



Module Code & Module Title
CC5009NI Cyber Security in Computing

Assessment Weightage & Type
40% Individual Coursework 01

Year and Semester
2024 -25 Autumn Semester

Student Name: Aayush Raj Kafle

London Met ID: 23047570

College ID: NP01NT04A230231

Assignment Due Date: 10th Dec 2024

Assignment Submission Date: 19th January 2025

Word Count:4303

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.

11% Overall Similarity


29 Matching Text Blocks

Compare submissions against ?

Select at least one source type to check for similarity.

- ☒ Submitted Works
- ☒ Internet content
- ☒ Publications

Figure 1 Turnitin report with filter





Page 2 of 132 - Integrity Overview

Submission ID trn::oid::3618:79630686




19% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

-  **41 Not Cited or Quoted 15%**
Matches with neither in-text citation nor quotation marks
-  **8 Missing Quotations 4%**
Matches that are still very similar to source material
-  **0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 12%  Internet sources
- 4%  Publications
- 18%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Figure 2 Turnitin report without filter

Abstract

Cryptography is securing confidential information and communications through encryption algorithms, ensuring only intended recipients can access the data. It has been instrumental in securing sensitive information, facilitating private communication, and maintaining trust in digital systems. This project focuses on understanding and developing a custom cryptographic algorithm while analysing its functionality, advantages, and limitations. The developed encryption mechanism demonstrates the fundamental principles of cryptography by converting alphabets into binary formats, modifying bit positions, and assigning symbols to binary sequences.

The objective of this project is to create a functional encryption system, test its performance, and explore its applications in mitigating security risks. Additionally, the historical context of cryptography is explored, from its origins in ancient Egypt and India to modern-day algorithms such as AES. The practical implementation of the algorithm involves encoding the phrase "Hello World" into binary, manipulating the binary sequence, and converting it into symbols, showcasing the encryption process. This project emphasizes the importance of cryptography in addressing contemporary cybersecurity challenges while fostering a deeper understanding of encryption and decryption mechanisms.

Table of Content

Abstract	0
Table of Contents	0
Table of Figures	0
Table Of Tables.....	0
1 Introduction.....	1
1.1 Aims	3
1.2 Objective	3
1.3 Types.....	4
1.4 Background	5
1.5 2.1) Rail fence Cipher	7
2 Development	9
2.1 Modified ASCII table	9
2.2 Encryption.....	14
2.3 Decryption.....	17
3 4) Flowchart	19
3.1 4.1) Encryption	19
3.2 4.2) Decryption	20
1. Testing.....	21
Test 1.....	21
3.2.1 Encryption.....	21
3.2.2 Decryption.....	22
3.3 Test 2.....	23
3.3.1 Encryption.....	23
3.3.2 Decryption.....	25

3.4	Test 3.....	26
3.4.1	Encryption.....	26
3.4.2	Decryption.....	27
3.5	Test 4.....	28
3.5.1	Encryption.....	28
3.5.2	Decryption.....	30
3.6	Test 5.....	31
3.6.1	Encryption.....	31
3.6.2	Decryption.....	33
6)	Evaluation	34
3.7	Advantages.....	34
3.8	Disadvantage.....	35
	Conclusion	36
4	References	37

Table of Figures

Figure 1 Turnitin report with filter.....	1
Figure 2 Turnitin report without filter.....	1
Figure 3 CIA Triad	3
Figure 4 Tomb of the nobleman Khnumhotep	5
Figure 5 IBMs cryptography in early 20th century.....	6
Figure 6 Flowchart of encryption.....	19
Figure 7 Flowchart of Decryption process	20

Table Of Tables

Table 1 Modified ASCII table 1	9
Table 2 Modified ASCII table 2	10
Table 3 Modified ASCII table 3	11
Table 4 Modified ASCII table 4	12
Table 5 Modified ASCII table 5	13
Table 6 XOR logic	14
Table 7 Example Encpyption Rail Fence pattern	15
Table 8 Example Encryption XOR logic	15
Table 9 Example New Rail FENCE	16
Table 10 After shift	16
Table 11 Example Decryption Rail Fence Pattern.....	17
Table 12 Example After reversing Shift	18
Table 13 Example Decryption XOR logic.....	18
Table 14 Test 1 Encryption Rail Fence Pattern	21
Table 15 Test1 Encryption XOR logic	21
Table 16 Test1 New Rail FENCE.....	21
Table 17 Test1 New Rail FENCE.....	22
Table 18 Test1 Decryption Rail Fence Pattern	22
Table 19 Test1 After reversing Shift	22
Table 20 Test1 Decryption XOR logic	23
Table 21Test1 Decryption rail fence pattern	23
Table 22 Test2 Encryption Rail Fence Pattern	23
Table 23 Test2 Encryption XOR logic	24
Table 24 Test2 New Rail FENCE.....	24
Table 25 Test2 After shift	24
Table 26 Test2 Decryption Rail Fence Pattern	25
Table 27 Test2 After reversing Shift	25

