Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework

Year and Semester

2023 -24 Autumn

Student Name: Prithak Babu Shrestha

London Met ID: 22067084

College ID: np01nt4a220180

Assignment Due Date: Jan 15th 2024

Assignment Submission Date: Jan 15th 2024

Word Count (Where Required): -

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 Contents

Contents

Table of Figures

Table of Table

Abstract

The research describes "Haze," a modified encryption approach that combines three cryptographic algorithms - Caesar Cipher, Columnar Transposition Cipher, and Rail Fence Cipher - to overcome the shortcomings of individual techniques. It underlines the significance of security in computing and investigates the CIA triad for information security. The document contains in-depth information on encryption, including symmetric and asymmetric algorithms, as well as hashing.

The historical progression of cryptography is described, culminating in the invention of Haze. The fundamental cryptographic methods are described, beginning with Caesar Cipher, then Columnar Transposition Cipher, and finally Rail Fence Cipher. The study goes over their operating principles, advantages, and downsides.

In the development part, the necessity of Haze is justified, emphasizing Caesar Cipher's flaws. Haze combines numerous encryption layers to build a strong technique that mitigates individual flaws. The research finishes by underlining the need of adopting layered encryption to improve data security and introducing Haze as a feasible option in current cybersecurity.

1. Introduction

1.1 Security

Security in computing is the process of defending our device, data, information, network, etc. against threat posing attacks by cyber criminals or other unauthorized hackers. Security is the most essential factor in each organization. Almost all of the business organization implement security measures to guard against cybercrimes such as Malware, Identity Theft, Data Breach, DDoS, Ransomware attacks (Kelly, 2023).

Cyber security deals with protecting systems and networks against cyber criminals who breach though various unethical methods. Security specialist intend to launch a defensive measure before a attack, majority of the specialists working today concentrate more on figuring out how to effectively protect all assets from cyber criminal's attacks (Kelly, 2023).

The two areas where It securities are implemented are: Physical and Information. Physical meaning safe guarding the data containing devices and Information meaning InfoSec or guarding against unauthorized personnel’s remotely (Kelly, 2023).

1.1.1 Physical Security

Physical security is the process protecting the hardware, software, networks, and data from physical activities that might cause harm an organization's data system. Physical security provides protection against burglary, theft, vandalism, terrorism, fire, flood, and other natural disasters. Physical security prioritizes damage reduction in order to reduce loss of time, money, and resources. Physical security protects the assets, personnel and organizational facilities from external dangers. The main focus of physical security to protect physical facilities from physical or real-world threats (Cobb, 2021).

1.1.2 Information Security

Information Security (InfoSec) is a collection of safety measures and procedures that helps to guard against unauthorized access, cyber-attacks and breaches and misuse or theft of sensitive data. It often includes technology like as deception tools, endpoint detection and response (EDR), cloud access security brokers (CASB), and security testing for DevOps (DevSecOps), and others. Information security involves security plans such as access control, data integrity and easily accessibility of data (Roohparvar, 2020).

1.2 CIA

CIA triad or Confidentiality, Integrity and Availability an information security model designed to protect an organization's security procedures and policies, consisting of those three fundamental elements to protect us from threats (Fasulo, 2021).

1.2.1 Confidentiality

Confidentiality in the CIA triad means maintaining the privacy of an organization's data. The confidentiality factor ensures that data can only be accessed and modified by authorized individuals and processes. Confidentiality can be maintained by preventing unauthorized individuals from accessing assets that are essential to the organization. By decreasing and selecting the people who can access the organizations data we can safely maintain confidentiality.

1.2.2 Integrity

Integrity in CIA simply means the reliability of the data. It must be maintained in an unhampered condition, be accurate, authentic, and trustworthy, and be kept in a correct state. Integrity must be maintained in data provided to the public so that clients can have faith in the organization. The data should be protected from unauthorized modifications, and any other modifications whether they are intentional or unintentional. Specialists should set up access controls, allow monitoring of modifications, and safeguard data during storage or transmission to prevent from data tampering.

1.2.3 Availability

Availability in CIA means that the data stored should be accessible to authorized users whenever they need it, just as it's essential to prevent unauthorized users from accessing the organization's data. This include maintaining the functionality of devices, networks, and systems. Unless the stored data is accessible to those within the organization and its clients, it is useless. This means applications, networks, and systems must all operate when and how they should. As well, the information must not take a lot of time to be accessible, and those who have access to it must be able to use it when needed.

1.3 Encryption

Encryption is the process of converting information into a secret code that disguises its true meaning. The science of encrypting and decrypting information is known as cryptography. An unencrypted data is known as plaintext, while encrypted data is known as ciphertext. The formulas used to encode and decode messages are known as encryption algorithms, or ciphers. Cipher includes a variable as part of its algorithm in order to function effectively. What distinguishes the output of a cipher is the variable known as a key. When an encrypted communication is intercepted by an unauthorized party, the intruder must guess the cipher used by the sender to encrypt the message, as well as the keys used as variables. The time and effort required to guess this information are what make encryption such an effective security measure (Loshin, 2022).

Encryption has been used to secure sensitive information. Originally, it was employed by soldiers and governments. Nowadays, encryption is used to safeguard data saved on computers and storage devices, as well as data in transit across networks. Encryption plays an important role in securing many different types of information technology assets. It provides Confidentiality by encoding the message's content, Authentication by verifying the origin of a message, Integrity by proving the contents of a message have not been changed since it was sent and Nonrepudiation by preventing senders from denying they sent the encrypted message.

Encryption is a crucial method used by organizations and individuals to secure sensitive information and data in transit and at rest. It involves selecting the best possible cipher to conceal the message's meaning and applying a unique variable as a key. The most common ciphers used are symmetric and asymmetric (Loshin, 2022).

1.3.1 Symmetric Encryption

Symmetric encryption, also known as secret key encryption, encrypts and decrypts data using a single shared secret key. But this method is vulnerable to unauthorized access if intercepted by a third party as the key must be discussed between the sender and receiver, demanding the creation of a secure key exchange process (Harmening, 2017).

Symmetric encryption is a mechanism in which the sender and receiver share the same key and calculate a shared key. DES and AES are two popular symmetric encryption systems. After AES, DES was phased out and replaced with 3-DES, often known as Triple DES and TDES. To protect against brute-force assaults, 3-DES hashes DES twice with a 56-bit algorithm and password. Some VPN software use these symmetric keys. A shared secrets system encrypts and decrypts data using preshared key agreement methods, with the key computed using a common identifier or public key (Harmening, 2017).

1.3.2 Asymmetric Encryption

Asymmetric encryption is also known as public key encryption. It is an effective method that uses a key pair of two mathematically linked keys, the public key and the private key, to generate secure encryption. The private key is kept secret and can only be used by the owner, but the public key is available to everyone. Because of the time and processing power required, it is theoretically impossible for anybody to recreate the private key.

Asymmetric encryption is a safe method that encrypts a message using a public key rather than a secret key. The sender uses the receiver's public key, which is publicly available, and the recipient decrypts the message with their private key. Only the private key linked to the public key may be used to decode the message.

This key pair can also be used to authenticate the sender's identity, with the message encrypted using the sender's private key. Although this approach does not guarantee confidentiality, it does validate the sender's identity because the message could only have been encrypted using the sender's private key.

