SNS COLLEGE OF TECHNOLOGY

Coimbatore-35

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade

Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

19ECT301-COMMUNICATION NETWORKS

III YEAR/ V SEMESTER

UNIT 4- NETWORK & DATA SECURITY

TOPIC 3– SUBSTITUTION TECHNIQUES

Types of Substitution Techniques

1. Mono-alphabetic Cipher:

In this technique, we simply **substitute any random key for each alphabet letter**, that is **'A'** can be being replaced with any letters from **B to Z** and **'B'** can be changed to **rest of the Alphabets** but itself and so on. Let's say we **substitute A with E that doesn't mean that B will be replaced by F**.

Mathematically, we have 26 alphabet permutation which means **(26 x 25 x 24 x...2)** which is about **4 x 1026** possibilities.

Types of Substitution Techniques

2. Homophonic Substitution Cipher:

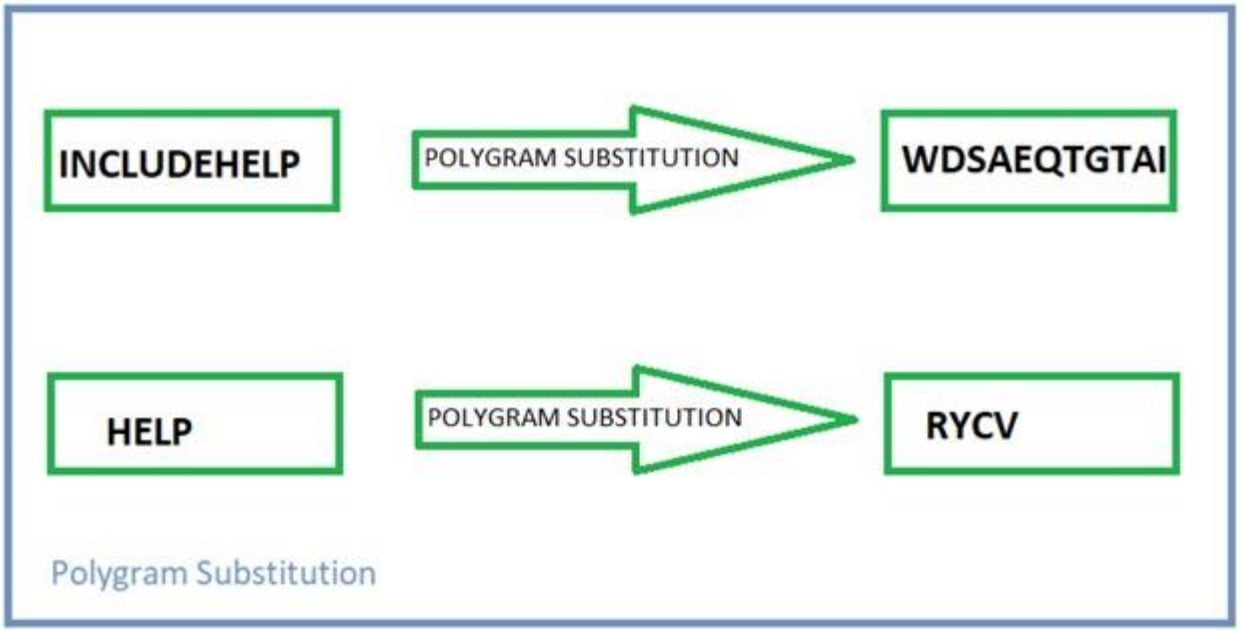
The Homophonic substitution and mono-alphabetic substitution are very much alike. Like in plain cipher substation we replace an alphabet with a key but in case of Homophonic Substitution, we map an alphabet with a set of fixed keys (more than one key). For instance, **A** can be replaced with **H, J, O, P and B** will replace with any of the following inspite of **A's** key set **D, I, W, Z** etc.

Types of Substitution Techniques

3.Polygram Substitution Cipher:

In Polygram substitution cipher, instead of replacing one plain-text alphabet we simply replace a block of the word with another block of a word. Example, **'INCLUDEHELP'** will change to **'WDSAEQTGTAI'** whereas **'HELP'** will replace to **'RYCV'**. This is true that the last four letters are the same but still different in both words.