Table 28 Test2 Decryption XOR logic	25
Table 29 Test2 Decryption rail fence pattern	25
Table 30 Test3 Encryption Rail Fence Pattern	26
Table 31 Test3 Encryption XOR logic	26
Table 32 Test3 New Rail FENCE.....	26
Table 33 Test3 After shift.....	27
Table 34 Test3 Decryption Rail Fence Pattern	27
Table 35 Test3 After reversing Shift	27
Table 36 Test3 Decryption XOR logic	28
Table 37 Test3 Decryption rail fence pattern	28
Table 38 Test4 Encryption Rail Fence Pattern	28
Table 39 Test4 Encryption XOR logic1	29
Table 40 Test4 Encryption XOR logic 2	29
Table 41 Test4 New Rail FENCE.....	29
Table 42 Test4 After shift.....	30
Table 43 Test4 Decryption Rail Fence Pattern	30
Table 44 Test4 After reversing Shift	30
Table 45 Test4 Decryption XOR logic 1	30
Table 46 Test4 Decryption XOR logic 2	31
Table 47 Test4 Decryption rail fence pattern	31
Table 48 Test5 Encryption XOR logic	31
Table 49 Test5 Encryption XOR logic	32
Table 50 Test5 New Rail FENCE.....	32
Table 51 Test5 After shift.....	32
Table 52 Test5 Decryption Rail Fence Pattern	33
Table 53 Test5 After reversing Shift	33
Table 54 Test5 Decryption XOR logic	33
Table 55 Test5 Decryption rail fence pattern	33

1 Introduction

Cryptography is the process of encrypting or entrapping to secure confidential information and communications through codes and algorithms to ensure that the only person the message was intended for can read it (Global Threat landscape report, 2024). Encryption, if data is done through These algorithms is used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transaction (Global Threat landscape report, 2024).

The prefix “crypt” means “hidden” and the suffix “graphy” means “writing”. (Anon., 2024). Modern cryptography is one of the cornerstones of modern cybersecurity, playing a very important role in protecting sensitive information and ensuring secure communication. It provides confidentiality through encryption of data, making it unintelligible to unauthorized individuals, and ensures data integrity by detecting alterations during transmission or storage. Cryptography also enables authentication, which verifies the identity of users and systems, and supports non-repudiation, preventing parties from denying their actions. It plays a crucial role in securing financial transactions, online communications, personal information, and the integrity of digital infrastructures. Given the growing threat of cyberattacks, cryptography remains an indispensable tool for privacy, security, and trust in a digitally interconnected world.

Security stands for the state of being or feeling secure, freedom from fear, anxiety, danger, doubt, etc or simply a state or sense of safety or certainty (Collins, 2021). n the context of information and cyber security, security is the practices, measures, and protocols implemented to protect digital assets, systems, and networks from unauthorized access, theft, damage, or disruption. It aims to ensure the confidentiality, integrity, and availability-CIA triad-of data, safeguarding it against cyber threats such as hacking, malware, and phishing. Security also involves the protection of systems from insider threats, ensuring that legal and regulatory standards are met, and retaining trust in digital interactions.

For instance, Stallings et al. (2018) highlight that cybersecurity refers to the protection of information systems from vulnerabilities, taking into consideration risks related to unauthorized access, denial of service, and data breaches. It involves preventive and responsive actions to reduce threats and ensure business continuity. (Stallings and Brown, 2018).

Further, Bishop (2003) has added weight to this view by mentioning that security would also involve the systems behaving as expected, where again, much emphasis is given to access control, authentication, and audit mechanisms. (Bishop, 2003)

The CIA triad, consisting of Confidentiality, Integrity, and Availability, is one fundamental model in information security that helps through the process of organizations in safeguarding data and systems. **Confidentiality** ensures sensitive information is kept private and accessed only by authorized users. The breach in confidentiality can be caused either due to direct attacks such as man-in-the-middle (MITM) and network spying, or human error resulting from sharing credentials and not encrypting communications. Meanwhile, various access controls, encryption methods, MFA, and employee training can help prevent these risks. Integrity refers to the validity of data against unauthorized and malicious modification or corruption. Integrity violation may range from intentional hacking and modifications of system logs to unintentional errors and inadequately designed security policies. These include hashing, encryption, digital signatures, and digital certificates that ensure authenticity, accuracy, and validity. Non-repudiation, such as the use of a digital signature, provides verification of the source and delivery of information. Availability: It means that systems and data are accessible to users when they need them. Disruptions in availability could be due to natural disasters, power outages, or intentional attacks like DoS or ransomware. To protect availability, an organization can use redundant systems, update and back up its systems regularly, and make disaster recovery plans. Together, these three principles in the CIA triad form a complete approach to building robust security systems that can address any threat or vulnerability. (fortinet, 2023)



Source: **IBM**

Figure 3 CIA Triad

1.1 Aims

To research about new, old and upcoming (cryptographic algorithm

Develop a new self-made (cryptographic algorithm

Test the (cryptographic algorithm

Learn about practical solution to mitigate various security issues

1.2 Objective

Develop a functional encryption mechanism

Ensure the algorithm is functional

Encrypt using the developed algorithm successfully

1.3 Types

- Symmetric Key Cryptography

It is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages. Symmetric Key cryptography is faster and simpler, but the problem is that the sender and receiver have to somehow exchange keys securely. (sealpath, 2024)

- Hash Functions

There is no usage of any key in this algorithm. A hash value with a fixed length is calculated as per the plain text which makes it impossible for the contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords. (sealpath, 2024)

- Asymmetric Key Cryptography

A pair of keys is used to encrypt and decrypt information. A sender's public key is used for encryption and a receiver's private key is used for decryption. (sealpath, 2024)

2 Background

Cryptography now is understood as changing the values of data inside a computer network so that data remains secure, cryptography has a history even longer than its name. The first ever evidence of use of cryptography in human civilization was in 1900 BC in ancient Egypt in the main chamber of the tomb of the nobleman Khnumhotep II a great chief of the Oryx name (upper Egypt).