1.4 Hashing

Hashing is the process of converting data into a fixed-length string of letters and digits using a hash function. The key, or input data, might be in a variety of forms, including text, numbers, graphics, or application files. The key may be in any format, including a string of text, a list of integers, an image, or an application file. The method ensures the data's integrity (Codecademy Team, 2023).

It divides a key into equal-sized blocks of data to produce a fixed-length string of characters. Popular hashing algorithms operate with block sizes ranging from 160 to 512 bits, where a bit is the fundamental unit of computer information. Hashing algorithms may analyse big datasets or files dozens, if not hundreds of thousands, of times before creating the final hash value, making them highly efficient and effective. Therefore, hashing algorithms must be efficient to be effective (Codecademy Team, 2023).

The hash function produces the hash value, which should be unique to each input. Hash values may only be used once for data authentication or they may be saved in a hash table for easy access (Codecademy Team, 2023).

Hashing is used in a variety of applications, including cyber security, block chain, and data privacy. It is essential as it helps in message and data authentication, detecting changes in the data, data privacy, block chain, database management and many more (Codecademy Team, 2023).

1.5 Cryptography

Cryptography is the method of securing data by converting it into a format which unauthorized parties and personnel cannot decipher. An initial human-readable message is known as plaintext. In this method the message is transformed into something that would appear to be meaningless to the observer. The meaningless text that the observer views to be gibberish with the help of cryptography with use of an algorithm, or a series of mathematical operations. This gibberish text is known as ciphertext (Fruhlinger, 2022).

1.5.1 History of Cryptography

Cryptology considered to a science and art that has been used for thousands of years to hide secret messages, began to be studied around one hundred years ago. The first known evidence of cryptography was found in an inscription carved around 1900 BC in Egypt, where the scribe used unusual hieroglyphic symbols to make the message appear dignified. This inscription is the oldest known text to do so. Evidence of cryptography has been found in most major early civilizations, such as Kautalya's "Arthshashtra" which describes espionage service in India and assigns spies in "secret writing." Around 100 BC, Julius Caesar used a substitution cipher, known as the Caesar cipher, to convey secret messages to his army generals. This substitution cipher is perhaps the most mentioned historic cipher in academic literature (Sidhpurwala, 2023).

Ciphers rely on the system's secrecy, not the encryption key, and can be easily decrypted once the system is known. Substitution ciphers can be broken using the frequency of letters in the language. In the 16th century, Vigenere designed the first cipher using an encryption key. The key was repeated multiple times across the entire message, and the cipher text was produced by adding the message character with the key character modulo 26. Vigenere's cipher, while easily broken, introduced the idea of introducing encryption keys, but it was poorly executed. In contrast, the secrecy of the message depends on the encryption key's secrecy, not the system's secrecy (Sidhpurwala, 2023).

In the 19th century, Hebern invented the Hebern rotor machine, an electro-mechanical contraption with a single rotor embedded in a rotating disc. The key encoded a substitution table, and each key press produced cipher text. The Enigma machine, invented by German engineer Arthur Scherbius, used multiple rotors to output cipher text. The cipher was eventually broken by Poland, and the technology was transferred to British cryptographers (Sidhpurwala, 2023).

During World War II, cryptography was primarily used for military purposes, but it gained commercial attention post-war. IBM formed a crypto group in the 1970s, designing a cipher called Lucifer. In 1973, the US National Bureau of Standards (NIST) requested proposals for a block cipher, which was accepted as DES. However, DES was broken by an exhaustive search attack in 1997 due to its small encryption key size. In 2000, NIST accepted Rijndael, naming it AES, a widely accepted symmetric encryption standard. Post-quantum cryptography is now being considered (Sidhpurwala, 2023).

2. Cryptographic Algorithms

2.1 Caesar Cipher

Caesar Cipher is a simple cryptography method, created by Julius Caesar to encrypt messages. This method involves sending a message or text using logic, and the receiver decrypting it by substituting certain letters. This method allows for secure communication and is used by many to protect sensitive information. In This method a plain text or a message is encrypted according to the key value given. The key value specifies the number of position each letter is shifted (Codedamn, 2023).

2.1.1 How does Caesar Cipher work?

En(x) = (x + k) mod 26

Where,

En(x) is the encrypted letter.

x is the original letter's assigned integer.

k is the amount of number the letter is to be shifted.

mod 26 is to ensure the k integer is below 26 and not above to the 26 so that the result is possible from the following formula.

Caesar Cipher uses the following formula for decryption:

Dn (x) = (x - k) mod 26

Where,

Dn(x) is the decrypted letter.

x is the original letter's assigned integer.

k is the amount of number the letter is to be shifted.

mod 26 is to ensure the k integer is below 26 and not above to the 26 so that the result is possible from the following formula.

Encryption:

Step 1: Take the input plaintext.

Step 2: Take the shift value (k) to ensure the amount to be shifted.

Step 3: Ensure if the shift value (k) is in between 0 to 25.

Step 4: Create a empty variable En(x) to store the result of the encryption.

Step 5: Determine if the character given to encrypt is a proper alphabet or not and if the character is within the key from 0 to 25.

Step 6: Apply the formula i.e. [En(x) = (x + k) mod 26] to the following letter.

Step 7: Maintain the case of the letter (uppercase or lowercase).

Step 8: If a certain character is not a alphabet then do not change it.

Step 9: Return the value of the encrypted letter the empty variable En(x).

Step 10: Loop the process until each character from the plain text has been converted into ciphertext.

Decryption:

Step 1: Take the ciphertext.

Step 2: Take the shift value (k).

Step 3: Ensure if the shift value (k) is in between 0 to 25.

Step 4: Create a empty variable Dn(x) to store the result of the decryption process.

Step 5: Determine if the character given to encrypt is a proper alphabet or not and if the character is within the the key from 0 to 25.

Step 6: Apply the formula i.e. [Dn(x) = (x - k) mod 26] to the following letter. The formula is similar to encryption but in this process we get need to know the key to revert the encryption.

Step 7: If a certain character is not a alphabet then do not change it.

Step 8: Return the value of the encrypted letter the empty variable Dn(x).

Step 9: Loop the process until each character from the cipher text has been decrypted to plaintext.

