter 3

Performance Evaluation

3.1 Results Analysis/Testing

The Result's Figure is given in below -

Figure 3.1: After run the program, the home page will be open and button will connected with next page which is substitution cipher section.

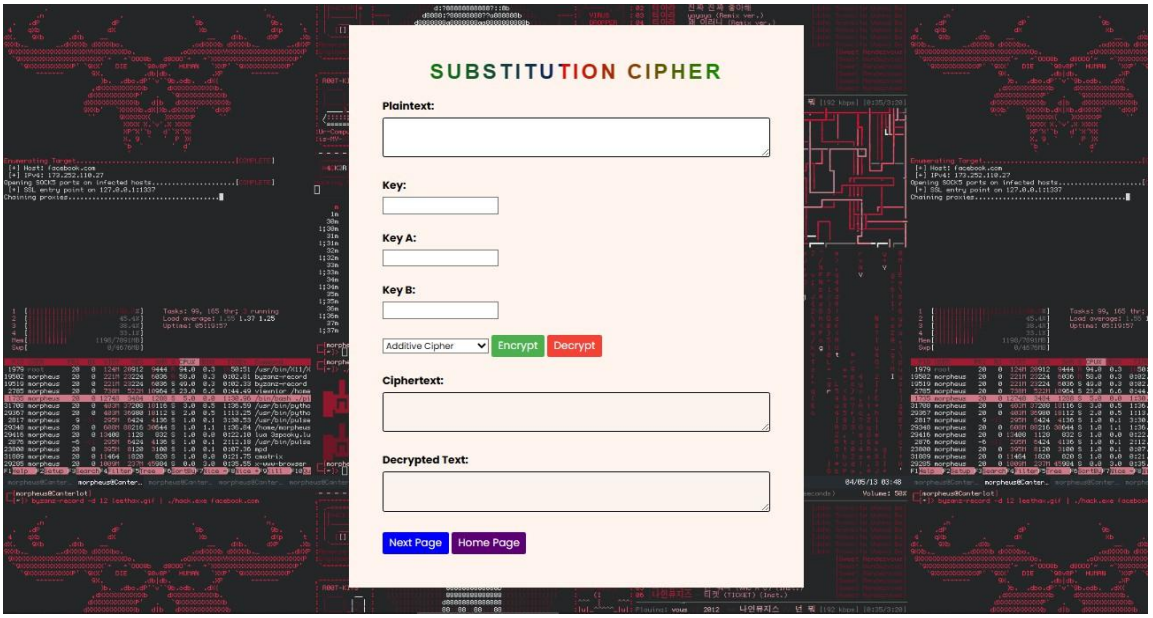

Figure 3.2: The picture of substitution cipher page where it contains plaintext box,algorithm select box where four algorithms- additve,multiplicative,affine and vigenere cipher, key and display and buttons for encryption and decryption and a button for move to the next page.

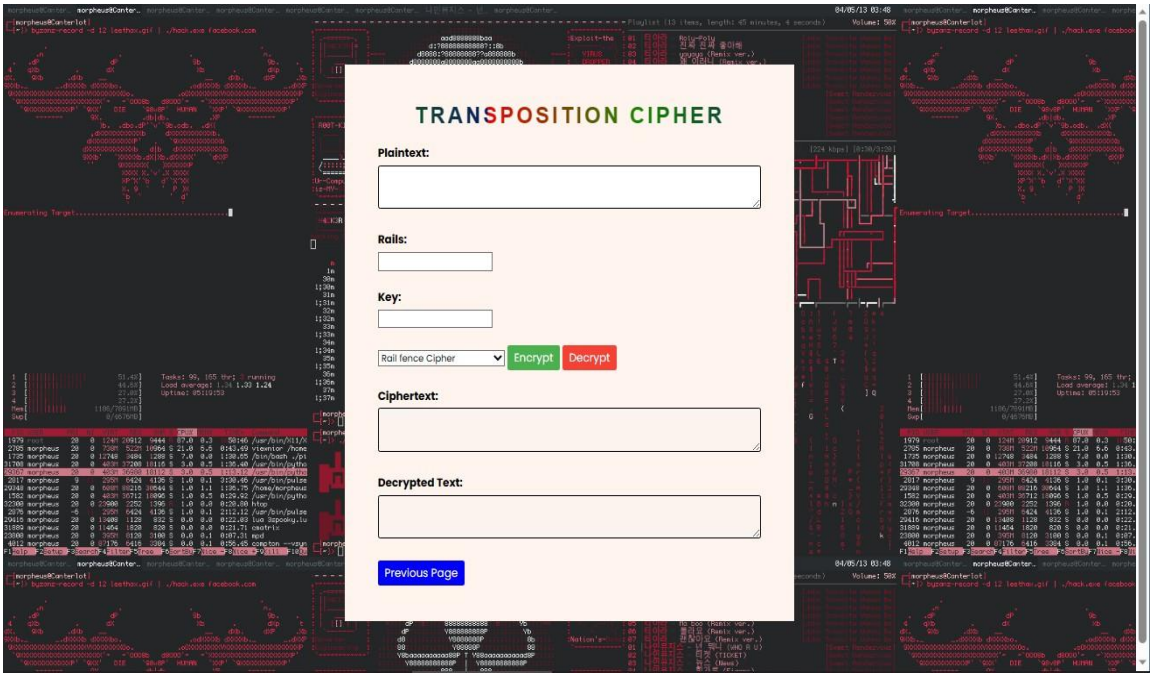

Figure 3.3: The picture of Transposition cipher page where it contains plain-text box,algorithm select box where four algorithms- rail fence and row transposition cipher, key and display and buttons for encryption and decryption and a button for move on previous page.

