Substitution ciphers

BY: DR. UPMA JAIN

Vernam cipher

- Need for ultimate defence against cryptanalysis.
- Length of keyword= length of plaintext.
- No statistical relation to it.
- At & T engineer named Gilbert Vernam in 1918.
- His system works on binary bits rather that letters.
- System can be expressed as follows:

$$C_i = P_i \text{ Xor } K_i$$

Vernam Cipher

- **Vernam Cipher** is a method of encrypting alphabetic text. It is one of the Substitution techniques for converting plain text into cipher text.
- In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, … z = 25).
- **Method to take key:** In the Vernam cipher algorithm, we take a key to encrypt the plain text whose length should be equal to the length of the plain text.
- **Encryption Algorithm:**
- Assign a number to each character of the plain-text and the key according to alphabetical order.
- Bitwise XOR both the number (Corresponding plain-text character number and Key character number).
- Subtract the number from 26 if the resulting number is greater than or equal to 26, if it isn't then leave it.

Example :

Plain-Text: O A K

Key: S O N

O ==> 14 = 0 1 1 1 0

S ==> 18 = 1 0 0 1 0

Bitwise XOR Result: 1 1 1 0 0 = 28

Since the resulting number is greater than 26, subtract 26 from it.

Then convert the Cipher-Text character number to the Cipher-Text character.

28 - 26 = 2 ==> C CIPHER-TEXT: C

Similarly, do the same for the other corresponding characters,

PT: O A K

NO: 14 00 10

KEY: S O N

NO: 18 14 13

New Cipher-Text is after getting the corresponding character from the resulting number.

CT-NO: 02 14 07

CT: C O F

One time pad cipher

- One-time pad cipher is a type of Vernem cipher which includes the following features –
- It is an unbreakable cipher.
- The key is exactly same as the length of message which is encrypted.
- The key is made up of random symbols.
- As the name suggests, key is used one time only and never used again for any other message to be encrypted.
- Due to this, encrypted message will not be vulnerable to attack for a cryptanalyst. The key used for a one-time pad cipher is called **pad**, as it is printed on pads of paper.

Why is it Unbreakable?

- The key is unbreakable owing to the following features –
  - The key is as long as the given message.
  - The key is truly random and specially auto-generated.
  - Key and plain text calculated as modulo 10/26/2.
  - Each key should be used once and destroyed by both sender and receiver.
  - There should be two copies of key: one with the sender and other with the receiver.

Security of One-Time Pad

- If any way cryptanalyst finds these two keys using which two plaintext are produced but if the key was produced randomly, then the cryptanalyst cannot find which key is more likely than the other. In fact, for any plaintext as the size of ciphertext, a key exists that produces that plaintext.
- So if a cryptanalyst tries the brute force attack(try using all possible keys), he would end up with many legitimate plaintexts, with no way of knowing which plaintext is legitimate. Therefore, the code is unbreakable.
- The security of the one-time pad entirely depends on the randomness of the key. If the characters of the key are truly random, then the characters of ciphertext will be truly random. Thus, there are no patterns or regularities that a cryptanalyst can use to attack the ciphertext.

Advantages

- One-Time Pad is the only algorithm that is truly unbreakable and can be used for low-bandwidth channels requiring very high security(ex. for military uses).

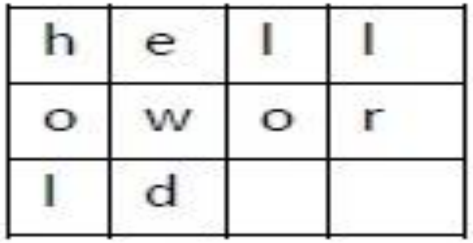
Disadvantages

- There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis.

Transposition

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

- A simple example for a transposition cipher is **columnar transposition cipher** where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.
- Consider the plain text **hello world**, and let us apply the simple columnar transposition technique as shown below-



h	e	l	l
o	w	o	r
l	d		

  - The plain text characters are placed horizontally and the cipher text is created with vertical format as:
  - **holewdlo lr.** Now, the receiver has to use the same table to decrypt the cipher text to plain text.

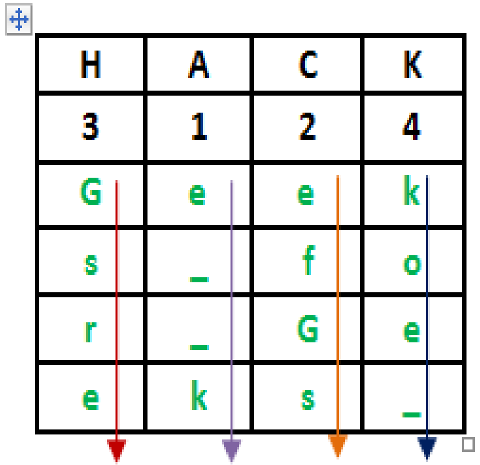
Encryption

- In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.
- The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.
- Width of the rows and the permutation of the columns are usually defined by a keyword.
- For example, the word HACK is of length 4 (so the rows are of length 4), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be “3 1 2 4”.
- Any spare spaces are filled with nulls or left blank or placed by a character (Example: _).
- Finally, the message is read off in columns, in the order specified by the keyword.

Encryption

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_

Decryption

- To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length.
- Then, write the message out in columns again, then re-order the columns by reforming the key word.

Rail Fence Cipher – Encryption and Decryption

- Given a plain-text message and a numeric key, cipher/de-cipher the given text using Rail Fence algorithm.
- The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

Examples:

Encryption Input : "GeeksforGeeks " Key = 3

Output : GsGsekfrek eoe

Decryption Input : GsGsekfrek eoe Key = 3

Output : "GeeksforGeeks "

Encryption Input : "defend the east wall" Key = 3

Output : dnhaweedtees alf tl

Decryption Input : dnhaweedtees alf tl Key = 3

Output : defend the east wall

Encryption Input : "attack at once" Key = 2

Output : atc toctaka ne

Decryption Input : "atc toctaka ne" Key = 2

Output : attack at once

- **Encryption**
- In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

- In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
- When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-zag manner.
- After each alphabet has been written, the individual rows are combined to obtain the cipher-text.
- For example, if the message is “GeeksforGeeks” and the number of rails = 3 then cipher is prepared as:

Decryption

- As we've seen earlier, the number of columns in rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.
- Hence, rail matrix can be constructed accordingly. Once we've got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).
- Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.
- Implementation:
  Let cipher-text = "GsGsekfrek eoe" , and Key = 3
- Number of columns in matrix = len(cipher-text) = 13
- Number of rows = key = 3