An example of encryptin a plaintext in to a ciphertext and decrypting it:

Encryption

Plaintext: Coursework

Shift value (k): 3

We know,

En(x) = (x + k) mod 26

C = C(2) + 3 = F

o = o(14) + 3 = r

u = u(20) + 3 = x

r = r(17) + 3 = u

s = s(18) + 3 = v

e = e(4) + 3 = h

w = w(22) + 3 = z

o = o(14) + 3 = r

r = r(17) + 3 = u

k = k(10) + 3 = n

Decryption

Ciphertext: Frxuvhzrun

We know,

Dn(x) = (x - k) mod 26

F = F(2) - 3 = C

r = r(14) - 3 = o

x = x(20) - 3 = u

u = u(17) - 3 = r

v = v(18) - 3 = s

h = h(4) - 3 = e

z = z(22) - 3 = w

r = r(14) - 3 = o

u = u(17) - 3 = r

n = n(10) - 3 = k

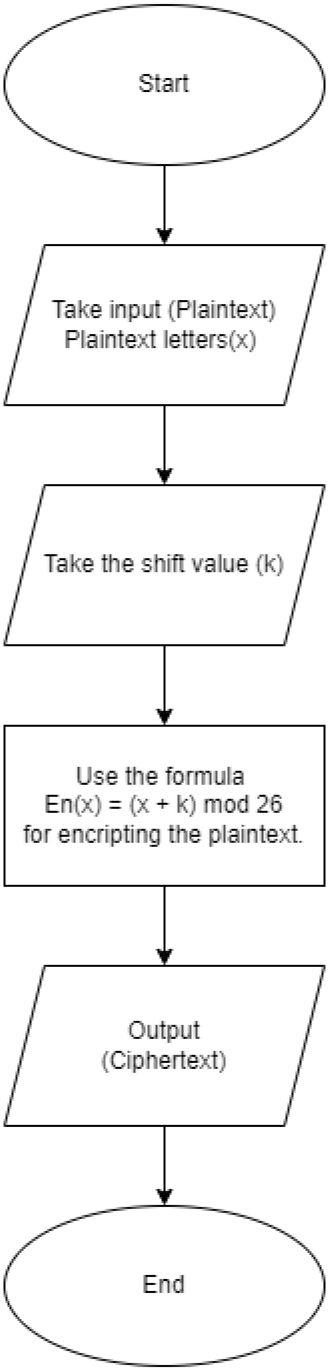

Figure 1: Caesar Cipher Encryption Flowchart

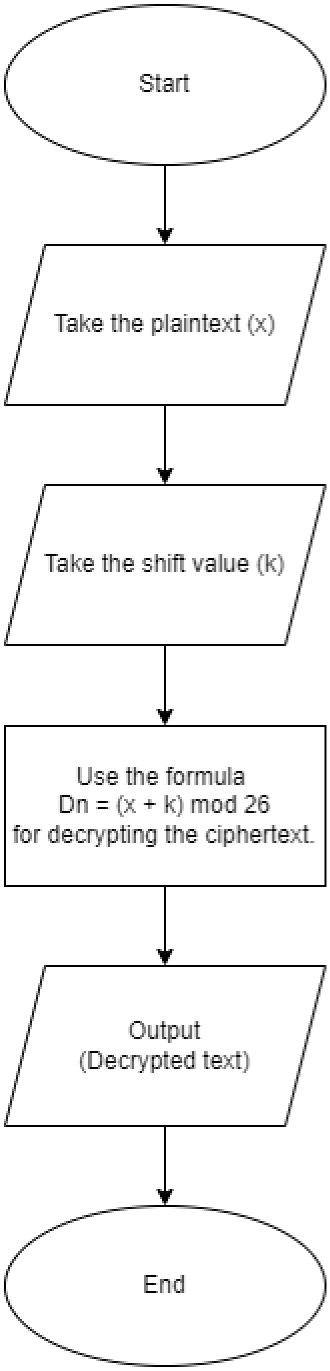

Figure 2: Caesar Cipher Decryption Flowchart.

2.1.2 Advantages of Caesar Cipher

- It is very easy to implement.

- This method is the simplest method of cryptography.
- Only one short key is used in its entire process.
- If a system does not use complex coding techniques, it is the best method for it.
- It requires only a few computing resources (Javapoint, 2021).

2.1.3 Disadvantages of Caesar Cipher

- It can be easily hacked. It means the message encrypted by this method can be easily decrypted.
- It provides very little security.
- By looking at the pattern of letters in it, the entire message can be decrypted (Javapoint, 2021).

2.2 Columnar Transposition Cipher

A transposition cipher is a technique for encrypting messages that involves moving letters around in a standard manner. Greater security and complexity can be achieved by combining the basic and straightforward columnar transposition cipher with a substitution cipher, which is susceptible to cracking. The columnar transposition cipher requires plain text to be set up in a table of columns, with each letter occupying one cell. To help with encryption, a keyword determines the width of the table (Rembert, 2021).

2.2.1 How does Columnar Transposition Cipher

Columnar Transposition Cipher uses the following steps for encryption:

Step 1: Take the input plaintext.

Step 2: Decide the amount of columns is required according to the plaintext and add a number to the top of each column.

Step 3: Place the plaintext horizontally in the rows of the column.

Step 4: If the rows of the column as filled than step down to the below row and fill the rows unit the plaintext as completely placed.

Step 5: After placing the plaintext in the rows and columns select the key by randomizing the column table numbers.

Step 6: Ensure that the key generated doesn’t have a number that is greater that the amount of columns itself.

Step 7: After the keys is place letter according to the key given.

Step 8: The cipher text should be written horizontally from the rows and move down applying the same process.

Columnar Transposition uses the following steps for decryption:

Step 1: Determine the same key that was used to encrypt the plaintext

Step 2: Determine the same amount of rows and column used in the encryption process.

Step 3: Arrange the columns in the ascending order.

Step 4: After placing the column according to their original or ascending order copy letters horizontally from the left.

Step 5: Repeat the following process until all the ciphertext have been converted from all the rows from top to the bottoms order wise.

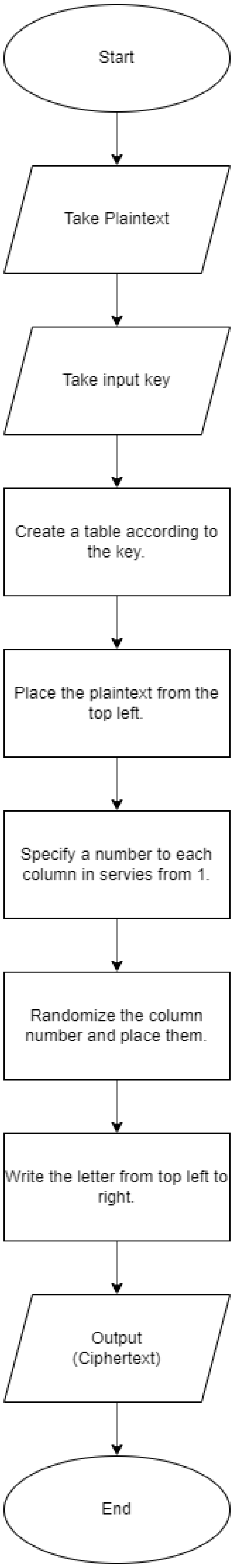
Start
Take Plaintext
Take input key
Create a table according to the key.
Place the plaintext from the top left.
Specify a number to each column in servies from 1.
Randomize the column number and place them.
Write the letter from top left to right.
Output (Ciphertext)
End

