International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 10, December- 2012

PA Substitution Cipher

Anuj Kumar[1]
[1]M.Tech*, Computer Science & Engineering
IEC CET, Greater Noida, (U.P.) India

Ankur Kumar Varshney [2]
[2]M.Tech*, Computer Science & Engineering
B.S.A College of Engineering &
Technology, Mathura, (U.P.) India

Pankaj Kumar[3]
[3]B.Tech, Computer Science & Engineering
S.R.M.S. College of Engineering &
Technology, Bareilly, (U.P.) India

Abstract

Cryptography which is considered as a science to send a message through network. Since early civilizations, different methods have been developed to send secret messages. But with advent of Internet, data privacy face more risks, these risks are data inconsistency, data integrity, alterations, data replication etc, thus need of information security increases which lead to the new developments of cryptography. In classic cryptography, mainly two techniques are used: SUBSTITUTION and PERMUTATION. And the fact is that Modern cryptography is mainly based on these two very basic techniques. In this paper we proposed a PA Substitution Cipher (Pankaj Ankur Substitution Cipher). By using this cipher technique a attacker does take more time than the other Substitution cipher technique.
Keyword - Cryptography, Cryptanalysis, Product cipher, Substitution cipher, Transposition cipher

1. Introduction

Cryptography is the art and science of making secure communication systems. The term is derived from the Greek words: ‘kryptos’ means “hidden” and ‘graphos’ means “word”. Cryptanalysis is derived from the Greek words: kryptos, and analyzing, means "to loosen “or "to untie" [1]. It is the study of methods for obtaining the meaning of encrypted information, without access to the secret information which is normally required to do so. Cryptanalysis is the flip-side of cryptography. It is the science of cracking codes, decoding secrets, violating authentication schemes, and in general, breaking cryptographic protocols [2]. Cryptography and Cryptanalysis comprise Cryptology. The science Cryptology is not a new science but it is quite an ancient art. Cryptography has a long and fascinating history [3]. The first recorded use of cryptography for correspondence was by the Spartans who (as early as 400 BC) employed as cipher device called a “Scytale” to send secret communication between military commanders [4]. In old times, from 1918 and until WWII, an encryption method known as the “enigma” was used in Germany. For this method, typewritten messages were encrypted by using a modified typewriter and today, with the invention of Cryptography. Classic cryptography involves: substitution and permutation and modern cryptography has Asymmetric cryptography, digital signatures, elliptic curve cryptography [5-7] etc.

1.1 Substitution Ciphers

Substitution technique is one in which each character in the plaintext is substituted for another character in the cipher text. The receiver inverts the substitution on the cipher text to recover the plaintext [2]. For example: Ceaser, Hill, Playfair etc.

1.1.1Types of Substitution cipher:

In classical cryptography there are 4 types of substitution cipher:

•**Mono-alphabetic substitution/Simple substitution cipher** is, where each character in the plain text is replaced with a corresponding character of cipher-text. The cryptograms in newspaper are simple substitution cipher.

•**Homo-phonic substitution cipher** is like a simple substitution cipher except that a single character of plain-text can map onto several characters of cipher text.

•**Polygram substitution** blocks of plain-text characters are encrypted in groups into blocks of cipher-text

•**Poly-alphabetic substitution cipher** is made up of multiple mono-alphabetic ciphers. The cipher changes with the position of each character in the plain text. It is used in American civil war.

1.2 Permutation Ciphers

Permutation technique is one in which the plaintext remains the same, but the order of characters is shuffled around. It forms the second basic building block of classic ciphers. In a simple columnar transposition cipher, the plaintext is written horizontally onto a piece of graph paper of fixed width and the cipher text is read off vertically [2]. The core idea is to rearrange the order of basic units (letters/bytes/bits) without altering their actual values. A transposition cipher simply rearranges the symbols in plaintext to produce cipher text.

