Report on Transposition Cipher

26 June 2024
Cryptography

Sthuthi V. Soans
MIST Manipal

TABLE OF CONTENTS

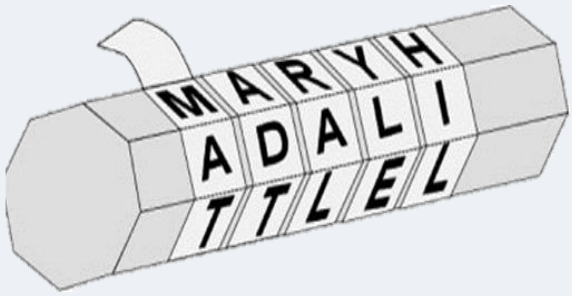
1. INTRODUCTION

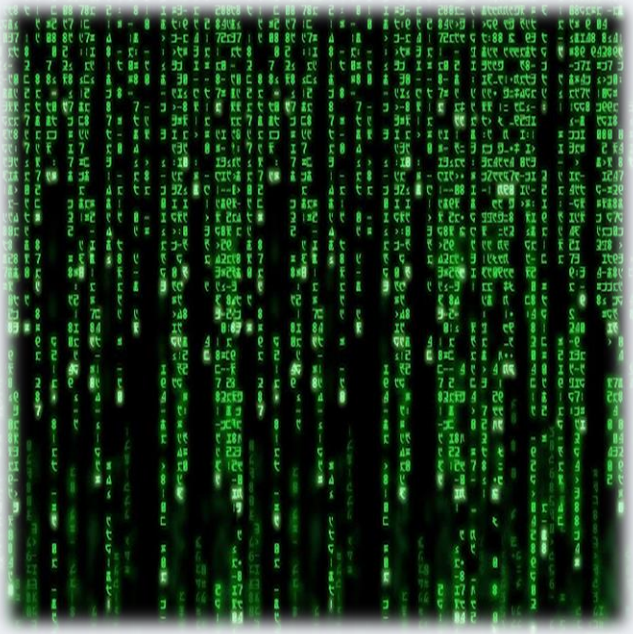
Cryptography is the process of hiding or coding data so that only the receiver for whom the message was intended can read it. The art of cryptography has been an age-old practice wherein kings, officials, police etc. could send secret messages to someone else. Modern cryptography includes algorithms that allow encryption and decryption of the information. These encryption algorithms are known as Ciphers. A cipher converts the plaintext (message) into ciphertext (encrypted text) using a key to determine how it is done.

Transposition Ciphers are essential part of cryptography where the positions of characters in the plaintext (message) is simply rearranged and encrypted into a ciphertext. There are many types of transposition ciphers. In this comprehensive report, we will dive into the details of these types of transposition ciphers.