Figure 3: Columnar Transposition Cipher Encryption Flowchart

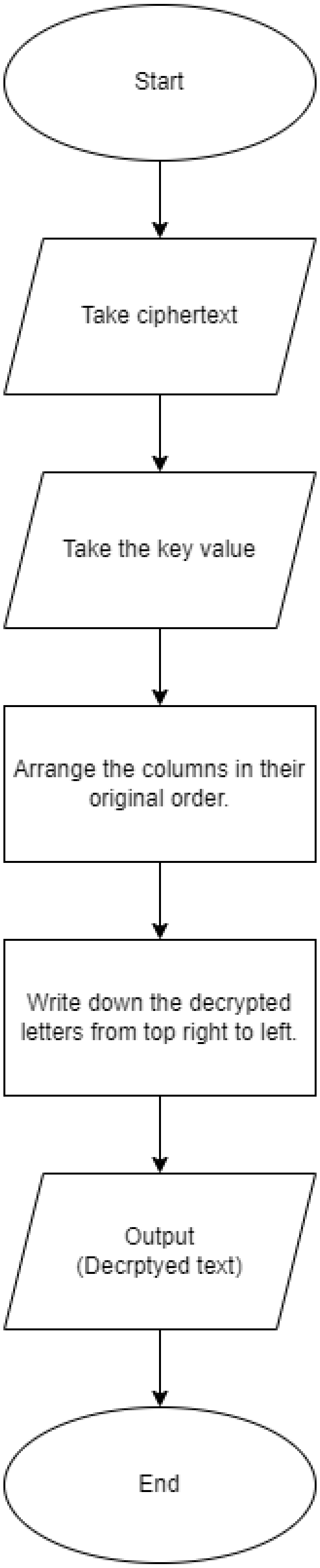
Start
Take ciphertext
Take the key value
Arrange the columns in their original order.
Write down the decrypted letters from top right to left.
Output
(Decrptyed text)
End

Figure 4: Columnar Transposition Cipher Decryption Flowchart.

An example of encrypting a plaintext in to a ciphertext and decrypting it:

Encryption

Plaintext: Coursework

Number of columns: 4

Key: 1342

Now,

1	2	3	4
C	o	u	r
s	e	w	o
r	k		

Now,

We encrypt the plain text using the given key.

1	3	4	2
C	u	r	o
s	w	o	e
r			k

Place the rows horizontally from left and from top to the bottom.

Therefore, the ciphertext is Curoswoerk.

Decryption

Ciphertext: Curoswoerk

Number of columns: 4

Key: 1342

We know,

The following table was used in the process of encryption.

1	3	4	2
C	u	r	o
s	w	o	e
r			K

Now, we revert the table back to its original state according to the key.

1	2	3	4
C	o	u	r
s	e	w	o
r	k		

Place the rows horizontally from left and from top to the bottom.

Therefore, the plaintext is Coursework.

2.2.2 Advantages and disadvantages of column transposition

Transposition ciphers don't require complicated algorithms, making them comparatively simple to comprehend and use. To generate encryption that is more secure, transposition ciphers can be used in conjunction with other cipher types. However, Transposition ciphers are rather weak on their own and can be cracked by pattern recognition or permutation guessing. A significant amount of the communication may become illegible due to a single encryption or transmission fault (Rembert, 2021).

2.3 Rail Fence Cipher

The rail fence cipher approach rearranges the characters of a message to produce a new, seemingly unrelated message. Our writing style is the inspiration for the name. The message is written in the first row of a table, the second letter is written in the second row, and so on, in order to encrypt a message using the rail fence method. In order to produce the encrypted message, we read the database row-wise (Datta, 2023).

In order to decode a message, we write the first letter in the first row, the second letter in the second row, and so on. We calculate the number of rows in the table based on the length of the encrypted message. Until every word in the message is typed, we keep going through this procedure (Datta, 2023).

The rail fence approach is comparatively easy to use, but even a rudimentary grasp of cryptography may readily break it, nor does it offer good protection. For straightforward communication, when a high level of security is not necessary, it can still be useful (Datta, 2023).

2.3.1 How does Rail Fence Cipher work?

Rail Fence Cipher uses the following steps for encryption:

Step 1: Take the input plaintext.

Step 2: Decide the amount of rows and columns to place the plain text

Step 3: Place the plaintext in a zigzag pattern starting from the left top. The zigzag pattern should form a v shape.

Step 4: If a cell in the rail fence table is empty then place it with a filler letter.

Step 5: After placing the plaintext in the rows and columns select the key by randomizing the column table numbers.

Step 6: After the rail is generated write the ciphertext from the top of the table vertically.

Step 7: Order wise following the process from the top row to the bottom row.

Rail Fence Cipher uses the following steps for decryption:

Step 1: Determine the number of rails used in the encryption.

Step 2: Create a table with rows and columns same as encryptionm table

Step 3: Arrange the rails in the zigzag pattern.

Step 4: After creating the same table with rows and column place the ciphertext letters in the patter horizontally.

Step 5: Repeat the following process from top row to the bottoms order wise until all ciphertext letter are filled.

Step 6: Finally, write down the letter in a zigzag pattern, after eliminating the filler and the ciphertext is decrypted.

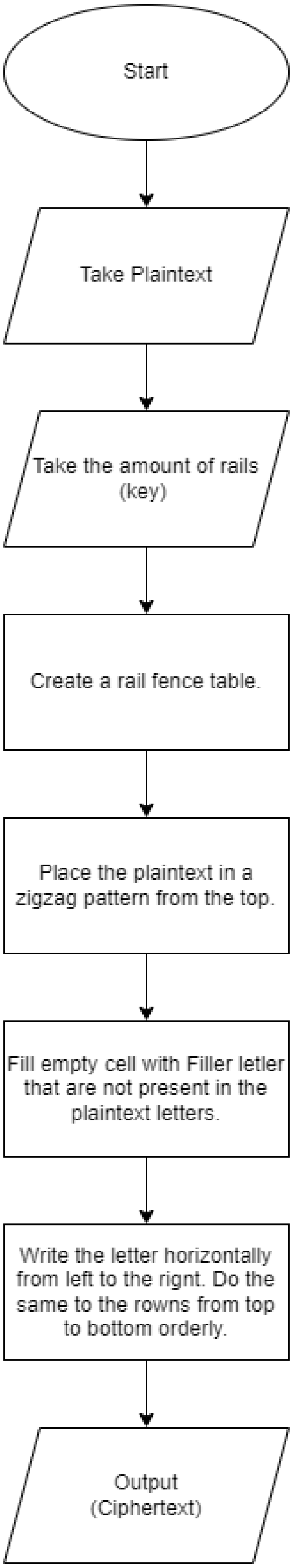
Start
Take Plaintext
Take the amount of rails (key)
Create a rail fence table.
Place the plaintext in a zigzag pattern from the top.
Fill empty cell with Filler letter that are not present in the plaintext letters.
Write the letter horizontally from left to the rignt. Do the same to the rowns from top to bottom orderly.
Output (Ciphertext)

Figure 5: Rail Fence Cipher Encryption Flowchart.