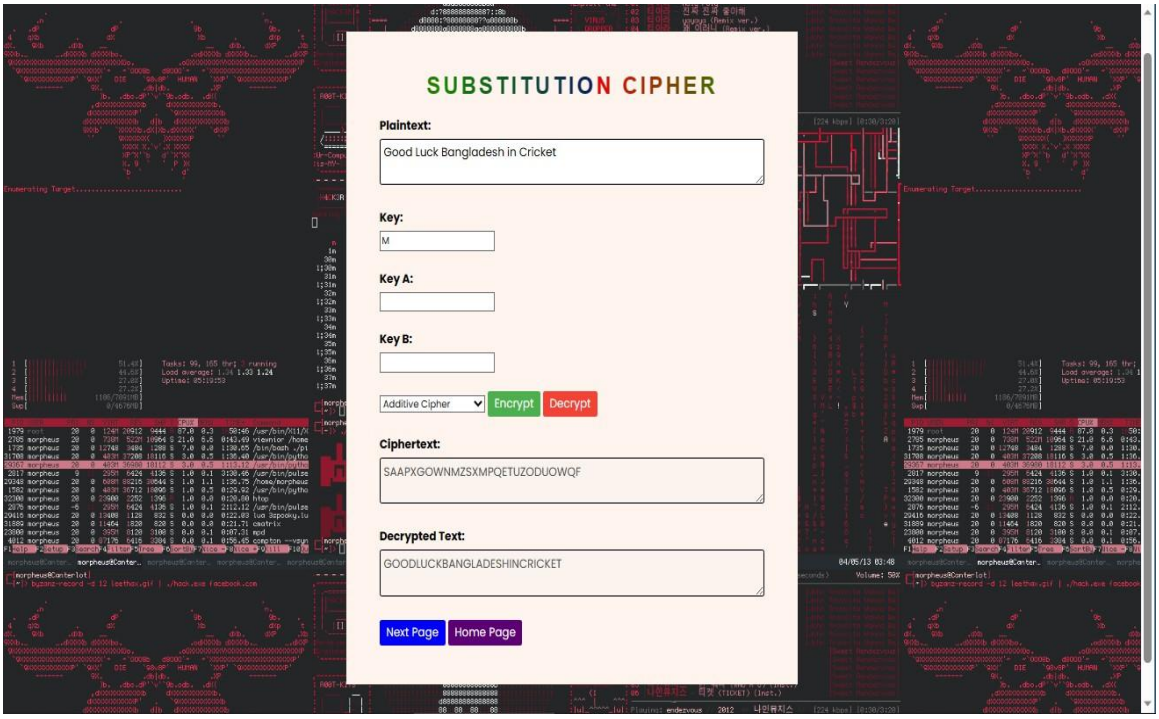

Figure 3.4: The picture of Encryption and Decryption of Addtive cipher which is shown in encyption and decryption display.

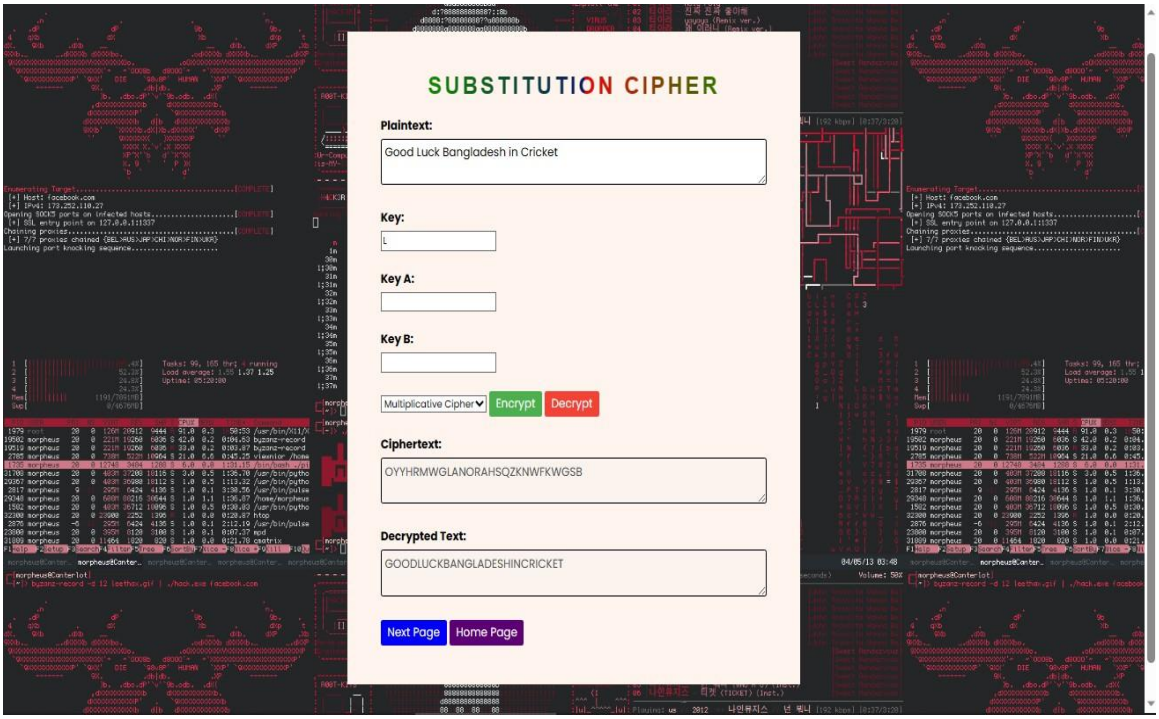

Figure 3.5: The picture of Encryption and Decryption of Multiplicative cipher which is shown in encryption and decryption display.