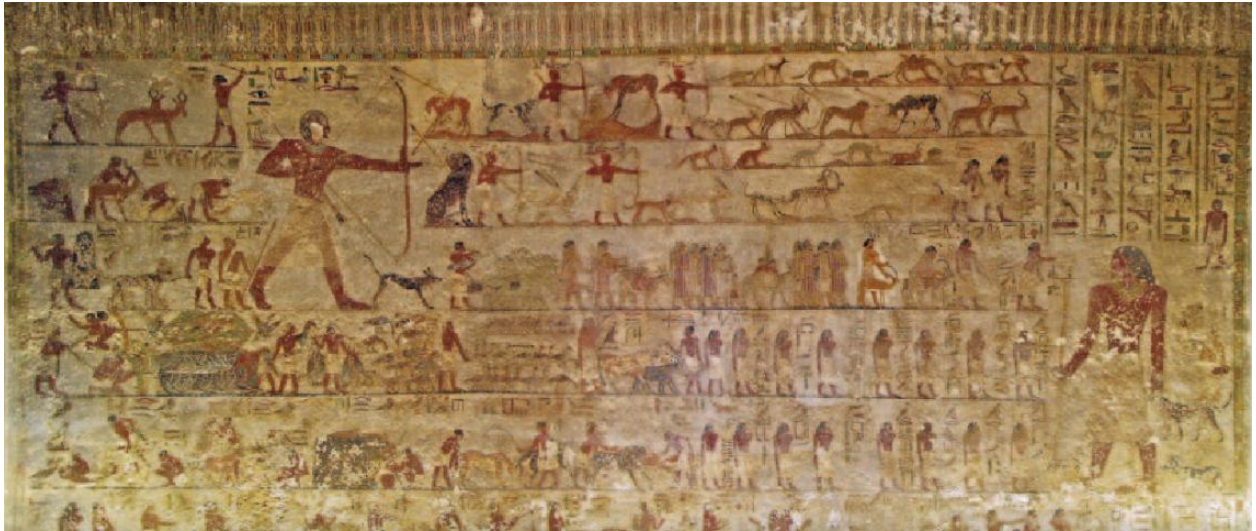


Figure 4 Tomb of the nobleman Khnumhotep

The tomb had some unique hieroglyphic among some common one. The purpose was not to hide the message but perhaps to change its form in a way which would make it appear dignified. Though the inscription was not a form of secret writing but incorporated some sort of transformation of the original text and is the oldest known text to do so. (Sidhpurwala, 2023). Then in ancient India some evidence of use of Cryptography was found written in Arthshashtra by Kautilya describing espionage service given to spies through secret writing. The fast forward to 100 BC Julius Caesar was known to use a form of encryption to convey secret messages to his army generals posted in the war front known as Caesar cipher. In the early 16th century Vigenere made a supposedly first cipher which used encryption Key. (Sidhpurwala, 2023)

In the early 1970's, IBM realized that their customers were demanding some form of encryption, so they formed a "crypto group" headed by Horst-Feistel.