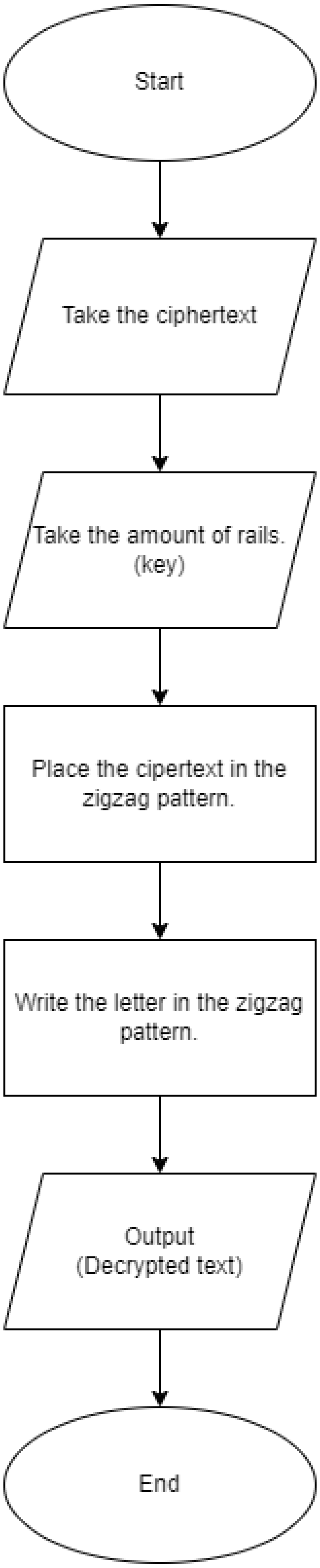
Start
Take the ciphertext
Take the amount of rails.
(key)
Place the cipertext in the zigzag pattern.
Write the letter in the zigzag pattern.
Output
(Decrypted text)
End

Figure 6: Rail Fence Cipher Decryption Flowchart.

An example of encrypting a plaintext in to a ciphertext and decrypting it:

Encryption

Plaintext: Coursework

Number of rails: 4

C						w			
	o				e		o		
		u		s				r	
			r						k

Table 1: Encryption Table for Rail Fence Cipher.

Therefore, the ciphertext is Cwoeousrrk

Decryption

We should create a table with same amount of rows and column. This is done so that the same amount of rails can be placed properly.

🟨						🟨			
	🟨				🟨		🟨		
		🟨		🟨				🟨	
			🟨						🟨

Table 2: Encryption Table Shades for Rail Fence Cipher.

Place the ciphertext horizontally in the highlighted cells rows wise from to the top to the bottom.

C						w			
	o				e		o		
		u		s				r	
			r						k

Table 3: Encrypted Rail Fence Cipher table.

Therefore, after decryption the result is Coursework.

2.3.2 Advantages of Rail Fence Cipher

The rail fence technique is a straightforward and user-friendly approach that provides simplicity and versatility. It is appropriate for basic communication without having strict security needs since it is simple to implement without the need for specialist hardware or software. Users may select the right amount of complexity based on their demands, as the approach can be applied with arbitrary numbers of rows.

2.3.3 Disadvantages of Rail Fence Cipher

The rail fence method is an insecure encryption technology that is open to intrusions. With a rudimentary understanding of cryptography, it may be quickly cracked, and its efficacy decreases with longer communications. It is also open to assaults by adversaries due to its susceptibility to known-plaintext attacks.

3. Development

Caesar Cipher itself is a very weak method of symmetric encryption system. This system was created around 1900 BC. This System uses only shifting method which can be easily decrypted which is why some modification process were implemented. In the following cipher that I have created consists of Caesar Cipher which uses shifting method, Columnar Transposition Cipher that uses rearrangement method and Rail Fence Cipher which uses the number of rails provided by the user.

3.1 Why is it necessary?

This cipher is necessary as Caesar Cipher alone cannot create a strong ciphertext. This cipher uses three types of Cipher process to encrypt a plaintext which is stronger than Caesar cipher. Caesar Cipher is mod 26 arithmetic that uses 26 alphabets. But, the addition to Caesar cipher this cipher uses Re-arranging method which replaces the plaintext letters, the mod 26 arithmetic implies a rule that ensures that the ciphertext doesn’t have unnecessary letters making the ciphertext simple for the users. Finally, Rail Fencing Cipher randomizes the already encrypted text furthermore.

3.2 The new modification Haze

In this cipher the first encryption is done through Caesar Cipher which shifts the value of the plaintext encrypting it. After the encryption takes place the ciphertext is encrypted again using Rail fence that randomizes the letters and finally Columnar Transposition Cipher is used to further to randomize the position by arranging the letters. This Cipher process makes attackers hard to crack the plaintext. This Cipher can be effective as encryption process are done plenty of time. To decrypt the ciphertext we would need three keys.

4. Algorithm and flowchart

Encryption:

Step 1: Take the input plaintext.

Step 2: Take the shift value (k) to ensure the amount to be shifted.

Step 3: Ensure if the shift value (k) is in between 0 to 25.

Step 4: Create a empty variable En(x) to store the result of the encryption.

Step 5: Determine if the character given to encrypt is a proper alphabet or not and if the character is within the key from 0 to 25.

Step 6: Apply the formula i.e. [En(x) = (x + k) mod 26] to the following letter.

Step 7: Maintain the case of the letter (uppercase or lowercase).

Step 8: If a certain character is not a alphabet then do not change it.

Step 9: Return the value of the encrypted letter the empty variable En(x).

Step 10: Loop the process until each character from the plain text has been converted into ciphertext.

Step 11: Take Ciphertext and use it as plaintext for columnar transposition cipher encryption.

Step 12: Decide the amount of columns is required according to the plaintext and add a number to the top of each column.

Step 13: Place the plaintext horizontally in the rows of the column.

Step 14: If the rows of the column as filled than step down to the below row and fill the rows unit the plaintext as completely placed.

Step 15: After placing the plaintext in the rows and columns select the key by randomizing the column table numbers.

Step 16: Ensure that the key generated doesn’t have a number that is greater than the amount of columns itself.

Step 17: After the keys is place letter according to the key given.

Step 18: The cipher text should be written horizontally from the rows and move down applying the same process.

Step 19: Take Ciphertext and use it as plaintext for Rail Fence Cipher encryption.

Step 20: Decide the amount of rows and columns to place the plain text

Step 21: Place the plaintext in a zigzag pattern starting from the left top. The zigzag pattern should form a v shape.

Step 22: If a cell in the rail fence table is empty then place it with a filler letter.

Step 23: After placing the plaintext in the rows and columns select the key by randomizing the column table numbers.

Step 24: After the rail is generated write the ciphertext from the top of the table vertically.

Step 25: Order wise following the process from the top row to the bottom row and the ciphertext is generated.

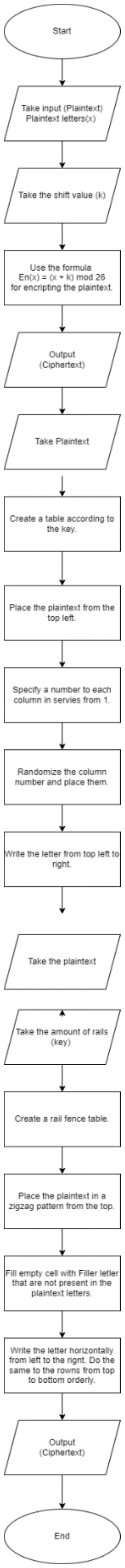
Start
Take input (Plaintext)
Plaintext letters(x)
Take the shift value (k)
Use the formula
En(x) = (x + k) mod 26
for encripting the plaintext.
Output
(Ciphertext)
Take Plaintext
Create a table according to the key.
Place the plaintext from the top left.
Specify a number to each column in servies from 1.
Randomize the column number and place them.
Write the letter from top left to right.
Take the plaintext
Take the amount of rails (key)
Create a rail fence table.
Place the plaintext in a zigzag pattern from the top.
Fill empty cell with Filler letler that are not present in the plaintext letters.
Write the letter horizontally from left to the rignt. Do the same to the rowns from top to bottom orderly.
Output
(Ciphertext)
End

Figure 7: Flowchart of encryption of "Haze"

Decryption:

Step 1: Determine the number of rails used in the encryption.