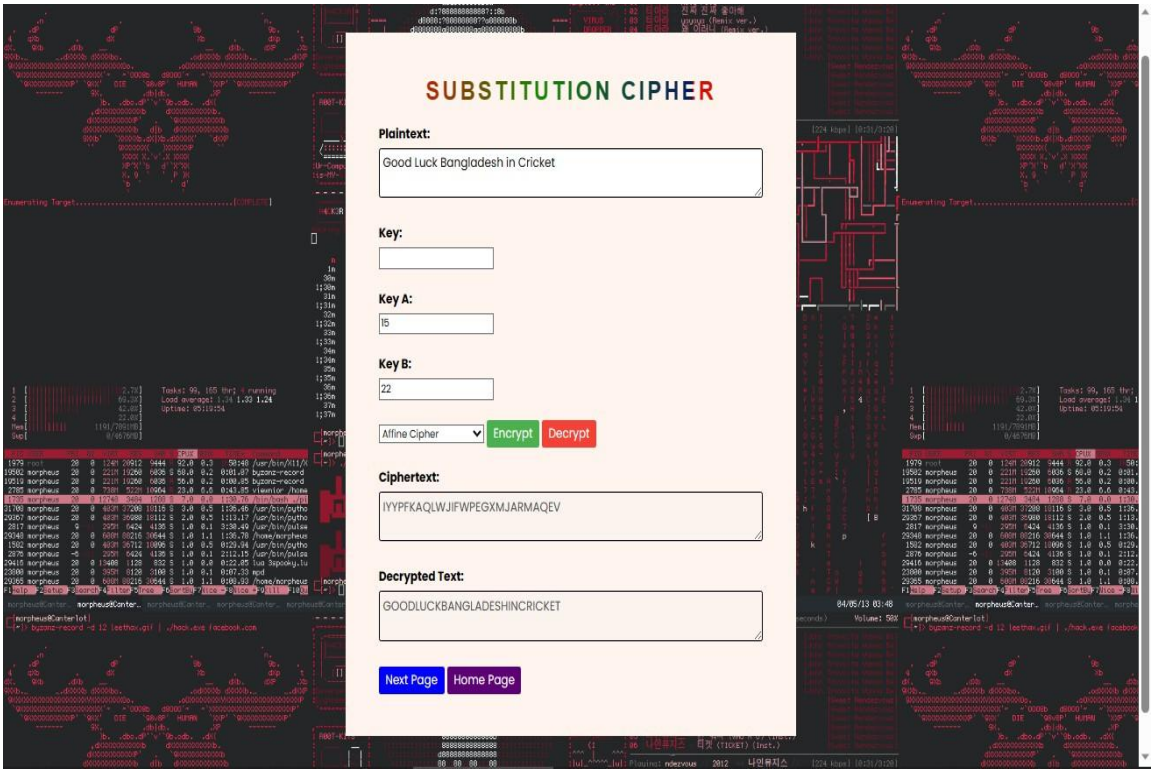

Figure 3.6: The picture of Encryption and Decryption of Affine cipher which is shown in encryption and decryption display.

