Volume 3, Issue 2, February 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Polyalphabetic Cipher Techniques Used For Encryption Purpose

Sonia Dhull, Sonal Beniwal, Preeti Kalra
School of Engineering & Sciences
BPS Mahila Vishwavidyalaya
Sonipat, Haryana
India

***Abstract*— this study will present a perspective on Polyalphabetic techniques which are currently used for encryption purpose. This paper mainly focuses on practically use of the Polyalphabetic techniques for encryption purpose. Aim a brief discussion about all three types of polyalphabetic techniques.**

***Keywords*— Plaintext, Ciphertext, XOR, Encryption, Polyalphabetic.**

I. INTRODUCTION

Encryption is an effective way to achieve the security of data. The word of encryption came in mind of King Julius Ceaser because he did not believe on his messenger so he thought to encrypt the data or message by replacing every alphabet of data by 3rd next alphabet[1]. The process of Encryption hides the data in a way that an attacker cannot hack the data. The main purpose of encryption is to hide the data from unauthorized parties from viewing, altering the data[3]. Encryption techniques occur or used by using the shifting techniques, mathematical operations and shifting techniques. The Simple data is known as Plain text and Data after encryption is known as Ciphertext. Substitution and transposition techniques are mainly used for it.

In encryption methods, two methods are used for encryption purpose-

a. Substitution techniques-Change the one letter by another using secret key.
b. Transposition techniques-Replace the place of letters of plaintext.

In substitution tech's monoalphabetic and polyalphabetic techniques are used. In monoalphabetic, a single cipher alphabet is used per message. This technique was easy to break because they show the frequency data of plaintext alphabet. So polyalphabetic techniques came into knowledge in which different monoalphabetic substitution as one proceeds through original message.

II. TYPES OF POLYALPHABETIC CIPHER

There are three types of polyalphabetic cipher, these are

A. Vignere cipher
B. Vernam cipher
C. One-time pad cipher

All these three techniques have two features in common-

- Set of related monoalphabetic substitution rules are used.
- A key is used for the transformation of plaintext into cipher text.

A. *Vignere Cipher*- This is the best one and one of the simplest techniques. In this the set of related monoalphabetic substitution rules consist of the 26 ceaser cipher from (0 to 25). Each cipher is denoted by a key letter, which is substitute for plaintext letters.
To understand this scheme, we use a table known as VIGNERE TABLEAU. All 26 ciphers (A-Z) letters is laid out horizontally with the key letter to its left.

a. Process used for Encryption- There is a given key letter(x) and plaintext letter (y), then ciphertext letter for it will be the intersections of the row labelled 'X' and column labelled 'Y'. To encrypt the message, there is a key required that is as long as the message. Here key is used as repeating keyword.
Example-

Key-	d e f e n s e d e f e n s e d e f e n s e d e f e n s
Plaintext-	w e a r e a c c e p t i n g y o u r c o n d i t i o n
Ciphertext-	z i f v r s g f i u x v f k b s z v p h r g m y m b f

b. Decryption Process- It is also as simple as encryption. The position of ciphertext letter in that row determines the column and plaintext will be letter at the top of that column. So in this example ciphertext came "zifvrsgfiuxvfkbszvphrgmymbf" and the key is "defensedefensedefensedefens" so at time of decryption first key letter is 'd' and first ciphertext letter is z then when we find ' z' in row of

key letter d, we get it in the column of 'w' of plaintext field. So, first letter that we decrypt is 'w' and so on.

c. *Advantage*- we get different ciphertext of same plaintext with changing the key letter.

d. *Disadvantage*- repetition of key letter again makes it less secure. As in above taken example after 7 key alphabets again repeat first letter of keyword. So an analyst can easily detect the repeated sequence of same ciphertext and make the assumption that the keyword is of same length.

Solution- this periodic nature of keyword can be eliminated by using non repeated sequence of keyword that is as long as the message itself.

VIGNERE proposed what is referred as "**AUTOKEY SYSTEM**", in which a keyword is concatenated with the plaintext itself to provide further key.

Key- d e f e n s e **w e a r e a c c e p t i n g y o u r c o**
P.Text- w e a r e a c c e p t i n g y o u r c o n d i t i o n
C.Text- z i f v r s g y i p k m n i a s j k k b t b w n z q b

So as shown here in this example now there is no repletion of alphabets. And we get this ciphertext with help of vignere tableau, when we pick 1st alphabet of plaintext and 1st alphabet of keyword and go to check the related alphabet as a ciphertext in vignere tableau then get the 'Z' as1st alphabet of ciphertext and so on till last. In above example it is clearly shown that how plaintext is used as a keyword after once using the keyword letter. When we use the plaintext to complete the keyword for encryption, we do not get the same frequency of letters in ciphertext which makes the poor security.

B. *VERNAM Cipher*- the Gilbert Vernam introduced this technique in 1918 which stated that "Choose a keyword that is as long as the plaintext and there should not be statically relationship to it".

That was expressed as-

$$\mathbf{C_i = P_i \oplus K_i}$$

Where-

P_i- i_{th} binary digit of plaintext
C_i- i_{th} binary digit of key letter
K_i- i_{th} binary digit of ciphertext
$\oplus$ - XOR Operation

So here ciphertext is generated by performing the bitwise XOR of plaintext and key.

