Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient Encryption Techniques In Cryptography Better Security Enhancement

Er. Reema Gupta, Dr. Sukhvir Singh, Pardeep Maan
NCCE,ISRANA(PANIPAT), Haryana, India

Abstract— There are many cryptography techniques that are used to encrypt and decrypt data that are transferred over a network. There are two basic types of cryptography :Symmetric Key and Asymmetric key. This paper describes various encryption techniques(Substitution and transposition) with their limitations .In this paper Encryption techniques are discussed with their limitations and procedure .Huffman coding and B2G,G2B is used for encryption. Various transpositional technique are also discussed –Simple columnar ,simple row,Route cipher, Myszkowski transposition.

Keywords—Cryptograhy;substitution;Caesar Cipher; Playfair;Transposition;Huffman coding; Route cipher; Myszkowski transposition

I. INTRODUCTION

The demand for effective network security is increasing exponentially day by day. Businesses have an obligation to protect sensitive data from loss or theft. Not only businesses see to the security needs; they have to understand where the computer is vulnerable and how to protect it. Cryptography[5] is the practice and study of techniques for secure communication in the presence of third parties. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and *public-key* systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

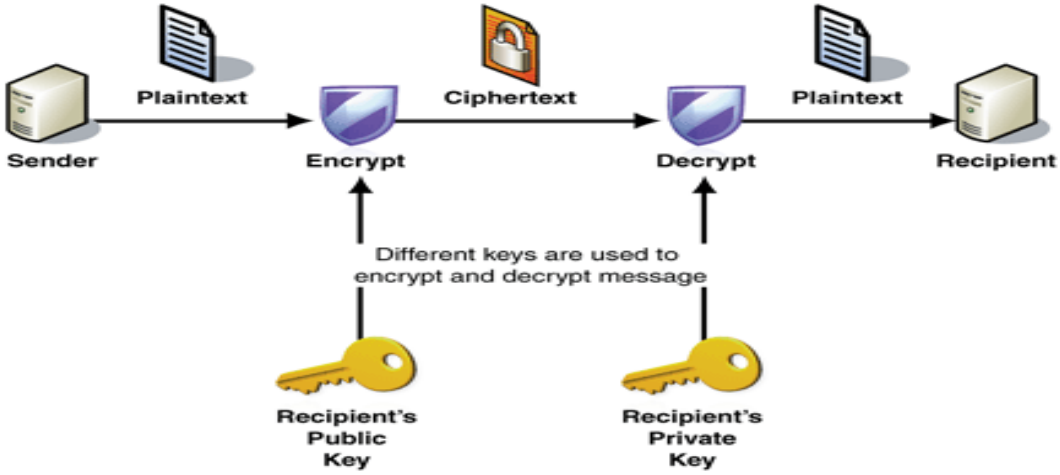

Fig1. Public Key System

II. ENCRYTION TECHNIQUES

A. *Caesar [7]Cipher*

It is one of the simplest method used for encryption .It replaces an alphabet with the one three places down the line.
e.g NCCE is codified as QFFH

But this is very weak scheme for hiding plain text messages.

B. *Modified Caesar[2] Cipher*

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1... Z = 25. Encryption of a letter *x* by a shift *n* can be described mathematically as,[2]

$$E_n(x) = (x + n) \mod 26.$$

Decryption is performed similarly,

$$D_n(x) = (x - n) \mod 26.$$

It is better than the Caesar cipher but still vulnerable to attack as there are only 25 possibilities to try out.

C. ***Mono-Alphabetic cipher***

In this cipher scheme we use random substitution each alphabet can be replaced by any other alphabet without any effect of consecutive positions.

But with this technique Language knowledge ,any if alphabet A codified as 'F' it will be remain F for whole plain text.This helps cryptanalyst to decode message easily.

D. ***PLAYFAIR CIPHER***

The 'key' for a Playfair cipher[6] is generally a word, for the sake of example we will choose

'ENGINEERS'

E N G I R
S A B C D
F G H K L
M O P Q T
U V W X Y

Any sequence of 25 letters can be used as a key, so long as all letters are in it and there are no repeats.Note that there is no 'j', it is combined with 'i'. We now apply the encryption rules to encrypt the plaintext.

But weakness is the fact that a digraph in the ciphertext (AB) and it's reverse (BA) will have corresponding plaintexts like UR and RU (and also ciphertext UR and RU will correspond to plaintext AB and BA, i.e. the substitution is self-inverse). That can easily be exploited with the aid of frequency analysis, if the language of the plaintext is known. If there are no double letter digraphs in the Cipher text then we can use Playfair cipher scheme.

E. ***B2G & G2B ENCRYPTION***

ENCRYPTION ALGORITHM:

Step1:Generate the ASCII value of the letter in the plain text.

Step2:Generate the corresponding binary value of it

Step3: Write Most Significant Bit (MSB) is same as the MSB in Binary Number.

