IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Enhanced key-generation algorithm using MRMCTT in Data encryption standard algorithm

Bhawana Singh[1], Rishi Sharma[2], Kamal Kant Verma[3], Satendar Kumar[4]

Student, Computer Science Engineering, Quantum school of Technology, Roorkee, India[1]

Senior Assistant Professor, Computer Science Engineering, Quantum school of Technology, Roorkee, India [2, 3, 4]

Abstract: The Data Encryption Standard is known as a block cipher technique which means a cryptographic key and an algorithm is applied with a block of data simultaneously rather than one bit at a time. To encrypt a plain textmessage, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit cipher text by means of permutation and substitution.The process involves 16 rounds and can run in four different modes, encrypting blocks individually or making each cipher block dependent on all the previous blocks.

Keywords: DES, cipher text, substitution, encryption.

I. INTRODUCTION

The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding ciphers text to plaintext is called Decryption. This can be done by two techniques symmetric-key cryptography and asymmetric key cryptography. Symmetric key cryptography [3,4,9] involves the usage of the same key for encryption and decryption. But the Asymmetric key cryptography involves the usage of one key for encryption and another, different key for decryption. Secret key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithms [7,8] etc. and public key cryptography includes RSA, Digital Signature and Message Digest algorithms. For each algorithm there are two key aspects used: Algorithm type (define size of plain text should be encrypted per step) and algorithm mode (define cryptographic Algorithm mode). Algorithm mode is a combination of a series of the basic algorithm and some block cipher and some feedback from previous steps.

II. LITERATURE REVIEW

An"**Govind Prasad Arya, AayushiNautiyal, Ashish Pant, Shiv Singh &TishiHanda**" [4] worked on "**A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations**" proposed Modern computing is observed to be highly dependent on communication and data transport. The security of data during communication has become a mandatory need since the introduction of e-commerce, mails, etc. Moreover a lot of data may be required to be kept secure on local devices also. The encryption of data is the basic requirement today and thus helps to maintain confidentiality of data. A number of algorithms are available for encrypting data while it is transferred from sender to receiver. In this paper we have proposed a cipher which uses basic encryption techniques of substitution and transposition along with application of logic gates, in order to encrypt the data. The algorithm makes cryptanalysis even more difficult because of the use of "Random Number Generator" function which further decides order of encryption rounds and keys to be used to encrypt the plain text. This eliminates the overhead of defining a fixed key by the user and makes algorithm secure also. It also facilitates to transfer the key to the receiver while being added with the plain text at random locations (like added at end or beginning).

"**R.L. Rivest, A. Shamir, and L. Adleman**" [6] worked on "**A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**" proposed an encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

1. Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intended recipient. Only he can decipher the message, since only he knows the corresponding decryption key.
2. A message can be \signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in \electronic mail" and \electronic funds transfer" systems.

"**Manikandan.G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G**" [2] worked on "**A Modified Crypto Scheme For Enhancing Data Security**" proposed that Most of the existing systems which offer security to a network or web or to a data are vulnerable to attacks and they are breached at some point of time by effective cryptanalysis, irrespective of its complex algorithmic design. In general, today's crypto world is restricted to a practice of following any one single encryption scheme and that too for a single iteration on a

single file basis. This is evident in the 99% of the encryption-decryption cases. So, A need for "practically strong and infeasible to get attacked" technique becomes vital. In this paper, we propose a Software tool which involves Cryptographic enciphering and deciphering along with File Splitting and Merging mechanisms. We used modified Blowfish algorithm for Encryption and Decryption of data. Though we use only one algorithm, we differentiate the cryptographic scheme by varying the key for varying file slices. Our results clearly justifies that our tool serves as a better solution both in terms of performance as well as security.

"**Shah Kruti R., BhavikaGambhava**" [3] worked on "**New Approach of Data Encryption Standard Algorithm**" proposed the principal goal guiding the design of any encryption algorithm must be security against unauthorized attacks. Within the last decade, there has been a vast increase in the accumulation and communication of digital computer data in both the private and public sectors. Much of this information has a significant value, either directly or indirectly, which requires protection. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. Performance and security level is the main characteristics that differentiate one encryption algorithm from another.

Here introduces a new method to enhance the performance of the Data Encryption Standard (DES) algorithm is introduced here. This is done by replacing the predefined XOR operation applied during the 16 round of the standard algorithm by a new operation depends on using two keys, each key consists of a combination of 4 states (0, 1, 2, 3) instead of the ordinary 2 state key (0, 1). This replacement adds a new level of protection strength and more robustness against breaking methods.