Types of Substitution Techniques



Transposition Technique in Cryptography

Transposition technique is an encryption method which is achieved by performing permutation over the plain text. Mapping plain text into cipher text using transposition technique is called transposition cipher.

Transposition Techniques

- Rail Fence Transposition
- Columnar Transposition
- Improved Columnar Transposition
- Book Cipher/Running Key Cipher

Rail Fence Cipher

The rail fence cipher is the simplest transposition cipher. The steps to obtain cipher text using this technique are as follow:

Step 1: The plain text is written as a sequence of diagonals.

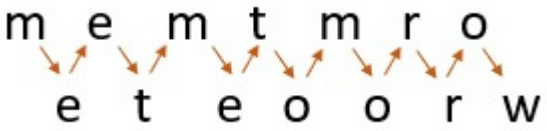
Step 2: Then, to obtain the cipher text the text is read as a sequence of rows.

To understand this in a better way, let us take an example:

Rail Fence Cipher

Plain Text: meet me Tomorrow

Now, we will write this plain text sequence wise in a diagonal form as you can see below:



Looking at the image, you would get it why it got named rail fence because it appears like the rail fence.

Rail Fence Cipher

Once you have written the message as a sequence of diagonals, to obtain the cipher text out of it you have to read it as a sequence of rows. So, reading the first row the first half of cipher text will be:

m e m t m r o

reading the second row of the rail fence, we will get the second half of the cipher text:

e t e o o r w

Now, to obtain the complete cipher text combine both the halves of cipher text and the complete cipher text will be:

Cipher Text: M E M T M R O E T E O O R W

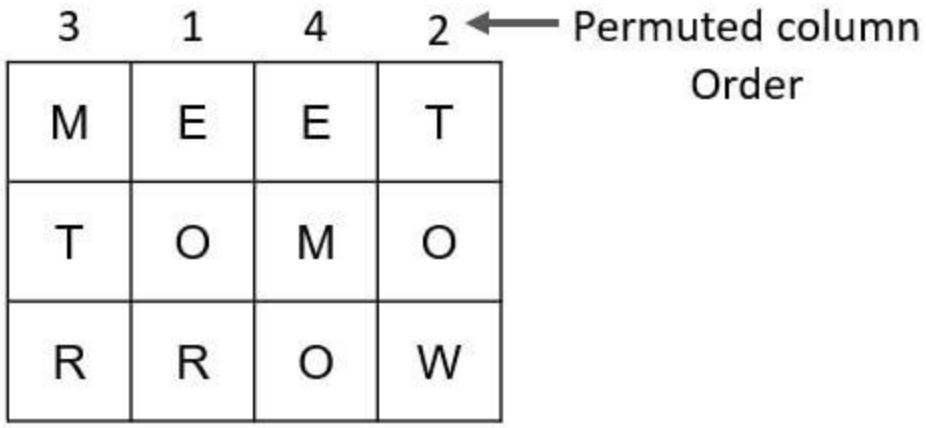
Columnar Transposition Technique

To understand the columnar transposition let us take an example:

Plain text: meet Tomorrow

Now, put the plain text in the rectangle of a predefined size. For our example, the predefined size of the rectangle would be 3×4. As you can see in the image below the plain text is placed in the rectangle of 3×4. And we have also permuted the order of the column.

Columnar Transposition Technique



Cipher Text: MTREOREMOTOW.

Book Cipher or Running Key Cipher

The book cipher or the running key cipher works on the basic principle of one-time pad cipher. In onetime pad cipher the key is taken as long as the plain text and is discarded after the use. Every time a new key is taken for a new message.

Book Cipher or Running Key Cipher

	M	E	E	T	T	O	M	O	R	R	O	W
Numeric form Plian Text	12	4	4	19	19	14	12	14	17	17	14	22

	A	N	E	N	C	R	Y	P	T	I	O	N
Numeric from Key Text	0	13	4	13	2	17	24	15	19	8	14	13

Add the numeric form of Plain text and Key Text:

	12	4	4	19	19	14	12	14	17	17	14	22
+	0	13	4	13	2	17	24	15	19	8	14	13
Subtract Numbers > 26 by 26	12	17	8	32	21	31	36	29	36	25	28	35
	12	17	8	6	21	5	10	3	10	25	3	9
New Cipher Text	M	R	I	G	V	F	K	D	K	Z	D	J

THANK YOU