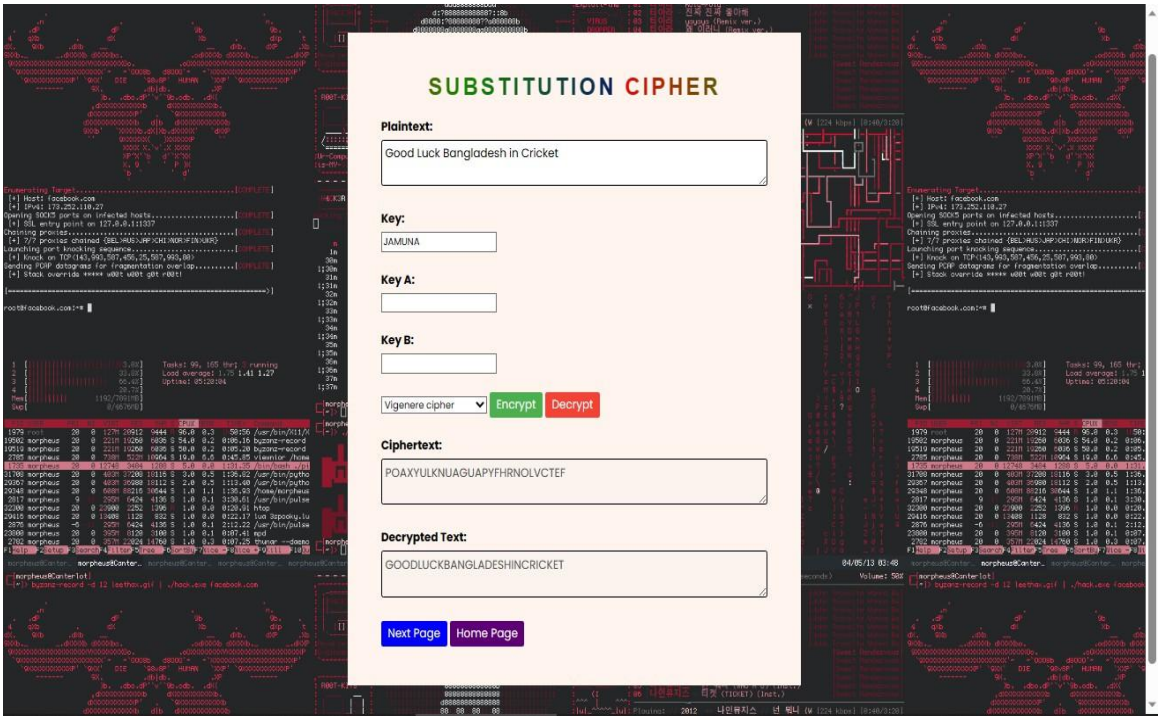

Figure 3.7: The picture of Encryption and Decryption of Vigenere cipher which is shown in encryption and decryption display.

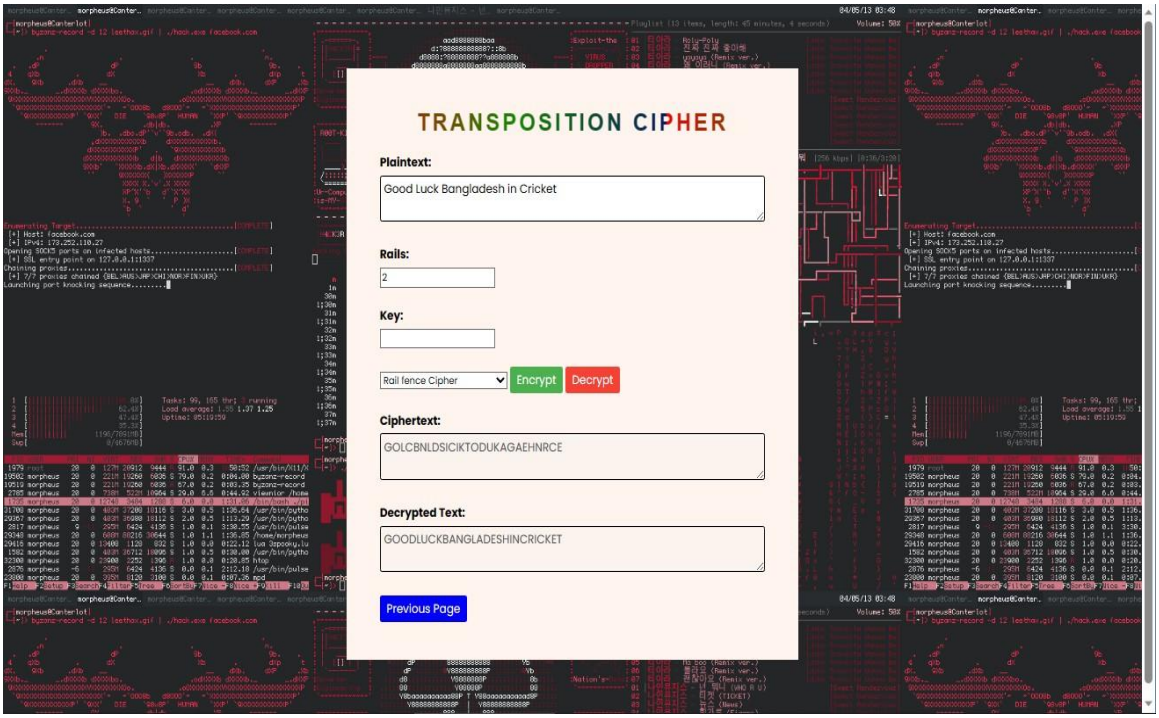

Figure 3.8: The picture of Encryption and Decryption of Rail fence cipher which is shown in encryption and decryption display.

