Volume 1, Issue 6, September 2016 ISSN: 2456-0006
International Journal of Science Technology Management and Research
Available online at: www.ijstmr.com

Fast and Efficient Bits Compressed Technique For Encryption and Decryption of Text Data

Thitme Sandip Karbhari
M. Tech. (CSE) IV Sem.
Lord Krishna College of Technology
Indore M.P. India

Vijay Kumar Verma
Asst. Prof Dept. of CSE
Lord Krishna College of Technology
Indore M.P. India

Abstract: - In era of Internet technology and smart phone commination are very fast Columniations include messages files, picture, audio and video data. Communication between a sender and receiver needs security. Security include changing the information to some unidentifiable form, can save it from assailants. For example, plain text can be coded using schemes so that a stranger cannot apprehend it.
Cryptography is a technique which deals with the secret transmission of messages, data between two parties' sender and receiver. Today several real life applications like ATM cards, computer passwords, and electronic commerce are used Cryptography based security techniques. There are several algorithms and methods have been developed by various researchers for Cryptography but improvement is always required there are two fundamental key issue which are always consider number of keys used and memory required for encryption and decryption . In this paper we proposed an efficient approach for encryption and decryption of text data. Proposed is based on hamming code and reduced memory requirement for encryption and decryption of text data.

Keywords:- Public, Private Security ,Encryption, Decryption, Hamming code.

I. INTRODUCTION

There are three important objectives of every cryptographic system.

A. Authentication:
Authentication is the act of confirming the truth of an attribute of an entity i.e. the assurance that the communication entity is the one that it claims to be.

B. Data Confidentiality:
It is about the protection of data from unauthorized access. To protect the data, encryption of messages is being used.

C. Data Integrity:
The assurance that data received is exactly as sent by an authorized entity i.e. contains no modification, insertion, deletion. It refers to trustworthiness of information over its entire transmission. Data integrity can be achieved by following some rules, by placing check values.

II. BASIC TERMINOLOGY USED IN CRYPTOGRAPHY

Basic terminology is very important to understand encryption and description. These are

A. Plain Text or Normal Text: - The original text or message used in communication in called as Plain text.

B Cipher Text: The plain text is encrypted in un-readable message. This meaningless message is called Cipher Text

C. Encryption: Encryption is a process of converting Plain text into Cipher text. This non-readable message can securely be communicated over the unsecure network. Encryption process is done using encryption algorithm.

D. Decryption: Decryption process is the reverse of Encryption process, i.e. Cipher text is converted into plain text using particular encryption algorithm.

E. Key: A key is a numeric or Alpha-numeric text (mathematical formula). In encryption process it takes place on Plain text and in decryption process it takes place on cipher text.

F. Key Size: Key size is the measure of length of key in bits, used in any algorithm.

G. Round: - Round of encryption means that how much time encryption function is executed in complete encryption process till it gives cipher text as output.

III. CLASSIFICATION OF CRYPTOGRAPHY SYSTEM

Cryptography systems can be broadly classified into two categories:

1. Symmetric encryption algorithms
2. Asymmetric encryption algorithms

Symmetric encryption algorithms, that use a single key that both the sender and recipient have. This key is kept secret among sender and receiver so that no intruder can steal the data to be transferred by encrypting it. Asymmetric encryption algorithm or public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. Individuals who practice this field are known as cryptographers. Asymmetric encryption provides more security as compared to symmetric key encryption but in case of encryption speed, symmetric encryption is on lead

IV LITERATURE REVIEW

In 2012 Ali Ahmad Milad & Hjh Zaiton Muda proposed "Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack)". They compared performance of the two of the popular secret key encryption algorithms (Blowfish and Skipjack). They implemented Blowfish and Skipjack and tested their performance and compared by encrypting input files of varying contents and sizes. They concluded that the Blowfish is the best performing algorithm for implementation [1].

In 2013 Mini Malhotra &, Aman Singh proposed "Study of Various Cryptographic Algorithms". They represented and published knowledge from IEEE online database. This paper provides a direction to the naive users and will allow many new future applications [2].