2. Methodology

We implement each of its cipher using substitution technique. For implementing PA Substitution Cipher we take a key which

will contain at least a letter 'A'. We decode each letter according to their alphabetic index in increasing order. Apply the formula for encryption. After encrypting the text we send the text through network channel with three information key value, cipher text and public value. After receiving the information decrypt it with the help of algorithm. The main concept with this is that, we transfer additional information that s the public value and this value has the same length as the plain text will contain.

Cipher Text= plain text% Key

Public value=Plain text/ Key

Plain text=key* Public Value+ Cipher text

Algorithm:

1. Choose a Key which will contain at least a character "A".
2. Assign the value 1-26 to each letter as in the alphabetic order and Assign $ in place of 0.
3. For Encryption Cipher Text= plain text% Key
4. Compute Public value=Plain text/ Key
5. Again Assign Alphabet to their values.
6. Send Cipher text, Public value and Key to the Receiver Through channel.
7. Decrypt it by Plain text=key* Public Value+ Cipher text

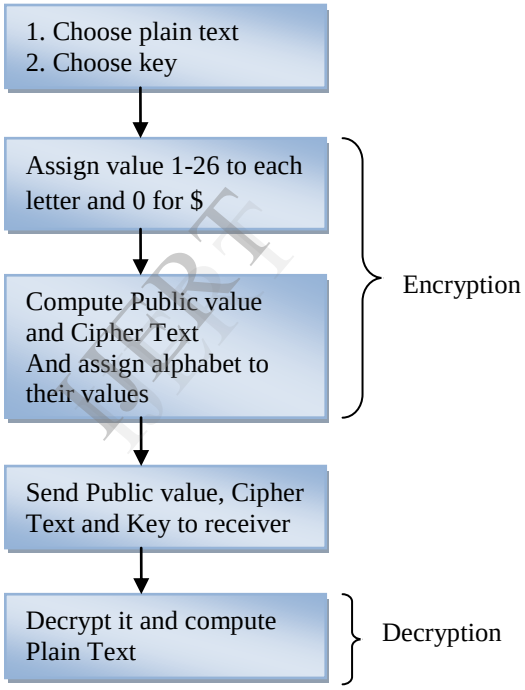

Figure 1 Algorithm for PA Substitution Cipher

Example:-

Let we transfer Plain Text="HELL" and Key="RABL"

1. Plain Text=

H	E	L	L
8	5	12	12

Key=

R	A	B	L
18	1	2	12

2. Cipher Text= plain text% Key

8	0	0	0
H	$	$	$

Public value= Plain text/ Key

0	5	6	1
$	E	F	A

3. Send “H$$$”, “$EFA” and “RABL” through channel.
4. For Decryption Plain text=key* Public Value+ Cipher text

8	5	12	12
H	E	L	L

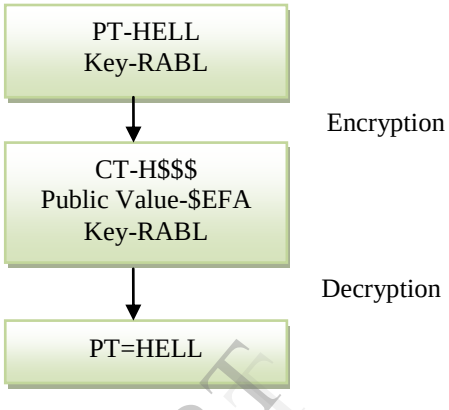

Figure 2 Block Diagram

3. Cryptanalysis of PA Cipher

Each permutation of the 26 letters of the English alphabet (there are 26! $=4*10^{26}$ in total) gives a unique key for encrypting a message. If a particular permutation is used to encrypt a message, then the inverse of that permutation can be used to decrypt it [5].But For PA Cipher we need more time to decrypt a plain text because channel does contain three information and we also provide a unique letter ‘A’ in key so this will enhance the security of the system. For a simple substitution cipher we will take N*M time while in the PA Cipher technique we will take N*M*O time.
Here N= Plain Text, M=Key, O= Public value

4. Result Analysis

After applying PA Substitution Cipher technique we increase the security of the system. Because the attacker will take more time to break the security. It will provide the better result than the simple substitution cipher technique. If we will make a graph for cryptanalysis than using PA Cipher technique attacker will take more time.
Here the value of public value and cipher text will be same. In the table-1 we compare the time to break the plain text.

