**TRANSPOSITION TECHNIQUES**

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

**Transposition Techniques** are based on the permutation of the plain-text instead of substitution.

1) Rail-Fence Technique

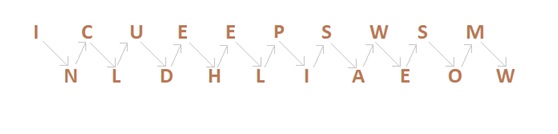
This technique is a type of Transposition technique and does is write the plain text as a sequence of diagonals and changing the order according to each row.

It uses a simple algorithm,

1. Writing down the plaintext message into a sequence of diagonals.
2. Row-wise writing the plain-text written from above step.

Example,

Let’s say, we take an example of “INCLUDEHELP IS AWESOME”.



So the Cipher-text are, **ICUEEPSWSMNLDHLIAEOW**.

First, we write the message in a zigzag manner then read it out direct row-wise to change it to cipher-text.

Now as we can see, Rail-Fence Technique is very to break by any cryptanalyst.

**1.1) Rail fence**is simplest of such cipher, in which the plaintext is written down as a sequence ofdiagonals and then read off as a sequence of rows.

Plaintext     = meet at the school house

To encipher this message with a rail fence of depth 2, we write the message as follows:

m  e  a         t        e        c  o    l         o        s

e   t    t  h    s        H       o        h        u e

The encrypted message is

MEATECOLOSETTHSHOHUE

2) Columnar Transition Technique

**A. Basic Technique**

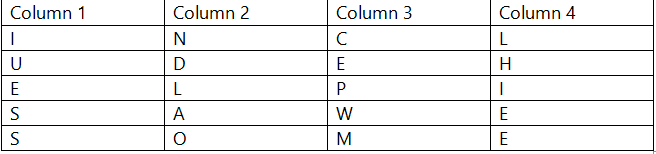
It is a slight variation to the Rail-fence technique, let’s see its algorithm:

1. In a rectangle of pre-defined size, write the plain-text message row by row.
2. Read the plain message in random order in a column-wise fashion. It can be any order such as 2, 1, 3 etc.
3. Thus Cipher-text is obtained.

**Let’s see an example:**

Original message: **"INCLUDEHELP IS AWESOME"**.

Now we apply the above algorithm and create the rectangle of 4 columns (we decide to make a rectangle with four column it can be any number.)



Now let’s decide on an order for the column as 4, 1, 3 and 2 and now we will read the text in column-wise.

Cipher-text: **LHIEEIUESSCEPWMNDLAO**

**B. Columnar Technique with multiple rounds**

In this method, we again change the chipper text we received from a Basic technique that is in round 1 and again follows the same procedure for the cipher-text from round 1.

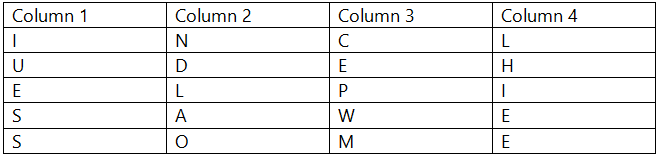
Algorithm:

1. In a rectangle of pre-defined size, write the plain-text message row by row.
2. Read the plain message in random order in a column-wise fashion. It can be any order such as 2, 1, 3 etc.
3. Thus, Cipher-text of round 1 is obtained.
4. Repeat from step 1 to 3.

**Example:**

Original message: **"INCLUDEHELP IS AWESOME"**.

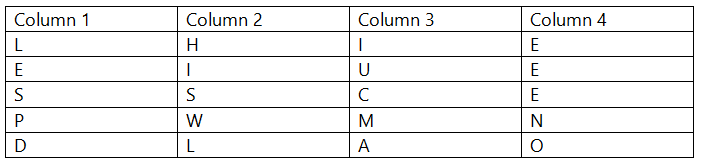
Now we apply the above algorithm and create the rectangle of 4 column (we decide to make a rectangle with four column it can be any number.)



Now let’s decide on an order for the column as 4, 1, 3 and 2 and now we will read the text in column-wise.

Cipher-text of round 1: **LHIEEIUESSCEPWMNDLAO**

**Round 2:**



Now, we decide to go with a previous order that is 4,1,3,2.

Cipher-text: **EEENLESPICUMHISW**

These multi-round columnar techniques are harder to crack as compared to methods seen earlier.

3) Vernam Cipher (One-Time Pad)

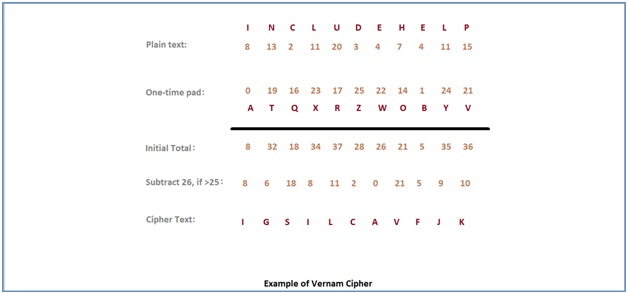
The **Vernam Cipher** has a specific subset **one-time pad**, which uses input ciphertext as a random set of non-repeating character. The thing to notice here is that, once an input cipher text gets used it will never be used again hence one-time pad and length of cipher-text is the size that of message text.

**Algorithm:**

1. Plain text character will be represented by the numbers as **A=0, B=1, C=2,... Z=25**.
2. Add each corresponding number of a plain text message to the input cipher text alphabet numbers.
3. If the sum is greater than or equal to 26, subtract 26 from it.
4. Translate each number back to corresponding letters and we got our cipher text.

**Example:**

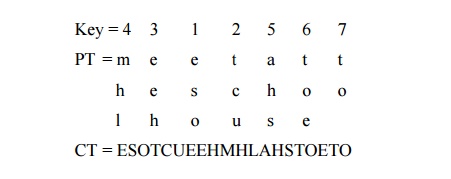
Our message is **"INCLUDEHELP"** and input cipher text is **"ATQXRZWOBYV"**



One time pad should be discarded after every single use and this technique is proved highly secure and suitable for small messages but illogical if used for long messages.

4)  **Row Transposition Ciphers**-A more complex scheme is to write the message in a rectangle,row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the school house



CT = ESOTCUEEHMHLAHSTOETO

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

5) Book/Running-Key Cipher

This technique also (incorrectly) known as running key cipher. This technique very simple and similar to our previous Vernam Cipher. For getting a cipher, some portion of text from a book is used as a one-time pad, rest it works in same way as Vernam cipher does.

REFERENCES

<http://www.brainkart.com/article/Classical-Encryption-Techniques_8339/>

<https://www.tutorialspoint.com/cryptography/index.htm>

<https://www.geeksforgeeks.org/cryptography-introduction/>

[https://www.techopedia.com/definition/1770/cryptography#:~:text=Cryptography%20involves%20creating%20written%20or,information%20to%20be%20kept%20secret.&text=Information%20security%20uses%20cryptography%20on,transit%20and%20while%20being%20stored](https://www.techopedia.com/definition/1770/cryptography).

<https://www2.slideshare.net/lineking/classical-encryption-techniques-in-network-security?qid=e388c29f-793d-4f2b-bcaf-9d22e9ca07b5&v=&b=&from_search=1>

<https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography>

<https://www.academia.edu/Documents/in/Cryptography>