Performance Analysis of Various Encryption Algorithms for Data Communication

[1]S. Padmapriya, [2]S. Saravanapriya, [3]D. Jayachitra
[1]Dept. of Computer Applications, Imayam College of IT, Tamil Nadu, India
[2]Dept. of Computer Science, Government Arts college for Men, Tamil Nadu, India
[3]Dept. of Computer Science, Nehru Memorial College, Tamil Nadu, India

Abstract
Communication without security is not reliable in today's networking world. Encryption algorithms provide the security to the users in the network. One of the tasks of the cryptosystem is to analyse the merits and demerits and select the algorithms that best address the problem to be solved. On the other side those algorithms consume a significant amount of computing resources such as CPU time and memory. This paper provides evaluation of four of the most common encryption algorithms. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as CPU time, memory and avalanche effect.

General Terms
Security, Algorithms.

Keywords
Cryptosystem, Cryptography, Encryption

I. Introduction

When the Internet provides essential communication between tens of millions of people security becomes a tremendously important issue to deal with. One essential aspect of secure communications is that of cryptography. Cryptography is the science of using mathematics to encrypt and decrypt data [3]. Cryptography enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. Many encryption algorithms are widely available and used in information security. They can be categorized into symmetric (private) and Asymmetric (public) keys encryption [1]. In symmetric key encryption or secret key only one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. Asymmetric key encryption or public key encryption two keys are used private and public keys. Public key is used for encryption and private key is used for decryption [5].

A. VIGENERE Scheme

- Use multiple mappings from plaintext to cipher text characters; the mappings are usually one-to-one as in simple substitution [5].
- Most polyalphabetic substitution ciphers are periodic substitution ciphers based on a period d.

Let: C1,…Cd, cipher alphabets

fi: A→Ci, mapping from plaintext alphabet A to the ith cipher

alphabet Ci ($1 \le i \le d$)

A plaintext message M is enciphered as follows:

M= m1…mdmd+1…m2d…

Ek(M)= f1(m1)…fd(md)f1(md+1)…fd(m2d)…

The key K is specified by a sequence of letters K=k1…kd, where ki (i=1,…,d) gives the amount of shift in the ith alphabet:

fi(a) = (a+ki) mod n.

Compute Ek(M), for M=RENAISSANCE, and K=BAND

B. PLAYFAIR Scheme

- The most general forms of substitution ciphers, permitting arbitrary substitutions for groups of characters.
- Enciphering larger blocks of letters makes cryptanalysis harder by destroying the significance of single-letter frequencies.

Digraph substitution cipher that uses a 5×5 matrix (J is not used) to generate the key.

Creation and population of Matrix:

1. The play fair cipher makes use of a 5*5 matrix (table), which is used to store a keyword or phrase that becomes the key for encryption and decryption. The way this is entered into 5*5 matrix is based on some simple rules:

- Enter the keyword in the matrix row-wise: left-to-right, and then top-to-bottom.
- Drop duplicate letters.
- Fill the remaining spaces in the matrix with the rest of the English alphabets (A-Z).
- While doing so, combine I and J in the same cell of the table. In other words, if I or J is a part of the keyword, disregard both I and J while filling the remaining slots.

```
[user@localhost ~]$ gcc vernam.c -lrt
[user@localhost ~]$ ./a.out

VERNAM CIPHER
---------------

1.Encryption
2.Decryption
Enter your choice: 1

Enter the file name: play.txt

File Content :
MYNAMEISATUL
Data :
TYGIMZYVRGCN
Starting time: 1300776858s 633824000ns
Ending time: 1300776858s 633828000ns
Processing Time: 4000ns
Enter the file for write : enc.txt
```

Fig. 1: Experimental Result for Vernam Cipher

C. COLUMNAR Scheme

Transposition ciphers rearrange characters according to some scheme. Many transposition ciphers permute the characters of the plaintext with a fixed period d.

A transposition cipher can be defined by providing an integer d, and a permutation f: Zd→Zd (where Zd is the set of integers 1 through d)[3].

- The key: K = (d,f)
- A plaintext message M is enciphered as follows:

M= m1…mdmd+1… m2d …
Ek(M) = mf(1)…mf(d)md+f(1)…md+f(d)…

1. Write the plain text message row-by-row in a rectangle of a pre-defined size. Read the message column-by-column. However, it need not be in the order of column 1, 2, 3 etc. It can be any random order such as 2,3,1 etc. The message thus obtain is the cipher text message.

D. VERNAM Scheme

A cipher in which the key is a random sequence of characters and is not repeated; the key is only used once.

1. Treat each plain text alphabet as a number in an increasing sequence i.e. A=0, B=1, C=2 and so on [3].
2. Do the same for each character of the input cipher text.
3. Add each number corresponding to the plain text alphabet to the corresponding input cipher text alphabet number.
4. If the sum thus produced is greater than 26, subtract 26 from it.
5. Translate each number of the sum back to the corresponding alphabet. This gives the output cipher text.

Experimental Design

All the four algorithms have been tested with different file size, and different keys

Several performance metrics are collected.