S.No.	N	M	O	Simple Cryptanalysis	PA Cryptanalysis
R1.	4	3	4	4*3=12	4*3*4=48
R2.	8	4	8	8*4=32	8*4*8=256
R3.	15	2	15	15*2=30	15*2*15=450
R4.	11	5	11	11*5=55	11*5*11=605
R5.	12	6	12	12*6=72	12*6*12=864

Table 1 Cryptanalysis Time

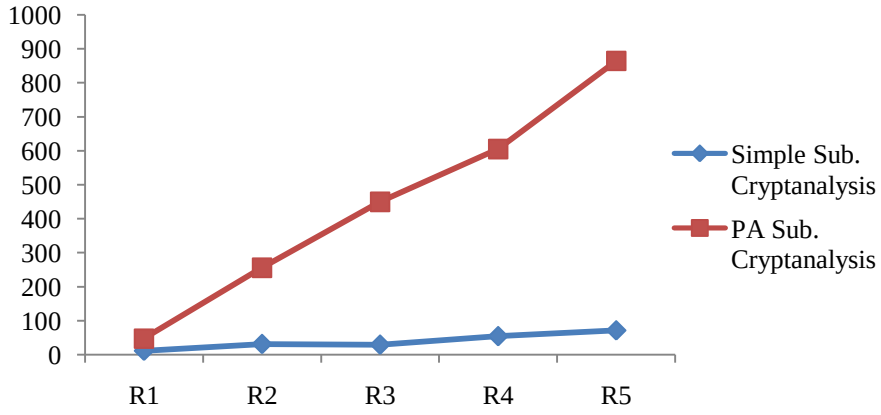

Figure 3 Times Taken for Break the Cipher Text

5. Conclusion

Substitution cipher is the main technology to cipher the plain text. But if we send it through network than an attacker easily break the plain text. But after applying PA Substitution Cipher we create the problem for the attacker because it will provide more security than the other substitution cipher technique. The result of this technique we have seen in the fig.-3

References

[1] W.Stallings; "Cryptography and Network Security" 2nd Edition, Prentice Hall, 1999.
[2] A.Menezes, P.van Oorschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
[3] D. Kahn, "Codebreakers: The Story of Secret Writing", Macmillan, 1967.
[4] Stamatios V. Kartalopoulos, the University of Oklahoma, **"**A Primer on Cryptography in Communications", IEEE Communications Magazine • April 2006.
[5] Sam Hasinoff "Solving Substitution Ciphers"

AUTHOR

Anuj Kumar: was born in India in April, 1986. He has completed his B.Tech in Information Technology from Hindustan Institute of Technology & Management, Agra, India in 2008.Currently he is pursuing M.Tech in Computer Science & Engineering from IEC-CET, Greater Noida, India.His interest areas are Security Application ,Network Security and Digital Image Processing.

Ankur Kumar Varshney: was born in India in August, 1986. He has completed his B.Tech in Computer Science & Engineering from Aligarh College of Engineering & Technology, Aligarh, India in 2008.Currently he is pursuing M.Tech in Computer Science & Engineering from B.S.A College of Engineering & Technology, Mathura, India. His interest areas are Security Application, Network Security and Digital Image Processing.

Pankaj Kumar: was born in Uttar Pradesh India in November, 1990. He has completed B.tech in Computer Science and Engineering from S.R.M.S. CET, Bareilly Uttar Pradesh, India in 2011. His interest areas are Data Compression, Network Security, Cryptography and Algorithm Analysis.