International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

A Reliable Secret Key Algorithm for Encryption and Decryption of Text Data

Pramod Gorakh Patil[1], Vijay Kumar Verma[2]
[1]*M.Tech IV Semester Lord Krishna College of Technology Indore*
[2]*Asst. Prof. CSE Dept. Lord Krishna College of Technology Indore*

Abstract: - Cryptography converts the original message into non-readable format andsends the message over an insecure channel.Classical cryptanalysis involves an interestingcombination of analytical reasoning andmathematical tools. Several algorithms have been developed and used complicated keys to produce cipher text from plain text or complicated algorithms for it. Security of all algorithms is dependent on length of keys and techniques used in the algorithm. In this paper we proposed an efficient reliable symmetric key based algorithm to encrypt and decrypt the text data. We use ASCII (8 bit) value of alphabet and perform some simple calculation like logical NOT and binary division to produce. The proposed method is easy to understand and easy to implement.
Keywords:-Cryptography, Binary Division, Encryption, Encryption, Security

I. INTRODUCTION

Cryptography having security mechanism that is designed to detect or prevent from a securityattacks.The major problem in symmetric key cryptography is that of the key distribution because the key must be shared secretly. Keys can be distributed by any one of the following ways

1. Sender can select the key and physically deliver it to receiver.
2. A trusted third party can select the key and physically deliver it to the sender and the receiver.
3. If sender and receiver have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
4. If sender and receiver each has an encrypted connection to a third party, then the third party can deliver a key on the encrypted links to receiver.

Security mechanism of cryptography is divided intotwo types

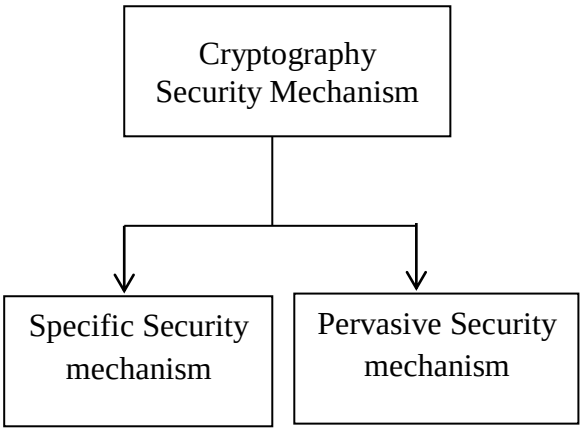

Figure 1: Types Cryptography Security Mechanism

Specific securitymechanism may be incorporated into the appropriateprotocol layer in order to provide some of the OSI securityservices for example digital signature.Pervasive security mechanisms those are not specific to anyparticular OSI security service or protocol layer for examplesecurity label, event detection, etc[10].

II. LITERATURE EVIEW

In 2011 B. Ravi Kumar, Dr. P. R. Murti proposed "Data Encryption and Decryption processUsing Bit Shifting and Stuffing Methodology". Incomputer system to represent a printable character it requires one byte, i.e. 8 bits. So a printablecharacter occupies 7 bits and the last bit value is 0 which is not useful for the character. In proposed methodwe are stuffing a new bit in the place of unused bit which is shifting from another printable character. Soin proposed BSSmethodology after encryption, for every eight bytes of plain text it will generate seven bytescipher text and in decryption, for every seven bytes of cipher text it will reproduce eight bytes of plaintext. They presented an implementation of BSS encryption algorithm. The main objective was toevaluate the performance of this algorithm in terms of data size [1].

In 2012 Neha Jain and Gurpreet Kaur proposed "Implementing DES Algorithm inCloud for Data Security". They presented Data security system in cloud computing using DES algorithm. The proposed cipher BlockChaining system is to be secure for clients and server. The proposed thatthe cloud data security must be considered to analyse the data security risk, the data security requirements, deployment of security functions and the data security process through encryption. They proposed a new data security solution with encryption, which is important and can be used as referencefor designing the complete security solution [2].

In 2012 Nilesh Kumbhar Virendra Singh Mohit A. Badhe proposed "The Comprehensive Approach for Data Security in Cloud Computing: A Survey". They have tried to access separate encryption and decryption service using RSA algorithm and computing is a paradigm in which information is stored in servers on the internet. They proposed a comprehensive and effective methodology to data storage and retrieval security issue in cloud computing. Proposed method achieved the availability, reliability and integrating though out the process. Even any unauthorized user trying to access the confidential data, out method should not allow to access within the cloud [3].