In 2014 K.B. Priya Iyer & R. Anusha "Comparative Study on Various Cryptographic Techniques". Their main objective is to provide the basic terms used in cryptography its purpose and to compare the encryption techniques used in cryptography [3].

In 2014 Ranjeet Masram & Vivek Shahare, Jibi Abraham proposed "Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based On Various File Features". They provides a analysis and comparison of some symmetric key cryptographic ciphers (RC4, AES, Blowfish, RC2, DES, Skipjack, and Triple DES) on the basis of encryption time with the variation of various file features like different data types, data size, data density and key sizes[4].

In 2014 Jitendra Singh Chauhan & S. K. Sharma proposed "A Comparative Study of Cryptographic Algorithms". They focused on the comparative study of various cryptographic algorithms like AES, DES, RSA, Blow Fish, Elliptic Curve, SHA and MD5 and give a proper direction to the users for use of proper algorithm for securing of data [5].

In 2015 Yousif Elfatih Yousif & Dr. Amin Babiker Mustafa proposed "Review on Comparative Study of Various Cryptography Algorithm". They defined and analyzed various cryptographic symmetric algorithms like DES, Triple DES, AES and asymmetric key cryptographic algorithms like RSA [6].

In 2015 Nivedita Bisht & Sapna Singh proposed "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms". They provide a comparative study between various encryption algorithms like AES, DES, RSA and DIFFIE-HELLMAN. They compare the different factors of both symmetric key and asymmetric key encryption algorithm[7].

In 2015 Rajdeep Bhanot & Rahul Hans proposed "A Review and Comparative Analysis of Various Encryption Algorithms". They analyzed ten data encryption algorithms DES, Triple DES, RSA, AES, ECC, Blowfish, Twofish, Threefish, RC5 and IDEA etc. Among them DES, Triple DES, AES, RC5, Blowfish, Twofish, Threefish and IDEA are symmetric key cryptographic algorithms. RSA and ECC are asymmetric key cryptographic algorithms. They analyzed encryption algorithms on the basis of different parameters and compared them to choose the best data encryption algorithm so that we can use it in our future work[8].

In 2015 Kranti M. Chaudhari & Megha V. Borole proposed "A Survey on Various Cryptographic Algorithms for Security Enhancement ". They provided details study on the data sharing services of cloud systems and surveyed on various cryptographic algorithms that are used during sharing data securely over the cloud[9].

In 2016 Ankita Verma1 & Paramita Guha proposed "Comparative Study of Different Cryptographic Algorithms". They classify the two types of Encryption Algorithm, Symmetric and Asymmetric Encryption Algorithm, and presented a comparative survey on its types like AES, DES, RSA and BLOWFISH.

V PROPOSED APPROACH

Consider a simple example of plain text

NETWORKS

ASCII size of the text 64 bits

TABLE 1 character with frequency and ASCII Code

Character	Frequency	ASCII value
N	1	78
E	1	69
T	1	84
W	1	87
O	1	79
R	1	82
K	1	75
S	1	83

TABLE 2 Character with ASCII Code and binary equivalent

Character	ASCII value	Binary equivalent
N	78	01001110
E	69	01000101
T	84	01010100
W	87	01010111

O	79	01001111
R	82	01010010
K	75	01001011
S	83	01010011

Now construct optimal merge code show in the table 3
Arrange these codes
000001010011100101110111=24 bits compressed code
Reversing this code
111110101100011010001000
Now use 1000 as secrete key and add into the above text
111110101100011010010000
Now group this code into 8 bits size

TABLE 3 Optimal merges code

Character	Compressed Optimal merge code
N	000
E	001
T	010
W	011
O	100
R	101
K	110
S	111

Arrange these codes
Compressed code reversing this code
Now use 1000 as secrete key and add into the above text
Now group this code into 8 bits size

TABLE 4 Encrypted code

Compressed code	Decimal equivalent	ASCII character
11111010	250	.
11000110	198	╝
10010000	144	É

Finally we got Cipher text is . ╝ É .For the decryption we apply the reverse process and get original text.
We repeat the reverse process of encryption to decrypt the message.