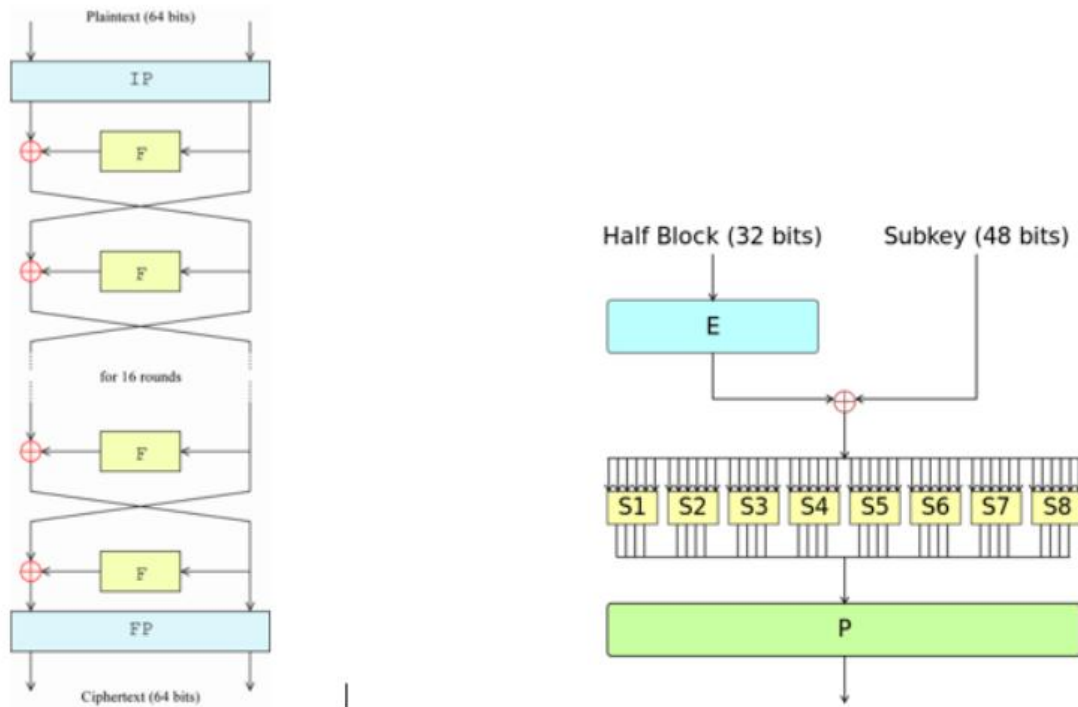


Figure 5 IBM's cryptography in early 20th century

They designed a cipher called Lucifer. In 1973, the Nation Bureau of Standards (now called NIST) in the US put out a request for proposals for a block cipher which would become a national standard (Sidhpurwala, 2023) . AES which is widely accepted as a standard use symmetric system encryption was Developed and started in use when NIST put out a request for proposal for a new block cipher in 1997 and was selected 3 years later in 2000. (Sidhpurwala, 2023)

Rail fence Cipher

The Rail Fence Cipher is a kind of symmetric key-based cryptography belonging to the class of transposition ciphers. It rearranges plaintext characters in a zigzag ($\backslash/\backslash/\backslash$) pattern over several "rails" or rows and then concatenates the characters row by row to form the ciphertext. The number of rails is used as a key for encryption, and decryption works the other way around by reversing the zigzag order with the same key to retrieve the plaintext. It is relatively simple to understand and implement with the least security and is, therefore, more useful for educative purposes than in secure communications. My algorithm borrows much from this cipher because its structured, yet simple method of juggling data makes it strong in laying the foundation for learning and designing encryption techniques. (GeeksforGeeks, 2023)

Advantage

- The integration of matrix operations into the traditional Rail Fence Cipher adds complexity, making it more resistant to brute force and pattern recognition attacks.
- The use of matrices introduces a flexible key space, allowing for different configurations and levels of encryption strength.
- The Rail Fence Matrix Cipher is computationally lightweight, making it suitable for resource-constrained environments, such as IoT devices or embedded systems.
- Combining Rail Fence Cipher and matrix operations is relatively straightforward to program, making it accessible for developers without extensive cryptographic expertise.
- Traditional attacks on the Rail Fence Cipher (e.g., frequency analysis) become less effective due to the additional layer of matrix-based transformation.
- It is suitable for non-critical encryption tasks, where moderate security and high efficiency are required.

Disadvantage

- Vulnerable to brute force attacks due to the limited number of possible keys
- Only rearranges letters and does not hide their identity, making it prone to frequency analysis.
- Easy to understand so it is quite predictable

3 Development

Rail Matrix Cipher

3.1 Modified ASCII table

Table 1 Modified ASCII table 1

Character	Custom DEC	Character	Custom DEC
A	0	N	13
B	1	O	14
C	2	P	15
D	3	Q	16
E	4	R	17
F	5	S	18
G	6	T	19
H	7	U	20
I	8	V	21
J	9	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

Table 2 Modified ASCII table 2

Character	Custom DEC	Character	Custom DEC
a	26	n	39
b	27	o	40
c	28	p	41
d	29	q	44
e	30	r	45
f	31	s	46
g	32	t	47
h	33	u	48
i	34	v	49
j	35	w	50
k	36	x	51
l	37	y	52
m	38	z	53

Table 3 Modified ASCII table 3

Character	Custom DEC	Character	Custom DEC
1	54	@	67
2	55	#	68
3	56	\$	69
4	57	%	70
5	58	^	71
6	59	&	72
7	60	*	73
8	61	(74
9	62)	75
0	63	{	76
Space	64	}	77
~	65	[78
!	66]	79

Table 4 Modified ASCII table 4

Character	Custom DEC	Character	Custom DEC
—	80	:	93
+	81	Gap1	94
-	82	Gap2 \	95
+	83	Gap3 ©	96
*	84	क	97
/	85	ख	98
.	86	ग	99
<	87	घ	100
>	88	ङ	101
?	89	च	102
"	90	छ	103
‘	91	ज	104
:	92	झ	105

Table 5 Modified ASCII table 5

Character	Custom DEC	Character	Custom DEC
ज	106	प	117
ट	107	फ	118
ठ	108	ब	119
ड	109	भ	120
ढ	110	म	121
ण	111	य	122
त	112	Δ	123
थ	113	∞	124
द	114	Σ	125
ध	115	∂	126
न	116	$\sqrt{\quad}$	127

3.2 Encryption

Encryption Algorithm

Step 1 Input plaintext P and key K! (number of rails always set to 3)

Step 2 Divide P into rows according to the zigzag traversal (rail pattern)

Step 3 Use the K1 rails to alternate between the descending and ascending paths($\backslash \swarrow \swarrow$) and

Step 4 Change every 3rd letter into decimal according to the Mod ASCII table then change into 7-bit long binary

Step 5 For each 3rd character in the zigzag pattern, apply the XOR operator (with the constant password)