In 2013 Sombir Singh Sunil K. Maakar Dr.Sudesh Kumar proposed "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques". They proposed an Enhanced DES algorithm the security has been improved which is very crucial in the communication and field of Internet. So the security is approximately double as compared to a simple DES algorithm. The original DES implementation has some weaknesses; to overcome the most of weakness the Enhanced DES algorithm is designed. The Designed system improved the security power of original DES. The only drawback of Enhanced DES is extra computation is needed but the todays computer have parallel and high speed computation power so the drawback of the Enhanced DES algorithm is neglected because aim is to enhance the security[4].

In 2013 Mansoor Ebrahim Shujaat Khan proposed "Symmetric Algorithm Survey: A Comparative Analysis". They presented a comprehensive comparative analysis of different existing cryptographic algorithms (symmetric) based on their Architecture, Scalability, Flexibility, Reliability, Security and Limitation that are essential for secure communication (Wired or Wireless).The main objective was to analyze the performance of the most popular symmetric key algorithms in terms of Authentication,

Flexibility, Reliability, Robustness, Scalability, Security, and to highlight the major weakness of the mentioned algorithms, making each algorithm's strength and limitation transparent for application [5].

In 2013 Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti,Mr.T. Sri Harish Reddy, Dr. S. Kiran proposed "An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding". They implemented security for image. They considered an image, read its pixels and convert it into pixels matrix of order as height and width of the image. Replace that pixels into some fixed numbers, generate the key using random generation technique.Encrypting the image using this key, performing random transposition on encrypted image, converting it into one dimensional encrypted array and finally applied Huffman coding on that array, due this size of the encrypted image is reduced and image is encrypted again [6].

In 2014 Satyajeet R. Shinge, Rahul Patil proposed "An Encryption Algorithm Based on ASCII Valueof Data". They presented a symmetric cryptographicalgorithm for data encryption and decryption based on ASCIIvalues of characters in the plaintext. This algorithm encryptsthe plaintext using their ASCII values. They proposed a symmetric encryptionalgorithm using ASCII values of data. The proposedalgorithm gives good result in less execution time. Thistechnique generates key automatically to encrypt themessage. The automatically generated key is converted to another string and same key is used for encryption anddecryption [7].

In 2014 Prakash G L, Dr. Manish Prateekand Dr. Inder Singh proposed "Data Encryption and Decryption Algorithms use Key Rotationsfor Data Security in Cloud System".They proposed an efficient data encryption to encrypt sensitive data before sending to thecloud server. This exploits the block level data encryption using 256 bit symmetric key with rotation. They analyse the privacy protection of outsourced datausing experiment is carried out on the repository of text files with variable size. The security and performance analysis shows thatthe proposed method is highly efficient than existing methods performance. They proposed an efficient data encryptionand data decryption algorithm to protect theoutsourcedsensitive data in cloud computing environment [8].
In 2015Sanket A. Nilesh Chaubey, Shyam P. Dubey proposed "AdvancedASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id". They proposed square measure proposing a brand new algorithm for cryptography technique, UPMM rule, which is applied on computer code worth of knowledge. Computer code values square measure encrypted using a key involving word numbers and distinctive alphanumeric id that is additionally reborn into computer code worth to provide authentication over the network. They proposed a technique to send information over the network in set of 3 keys. The proposed approach a combination of word range and matrix multiplication is employed for encrypting the info. Within the same manner decryption will be done at receiver's facet by victimization inverse of encoding matrix [9].

III. PROPOSED METHOD

We propose a simple and reliable algorithm for encryption and decryption of text data. Our proposed algorithm used the following steps.

Encryption Process

Step1: Find the 8 bit binary code of the alphabets.
Step 3: Generate its reverse the binary number.
Step 4: Use any four digit binary number as divisor which is a key.
Step 5: Now divide the binary eight bit code with the divisor.
Step 6: Store the remainder in first 3 bits & quotient in 5 bits.

Step 7: Now generate binary 8 bit code using first 3 bit remainder followed by 5 bit quotient.
Step 8: replace the code by its equivalent alphabets as cipher text.

Decryption Process

Step1: Multiply last 5 bits of the ciphertext by the Key
Step 2: Add first 3 bits of the ciphertext with the result producedin the previous step
Step 3: If the result produced in the previous is notan 8-bit number we need to make it an 8- bit number
Step 4: Reverse the number to get the original text.