2. HISTORY

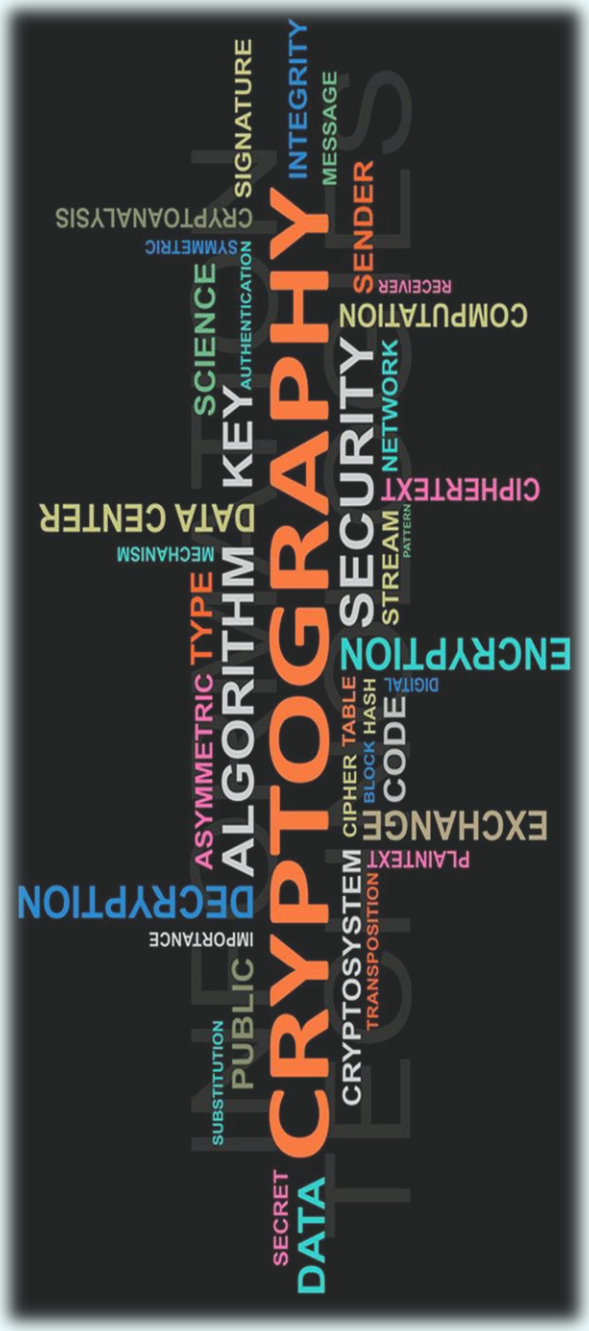
Cryptography is not a newly invented process but has been used in the past with different terms to describe it. One of the oldest known implementations of the transposition cipher was the Spartan Scytale. In ancient Greece (around 475 BC), the spartan army commanders created a scytale, a device they designed for sending secret messages and information.





The army commanders would wrap a strip of parchment or leather around the Scytale wooden staff. They would then write the secret message along the length of the staff. The message would then be unwound from the staff and delivered to another commander. The receiving commander would then take his identical Scytale and would wrap the message strip around it to reveal the secret message. This repositioning technique is one of the earliest known transposition ciphers.

3. DESCRIPTION



Transposition cipher is a method of shuffling characters within the plaintext to create the cipher text, whereas Substitution cipher involves the process of substituting a character of plaintext with another character.

Transposition cipher is one of the simplest ciphers used in cryptography.

3.1 Rail Fence Cipher

This is one of the simplest transposition cipher techniques. It is also termed as zig zag cipher.

In rail fence cipher, the plaintext is written diagonally from up to down on successive rails. When we reach the bottom of the rail, we traverse upwards diagonally. After reaching the top of the rails, we traverse downwards again. The process continues until plaintext finishes.

The spaces between the words are also considered while writing the plaintext on the rails. The rails are determined by the *Key*. The value of the key tells us how many rails have to be made in each diagonal column.

Finally, the text can be encrypted by grouping all the rows separately. Decryption can be done in the same manner.

3.2 Route Cipher

Route cipher is a transposition cipher where the key is which *route* to follow when reading the cipher text from the block created with the plaintext. The plaintext is written in a grid and then read off following the route chosen.

Route cipher was used in the past by the *Union forces* during the American Civil War. It was called the *Union Route Cipher* back then.

For *encryption*, we write the plaintext in a block of reasonable size for the plaintext. Part of your key is the size of this grid, so you need to decide on either a number of columns or number of rows in the grid before starting. Once the plaintext is written out in the grid, you use the Route assigned. This could be spiraling inwards from the top right corner in a clockwise direction, or zigzagging up and down.

To *decrypt* a message received that has been encoded with the Route Cipher, we need to know the route used and the width or height of the grid. We then start by constructing a blank grid of the right size, and then place the ciphertext letters in the grid following the route specified.

Route cipher can be customized by changing the number of rows and columns used to rearrange the letters and also it can be combined with other encryption techniques like substitution cipher or encryption algorithms to increase security. One of the weaknesses of route cipher is that it is vulnerable to brute force attacks as well as frequency analysis attacks.

3.3 Columnar Cipher

Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one. The width of the rows and the permutation of the columns are usually defined by a keyword. The message is written out in rows of a fixed length, and then read out column by column, and the columns are chosen in some random order.