Table 6 XOR logic

A	B	X
0	0	0
0	1	1
1	0	1
1	1	0

Step 6 Using the Mod ASCII table find the appropriate NEW value and assign it in the old character place

Step 7 SHIFT all the words positioned by +1 in the rail's column

Step 9 Combine the rows in a concatenate manner to sequentially form the final ciphertext

Step 8 Output is Ciphertext

Encryption Process

1) Input:

- Plaintext: Choose your message (e.g., "HELLOWORLD").
- Key1: The number of rails always should be 3

2) Create Zigzag Pattern:

- Arrange the plaintext characters in a zigzag pattern across the given number of rails.
- Example for "HELLOWORLD"

Table 7 Example Encpytion Rail Fence pattern

H				O				L	
	E		L		W		R		D
		L				O			

3) XOR operation:

Applying XOR operation

Password (K2) = 0101000

Mod ASCII > every 3rd letter after XOR operation

Table 8 Example Encryption XOR logic

Character	L	W	L
DEC	11	22	11
Binary	0001011	0010110	0001011
Password	0101000		
NEW Binary	0100011	0111110	0100011
New DEC	35	62	35
NEW Char	w	!	w

4) NEW Cipher rail

Table 9 Example New Rail FENCE

H				O				w	
	E		L		!		R		D
		w				O			

Shit by +1

Table 10 After shift

		W				H				O	
	R		D		\		E		L		!
O								w			

5) Concatenate Rows:

- After applying the transformations, concatenate all rows to form the final ciphertext.
- Ciphertext text: .wHORD\EL!O|w

6) Define the top rail length

- The last letter should always carry the top rail length
- 3rd letter should always carry the second rail length
- Ciphertext text: wHO6RD\EL!O|w 3

3.3 Decryption

Decryption Algorithm

Step 1 Input Ciphertext C and key K! (number of rails always set to 3)

Step 2 Divide P into rows according to the zigzag traversal (rail pattern)

Step 3 shifts the rows by -1 and the top left is at the starting point.

Step 4 Reverse XOR operation using the given key2 (i.e. 7-bit long password)

Step 5 Assemble the word in a concatenated manner by selecting in descending then ascending manner.

Decryption Process

1) Input:

- Assemble the ciphered text in the rail (rail key is set to 3)
- Ciphertext text: .wHO6RD\EL!O|w 3

2) Recreate Plaintext

Write the characters in the zigzag order to retrieve the plaintext.

Table 11 Example Decryption Rail Fence Pattern

		W				H				O	
	R		D		\		E		L		!
O								w			

3) OLD Cipher Rail

Shift by -1

Table 12 Example After reversing Shift

H				O				w	
	E		L		!		R		D
		w				O			

HEwLO!ORwD

4) Reversing XOR operation

Applying XOR operation

Password (K2) = 0101000

Table 13 Example Decryption XOR logic

Character	w	!	w
DEC	35	62	35
Binary	0100011	0111110	0100011
Password	0101000		
NEW Binary	0001011	0010110	0001011
New DEC	11	22	11
NEW Char	L	W	L

5) Concatenate ROWS:

- After applying the transformations, concatenate all rows in zigzag pattern to form the final ciphertext.
- Plaintext: .HELLOWORLD