Step 2: Create a table with rows and columns same as encryptionm table

Step 3: Arrange the rails in the zigzag pattern.

Step 4: After creating the same table with rows and column place the ciphertext letters in the patter horizontally.

Step 5: Repeat the following process from top row to the bottoms order wise until all ciphertext letter are filled.

Step 6: Finally, write down the letter in a zigzag pattern, after eliminating the filler and the ciphertext is decrypted.

Step 7: Take the ciphertext and use the Columnar Transposition Cipher decryption process.

Step 8: Determine the same key that was used to encrypt the plaintext

Step 9: Determine the same amount of rows and column used in the encryption process.

Step 10: Arrange the columns in the ascending order.

Step 11: After placing the column according to their original or ascending order copy letters horizontally from the left.

Step 12: Repeat the following process until all the ciphertext have been converted from all the rows from top to the bottoms order wise.

Step 13: Take the ciphertext and use it for Caesar cipher decryption process.

Step 14: Take the ciphertext.

Step 15: Take the shift value (k).

Step 16: Ensure if the shift value (k) is in between 0 to 25.

Step 17: Create a empty variable Dn(x) to store the result of the decryption process.

Step 18: Determine if the character given to encrypt is a proper alphabet or not and if the character is within the the key from 0 to 25.

Step 19: Apply the formula i.e. [Dn(x) = (x - k) mod 26] to the following letter. The formula is similar to encryption but in this process we get need to know the key to revert the encryption.

Step 20: If a certain character is not a alphabet then do not change it.

Step 21: Return the value of the encrypted letter the empty variable Dn(x).

Step 22: Loop the process until each character from the cipher text has been decrypted to plaintext.

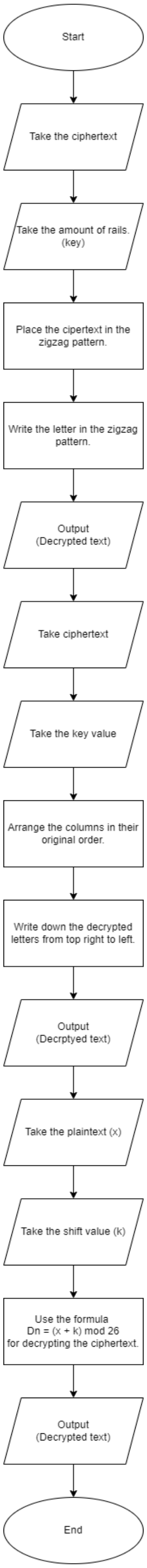
Start
Take the ciphertext
Take the amount of rails. (key)
Place the cipertext in the zigzag pattern.
Write the letter in the zigzag pattern.
Output (Decrypted text)
Take ciphertext
Take the key value
Arrange the columns in their original order.
Write down the decrypted letters from top right to left.
Output (Decrptyed text)
Take the plaintext (x)
Take the shift value (k)
Use the formula Dn = (x + k) mod 26 for decrypting the ciphertext.
Output (Decrypted text)
End

Figure 8: Flowchart of decryption of "Haze".

5. Testing

5.1 Test A

Encryption

Using Caesar Cipher with the shift value 5 to encrypt the plaintext.

Plaintext: FRANKLIN

Shift Value (k): 5

The following formula is used to encrypt the plain text

(x + k) mod 26 = En(x)

F + 5 = K

R + 5 = W

A + 5 = F

N + 5 = S

K + 5 = P

L + 5 = Q

I + 5 = N

N + 5 = S

Ciphertext: KWFSPQNS

Using Columnar Transposition to encrypt the plaintext.

Plaintext: KWFSPQNS

Number of column: 3

Shift Value: 312

The following column is used to encrypt the plaintext.

1	2	3
K	W	F
S	P	Q
N	S	

Table 4: Test A Columnar Transposition Cipher table.

3	1	2
F	K	W
Q	S	P
	N	S

Table 5: Test A Encrypted Columnar Transposition Cipher table.

Ciphertext: FKWQSPNS

Using Rail Fence Cipher to encrypt the plaintext with key value 3 (Number of rails).

Plaintext: FKWQSPNS

Key (Number of rails): 3

The following table is used to encrypt the plaintext.

F				S				X
	K		Q		P		S	
		W				N		

Table 6: Test Rail Fence Cipher Encrypted table.

Ciphertext: FSXKQPSWN

Decryption

Using Rail Fence Cipher Table to decrypt the ciphertext by placing them in the same rails as the encryption process.

Ciphertext: FSXKQPSWN

Key (Number of rails): 3

F				S				X
	K		Q		P		S	
		W				N		

Table 7: Test A Decrypted Columnar Transposition Cipher table.

Remove the filler letter.

Plaintext: FKWQSPNS

Using Columnar Transposition to encrypt the plaintext.

Ciphertext: FKWQSPNS

Shift Value: 312

The following column is used to encrypt the plaintext.

3	1	2
F	K	W
Q	S	P
	N	S

Table 8: Test Columnar Transposition Cipher table

1	2	3
K	W	F
S	P	Q
N	S	

Table 9: Test A Decrypted Columnar Transposition Cipher table

Plaintext: KWFSPQNS

Using Caesar Cipher with the shift value 5 to decrypt the ciphertext.

Ciphertext: KWFSPQNS

Shift Value (k): 5

The following formula is used to encrypt the plain text

(x - k) mod 26 = Dn(x)

K + 5 = F

W + 5 = R

F + 5 = A

S + 5 = N

K + 5 = K

Q + 5 = L

N + 5 = I

S + 5 = N

Plaintext: FRANKLIN

5.2 Test B

Encryption

Using Caesar Cipher with the shift value 7 to encrypt the plaintext.

Plaintext: SZOBOSZLAI

Shift Value (k): 7

The following formula is used to encrypt the plain text

(x + k) mod 26 = En(x)

S + 7 = Z

Z + 7 = G

O + 7 = V

B + 7 = I

O + 7 = V

S+ 7 = Z

Z + 7 = G

L + 7 = S

A + 7 = H

I + 7 = P

Ciphertext: ZGVIVZGSHP

Using Columnar Transposition to encrypt the plaintext.

Plaintext: ZGVIVZGSHP

Number of column: 4

Shift Value: 2134

The following column is used to encrypt the plaintext.

1	2	3	4
Z	G	V	I
V	Z	G	S
H	P		

Table 10: Test B Columnar Transposition Cipher table.

2	1	3	4
G	Z	V	I
Z	V	G	S
P	H		

Table 11: Test B Encrypted Columnar Transposition Cipher table

Ciphertext: GZVIZVGSPH

Using Rail Fence Cipher to encrypt the plaintext with key value 4 (Number of rails).

Plaintext: GZVIZVGSPH

Key (Number of rails): 4

The following table is used to encrypt the plaintext.