- CPU-Time
- Encrypted file size
- Avalanche Effect

1. CPU-TIME

The time complexity of an algorithm quantifies the amount of time taken by an algorithm to run as a function of the input to the problem. The running time of these four algorithms are calculated and tabulated.Figure1 represents this comparison for Vernam cipher.

The Table1 illustrates the CPU-Time computation among these algorithms.

Table 1: CPU-Time Comparison

Input size in bytes	Time in Nano seconds			
	Vignere cipher	Playfair cipher	Columnar cipher	Vernam Cipher
100	6000	9000	5000	4000
250	11000	16000	7000	5000
500	18000	28000	10000	6000
1024	33000	51000	17000	9000
Average Time	17000	26000	9750	6000

Fig. 1: Represents the time complexity analysis among these four algorithms. The results shows that vernam cipher is proven best than the other algorithms.

II. Encrypted File Size

This type of comparison is made to find out the length of the message before and after comparison. The experimental results shows that the columnar and vernam cipher and vignere except play fair produces the cipher text size which is same as that of the plaintext [5]. The Table 2 and fig. 2, represent the encrypted file size in Kb.

Table 2: Size Comparison

File Size in KB	Vignere cipher	Play Fair cipher	Columnar cipher	Vernam cipher
5Kb	5 Kb	5.21 Kb	5 Kb	5 Kb
4 Kb	4 Kb	4.15 Kb	4 Kb	4 Kb
3 Kb	3 Kb	3.11 Kb	3 Kb	3 Kb

III. Avalnche Effect

A desirable property of any encryption algorithm is that a small change in either the plain text or the key should produce a significant change in the cipher text. Avalanche effect is the phenomenon that describes the effect in the output cipher text if a single or few bits are changed in the plain text, whereas this change that occurs at the output should be sufficient if we want to create a secure algorithm [4].

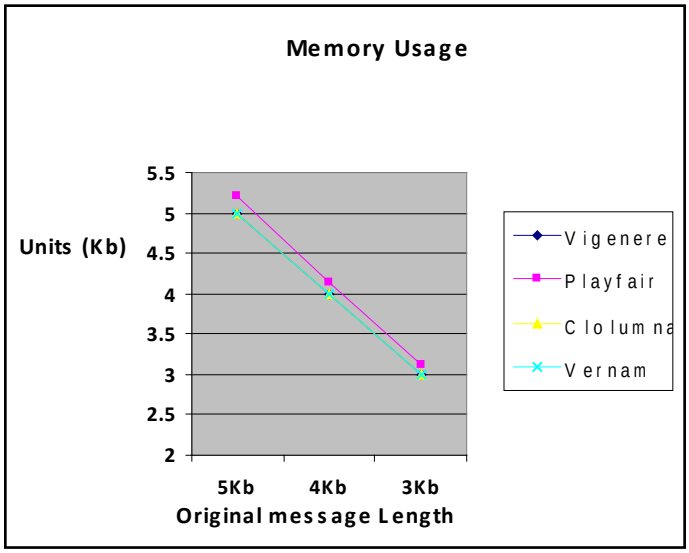

Fig. 2: Comparision of Encrypted File Size

Here we made a comparison between Vigenere, Playfair, Columnar and Vernam on the basis of avalanche effect with same key and plaintext. This analysis shows that the Vernam cipher exhibits a strong avalanche effect because vernam cipher generates different key for every iteration. The table3 illustrates the avalanche effect.

Table 3: Avalanche Comparison

Encryption Technique	Avalanche effect	Percentage (%)
Vigenere	3bits	5.4
Playfair	6bit	10.7
Columnar	2bit	3.6

III. Conclusion And Future Scope

This paper presents the performance evaluation of selected encryption algorithms. Several points can be concluded from the experimental results. First; in the case of time it was concluded that vignere has better performance than the other common encryption algorithms used. Secondly in the case of encrypted file size the Play fair cipher consumes more memory than the original plain text whereas the others consume the same as plain text. Third: In the case of avalanche comparison vernam cipher exhibits a strong

avalanche affect. In future we can perform the same analysis with public key algorithms and also we can perform it on images audio and video files.

References

[1] Neetu Settia,"cryptanalysis of modern cryptographic Algorithms", IJCST Vol. 1, Issue 2, December 2010.
[2] Shashi Mehrotra Seth, Rajan Mishra,"Comparative Analysis of Encryption Algorithm for data communication", IJCST Vol. 2, Issue 2, June-2011.
[3] Cryptography and Network Security, second edition,Tata McGrawHill.
[4] Wikipepedia, [Online] Availavle: http://en.wikipedia.org/wiki/Avalanche_effect
[5] S.William,"Cryptography and Network Security", Second Edition,Prentice Hall.
[6] Mani Arora, Dr. Derick Engeles,"Analysis of ciphertext size produced by various encryption Algorithms", IJEST Vol 3, No. 7, July2011.
[7] Andrew S.Tanenebaum,"Computer Networks", by Prentice Hall.