VI PROPOSED ALGORITHM

We use the following step to encrypt the message.
Step1.Find the ASCII value of the each letter of the given word.
Step2.Find the binary equivalents of the ASCII value obtained in the first step.
Step3.Now compressed the binary value according to the optimal merge pattern.
Step4 Arrange these compressed code and find its reversing this code
Step 5.Use a secrete key to generate encrypted text.

VII. COMPARATIVE ANALYSIS

We compare the proposed method with symmetric key approach by using file size and execution time for encryption as parameter. Form the graph it is clear that the proposed approach takes less time for encryption as compared to the existing method.

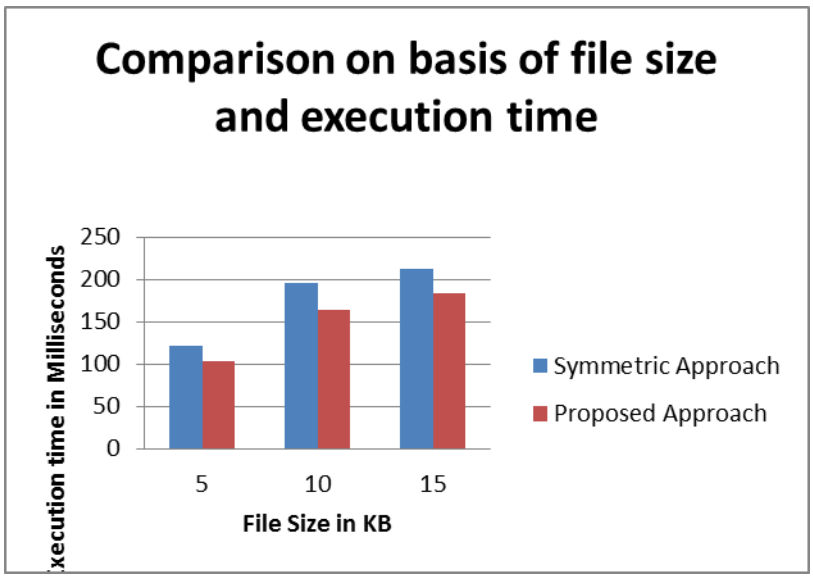

Figure 1- Comparison on the basis of file size and execution time

REFERENCES

[1]Ali Ahmad Milad, Hjh Zaiton Muda "Comparative Study of Performance in Cryptography Algorithms" (Blowfish and Skipjack) Journal of Computer Science 2012 ISSN 1549-3636 © 2012 Science Publications

[2]Mini Malhotra, Aman Singh "Study of Various Cryptographic Algorithms" International Journal of Scientific Engineering and Research (IJSER) Volume 1 Issue 3, November 2013

[3]K.B. Priya Iyer & R. Anusha "Comparative Study on Various Cryptographic Techniques" International Journal of Computer Applications International Conference on Communication, Computing and Information Technology *(ICCCMIT-2014)*

[4] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona "Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based On Various File Features" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014

[5]Jitendra Singh Chauhan & S. K. Sharma "Comparative Study of Cryptographic Algorithms" International Journal for Innovative Research in Multidisciplinary Field ISSN – 2455-0620 Volume - 1, Issue - 2, Sept – 2015

[6]Yousif Elfatih Yousif, 2Dr.Amin Babiker A/Nabi Mustafa, 3Dr.Gasm Elseed Ibrahim Mohammed "Review on Comparative Study of Various Cryptography Algorithm " Volume 5, Issue 4, 2015 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[7]Nivedita Bisht, Sapna Singh "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms International Journal of Innovative Research in Science, Engineering and Technology. (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2015.

[8]Rajdeep Bhanot and Rahul Hans "A Review and Comparative Analysis of Various Encryption Algorithms International Journal of Security and Its Applications Vol. 9, No. 4 (2015)

[9]Kranti M. Chaudhari & Megha V. Borole "A Survey on Various Cryptographic Algorithms for Security Enhancement International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 7, January 2015

[10]Ankita Verma, Paramita Guha & Sunita Mishra "Comparative Study of Different Cryptographic Algorithms" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 5, Issue 2, March - April 2016