IV. ILLUSTRATE THROUGH EXAMPLE

Let, the character is T. Now according to the steps we will getthe following:
Binary code of Tis 1010100. Since it is not an 8 bitbinary numbers we need to make it 8 bit number as per the encryption algorithm. So it would be 01010100. Reverse of this binary number would be 00101010. Let 1000 as divisor i.e. Key. Divide 00101010 (dividend) by 1000(divisor)the remainder would be 10 and the quotient would be 101.
So as per the algorithm the cipher text would be 01000101 which i E.
We have got E as the ciphertext. Nowaccording to decryption go back the originaltext T. After multiplying 00101 by1000 (Key) the result would be 101000. After adding 010 first 3 digits of the cipher text with101000 the result would be 101010. Since 101010 is not an 8-bit number we need to make it00101010. After reversing the number it would be 01010100 which is equivalent of binary code of T, This was the original character.

V. EXPONENTIAL ANALYSIS

We have implemented the proposed method and Symmetric Key Encryption Algorithm using VB DOT Net 2010, window 7 operating system with i3 processor. We use simple text file with different size .We compare the proposed algorithm with Symmetric Key Encryption Algorithm using different parameter like file size, encryption time , memory , and decryption time.

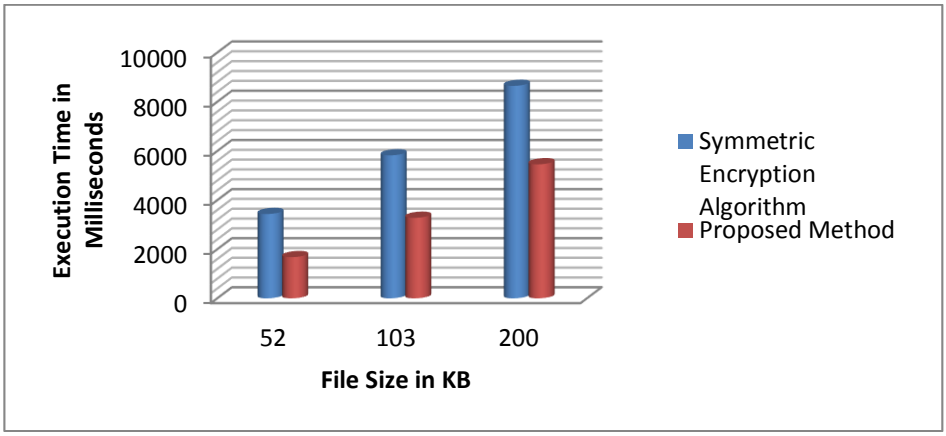

Figure 2: comparison using file size and execution time

VI. CONCLUSION

The objective of every algorithm is key of length used for encrypt and decrypt the data. From the experimental analysis it is clear that the proposed method works efficiently. The aim of this proposed algorithms cost-effective in term of memory, execution time and scalability to encrypt and decrypt the text data.

REFERENCE

i. B. Ravi Kumar, Dr.P.R.K.Murti "Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology" International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 7 July 2011

ii. Neha Jain and GurpreetKaur "Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 (4), 2012

iii. Nilesh N. Kumbhar Virendrasingh V. ChaudhariMohit A. Badhe "The Comprehensive Approach for Data Security in Cloud Computing: A Survey" International Journal of Computer Applications Volume 39 No.18, February 2012.

iv. Somber Singh "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques" Volume 3, Issue 6, June 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

v. Mansour Ebrahim "Symmetric Algorithm Survey: A Comparative Analysis" International Journal of Computer Applications Volume 61 No.20, January 2013

vi. Dr. T. Bhaskara Reddy, Miss. Hema Suresh Yaragunti ,Mr.T. Sri Harish Reddy , Dr. S. Kiran " An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding" IJCTA Nov-Dec 2013

vii. Satyajeet R. Shinge , Rahul Patil "An Encryption Algorithm Based on ASCII Value of Data" Satyajeet R. Shinge et al, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234

viii. Prakash G L ,Dr. Manish Prateek and Dr. Inder Singh "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System "International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 4 April, 2014 Page No. 5215-5223

ix. Sanket A. Ubhad, Nilesh Chaubey, Shyam P. Dubey " Advanced ASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id" International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 8, August 2015

x. Saranya K "A Review on Symmetric Key Encryption Techniques in Cryptography" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014

