International Journal of Research in Engineering, Science and Management
Volume 4, Issue 11, November 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Use of Transposition Cipher and its Types

Kuriakkottu Amalraj Rajan*
Student, Department of Information Technology, Keralya Samajam Regd. Model College, Kalyan, India

***Abstract*: Transposition cipher is one of the types of algorithms present in cryptography, wherein the plaintext is changed to a ciphertext just like any other algorithms present cryptography but only with the catch that the encryption is created in combination of permutation of letters or numbers present in the text. Transposition cipher is more like a type or method of encryption algorithm wherein the positions acquired by text such as a character or a group of character is shifted using a regular system wherein the ciphertext would contain the permutation of the plain text which got encrypted. Basically, here a bijective function is applied on the plain text to encrypt it and then inverse function is used to decrypt the same. So, this research explores this concept called transposition cipher and its various types. *Methodology:* The research for this paper was done and reviewed on google scholar, Microsoft academic research. The data collected for this paper has been checked for its integrity and staying true to the content present in the research as well as that present in the worldwide web. The data has been analyzed in such a way that it represents how the transposition cipher is used and why in cryptography. *Findings:* It could be seen that most of the algorithms present in the cryptography uses algorithms. These algorithms are basically used for encryption and decryption. Wherein these algorithms as we say are technically known as ciphers and there are different ciphers present in the web more precisely in the market for using and developing it. And one such is transposition cipher this research paper showcases the uses of the same. *Conclusion:* Hence this research is conducted to produce a report wherein we explore the ciphers called transposition cipher and how they are implemented in algorithms present in the cryptography. And their different types present in it.**

***Keywords*: transposition, ciphers, algorithm.**

1. Introduction

This Research paper focuses on the aspect of the usage of transposition cipher in the algorithms used for the encryption purpose under cryptography and how it differs from that of other algorithms present in cryptography. The Transposition cipher also contains various amount of its subtypes which is going to be discussed in detail in this research paper. So, to understand the transposition cipher, we must first understand ciphers. In simple terms we can say that cipher is nothing, but encrypting and decrypting data given to an algorithm wherein the plain text which is the data will be converted to ciphertext. So, if a person sees this data the ciphertext would appear to be random text and the person would not understand anything out of it.

So why are ciphers used. It's used to have a have private communication between several internet protocols. Wherein it would offer security to the traffic present on the internet [2].

So, transposition cipher is one such cipher wherein the data is arranged in a regular pattern with its cyphertext generated with a combination of permutations. So, it basically saves the data in the order of byte but mixes its arrangement.

2. Findings

Cryptography has two parts, and they are cryptography as well as crypto analysis. In cryptography we create the codes to encrypt the data whereas in crypto analysis we analyze the data or code and then break it down, simply decrypt it. So transposition being one of them also has algorithm that would encrypt and decrypt it.

There is different type of ciphers present in transposition ciphers. Such as rail fence cipher, columnar transposition cipher, scytale cipher, route cipher Double transposition cipher.

A. Rail-Fence Cipher

Rail Fence cipher is also known as zig-zag cipher. They are easy to understand hence making it easily a breakable code.

1) Encryption in Rail-Fence

Here the plain text given is written downwards and to be more precise diagonally on a rail of imaginary fence, then moving up we get to the bottom. The message encrypted is then read in rows.

Example: We will divide Helloworld! into 3 rows

H . . o . . . . l .
. e . l . w . r . d .
. . l . . . o . . . !

2) Decryption in Rail-Fence

Once when we get hold of the matrix, we can then figure the places where the text will be placed. Then we will fill those places with the cipher text and then it will get converted to the original text.

B. Columnar Transposition Cipher

1) Encryption: In Columnar Transposition Cipher

In this cipher the plain text is written out in rows of fixed length and then read put again by columns and this column are not in correct order but in disarranged way. The length of the row and the permutation of the column are defined by a keyword.

2) Decryption in Columnar Transposition Cipher

To decipher it the receiver will have to work on the column

*Corresponding author: amalrajrajan.model@gmail.com

length by dividing the message length. Then read the message in columns and then re-arrange it by reforming the keyword.

C. Route Cipher

1) Encryption

In this cipher the plain text is written out in the form of grid in given dimensions then read of in each pattern by the key provided.

The route cipher has many more keys compared to that of a rail-fence cipher.

D. Double Transposition Cipher

1) Encryption

Double Transposition cipher is an Enhanced version of columnar transposition cipher. It can be said that Double Transposition cipher is nothing but applying the columnar transposition twice on a plain text.

Here for one transposition multiple keys or the same key can be used.

Decryption can be performed easily if both messages is using same key.

3. Discussion

So where are these transposition ciphers used? They are mostly used in network communication as well as in privacy management. To be more precise they are created to withstand upcoming attacks on the network traffic, or the network created. The transposition cipher does the same wherein it would encrypt the data with algorithms present in it and could only be decrypted according to the keywords present for it. But as new technologies emerge their uses are getting diminished as great number of other techniques are being used to secure the online threats and them being only used in cryptography.

4. Conclusion

It could be found that as of now the ciphers are considerably lower in use as compared to the previous generation of their usage, but they are being definitely used for the privacy and protection of the network traffic as well as for online communication. And are definitely worth for the investment of time and money.

References

[1] https://searchsecurity.techtarget.com/definition/cipher
[2] https://en.wikipedia.org/wiki/Transposition_cipher
[3] https://www.geeksforgeeks.org/columnar-transposition-cipher/?ref=lbp
[4] https://www.cs.uri.edu/cryptography/classicaltransposition.htm
[5] A. P. U. Siahaan, “Rail-Fence-Cryptography-in-Securing-Information,” Sept. 2017.