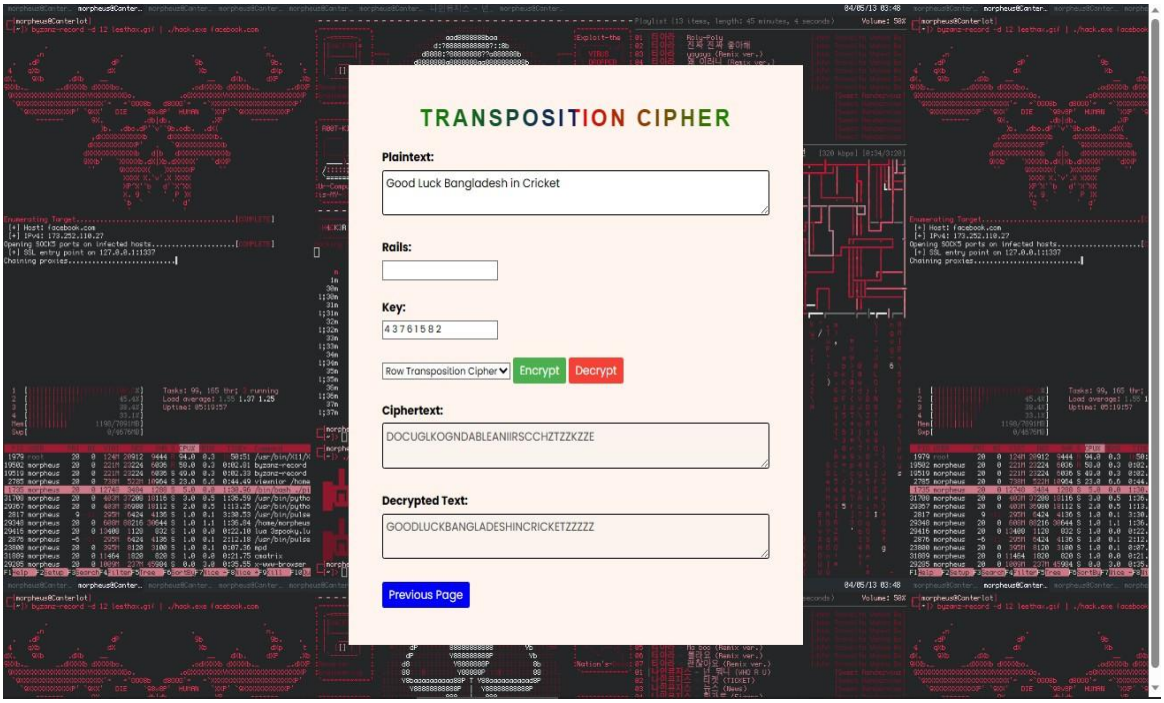

Figure 3.9: The picture of Encryption and Decryption of Row Transposition cipher which is shown in encryption and decryption display.

3.2 Solution Examples:

Example of the Additive Cipher encryption and decryption solution:

Given that,

Plaintext (P) = Good Luck Bangladesh in Cricket

Key (K) = M ⟶ 12

Now, Encryption: C = (P + K) mod 26

Plaintext	Encryption	Ciphertext
G → 06	(6+12) mod 26	18 → S
o → 14	(14+12) mod 26	00 → A
o → 14	(14+12) mod 26	00 → A
d → 03	(03+12) mod 26	15 → P
L → 11	(11+12) mod 26	23 → X
u → 20	(20+12) mod 26	06 → G
c → 02	(02+12) mod 26	14 → O
k → 10	(10+12) mod 26	22 →W
B → 01	(01+12) mod 26	13 → N
a → 00	(00+12) mod 26	12 → M
n → 13	(13+12) mod 26	25 → Z
g → 06	(06+12) mod 26	18 → S
l → 11	(11+12) mod 26	23 → X
a → 00	(00+12) mod 26	12 → M
d → 03	(03+12) mod 26	15 → P
e → 04	(04+12) mod 26	16 → Q
s → 18	(18+12) mod 26	04 → E
h → 07	(07+12) mod 26	19 → T
i → 08	(08+12) mod 26	20 → U
n → 13	(13+12) mod 26	25 → Z
C → 02	(02+12) mod 26	14 → O
r → 17	(17+12) mod 26	03 → D
i → 08	(08+12) mod 26	20 → U
c → 02	(02+12) mod 26	14 → O
k → 10	(10+12) mod 26	22 → W
e → 04	(04+12) mod 26	16 → Q
t → 19	(19+12) mod 26	05 → F

After Encryption the Plaintext: Good Luck Bangladesh in Cricket

The Ciphertext is: SAAPXGOWNMZSXMPQETUZODUOWQF.

Figure 3.10: Additive Cipher Encryption

Now, Decryption: P = (C - K) mod 26

Ciphertext	decryption	Plaintext
S → 18	(18-12) mod 26	06 → G
A → 00	(00-12) mod 26 (-12+26) =14	14 → O
A → 00	(00-12) mod 26	14 → O
P → 15	(15-12) mod 26	03 → D
X → 23	(23-12) mod 26	11 → L
G → 06	(06-12) mod 26 (-06+26) =20	20 → U
O → 14	(14-12) mod 26	02 → C
W → 22	(22-12) mod 26	10 →K
N → 13	(13-12) mod 26	01 → B
M → 12	(12-12) mod 26	00 → A
Z → 25	(25-12) mod 26	13 → N
S → 18	(18-12) mod 26	06 → G
X → 23	(23-12) mod 26	11 → L
M → 12	(12-12) mod 26	00 → A
P → 15	(15-12) mod 26	03 → D
Q → 16	(16-12) mod 26	04 → E
E → 04	(04-12) mod 26 (-08+26) =18	18 → S
T → 19	(19-12) mod 26	07 → H
U → 20	(20-12) mod 26	08 → I
Z → 25	(25-12) mod 26	13 → N
O → 14	(14-12) mod 26	02 → C
D → 03	(03-12) mod 26 (-09+26) =17	17 → R
U → 20	(20-12) mod 26	08 → I
O → 14	(14-12) mod 26	02 → C
W → 22	(22-12) mod 26	10 → K
Q → 16	(16-12) mod 26	04 → E
F → 05	(05-12) mod 26 (-07+26) =19	19 → T

After decryption the ciphertext: SAAPXGOWNMZSXMPQETUZODUOWQF.