For *encryption*, the keyword is first written in the form of a grid, where each character is in a different column (thus making the number of columns equal to the number of characters in the keyword). Now we need to fill in the grid with the plaintext which is written row wise. The ciphertext is created by reading the characters in each column separately.

To determine the order of the column, we can consider the position of the characters in the keyword in the alphabetical order. Thus, we get the encoded text.

For *decryption*, first of all we need to write down the keyword in alphabetical order. Then we need to divide the entire encrypted text by the number of characters in the keyword; this determines the number of rows in the grid. Then we need to start writing the ciphertext column wise under the keyword (in the encryption process we wrote the text row wise, whereas here we need to write it column wise). On completing the grid, we can receive the decrypted text.

One of the key benefits of a transposition cipher over a substitution cipher is that they can be applied more than once. For example, the columnar transposition cipher could be applied twice on the plaintext which is called *Double Columnar Cipher*. This double transposition increases the security of the cipher significantly. It could also be implemented with a different keyword for the second iteration of the cipher.

3.4 Grille Cipher

The Grille Cipher also known as the *Cardan Grille*, is a transposition cipher that uses a physical template, or "grille," to determine where characters should be placed in the plaintext. Over a blank grid, a sheet with holes cut out serves as the grille. There is a set order in which characters are written into the holes. The remaining grid is subsequently filled in by rotating or moving the grille, which results in the ciphertext.

The Fleissner Grille is a variation of grilles that was described by Baron Edouard Fleissner von Wostrowitz in the 1880s, and used in World War I. It's based on the 8x8 grid of the chess board.

For *encryption*, firstly, holes are cut out of a grille according to a specified pattern. The size of the grid determines the size of the grille and the number of holes. The plaintext message is written into the holes of the grille, which is positioned above a blank grid. The grille is rotated or moved to a different location after the initial placement. Then, the following plaintext section is inserted into the freshly created holes. Until the full grid is filled, these steps are repeated. After all of the plaintext characters have been added to the grid, the grid is read in a predefined order to create the ciphertext (row wise or column wise).

3.5 Myszkowski Cipher

Myszkowiski Cipher was proposed by Émile Victor Théodore Myszkowski in 1902. It is same as columnar cipher but there is a slight change in the process that takes place when the keyword has two or more same characters.

For *encryption*, we have to choose our keyword. We then write out the plaintext in a grid, where the number of columns in the grid is the number of letters in the keyword (same as columnar cipher). We then number each letter in the keyword with its alphabetical position, giving repeated letters the same numbers. We then start at number 1 (the first letter alphabetically in the keyword), and if it is the only appearance of 1, we read down the column just like in columnar transposition. If, anyhow, the number 1 appears more than once, we read from left to right all the first letters of the columns headed by 1. Then we move to the next row, and read across, left to right, the letters in the rows headed by 1. Once complete, we move on to the number 2, and so on.

For *decryption*, the process is again same as columnar cipher, but the change occurs when we have a keyword with 2 or more characters that are repeating. At that situation, we move from left to right across the columns with that number heading them i.e. we fill in the rows of the repeating characters one by one and then continue filling the columns for the rest of the characters.

3.6 Disrupted Transposition Cipher

Disrupted transposition cipher is another variant of the columnar cipher. Here, we purposely add extra spaces or random alphabets in between the plaintext in the grid. These spaces are sometimes filled with another part of the plaintext. It helps make the message safer as we randomly disrupt the original process of columnar cipher, thus making it more complicated.

4. ILLUSTRATIONS

Let us now look at some examples for the above-mentioned ciphers:

4.1 Rail Fence Cipher

Let us take the *key* to be '3'.

