Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Techniques used for Encryption Purpose

Ritu, Yuvinder Dandiwal
Assistant Professor, Department of CSE
Chandigarh Group of Colleges, Landran,
Mohali, Punjab, 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 techniques that are used for encryption purpose. Aim a brief discussion about three types of techniques used for encryption purpose.

Keywords — Plain Text, Cipher Text, Key, Transposition, substitution.

I. INTRODUCTION

Cryptography is an art and science of converting original message into no readable form. 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 Cipher text. 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.

II. TYPES OF ENCRYPTION TECHNIQUES

Here we will discuss three types of encryption techniques used for encryption purpose.

a) Vernam cipher.
b) Simple Columnar Transposition Technique.
c) One-time pad cipher.

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-

Ci = Pi-Ki
Where-
Pi- ith binary digit of plaintext
Ci- ith binary digit of key letter
Ki- ith binary digit of ciphertext
- XOR Operation

So here cipher text is generated by performing the bitwise XOR of plaintext and key.
Decryption-

Pi = Ci Ki

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 cipher text. And will send it.

P.TEXT- A F T E R
KEY- A C C U R
C.TEXT- A H R Q A

To get this cipher text 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 cipher text 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 cipher text of it will be „H‟ and so on. At last we will get the „AHRQA‟ as a cipher text of above taken plaintext using that key.

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)
KEY- 00000 (A) 00010 (C) 00010 (C) 10100 (U) 10001 (R)
CTEXT- 00000 (A) 00111(H) 10001 (R) 10000 (Q) 00000 (A)

Disadvantage- It can be broken with sufficient cipher text, 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.

Simple Columnar Transposition technique

It is the second easiest transposition technique. This states that simply arranges the plain text as a sequence of rows of a rectangle that are read in columns randomly.

Encryption Process: This process involve two step as follows

Write the plain text message in a rectangle format of predefined size row by row.To obtain the cipher text read the message in random order column by column.

Example: Original Plain text message: Have a nice day dear

(a) Let us suppose a rectangle with six columns. Now write the plain text message in a rectangle row by row, it would look as follows

Column-1	Column-2	Column-3	Column-4	Column-5	Column-6
H	A	V	E	A	N
I	C	E	D	A	Y
D	E	A	R		

b) In this step decide the order of column as some random order, suppose 4, 5,2,1,6 and 3. Then read the text in the order of these columns

c) The cipher text thus obtained would be EDRAAACEHIDNYVEA

KEY: 4 5 2 1 6 3
PLAIN TEXT: H A V E A N
I C E D A Y
D E A R
CIPHER TEXT: EDRAAACEHIDNYVEA

Decryption Process: Decrypting the message is very much easy in this technique if the column order is known. In this Technique column order will used as key.

Advantage: Easy to implement.

Disadvantages: It is also quite simple to break into. It is just a matter of trying out a few permutations and Combinations of column order to get hold of the original plain text.

Solution: To make matter complex for cryptanalyst perform more than one rounds of transposition using the same Technique.

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 27th 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-

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 cipher text will be truly random.

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.

III. CONCLUSION

In this paper we discussed about all type of encryption 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.

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