4 Flowchart

4.1) Encryption

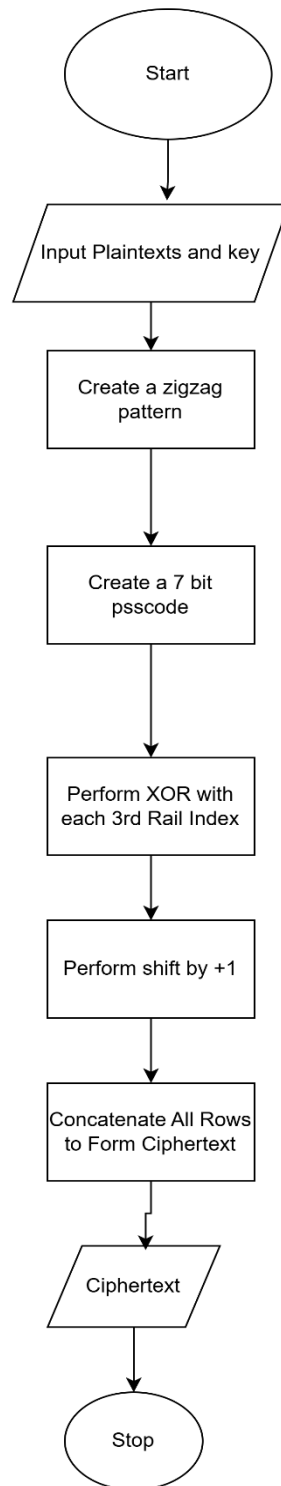


Figure 6 Flowchart of encryption

4.2) Decryption

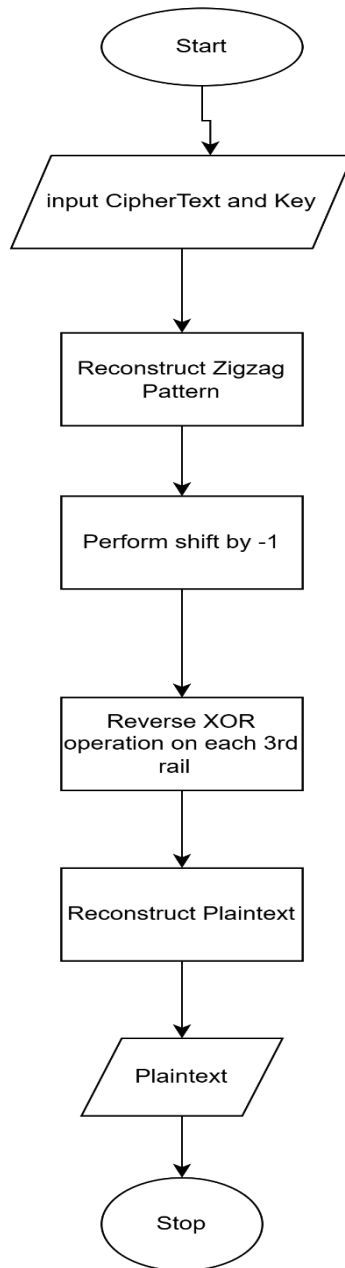


Figure 7 Flowchart of Decryption process

5 Testing

Password is always constant in a test.

Test 1

Hello Nepal123

Password:1011000

Encryption

Table 14 Test 1 Encryption Rail Fence Pattern

H				o				p				2	
	e		l		<Space>		e		a		1		3
		1				N				l			

Applying XOR operation

Table 15 Test1 Encryption XOR logic

Char	l	<Space>	p	1
DEC	37	64	41	54
Binary	0100101	1000000	0101001	0110110
Password	1011000			
New Binary	1111101	0011000	1110001	1101110
New DEC	125	24	113	110
New Char	Σ	Y	थ	ढ

New ciphered rail

Table 16 Test1 New Rail FENCE

H				o				थ				2	
	e		l		Y		e		a		ढ		3
		Σ				N				l			

Shift by +1

Table 17 Test1 New Rail FENCE

၃				2				H				o			
	a		၆		3		\		e		l		Y		e
		l								Σ				N	

Ciphred text ၃2H8oa၆3\elYel|ΣN4

Decryption

Matrix rail fence

Table 18 Test1 Decryption Rail Fence Pattern

၃				2				H				o			
	a		၆		3		\		e		l		Y		e
		l								Σ				N	

Shift by -1

Table 19 Test1 After reversing Shift

H				o				၃				2			
	e		l		Y		e		a		၆		3		
		Σ				N				l					

Table 20 Test1 Decryption XOR logic

Char	Σ	Y	थ	ढ
DEC	125	24	113	110
Binary	1111101	0011000	1110001	1101110
Password	1011000			
New Binary	0100101	1000000	0101001	0110110
New DEC	37	64	41	54
New Char	l	<Space>	p	l

Table 21 Test1 Decryption rail fence pattern

H				o				p				2	
	e		l		<Space>		e		a		1		3
		l				N				l			

Plaintext Hello Nepal123

Test 2

CYBERSECURITY

Password:0011000

Encryption

Table 22 Test2 Encryption Rail Fence Pattern

C				R				U				Y
	Y		E		S		C		R		T	
		B				E				I		

Applying XOR operation

Table 23 Test2 Encryption XOR logic

Char	B	S	U	T
DEC	1	18	20	19
Binary	0000001	0010010	0010100	0010011
Password	0011000			
New Binary	0011001	0001010	0001100	0001011
New DEC	25	10	12	11
New Char	Z	K	M	L

New Cipher Rail

Table 24 Test2 New Rail FENCE

C				R				M				Y
	Y		E		K		C		R		L	
		Z				E				I		

Shift by +1

Table 25 Test2 After shift

Y				C				R				M			
					Y		E		K		C		R		L
		\				Z				E				I	

Ciphered text: RMY8CKCRL|©YEEI\Z4

Decryption

Matrix Rail fence

Table 26 Test2 Decryption Rail Fence Pattern

R				M				Y				C			
	K		C		R		L				©		Y		E
		E				I				\				Z	

Shift by -1

Table 27 Test2 After reversing Shift

C				R				M					Y
	Y		E		K		C		R		L		
		Z				E				I			

Table 28 Test2 Decryption XOR logic

Char	Z	K	M	L
DEC	25	10	12	11
Binary	0011001	0001010	0001100	0001011
Password	0011000			
New Binary	0000001	0010010	0010100	0010011
New DEC	1	18	20	19
New Char	B	S	U	T

Table 29 Test2 Decryption rail fence pattern

C				R				U				Y
	Y		E		S		C		R		T	
		B				E				I		

Plain text CYBERSECURITY

Test 3

123456789

Encryption*Table 30 Test3 Encryption Rail Fence Pattern*

1				5				9
	2		4		6		8	
		3				7		

Applying XOR operation

Table 31 Test3 Encryption XOR logic

Char	3	6	9
DEC	56	59	62
Binary	0111000	0111011	0111110
Password	0001011		
New Binary	0110011	0110000	0110101
New DEC	51	48	53
New Char	x	u	z