Step4:. The second bit of the Grey code can be found by performing the Exclusive-OR (EX-OR) operation between the First and second bits of the Binary Number.

EX-OR Operation:

1. Both the bits are 0 or 1 then the output of EX-OR gate will be 0.
2. Any one of the bit in two bits is 1 then the output of EX-OR gate will be 1.

Step5: Then convert the gray code back to the alphabet according to ASCII value.

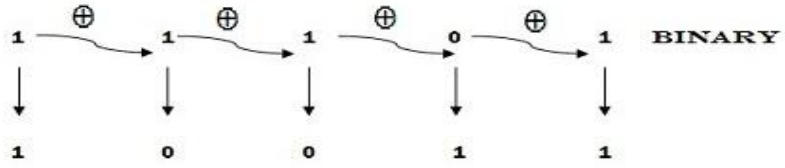

Fig.2 B2G conversion

DECRYPTION ALGORITHM:

Step1:Generate the ASCII value of the letter in the Cipher text.

Step2:Generate the corresponding binary value of it

Step3: Write Most Significant Bit (MSB) is same as the MSB in Binary Number.

Step4:. If the second Gray Bit is 0 then the second bit of the Binary is bit will be same as that of the First Binary bit; if the Second Gray Bit is 1 then the Second Bit of the Binary will be inverse of its previous binary bit.

EX-OR Operation:

1. Both the bits are 0 or 1 then the output of EX-OR gate will be 0.
2. Any one of the bit in two bits is 1 then the output of EX-OR gate will be 1.

Step5: Then convert the binary code back to the alphabet according to ASCII value and now text is Plain text .

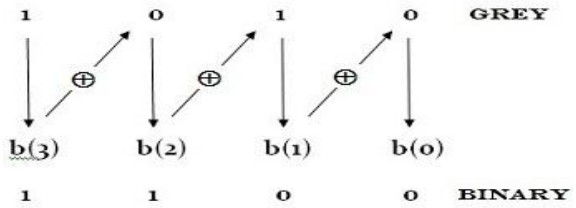

Fig 3. G2B Conversion

This encryption technique uses X-OR operation which is reversible in nature and we can decode text easily from the cipher text.Method of encryption(B2G) and decryption(G2B) is simple and effective for small amount of data.

F. USING HUFFMAN CODING [3]

The Huffman (or variable length coding) method is a lossless data compression algorithm based on the fact that some symbolshave a higher frequency of occurence than others. These symbols are encoded in fewer bits than the fixed length coding producing in average a higher compression. The idea behind Huffman coding is to use shorter bit patterns for more frequent symbols. To achieve that goal, Huffman algorithm needs the probability of occurence of each symbol. These symbols are stored in nodes and then sorted in ascending order
of their probability value.

ENCRYPTION ALGORITHM:

Step1: Generate random frequency probability between 0 & 1 for all symbols that are in plain text.
Step2: Then assign each probability to each symbol .
Step3:Then assign 0 or 1 based on its probability and its tree structure.
Step4: Then formulate a table that contain all letters and their corresponding codewords.

Symbols	Code words
0	1010
1	1011
2	1100
3	1101
4	1110
5	1111
6	00000

Then transmit it as a cipher text .This scheme helps us to reduce the length of data by assigning less no of bits to most frequent used letter in plain text.

DECRYPTION ALGORITHM:-

Step1. Create the Huffman tree based on that information.
Step2. Read data out of the file and search the tree to find the correct char to decode (a 0 bit means go left, 1 go rightfor binary tree).

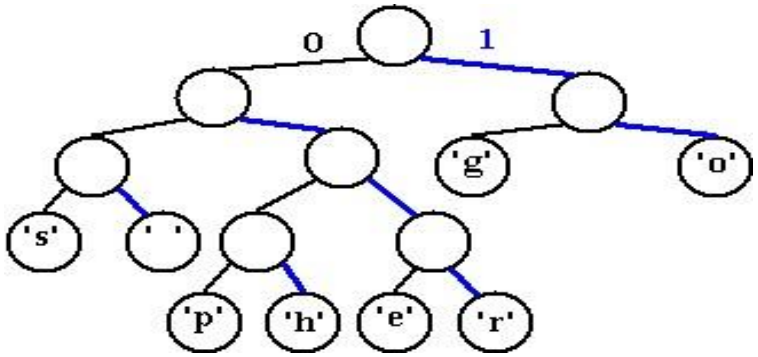

Fig. 4 Huffman coding tree

G. RAIL FENCE TECHNIQUE

It is transpositional technique (zigzag cipher). In the rail fence cipher, the plaintext is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail. When we reach the top rail, themessage is written downwards again until the whole plaintext is written out.

t i e
h s s t s

But this is easy to attack for the attackers .Differ from the other substitution techniques as it perform some permutation over the plain text alphabets.