The plain text: Manipal Mist

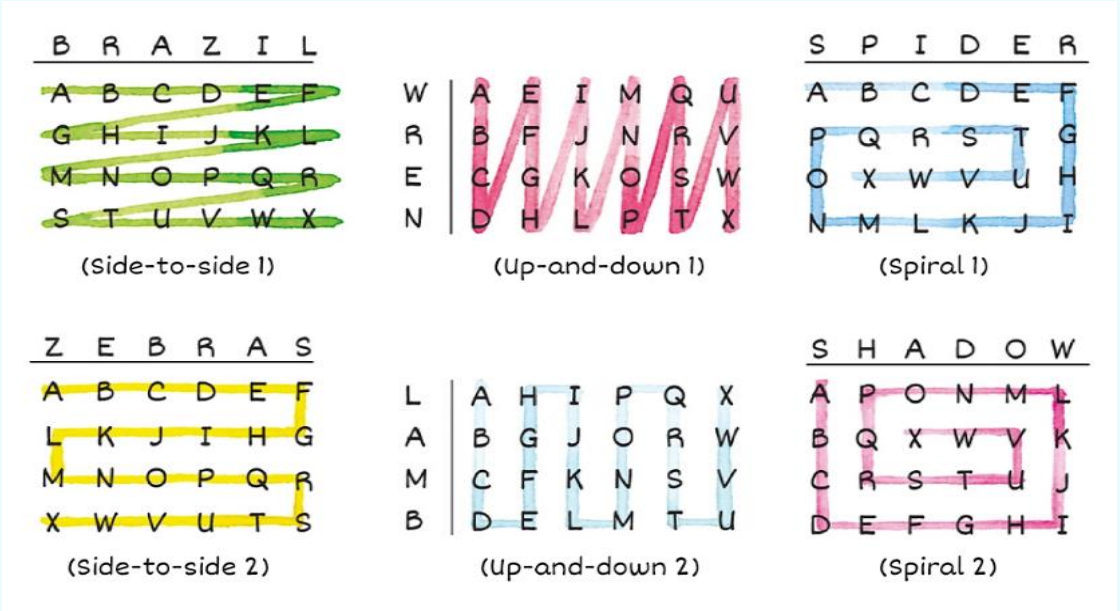
M . . . . . P. I

. . . A. . . . I. . . . A . . . . M. . . . .S

. . . . . N. . . . . L. . . . . .T

Therefore, the ciphertext will be: MPI AIAMS NLT

4.2 Route Cipher



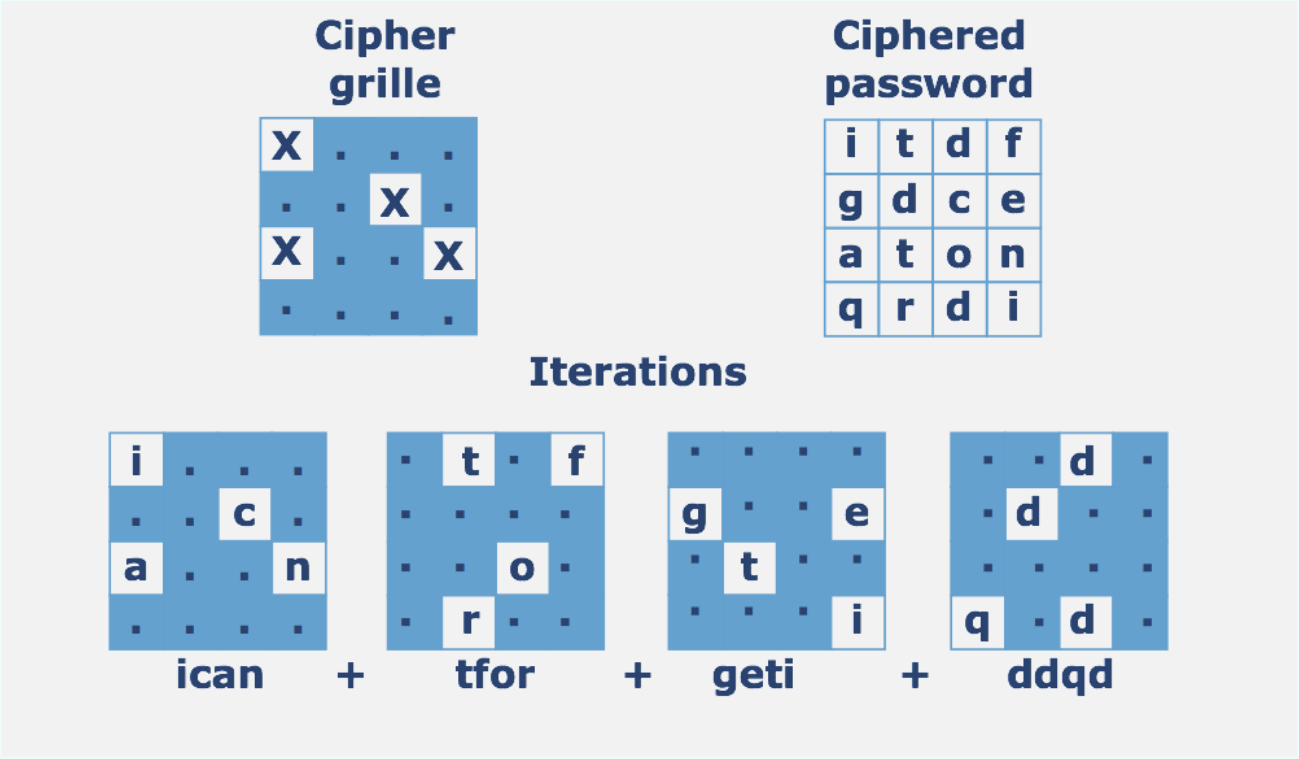
4.3 Columnar Cipher

Given text = Geeks for Geeks
Keyword = HACK **Length of Keyword** = 4 (no of rows) **Order of Alphabets in HACK** = 3124