G						G			
	Z				V		S		
		V		Z				P	
			I						H

Table 12: Test B Encrypted Rail Fence Cipher table

Ciphertext: GGZVSVZPIKH

Decryption

Using Rail Fence Cipher Table to decrypt the ciphertext by placing them in the same rails as the encryption process.

Ciphertext: GGZVSVZPIKH

Key (Number of rails): 4

G						G			
	Z				V		S		
		V		Z				P	
			I						H

Table 13: Test B Decrypted Rail Fence Cipher table

Plaintext: GZVIZVGSPH

Using Columnar Transposition to encrypt the plaintext.

Ciphertext: GZVIZVGSPH

Shift Value: 2134

The following column is used to encrypt the plaintext.

2	1	3	4
G	Z	V	I
Z	V	G	S
P	H		

Table 14: Test B Columnar Transposition Cipher table

1	2	3	4
Z	G	V	I
V	Z	G	S
H	P		

Table 15:Test B Decrypted Columnar Transposition Cipher table

Plaintext: ZGVIVZGSHP

Using Caesar Cipher with the shift value 7 to decrypt the ciphertext.

Ciphertext: ZGVIVZGSHP

Shift Value (k): 7

The following formula is used to encrypt the plain text

(x - k) mod 26 = Dn(x)

Z - 7 = S

G - 7 = Z

V - 7 = O

I - 7 = B

V - 7 = O

Z - 7 = S

G - 7 = Z

S - 7 = L

H - 7 = A

P - 7 = I

Plaintext: SZOBOSZLAI

5.3 Test C

Encryption

Using Caesar Cipher with the shift value 2 to encrypt the plaintext.

Plaintext: ENCHANTRESS

Shift Value (k): 2

The following formula is used to encrypt the plain text

(x + k) mod 26 = En(x)

E + 2 = G

N + 2 = P

C + 2 = E

H + 2 = J

A + 2 = C

N + 2 = P

T + 2 = V

R + 2 = T

E + 2 = G

S + 2 = U

S + 2 = U

Ciphertext: GPEJCPVTGUU

Using Columnar Transposition to encrypt the plaintext.

Plaintext: GPEJCPVTGUU

Number of column: 5

Shift Value: 54321

The following column is used to encrypt the plaintext.

1	2	3	4	5
G	P	E	J	C
P	V	T	G	U
U				

Table 16: Test C Columnar Transposition Cipher table

5	4	3	2	1
C	J	E	P	G
U	G	T	V	P
				U

Table 17: Test C Encrypted Columnar Transposition Cipher table

Ciphertext: CJEPGUGTVPU

Using Rail Fence Cipher to encrypt the plaintext with key value 5 (Number of rails).

Plaintext: CJEPGUGTVPU

Key (Number of rails): 5

The following table is used to encrypt the plaintext.

C								V				
	J						T		P			
		E				G				U		
			P		U						X	
				G								F

Table 18: Test C Encrypted Rail Fence Cipher table

Ciphertext: CVJTPEGUPUXGF

Decryption

Using Rail Fence Cipher Table to decrypt the ciphertext by placing them in the same rails as the encryption process.

Ciphertext: ATHRNCESNSXEF

Key (Number of rails): 5

C								V				
	J						T		P			
		E				G				U		
			P		U						X	
				G								F

Table 19: Test C Decrypted Rail Fence Cipher table

Remove the filler letter.

Plaintext: CJEPGUGTVPU

Using Columnar Transposition to encrypt the plaintext.

Ciphertext: CJEPGUGTVPU

Shift Value: 54321

The following column is used to encrypt the plaintext.

5	4	3	2	1
C	J	E	P	G
U	G	T	V	P
				U

Table 20: Test C Columnar Transposition Cipher table

1	2	3	4	5
G	P	E	J	C
P	V	T	G	U
U				

Table 21: Test C Decrypted Columnar Transposition Cipher table

Plaintext: GPEJCPVTGUU

Using Caesar Cipher with the shift value 2 to decrypt the ciphertext.

Ciphertext: KWFSPQNS

Shift Value (k): 5

The following formula is used to encrypt the plain text

(x - k) mod 26 = Dn(x)

G - 2 = E

P - 2 = N

E - 2 = C

J - 2 = H

C - 2 = A

P - 2 = N

V - 2 = T

T - 2 = R

G - 2 = E

U - 2 = S

U - 2 = S

Plaintext: ENCHANTRESS

5.4 Test D

Encryption

Using Caesar Cipher with the shift value 1 to encrypt the plaintext.

Plaintext: BOWLER

Shift Value (k): 1

The following formula is used to encrypt the plain text

(x + k) mod 26 = En(x)

B + 1 = C

O + 1 = P

W + 1 = X

L + 1 = M

E + 1 = F

R + 1 = S

Ciphertext: CPXMFS

Using Columnar Transposition to encrypt the plaintext.

Plaintext: CPXMFS

Number of column: 2

Shift Value: 21

The following column is used to encrypt the plaintext.

1	2
C	P
X	M
F	S

Table 22: Test D Columnar Transposition Cipher table.

2	1
P	C
M	X
S	F

Table 23: Test D Encrypted Columnar Transposition Cipher table.

Ciphertext: PCMXSF

Using Rail Fence Cipher to encrypt the plaintext with key value 2 (Number of rails).

Plaintext: PCMXSF

Key (Number of rails): 2

The following table is used to encrypt the plaintext.

P		M		S	
	C		X		F

Table 24: Test D Encrypted Rail Fence Cipher table

Ciphertext: PMSCXF

Decryption

Using Rail Fence Cipher Table to decrypt the ciphertext by placing them in the same rails as the encryption process.

Ciphertext: PMSCXF

Key (Number of rails): 2

P		M		S	
	C		X		F

.Table 25: Test D Decrypted Rail Fence Cipher table

Plaintext: PCMXSF

Using Columnar Transposition to encrypt the plaintext.

Ciphertext: PCMXSF

Shift Value: 54321

The following column is used to encrypt the plaintext.

2	1
P	C
M	X
S	F

Table 26: Test D Columnar Transposition Cipher table.

1	2
C	P
X	M
F	S

Table 27: Test D Decrypted Columnar Transposition Cipher table.

Plaintext: CPXMFS

Using Caesar Cipher with the shift value 1 to decrypt the ciphertext.

Ciphertext: CPXMFS

Shift Value (k): 1

The following formula is used to encrypt the plain text

(x - k) mod 26 = Dn(x)

C - 1 = B

P - 1 = O

X - 1 = W

M - 1 = L

F - 1 = E

S - 1 = R

Plaintext: BOWLER

5.5 Test E

Encryption

Using Caesar Cipher with the shift value 5 to encrypt the plaintext.

Plaintext: JORMUNGANDR

Shift Value (k): 8

The following formula is used to encrypt the plain text

(x + k) mod 26 = En(x)

J + 8 = R

O + 8 = W

R + 8 = Z

M + 8 = U

U + 8 = C

N + 8 = V

G + 8 = O

A + 8 = I

N + 8 = V

D + 8 = L

R + 8 = Z

Ciphertext: RWZUCVOIVLZ

Using Columnar Transposition to encrypt the plaintext.

Plaintext: RWZUCVOIVLZ

Number of column: 4

Shift Value: 1423

The following column is used to encrypt the plaintext.