The plaintext is: GOODLUCKBANGLADESHINCRICKET

Figure 3.11: Additive Cipher Decryption

Example of the Multiplicative Cipher encryption and decryption solution:

Plaintext (P) = Good Luck Bangladesh in Cricket

Key (K) = L ⟶ 11

Now, Encryption: C = (P.K) mod 26

Plaintext	Encryption	Ciphertext
G → 06	(6.11) mod 26 (66 mod 26) = 14	14 → O
o → 14	(14.11) mod 26	24 → Y
o → 14	(14.11) mod 26	24 → Y
d → 03	(03.11) mod 26	07 → H
L → 11	(11.11) mod 26	17 → R
u → 20	(20.11) mod 26	12 → M
c → 02	(02.11) mod 26	22 → W
k → 10	(10.11) mod 26	06 → G
B → 01	(01.11) mod 26	11 → L
a → 00	(00.11) mod 26	00 → A
n → 13	(13.11) mod 26	13 → N
g → 06	(06.11) mod 26	14 → O
l → 11	(11.11) mod 26	17 → R
a → 00	(00.11) mod 26	00 → A
d → 03	(03.11) mod 26	07 → H
e → 04	(04.11) mod 26	18 → S
s → 18	(18.11) mod 26	16 → Q
h → 07	(07.11) mod 26	25 → Z
i → 08	(08.11) mod 26	10 → K
n → 13	(13.11) mod 26	13 → N
C → 02	(02.11) mod 26	22 → W
r → 17	(17.11) mod 26	05 → F
i → 08	(08.11) mod 26	10 → K
c → 02	(02.11) mod 26	22 → W
k → 10	(10.11) mod 26	06 → G
e → 04	(04.11) mod 26	18 → S
t → 19	(19.11) mod 26	01 → B

After Encryption the Plaintext: Good Luck Bangladesh in Cricket.

The Ciphertext is: OYYHRMWGLANORAHSQZKNWFKWGSB.

Figure 3.12: Multiplicative Cipher Encryption

Now, Decryption: $P = (C.k^{-1}) \bmod 26$

Ciphertext	decryption	Plaintext
O → 14	$(14.11^{-1}) \bmod 26$	06 → G
Y → 24	$(24.11^{-1}) \bmod 26$	14 → O
Y → 24	$(24.11^{-1}) \bmod 26$	14 → O
H → 07	$(07.11^{-1}) \bmod 26$	03 → D
R → 17	$(17.11^{-1}) \bmod 26$	11 → L
M → 12	$(12.11^{-1}) \bmod 26$	20 → U
W → 22	$(22.11^{-1}) \bmod 26$	02 → C
G → 06	$(06.11^{-1}) \bmod 26$	10 →K
L → 11	$(11.11^{-1}) \bmod 26$	01 → B
A → 00	$(00.11^{-1}) \bmod 26$	00 → A
N → 13	$(13.11^{-1}) \bmod 26$	13 → N
O → 14	$(14.11^{-1}) \bmod 26$	06 → G
R → 17	$(17.11^{-1}) \bmod 26$	11 → L
A → 00	$(00.11^{-1}) \bmod 26$	00 → A
H → 07	$(07.11^{-1}) \bmod 26$	03 → D
S → 18	$(18.11^{-1}) \bmod 26$	04 → E
Q → 16	$(16.11^{-1}) \bmod 26$	18 → S
Z → 25	$(25.11^{-1}) \bmod 26$	07 → H
K → 10	$(10.11^{-1}) \bmod 26$	08 → I
N → 13	$(13.11^{-1}) \bmod 26$	13 → N
W → 22	$(22.11^{-1}) \bmod 26$	02 → C
F → 05	$(05.11^{-1}) \bmod 26$	17 → R
K → 10	$(10.11^{-1}) \bmod 26$	08 → I
W → 22	$(22.11^{-1}) \bmod 26$	02 → C
G → 06	$(06.11^{-1}) \bmod 26$	10 → K
S → 18	$(18.11^{-1}) \bmod 26$	04 → E
B → 01	$(01.11^{-1}) \bmod 26$	19 → T

- Calculation for decryption, $P = (C.k^{-1}) \bmod 26$

  For First character O,

  $P = (C.k^{-1}) \bmod 26$

  $= (14.11^{-1}) \bmod 26$

  $= (14.19) \bmod 26 = 266 \bmod 26 = 6$

For 11^{-1} equivalent value -

$11^{-1} \bmod 26$

q	r1	r2	r	t1	t2	t = t1 - q * t2
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	**0**		**-7**	26	

So, 11^{-1} equivalent value: -7 + 26 = 19

After decryption the ciphertext: OYYHRMWGLANORAHSQZKNWFKWGSB.

The plaintext is: GOODLUCKBANGLADESHINCRICKET.

Figure 3.13: Multiplicative Cipher decryption

Example of the Affine Cipher encryption and decryption solution:

Plaintext (P) = Good Luck Bangladesh in Cricket

K_1 = "P" → 15

K_2 = "W" → 22

Now, Encryption: $C = (P*K_1) + K_2 \bmod 26$

Plaintext	**Encryption**	**Ciphertext**
G → 06	(6*15) +22 mod 26 (90+22) mod 26 112 mod 26 = 08	08 → I
o → 14	(14*15) +22 mod 26	24 → Y
o → 14	(14*15) +22 mod 26	24 → Y
d → 03	(03*15) +22 mod 26	15 → P
L → 11	(11*15) +22 mod 26	05 → F
u → 20	(20*15) +22 mod 26	10 → K
c → 02	(02*15) +22 mod 26	00 → A
k → 10	(10*15) +22 mod 26	16 → Q
B → 01	(01*15) +22 mod 26	11 → L
a → 00	(00*15) +22 mod 26	22 → W
n → 13	(13*15) +22 mod 26	09 → J
g → 06	(06*15) +22 mod 26	08 → I
l → 11	(11*15) +22 mod 26	05 → F
a → 00	(00*15) +22 mod 26	22 → W
d → 03	(03*15) +22 mod 26	15 → P
e → 04	(04*15) +22 mod 26	04 → E
s → 18	(18*15) +22 mod 26	06 → G
h → 07	(07*15) +22 mod 26	23 → X
i → 08	(08*15) +22 mod 26	12 → M
n → 13	(13*15) +22 mod 26	09 → J
C → 02	(02*15) +22 mod 26	00 → A
r → 17	(17*15) +22 mod 26	17 → R
i → 08	(08*15) +22 mod 26	12 → M
c → 02	(02*15) +22 mod 26	00 → A
k → 10	(10*15) +22 mod 26	16 → Q
e → 04	(04*15) +22 mod 26	04 → E
t → 19	(19*15) +22 mod 26	21 → V

After Encryption the Plaintext: Good Luck Bangladesh in Cricket.