H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

Print Characters of column 1,2,3,4
Encrypted Text = e kefGsGsrekoe_

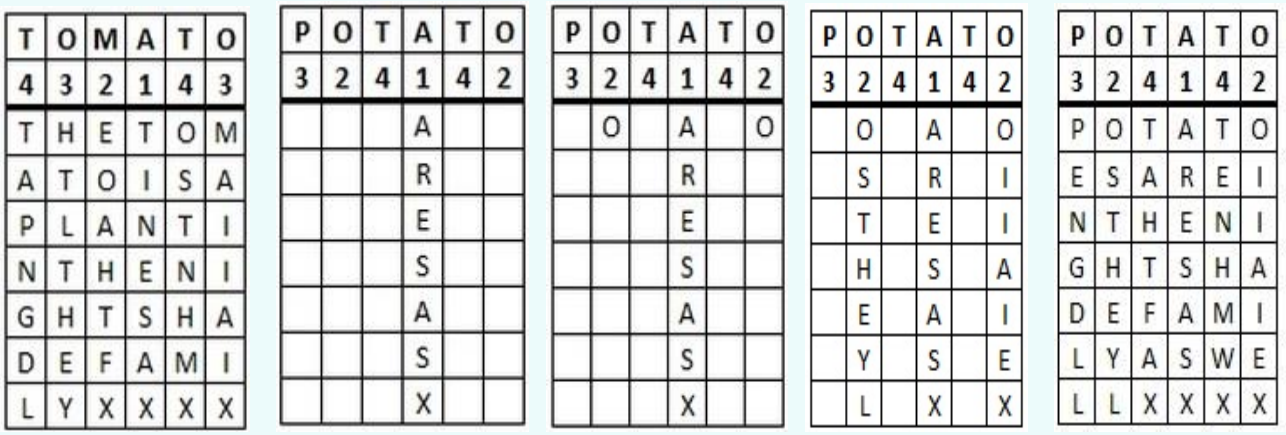
4.4 Grille Cipher



4.5 Myszkowski Cipher

Plaintext: "The tomato is a plant in the nightshade family"
Keyword: Tomato

Encryption: Decryption:



T	O	M	A	T	O
4	3	2	1	4	3
T	H	E	T	O	M
A	T	O	I	S	A
P	L	A	N	T	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	X	X	X	X