"**Ms. Ramya G., Ms. Anita Madona M.**" [10] worked on "**Enhancing DES and AES with 1024 Bits Key**" proposed Cryptography is the art of achieving security by encoding messages to make them non-readable. There are two basic types of cryptography: Symmetric and Asymmetric cryptography. Symmetric Key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known Symmetric Key algorithms: DES, RC2, RC4, AES etc. are much private but some are less private because the attacker or the hackers can hack the messages. DES is now considered to be insecure for many applications because the 56-bit key size is too small and possible to brute-force in finite time on modern processor.

The AES algorithm was believed to provide more security than the DES. A new scheme of Symmetric Key algorithm DES and AES is proposed with 1024 bit key. This technique provides more security and increases the efficiency with different key length settings. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) with 1024 bit key is implemented using NS2 software to make comparison on the basis of parameters like speed, block size, and key size.

"**Ms. Priya S, Ms. Anita Madona M**" [11] worked on "**Hybrid Data Encryption Standard**" proposed Security is playing an important role in the field of network communication system. Cryptography is the branch of computer science that deals with hiding information for secure communication of data. It uses the codes to convert plain text into cipher text, so that only the intended recipient will be able to read it using the key. The cryptographic algorithms are mainly divided into two categories as Symmetric and Asymmetric on the basis of using the same or different key for encryption and decryption.

The most popular and widely used symmetric-key system is the Data Encryption Standard (DES) in which both the sender and receiver use a shared secret key to encrypt or decrypt the data. DES is the block cipher which takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. The key basically consists of 64 bits however, only 56-bits of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56-bits. DES is now considered to be insecure for many applications. This is due to the 56-bit key size being too small which is not so powerful against the Brute force attack. To improve the security of DES algorithm and to avoid the Brute force attack, the substitution technique-Affine Cipher is used to mask the plaintext and then pass it as input to the DES algorithm to perform encryption. This Affine Cipher is used before the original DES algorithm, to make cryptanalysis difficult and improve the security of DES. The Simulation tool NS-2 is used to compare and analyze the performance of DES and the Hybrid DES.

III.PROPOSED WORK

The proposed scheme has first to process the Multiple Rounds for Modified Columnar Transposition Technique (MRMCTT). The plain text message is first converted into the cipher text by using Modified Columnar Transposition Technique as the cipher text is again applied to the columnar technique and for this the cipher will be stronger. Also in every round the enhanced key generation algorithm is applied. The various rounds of MRMCTT may depend upon the security to provide the message. If more security is needed then added more rounds of the MRMCTT scheme and if the normal security then uses minimum 1 or 2 rounds. The input to the MRMCTT is a plain text message and the output is ciphered text message. To apply this scheme we required the matrix or table to perform the encryption process and column number which provide the security key. The output from MRMCTT is then converted into a bit form because the DES algorithm applies its process on bit level as usual. Then the DES has performed its work same as original DES.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

The Enhanced DES has the following advantages over simple DES:

a. The security of the algorithm is increased. The Simple Columnar Transposition Technique with multiple rounds is used before DES and the round can be increased and decreased according to need.

b. The Brute Force attack is weak against the Enhanced DES because the intruder required breaking the DES and Simple Columnar Approach both. He required extra time to hack the algorithm.

c. If the intruder is success to hack the key of DES in any way then he required the random number of the columnar approach to reach the plain text.