The Ciphertext is: IYYPFKAQLWJIFWPEGXMJARMAQEV

Figure 3.14: Affine Cipher Encryption

Now, Decryption: $P = (C-K_2) * K_1^{-1} \bmod 26$

Ciphertext	decryption	Plaintext
I → 08	(08-22) * 15^{-1} mod 26	06 → G
Y → 24	(24-22) * 15^{-1} mod 26	14 → O
Y → 24	(24-22) * 15^{-1} mod 26	14 → O
P → 15	(15-22) * 15^{-1} mod 26	03 → D
F → 05	(05-22) * 15^{-1} mod 26	11 → L
K → 10	(10-22) * 15^{-1} mod 26	20 → U
A → 00	(00-22) * 15^{-1} mod 26	02 → C
Q → 16	(16-22) * 15^{-1} mod 26	10 →K
L → 11	(11-22) * 15^{-1} mod 26	01 → B
W → 22	(22-22) * 15^{-1} mod 26	00 → A
J → 09	(09-22) * 15^{-1} mod 26	13 → N
I → 08	(08-22) * 15^{-1} mod 26	06 → G
F → 05	(05-22) * 15^{-1} mod 26	11 → L
W → 22	(22-22) * 15^{-1} mod 26	00 → A
P → 15	(15-22) * 15^{-1} mod 26	03 → D
E → 04	(04-22) * 15^{-1} mod 26	04 → E
G → 06	(06-22) * 15^{-1} mod 26	18 → S
X → 23	(23-22) * 15^{-1} mod 26	07 → H
M → 12	(12-22) * 15^{-1} mod 26	08 → I
J → 09	(09-22) * 15^{-1} mod 26	13 → N
A → 00	(00-22) * 15^{-1} mod 26	02 → C
R → 17	(17-22) * 15^{-1} mod 26	17 → R
M → 12	(12-22) * 15^{-1} mod 26	08 → I
A → 00	(00-22) * 15^{-1} mod 26	02 → C
Q → 16	(16-22) * 15^{-1} mod 26	10 → K
E → 04	(04-22) * 15^{-1} mod 26	04 → E
V → 21	(21-22) * 15^{-1} mod 26	19 → T

Calculation for decryption, $P = (C-K_2) * K_1^{-1} \bmod 26$

- For First character I,

$I = (C-K_2) * K_1^{-1} \bmod 26$

$= (08-22) * 15^{-1} \bmod 26 = (-14 * 15^{-1}) \bmod 26$

$= (-14*7) \bmod 26 = -98 \bmod 26 = -20 \bmod 26 = -20+26 = 6$

For 15^{-1} equivalent value - $15^{-1} \bmod 26$

q	r1	r2	r	t1	t2	t = t1 - q * t2
1	26	15	11	0	1	-1
1	15	11	4	1	-1	2
2	11	4	3	-1	2	-5
1	4	3	1	2	-5	7
3	3	1	0	-5	7	-26
	1	**0**		**7**	-26	

So, 15^{-1} equivalent value: 7

After decryption the ciphertext: IYYPFKAQLWJIFWPEGXMJARMAQEV

The plaintext is: GOODLUCKBANGLADESHINCRICKET.

Figure 3.15: Affine Cipher Decryption

Example of the Vigenere Cipher encryption and decryption solution:

Plaintext (P) = Good Luck Bangladesh in Cricket

Key (K) = JAMUNA

Key Stream = 9 0 12 20 13 0

Now, Encryption: C = (P+K) mod 26

P. T	G	o	o	d	L	u	c	k	B	a	n	g	l	a	d	e	s	h	i	n	C	r	i	c	k	e	t
P. V	06	14	14	03	11	20	02	10	01	00	13	06	11	00	03	04	18	07	08	13	02	17	08	02	10	04	19
Key	09	00	12	20	13	00	09	00	12	20	13	00	09	00	12	20	13	00	09	00	12	20	13	00	09	00	12
C. V	15	14	0	23	24	20	11	10	13	20	00	06	20	00	15	24	05	07	17	13	14	11	21	02	19	04	05
C. T	P	O	A	X	Y	U	L	K	N	U	A	G	U	A	P	Y	F	H	R	N	O	L	V	C	T	E	F

After Encryption the Plaintext: Good Luck Bangladesh in Cricket.