1	2	3	4
R	W	Z	U
C	V	O	I
V	L	Z	

Table 28: Test E Columnar Transposition Cipher table.

1	4	2	3
R	U	W	Z
C	I	V	O
V		L	Z

Table 29: Test E Encryption Columnar Transposition Cipher table.

Ciphertext: RUWZCIVOVLZ

Using Rail Fence Cipher to encrypt the plaintext with key value 4 (Number of rails).

Plaintext: RUWZCIVOVLZ

Key (Number of rails): 4

The following table is used to encrypt the plaintext.

R						V						B
	U				I		O				A	
		W		C				V		Z		
			Z						L			

Table 30: Test E Encrypted Rail Fence Cipher table

Ciphertext: RVBUIOAWCVZZL

Decryption

Using Rail Fence Cipher Table to decrypt the ciphertext by placing them in the same rails as the encryption process.

Ciphertext: RVBUIOAWCVZZL

Key (Number of rails): 4

R						V						B
	U				I		O				A	
		W		C				V		Z		
			Z						L			

Table 31: Test B Decrypted Rail Fence Cipher table

Remove the filler letter.

Plaintext: RUWZCIVOVLZ

Using Columnar Transposition to encrypt the plaintext.

Ciphertext: RUWZCIVOVLZ

Shift Value: 1423

The following column is used to encrypt the plaintext.

1	4	2	3
R	U	W	Z
C	I	V	O
V		L	Z

Table 32: Test E Columnar Transposition Cipher table.

1	2	3	4
R	W	Z	U
C	V	O	I
V	L	Z	

Table 33: Test E Decrypted Columnar Transposition Cipher table.

Plaintext: RWZUCVOIVLZ

Using Caesar Cipher with the shift value 5 to decrypt the ciphertext.

Ciphertext: RWZUCVOIVLZ S

Shift Value (k): 8

The following formula is used to encrypt the plain text

(x - k) mod 26 = Dn(x)

R - 8 = J

W - 8 = O

Z - 8 = R

U - 8 = M

C - 8 = U

V - 8 = N

O - 8 = G

I - 8 = A

V - 8 = N

L - 8 = D

Z - 8 = R

Plaintext: JORMUNGANDR

6. Evaluation of “Haze”

6.1 Strength of “Haze”

- It has improved security since the cipher consists of three cipher’s encryption because of its multi-layer security.
- It focuses on maintaining confidentiality, availability and integrity.
- It introduces complexity by applying different encryption techniques.
- It has resistance to Known-Plain text attacks
- It can be integrated into various systems and applications that require robust encryption. Its adaptability makes it suitable for diverse use cases where data security is paramount.

6.2 Weakness of “Haze”

- It is limited to 26 alphabetical characters
- It uses symmetric encryption
- It relies on symmetric encryption for its initial layer, lacking the benefits of a public key infrastructure. This absence makes secure key exchange and communication between parties more challenging
- It does not function properly in real world as the cipher that have been used are old and have may decryption processes.
- Its resistance to quantum computing attacks is not guaranteed. As quantum computing capabilities advance, traditional encryption methods may become more susceptible, potentially compromising the security.

6.3 Applications

- Researchers and cryptographers can utilize the Cipher to conduct experiments and analyses. It may be used to investigate the strengths and weaknesses of various cryptographic levels, identify potential flaws, and get a better knowledge of encryption systems.

- The Cipher may be used to compare the performance of various encryption schemes. Researchers can learn about each layer's strengths and weaknesses by assessing its resistance to various cryptanalysis techniques.
- The Cipher's modular architecture enables developers to experiment with and alter individual layers. This might be a starting point for developing unique encryption methods customized to specific needs.

7. Conclusion

The "Haze" encryption method provides a robust solution for information security by combining three cryptographic techniques – Caesar Cipher, Columnar Transposition Cipher, and Rail Fence Cipher. This multi-layered approach addresses the shortcomings of individual methods, enhancing the overall security of data in computing environments. Rooted in the principles of confidentiality, integrity, and availability (CIA triad), Haze offers a nuanced strategy that evolves cryptography beyond historical limitations.

The historical overview of cryptography highlights the constant quest for secure practices, from ancient ciphers to modern methodologies. Haze, as a product of this evolution, exemplifies the need for adaptive and fortified encryption strategies in response to contemporary cybersecurity challenges.

Developed to overcome vulnerabilities in Caesar Cipher, Haze introduces complexity by requiring multiple keys for decryption, significantly strengthening its resistance to unauthorized access. This aligns with the dynamic defense requirements of modern cybersecurity landscapes.

As organizations face increasingly sophisticated cyber threats, the adoption of layered encryption mechanisms becomes crucial. Haze, with its intricate combination of cryptographic elements, emerges as a reliable safeguard for sensitive information, urging a shift toward integrated encryption strategies for a more secure digital future.

8. References

Bibliography

Cobb, M., 2021. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchsecurity/definition/physical-security#:~:text=Physical%20security%20is%20the%20protection,an%20enterprise%2C%20agency%20or%20institution.
[Accessed 12 December 2023].

Codecademy Team, 2023. *Codecademy.* [Online]
Available at: https://www.codecademy.com/resources/blog/what-is-hashing/
[Accessed 12 December 2023].

Codedamn, 2023. *Codedamn.* [Online]
Available at: https://codedamn.com/news/cryptography/caesar-cipher-introduction
[Accessed 13 December 2023].

Datta, S., 2023. *Baeldung.* [Online]
Available at: https://www.baeldung.com/cs/cryptography-rail-fence-technique
[Accessed 20 December 2023].

Fasulo, P., 2021. *SecurityScoreCard.* [Online]
Available at: https://securityscorecard.com/blog/what-is-the-cia-triad/
[Accessed 12 December 2023].

Fruhlinger, J., 2022. *csoonline.* [Online]
Available at: https://www.csoonline.com/article/569921/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html
[Accessed 13 December 2023].

Harmening, J. T., 2017. *ScienceDirect.* [Online]
Available at: https://www.sciencedirect.com/topics/computer-science/symmetric-encryption
[Accessed 12 December 2023].

Javapoint, 2021. *Javapoint.* [Online] Available at: https://www.javatpoint.com/caesar-cipher-technique
[Accessed 13 December 2023].

Kelly, K., 2023. *Simplilearn.* [Online] Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security
[Accessed 12 December 2023].

Loshin, P., 2022. *TechTarget.* [Online] Available at: https://www.techtarget.com/searchsecurity/definition/encryption
[Accessed 12 December 2023].

Rembert, L., 2021. *Privacy Canada.* [Online] Available at: https://privacycanada.net/columnar-transposition-cipher/
[Accessed 18 December 2023].

Roohparvar, R., 2020. *infoguardsecurity.* [Online] Available at: https://www.infoguardsecurity.com/what-is-information-security-definition-principles-and-policies/
[Accessed 12 December 2023].

Sidhpurwala, H., 2023. *Red Hat.* [Online] Available at: https://www.redhat.com/en/blog/brief-history-cryptography#:~:text=The%20first%20known%20evidence%20of,nobleman%20Khnumhotep%20II%2C%20in%20Egypt.
[Accessed 13 December 2023].