Decryption-

$$\mathbf{P_i = C_i \oplus K_i}$$

Vernam purpose the use of running loop of tape that eventually repeated the key, so system works but repeating keyword.

Example- If plaintext is "AFTER" and key is "ACCUR" then using Binary Notation and applying the XOR operation on it we will get the "AHRQA" as a ciphertext. And will send it.

P.TEXT- **A F T E R**
KEY- $\oplus$ **A C C U R**
C.TEXT- **A H R Q A**

To get this ciphertext we will first of all convert these alphabets into binary notation and then apply the XOR operation on it.

Binary notation of first letter of plaintext 'A' will be '00000' and also of the first alphabet of ciphertext is 'A' so binary notation of this will be same as plaintext alphabet. When we apply XOR operation on it then we will get '00000' means 'A' alphabet will come as cipher text. And now 2nd alphabet of plaintext is 'F' so binary notation of it will be '00101' and 2nd alphabet of key is 'C' so binary notation of it will be '00010' so XOR of these will be '00111' means ciphertext of it will be 'H' and so on. At last we will get the 'AHRQA' as a ciphertext of above taken plaintext using that key.

a. *DECRYPTION*- When we will decrypt it again then will get the same plaintext of it.at the receiver side using the same key can get the original message from encrypted message applying XOR operation.

So when receiver gets the encrypted message or can say a secure message then apply the same key on it using XOR operation on it and gets the original message that sender wants to send.

PLAINTEXT-	**00000 (A)**	**00101 (F)**	**10011 (T)**	**00100 (E)**	**10001 (R)**
$\oplus$ KEY-	**00000 (A)**	**00010 (C)**	**00010 (C)**	**10100 (U)**	**10001 (R)**
CTEXT-	**00000 (A)**	**00111(H)**	**10001 (R)**	**10000 (Q)**	**00000 (A)**

b. *Disadvantage*- It can be broken with sufficient ciphertext, the use of known or probable plaintext sequences or both. So need a more secure technique to improve the security. So then came into knowledge a technique known as One-Time Pad.

C. *ONE TIME PAD*- Army Signal Corp. Officer, Joseph Mauborgne, proposed an improvement to Vernam Cipher that was the ultimate in security[4]. He suggested that we use a random key that is as long as the message means

the key need not to be repeated. In additional key must be use once for encryption and decryption of a single message and then that key is discarded. So this technique is called as One Time Pad and there is relationship between key and plaintext and it is unbreakable.
In this as advance of vignere cipher scheme we Can use 27 character in which 27th character is SPACE, so in this key will be as long as message. So table of Vignere cipher must be expanded to 27*27.

Example-
P.Text- MR JACK ON TOUR
Key- ZQQHRCBN-BNXFBG
C.Text- AGPQRELMNOMPTVX

As shown in example, in key (-) is used, meaning of this is from a space. So it is clear from this is example that SPACE character is also used in One-Time Pad technique as 27^{th} alphabet.

Then if apply two key on it then every time will come different plaintext. So an Analyst or an Attacker will fail to understand which key is correct and which plaintext is correct.

Example of Attacking in One-Time Pad-

i. C.Text- AGPQRELMNOMPTVX
Key- ZQQHRCBN-BNXFBG
P.Text- MR JACK ON TOUR AND

ii. C.Text- AGPQRELMNOMPTVX
Key- ZQQHRCBNNWNIFJT
P.Text- MR JACK AT HOME

As shown in above example, if attacker finds this cipher text and then applies different keys then every time will get different plaintext and he will be confused that which one is original message. When an attacker gets encrypted data and tries to use a key then so tough to get actual message just because of the use of a non-repeating key. If an attacker uses two different keys on encrypted data then every times get a different plaintext and gets totally puzzle that which one is the actual data that sender wants to forward to receiver.

So, entire security of One Time Pad scheme is due to randomness of key. If stream of character of key is truly random then the stream of characters that constitute the ciphertext will be truly random.

It provides full security but has two fundamental difficulties-

- Practical problem of making large quantities of random keys. So a heavily Used system may require millions of random characters that are practically tough.
- There is also a big problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver.

USE of One Time Pad- This scheme is used only for low Bandwidth Channels requiring very high security. In this technique, comes problem of generation of keys in so much quantity which is so tough to handle that increases the cost of this technique[4].

III. CONCLUSION

In this paper we discussed about all type of Polyalphabetic cipher techniques. If we have knowledge of these techniques in detail then we can improve the cryptographic algorithm or encryption techniques. This type of deep knowledge of all type encryption techniques helps us to move in direction of making our data more secure and safe from any cryptographic attack.

ACKNOWLEDGMENT

We would like to give our sincere gratitude to our guide Mrs. Sonal Beniwal who guides us to pursue this topic and help us to complete this topic.

REFERENCES

[1] William Stalling "Network Security Essentials (Applications and Standards)", Pearson Education,2004
[2] Atul Kahate (2009), Cryptography and Network Security, 2nd edition, McGraw-Hill.
[3] Stallings (1999), Cryptography and Network Security, 2nd edition, Prentice Hall.
[4] William Stallings (2003), Cryptography and Network Security, 3rd edition, Pearson Education.