The Ciphertext is: POAXYULKNUAGUAPYFHRNOLVCTEF

Now, Decryption: P = (C-K) mod 26

C. T	P	O	A	X	Y	U	L	K	N	U	A	G	U	A	P	Y	F	H	R	N	O	L	V	C	T	E	F
C. V	15	14	0	23	24	20	11	10	13	20	00	06	20	00	15	24	05	07	17	13	14	11	21	02	19	04	05
Key	09	00	12	20	13	00	09	00	12	20	13	00	09	00	12	20	13	00	09	00	12	20	13	00	09	00	12
P. V	06	14	14	03	11	20	02	10	01	00	13	06	11	00	03	04	18	07	08	13	02	17	08	02	10	04	19
P. T	G	O	O	D	L	U	C	K	B	A	N	G	L	A	D	E	S	H	I	N	C	R	I	C	K	E	T

- Calculation for decryption, P = (C-K) mod 26
  For Third character A,
  P = (C-K) mod 26
  = (00-12) mod 26
  = -12 mod 26 = -12 + 26 = 14

After decryption the ciphertext: SUCROFWMLBNTRLDHWZPVPTZJMON.

The plaintext is: GOODLUCKBANGLADESHINCRICKET.

Figure 3.16: Vigenere Cipher Encryption and Decryption

Example of the Rail-fence Cipher encryption and decryption solution:

Plaintext (P) = Good Luck Bangladesh in Cricket

Rails/depth = 2

Now, Encryption:

G		O		L		C		B		N		L		D		S		I		C		I		K		T
	O		D		U		K		A		G		A		E		H		N		R		C		E	

So, Cipher text: GOLCBNLDSICIKTODUKAGAEHNRCE.

Now, Decryption:

L = 27

N = 2

$$K = \frac{L}{2(N-1)} = \frac{27}{2(2-1)} = 13.5$$

Here after divided into half, we get fractional value.

In this case the first one half has one more character than second half which means 14 character for first half and 13 character is for second half and each character arranged by a space in their half.

After decryption the ciphertext: GOLCBNLDSICIKTODUKAGAEHNRCE.

So, The Plaintext is: GOODLUCKBANGLADESHINCRICKET.

Figure 3.17: Rail fence Cipher Encryption and Decryption

Example of the Row Transposition Cipher encryption and decryption solution:

Plaintext (P) = Good Luck Bangladesh in Cricket, Key (K) = 43761582

Now, Encryption:

1	2	3	4	5	6	7	8
G	O	O	D	L	U	C	K
B	A	N	G	L	A	D	E
S	H	I	N	C	R	I	C
K	E	T	Z	Z	Z	Z	Z

Key (K) = 43761582

4	3	7	6	1	5	8	2
D	O	C	U	G	L	K	O
G	N	D	A	B	L	E	A
N	I	I	R	S	C	C	H
Z	T	Z	Z	K	Z	Z	E

The cipher text is: DOCUGLKOGNDABLEANIIRSCCHZTZZKZZE

Now, Decryption:

The cipher text is: DOCUGLKOGNDABLEANIIRSCCHZTZZKZZE

4	3	7	6	1	5	8	2
D	O	C	U	G	L	K	O
G	N	D	A	B	L	E	A
N	I	I	R	S	C	C	H
Z	T	Z	Z	K	Z	Z	E

1	2	3	4	5	6	7	8
G	O	O	D	L	U	C	K
B	A	N	G	L	A	D	E
S	H	I	N	C	R	I	C
K	E	T	Z	Z	Z	Z	Z

After decryption, So, The Plaintext is: GOODLUCKBANGLADESHINCRICKET.

Figure 3.18: Row Transposition Cipher Encryption and Decryption

3.3 Results Overall Discussion

Here in the output section, there are all the output snapshots are given and details mention in figure name. There are given start to end of the projects output which are start from home page then substitution page and the four ciphers encryption-decryption and the end with shown the transposition cipher's encryption and decryption. From the output section see that, the result is accurately found with expected output which means the encryption and decryption result is accurately found. The project's program is executed successfully without any bugs or errors. So, we agree that this project program can be used to for a encryption and decryption of cipher algorithm's in cyber security.

3.4 Learning/Achievement

By completing this project, some potential learning/achievements that could come out of working on a project which are given in below-

- Implementing classical ciphers provides an opportunity to understand the principles of encryption, including substitution, transposition, and key management.
- Implementing classical ciphers involves coding and programming, which can help improve skills in web programming languages such as Html, CSS and Javascript etc.
- Implementing classical ciphers requires problem-solving skills, including analyzing and understanding complex algorithms, finding creative solutions to complex problems, and developing strategies to break encrypted messages.
- Learning about encryption techniques can help individuals understand the importance of securing communications and the risks associated with insecure transmission of information.

3.5 Challenge face/Difficulties

In this project, We faced some challenges when doing the tasks which are given below -

- Working with the DOM and event handlers can definitely be challenging, and it's common to encounter unexpected behavior or bugs. It's great that we were able to identify the problem and resolve it by carefully checking our code and trying different approaches.
- When converting between ASCII values and text in the project, which is challenging for us to find out accurate decryption result.

Chapter 4

Conclusion

4.1 Discussion

The project report details the development of a web-based application for cyber security using HTML, CSS, and JavaScript. This project allowed us to explore classical cipher techniques and gain practical experience in their implementation. By comparing the different techniques, we have gained insights into their strengths and weaknesses and how they compare to each other. The project also highlights the importance of key management in ensuring secure communication and the need for more advanced encryption techniques in modern-day communication. During the project, we faced challenges such as working with DOM manipulation, ASCII values, and ensuring code accuracy. Through careful testing and debugging, these challenges were successfully overcome. Overall, the project provided an opportunity to acquire new skills and knowledge, and the resulting application demonstrates a fundamental understanding of cyber security concepts With further development and improvement, the application can be useful for educational purposes or as a basic tool for cyber security enthusiasts. This project is enough to be an exhibition. So, we can said that our project is completed.