F. Modified Rail Fence Technique

In this technique we use Rail fence key which has minimum value of 2 which tell us about no of rows to use for the permutation of the plain text and read data row by row as was in simple rail fence algorithm.

t i e
h s s t s
i a t

with rail fence key=3

H. Vernam's One-Time-Pad

Suppose Alice wishes to send the message "SUITS"
to Bob. Assume[8] two pads of paper containing identical random sequences of letters were somehow previously produced and securely issued to both. Alice chooses the appropriate unused page from the pad. Each letter from the pad will be combined in a predetermined way with one letter of the message. It is common, but not required, to assign each letter a numerical value: e.g. "A" is 0, "B" is 1, and so on.

In this example, the technique is to combine the key and the message using modular addition. The numerical values of corresponding message and key letters are added together, modulo 26.If key material begins with "hello" and the message is "suits", then the coding would be done as follows:

S U I T S Message
18S 2OU 8I 19T 18S Message
+ 7H 4E 11L 11L 14O Key
= 25 24 19 30 32 Message+Key
25Z 24Y 19T 4E 6G Message+Key(Mod 26)
Z Y T E G

Cipher computations "go past" Z, the sequence starts againat A. The cipher text to be sent to Bob is thus same process, but in reverse, to obtain the plaintext.Here the key is *subtracted* from the cipher text,again using modular arithmetic:

Z Y T E G Cipher text
25Z 24Y 19T 4E 6G Cipher text
-7H 4E 11L 11L 14O Key
=18 20 8 -7 -8 Cipher text-Key
=18S 20U 8I 19T 18S Cipher text-Key(mod26)
S U I T S Message

One time pad technique is highly secure and suitable for small plain text but is clearly impractical for large messages.

H. TRANSPOSITIONAL[1] TECHNIQUE

Transpositional technique can be row wise or column wise

- Simple Columnar [7]Transposition Technique:- In a columnar transposition, 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. Both the width of the rows and the permutation of the columns are usually defined by a keyword. permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".
- Simple Row Transposition Technique:- In a row transposition, the message is written out in columns of a fixed length, and then read out again row by row, and the row are chosen in some scrambled order. Both the width of the columns and the permutation of the rows are usually defined by a keyword. permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "3 2 1 ".
- Route Cipher:-Route cipher is a transpositional cipher where the key is the route chosen to read the text.Plain text is written out in the grid and use the route assigned . For the decryption purpose we need to know the size of grid(height,width) and the route used. It is easy to use to jumble a message.However, for a large message there are many routes that can be followed careful selection of route is required.
- Myszkowski transposition:-This transposition is variant of simple columnar transposition in the way it deals with recurring letters in the keyword.
  ENCRYPTION ALGORITHM:-
  We have to choose our keyword for the encryption process first.We then write out the plaintext in a grid, where the number of columns in the grid is equal to number of letters in the keyword.We then number each letter in the keyword with its alphabetic position giving repeated letters the same number.We then start at number 1,if a number appears more than once ,we read from left to right.Once completed move to next number.

T	O	M	A	T	O
4	3	2	1	4	3
T	H	E	T	O	M
A	T	O	I	S	A
P	L	A	N	T	I
N	T	H	E	N	I
G	H	T	S	H	A
D	E	F	A	M	I
L	Y	X	X	X	X

III. DECRYPTION ALGORITHM:-

We start by writing out the keyword,and the alphabetical order of the letters remembering to give repeated letters the same number.We then divide the length of the cipher text by the length of the keyword giving the number of rows. Start at number1,move to higher number and if number comes once,write the letters in the column .If the number appears twice,we move from left to right across the columns with that number heading them.
It is possible to perform multiple iterations to make it more secure.

CONCLUSION

We have many encryption/decryption techniques which we can use to codify data so that cannot be decoded by third person. Each technique has its pros and cons. We have to utilize each technique effectively depending upon our needs. In this paper B2G &G2B technique ,Huffman coding is also very useful to encode the data with reduced number of bits. Many different techniques can be combined to give more security.

References

Devendra Kumar Malakar, Prof. Dineshchandra Jain ,The Problem Analysis on Encryption techniques in Cryptography Vol 2 Issue 5 May 2013 ISSN 2319 – 8443

[1] Modified Caesar Cipher for Better Security Enhancement

[2] International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July

[3] Modelling data transmission through a channel based on Huffman coding and Encryption methods (IJCSIS) International Journal of Computer Science and Information Security 2010

[4] Dhananjay Pugila, Harsh Chitrala,AN EFFICEIENT ENCRPYTION ALGORITHM BASED ON PUBLIC KEY

[5] Ayushi,A Symmetric key cryptographic algoritm,International Journal of computer applications Volume 1-No 15

[6] AN ENHANCE SECURITY OF PLAYFAIR CIPHER SUBSTITUTION USING A SIMPLE COLUMNAR TRANSPOSITION TECHNIQUE WITH MULTIPLE ROUNDS (SCTTMR).

[7] Using Letters Frequency Analysis in Caesar Cipher with Double Columnar Transposition Technique, INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY
One Time Pad Data Security Scheme: Random Key Generation Approach