P	O	T	A	T	O
3	2	4	1	4	2
			A		
			R		
			E		
			S		
			A		
			S		
			X		

P	O	T	A	T	O
3	2	4	1	4	2
	O		A		O
			R		
			E		
			S		
			A		
			S		
			X		

P	O	T	A	T	O
3	2	4	1	4	2
	O		A		O
	S		R		I
	T		E		I
	H		S		A
	E		A		I
	Y		S		E
	L		X		X

P	O	T	A	T	O
3	2	4	1	4	2
P	O	T	A	T	O
E	S	A	R	E	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	A	S	W	E
L	L	X	X	X	X

4.6 Disrupted Transposition Cipher

F O R E V E R J I G S A W ---- Key

4 8 9 2 12 3 10 7 6 5 11 1 13

C O M P L I C A T E S T *

H E T R * * * * * * * * *

A N S P O S * * * * * * *

I * * * * * * * * * * * *

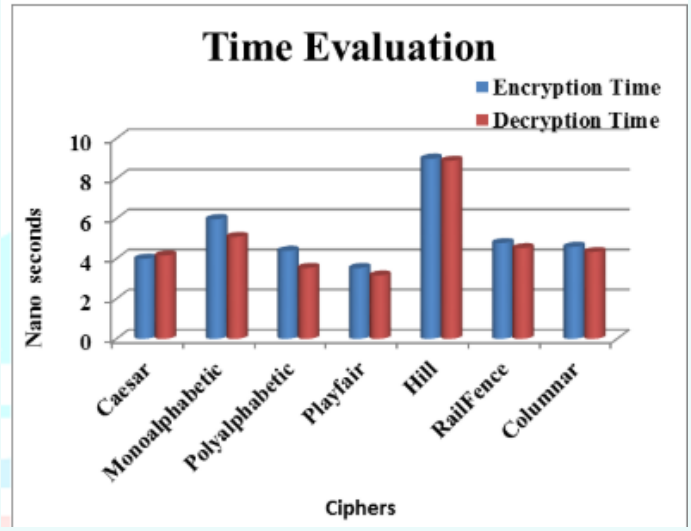
T I O N P A T T E R * * *

N L I K E A C O M * * * *

B * * * * * * * * * * * *

5.Some Comparisons

Here is a graph that shows the comparison between some substitution ciphers and some transposition ciphers.



The graph 1 shows the time evaluation of the graphs, i.e. the time each cipher technique takes to encrypt or decrypt the given plaintext. The y-axis represents the time in nano seconds.
From the graph we can understand that rail fence cipher and columnar cipher takes almost the same time but rail fence cipher takes slightly more time than columnar cipher.

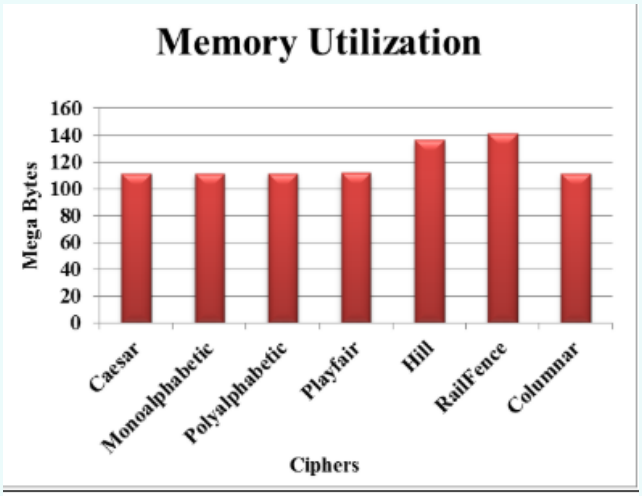


Fig 2: Analysis of Memory Utilization

The graph 2 shows the Memory utilization of the ciphers. As we can see rail fence cipher takes almost 30 megabytes storage more than columnar cipher. The other ciphers are substitution ciphers and hence take the same time except playfair cipher.

6.APPLICATIONS & IMPORTANCE

Cryptography finds its applications in wide realms of the modern world. Its most basic application is found in the security domains especially in major companies, national services, international services etc. Every day, people and organizations use cryptography to safeguard their privacy and maintain the confidentiality of their communications and data. It makes sure that a certain important message is passed on to the receiver without any third person getting to know about it. By encrypting communicated messages with an algorithm and a key that is only known to the sender and receiver, cryptography maintains confidentiality.