New Rail Fence

Table 32 Test3 New Rail FENCE

1				5				z
	2		4		u		8	
		x				7		

Shift by +1

Table 33 Test3 After shift

z				1				5			
			©		2		4		u		8
		\				x				7	

Ciphered text z155|© 24u8\x73

Decryption

Matrix rail fence table

Table 34 Test3 Decryption Rail Fence Pattern

z				1				5			
			©		2		4		u		8
		\				x				7	

Shift by -1

Table 35 Test3 After reversing Shift

1				5				z
	2		4		u		8	
		x				7		

Reversing XOR operation

Table 36 Test3 Decryption XOR logic

Char	x	u	z
DEC	51	48	53
Binary	0110011	0110000	0110101
Password	0001011		
New Binary	0111000	0111011	0111110
New DEC	56	59	62
New Char	3	6	9

Table 37 Test3 Decryption rail fence pattern

1				5				9
	2		4		6		8	
		3				7		

Plain text 123456789

Test 4

This is a rail fence Cipher

Password: 0100111

Encryption

Table 38 Test4 Encryption Rail Fence Pattern

T				<s>				a				i			n				c				e		
	h		s		i		<s>		<s>		a		l		e		c		<s>		i		h		r
		i				s				R			f			e					p				

Applying XOR operation.

Table 39 Test4 Encryption XOR logic1

Char	i	i	a	a
DEC	34	34	26	26
Binary	0100010	0100010	0011010	0011010
Password	0100111			
New Binary	0000101	0000101	0111101	0111101
New DEC	5	5	61	61
New Char	F	F	8	8

Table 40 Test4 Encryption XOR logic 2

Char	f	c	c	h
DEC	31	28	28	33
Binary	011111	0011100	0011100	0100001
Password	0100111			
New Binary	0011000	0111011	0111011	01111101
New DEC	24	59	59	125
New Char	Y	6	6	Σ

New ciphered rail

Table 41 Test4 New Rail FENCE

T				<s>				8				i				n				6				e
	h		s		F		<s>		<s>		8		l		e		6		<s>		i		Σ	r
		F				s				R			Y				e					p		

Here <s> is <Space>.

Shift by +1

Table 42 Test4 After shift

e				T				<s>				8				i			n				6			
	r		\		h		s		F		<s>		<s>		8		l		e		6		<s>		i	Σ
						F				s				R			Y				e				p	

Ciphered text: eT 8<14>in6r\hsF 8le6 i Σ |FsRYep7

Decryption

Matrix Rail fence table

Table 43 Test4 Decryption Rail Fence Pattern

e				T				<s>				8				i			n				6			
	r		\		h		s		F		<s>		<s>		8		l		e		6		<s>		i	Σ
						F				s				R			Y				e				p	

Shift by -1

Table 44 Test4 After reversing Shift

T				<s>				8				i			n				6				e		
	h		s		F		<s>		<s>		8		l		e		6		<s>		i		Σ		r
		F			s					R			Y				e				p				

Reverser applying XOR operations

Table 45 Test4 Decryption XOR logic 1

Char	F	F	8	8
DEC	5	5	61	61
Binary	0000101	0000101	0111101	0111101
Password	0100111			
New Binary	0100010	0100010	0011010	0011010
New DEC	34	34	26	26
New Char	i	i	a	a

Table 46 Test4 Decryption XOR logic 2

Char	Y	6	6	Σ
DEC	24	59	59	125
Binary	0011000	0111011	0111011	01111101
Password	0100111			
New Binary	011111	0011100	0011100	0100001
New DEC	31	28	28	33
New Char	f	c	c	h

Table 47 Test4 Decryption rail fence pattern

T				<s>				a				i				n				c				e	
	h		s		i		<s>		<s>		a		l		e		c		<s>		i		h		r
		i				s				R				f				e				p			

Plaintext: This is a rail fence Cipher

Test 5

www.google.com

Password: 0100111

Encryption

Table 48 Test5 Encryption XOR logic

w				g				l					o	
	w		.		o		g		e		c			m
		w				o				.				

Table 49 Test5 Encryption XOR logic

Char	w	o	l	c
DEC	50	40	37	28
Binary	0110010	0101000	0100101	0011100
Password	0100111			
New Binary	0010101	0001111	0000010	0111011
New DEC	21	15	2	59
New Char	V	P	C	6

New Cipher rail

Table 50 Test5 New Rail FENCE

w				g				C				o	
	w		.		P		g		e		6		m
		V				o				.			

Shift by +1

Table 51 Test5 After shift

o				w				g				C			
	m		\		w		.		P		g		e		6
						V				o				.	

Ciphered text **ewgCm\w.Pge6|Vo.**

Decryption

Rail fence table

Table 52 Test5 Decryption Rail Fence Pattern

o				w				g				C			
	m		\		w		.		P		g		e		6
						V				o				.	

Shift by -1

Table 53 Test5 After reversing Shift

w				g				C				o		
	w		.		P		g		e		6		m	
		V				o				.				

Table 54 Test5 Decryption XOR logic

Char	V	P	C	6
DEC	21	15	2	59
Binary	0010101	0001111	0000010	0111011
Password	0100111			
New Binary	0110010	0101000	0100101	0011100
New DEC	50	40	37	28
New Char	w	o	l	c

Table 55 Test5 Decryption rail fence pattern

w				g				l				o	
	w		.		o		g		e		c		m
		w				o				.			

Plaintext: **www.google.com**

6 Evaluation

The Matrix Rail Fence Cipher is an innovative approach to encryption that combines elements of the traditional Rail Fence Cipher with matrix-based transformations. This hybrid design aims to enhance security by introducing an additional layer of complexity while maintaining the lightweight and efficient characteristics of classical transposition ciphers. By leveraging matrix operations, the algorithm achieves flexibility and customizability, making it suitable for various encryption scenarios. However, like any novel cryptographic method, it comes with its own set of advantages, disadvantages, and considerations that determine its practical applicability and effectiveness.

6.1 Advantages

- **Increased Complexity:**

By integrating matrix transformations with the traditional Rail Fence Cipher, the algorithm increases its resistance to basic frequency analysis and brute-force attacks compared to the classical Rail Fence Cipher.

- **Layered Encryption:**

The combination of two distinct techniques (matrix manipulation and transposition) adds a layer of complexity, making it harder for attackers to decrypt without access to the specific algorithm structure.

- **Customizability:**

The use of a matrix structure allows for flexibility in key design, potentially accommodating different sizes or patterns to strengthen encryption.

- **Lightweight and Fast:**

Rail Fence Cipher and matrix operations are computationally lightweight, making the algorithm suitable for resource-constrained devices and real-time encryption.

- **Ease of Implementation:**

Both Rail Fence Cipher and matrix operations are straightforward to implement and understand, reducing the risk of errors during coding.

6.2 Disadvantage

- **Limited Security for Advanced Threats:**

While the algorithm improves over the basic Rail Fence Cipher, it may still be vulnerable to modern cryptanalytic techniques if the keyspace or design is insufficiently robust.

- **Key Management:**

If the algorithm uses large or complex matrices as keys, securely distributing and storing these keys may pose challenges.

- **Predictable Patterns:**

If the Rail Fence pattern or matrix structure is predictable, it could reduce the overall security, especially against dedicated attackers with knowledge of the algorithm.

- **No Proven Cryptographic Standards:**

The Matrix Rail Fence Cipher is a novel approach and lacks widespread scrutiny or validation by cryptographic experts, which may limit its trustworthiness in critical applications.

Conclusion

The Matrix Rail Fence Cipher is a hybrid encryption scheme in which the idea of the Rail Fence Cipher is mixed with matrix transformations. In that way, some drawbacks of these ciphers may be avoided and their drawbacks remedied by introducing several additional layers of complication to the security level without a significant computational load. The proposed algorithm ensures considerable resistance against some simple cryptanalytic attacks, flexible key design, and suitability for lightweight encryption tasks due to its simplicity.

However, according to the report, the algorithm also has a number of significant limitations, including on its vulnerability to advanced cryptanalysis and challenges in key management. Its dependence on a hybrid model adds additional complexity that, while beneficial for security, may provide implementation and usability challenges if not appropriately managed. Furthermore, without wider validation by the cryptographic community, it has limited adoption in high-security scenarios.

The Matrix Rail Fence Cipher would find practical applications where lightweight encryption and ease of implementation are the major considerations in non-critical applications. In sensitive data, refinements such as increasing the keyspace, integrating other methods of cryptography, and rigorous testing of the algorithm would be required to establish it as a reliable and secure method of encryption.

Hence, the conclusion will be that though the Matrix Rail Fence Cipher is an innovative contribution to cryptography, its potential remains in its ability to be a good foundation for further development. With more research and enhancements, it has a good potential of evolving into a more robust encryption technique that is simple, efficient, and secure enough to meet modern encryption demands.

References

Anon., 2024. *Cryptography and its Types*. [Online]

Available at: <https://www.geeksforgeeks.org/cryptography-and-its-types/>

Bishop, M., 2003. *Computer Security: Art and Science*, Davis: University of California.

Collins, 2021. *Definition of 'security'*. [Online]

Available at:

<https://www.collinsdictionary.com/dictionary/english/security#:~:text=forms%3A%20plural%20se%CB%88curities-,1.,%2C%20etc.%3B%20protection%3B%20safeguard>

[Accessed 10 12 2024].

fortinet, 2023. *CIA Triad*. [Online]

Available at: <https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,and%20methods%20for%20creating%20solutions.>

[Accessed 10 12 2024].

GeeksforGeeks, 2023. *GeeksforGeeks*. [Online]

Available at: [Rail Fence Cipher – Encryption and Decryption](#)

[Accessed 9 12 2024].

Global Threat landscape report, 2024. *What Is Cryptography?*. [Online]

Available at: <https://www.fortinet.com/resources/cyberglossary/what-is-cryptography#:~:text=Cryptography%20is%20the%20process%20of,%2C%20computer%20passwords%2C%20and%20e-commerce.>

[Accessed 8 12 2024].

sealpath, 2024. *A Deep Dive into Encryption Types*. [Online]

Available at: <https://www.sealpath.com/blog/types-of-encryption-guide/#:~:text=Symmetric%20encryption%20uses%20the%20same,essential%20tool%20enhancing%20password%20security.>

[Accessed 7 1 2025].

Sidhpurwala, H., 2023. *A Brief History of Cryptography*. [Online]
Available at: <https://www.redhat.com/en/blog/brief-history-cryptography>
[Accessed 5 12 2024].

Staling and Brown, 2018. *Computer Security: Principles and Practice*. 4th ed. Pearson.,
Michigan: University iof Delta.