A popular illustration of this is the messaging app WhatsApp, which encrypts user communications to prevent hacking or interception. Through the use of virtual private networks (VPNs), which employ encrypted tunnels, asymmetric encryption, and public and private shared keys, cryptography also secures web browsing.

Transposition ciphers are simple to set up, but they are susceptible to cryptanalysis, particularly if the pattern or key is found. It is possible to decipher simple transposition ciphers by pattern recognition and frequency analysis. They can, however, create more reliable encryption schemes when paired with other encryption techniques, including substitution ciphers. In contemporary cryptography, transposition principles are integrated into more sophisticated algorithms. The combination of substitution and transposition forms the basis of many block ciphers, enhancing security by diffusing the plaintext's structure and hiding character patterns.

7. CONCLUSION

Transposition Cipher is a simple yet effective cipher technique that is not only used in cryptography in the modern day but has emerged from a very primitive form from the past. Its historical evidences have proved effective in the past and is used widely in the present. Transposition Cipher is a very suitable cipher to teach students who are new to cryptography since it is simple yet challenging to deal with. Understanding transposition ciphers provides a foundation for learning more advanced methods and appreciating the evolution of secure communication.

Despite their vulnerabilities, they offer valuable insights into the development of modern cryptographic techniques. Cryptography as a whole is a vast topic and transposition cipher is just another small part of it. It may seem like an insignificant topic but this could lead to building more complex and stronger ciphers in the future.

“Great things are done by a series of small things brought together”.

8. BIBLIOGRAPHY

1. https://www.hypr.com/security-encyclopedia/cipher#:~:text=Ciphers%2C%20also%20called%20encryption%20algorithms,determine%20how%20it%20is%20done.

2. https://crypto.interactive-maths.com/route-cipher.html

3. https://www.google.com/search?sca_esv=cfcd3706826e13a2&sca_upv=1&rlz=1C1GCEA_enOM1089OM1089&q=rail+fence+cipher&udm=2&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWd8nbOJfsBGGB5IQQO6L3J_86uWOeqwdnV0yaSF-x2joZDvir2QxhZkTA8rK1etu4Y30670-fAl7lygmK690uJyNhakMg---uzr_Yo0p3ZtGQanELZDOaVjFN7yUDe4fgm8aQJKQiASDBoi8CDjwBb6GIRacDnd6jmUt3-NxqSASwMc-y&sa=X&sqi=2&ved=2ahUKEwiA5NCFgPWGAxWRR_EDHUzIBAoQtKgLegQIDhAB&biw=1366&bih=599&dpr=1#vhid=PkV2u3yBYV9UIM&vssid=mosaic

4. https://www.hypr.com/security-

5. https://www.fortinet.com/resources/cyberglossary/what-is-cryptography

6. https://www.geeksforgeeks.org/transposition-cipher-techniques-in-cryptography/

7. https://www.sciencedirect.com/topics/computer-science/transposition-cipher#:~:text=Probably%20one%20of%20the%20oldest,secret%20messages%20(Figure%201.9)

8. https://cyberw1ng.medium.com/route-cipher-a-comprehensive-guide-to-encryption-and-decryption-2023-f0b12a64653

9. https://www.geeksforgeeks.org/columnar-transposition-cipher/

10. https://crypto.interactive-maths.com/columnar-transposition-cipher.html

11. https://en.wikipedia.org/wiki/Transposition_cipher#:~:text=A%20disrupted%20transposition%20cipher%20further,the%20plaintext%20or%20random%20letters.

12. https://www.pinterest.ca/pin/route-cipher-paterns--357473289166477348/

13. https://www.geeksforgeeks.org/columnar-transposition-cipher/

14. https://www.instructables.com/Fleissner-Grille-Cipher/

15. https://py.checkio.org/mission/cipher-map2/lang/en/share/1ff972dbc2429b075819a062e65bf190/

16. https://ijcrt.org/papers/IJCRT1801021.pdf