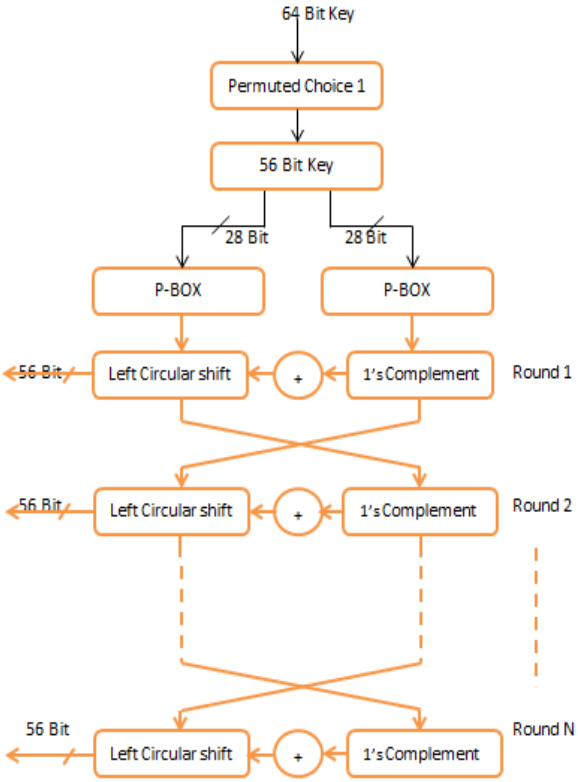

Figure 1: Proposed Enhanced Key generation algorithm flowchart of DES

Figure 1 shows key generation method first 64- bit key is permuted using permuted choice 1 which convert it into a 56- bit key. Now that 56- Bit is divided into two halves of 28-bit each having a P-BOX applied on both. The output of P-BOX at one side has left circular shift and on other side it has 1's complement. Now the result of both sides is combined together as 56- Bit and on these 56-Bit again permuted choice 2 will be applied. Now these bits are converted into 48 bit and lastly these bits are applied in Round function.

```
Consider a [8] [8];
Apply permuted choice1 (a [8] [8]);
Arr = PBox (c);
Brr = PBox (d);

While (i<=6)
{
i=1;
Round (c, d)
{
A[i] = LCS (c);
B[i] = 1's Comp (d);
C[i] = A[i] + B[i];
Swap (A[i], B[i]);
i=i+1;
Round (A[i] + B[i]);
}
// Permuted Choice 1 table
        private static final byte[] PC1 = {
                57, 49, 41, 33, 25, 17, 9,
                1,  58, 50, 42, 34, 26, 18,
                10, 2,  59, 51, 43, 35, 27,
                19, 11, 3,  60, 52, 44, 36,
                63, 55, 47, 39, 31, 23, 15,
                7,  62, 54, 46, 38, 30, 22,
                14, 6,  61, 53, 45, 37, 29,
                21, 13, 5,  28, 20, 12, 4
        };
// Permuted Choice 1 is done here
                for(i=0 ; i < 28 ; i++) {
                        C[i] = keyBits[PC1[i]-1];
                }
                for( ; i < 56 ; i++) {
                        D[i-28] = keyBits[PC1[i]-1];
                }
//1's Complement is done here
public static void main(String args[]) throws IOException
{
BufferedReader
br=new;
BufferedReader(newInputStreamReader(System.in));
intn1,n2,i=0;
 intbin[]=new;
int[32]
System.out.println("\nEnternumber:")n1=Integer.parseInt(
br.readLine());
n2=n1;
i=31;
while(n1!=0)   //loop for finding binary number
{
bin[i]=Math.abs(n1%2);
n1=n1/2;
i=i-1;
}
while(i>=0)      // insert 0's in the remaining places
{
bin[i]=0;
i=i-1;
}
System.out.println("");
for(i=0;i<32;i++)
System.out.print(bin[i]);
if(n2<0)
{
for(i=0;i<32;i++)// loop for obtaining 1's complement
{
if(bin[i]==1)
```

```
bin[i]=0;
else
bin[i]=1;
}
}
System.out.println("");
for(i=0;i<32;i++)
System.out.print(bin[i]);
}
}
// Left shifting a byte value.
class ByteShift
{
public static void main(String args[])
{
byte a = 64, b;
int i;
i = a << 2;
b = (byte) (a << 2);
System.out.println("Original value of a: " + a);
System.out.println("i and b: " + i + " " + b);
}
}
```

IV. CONCLUSION

0Multiple Rounds for Modified Columnar Transposition Technique (MRMCTT) is a scheme that will convert plain text message into the cipher text by using Modified Columnar Transposition Technique and take the cipher text as input and then apply is again columnar technique and for this the cipher will be stronger.Also Enhanced Key Generation Algorithm is applied, in which 1,s complement is added in key generation. By this algorithm the output will be reflected and generates non-linear function. It comes to be very effective technique for data security purpose and in future can be improved by applying more DES algorithm and help to make data more secure in network.

REFERENCES

[1] Alani, M.M.," A DES96 - improved DES security ", 7th International Multi-Conference on Systems, Signals and Devices, Amman , 27-30 June 2010.
[2] Manikandan. G, Rajendiran.P, Chakarapani.K, Krishnan.G, Sundarganesh.G,"A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.
[3] Shah Kruti R., BhavikaGambhava,"New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
[4] Govind Prasad Arya, AayushiNautiyal, Ashish Pant, Shiv Singh, TishiHanda,"A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations", The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 1, No. 1, March-April 2013.
[5] Duncan S. Wong, Hector Ho Fuentes and Agnes H. Chan, "The Performance Measurement of Cryptographic Primitives on Palm Devices", College of Computer Science, Northeastern University, Boston, MA 02115, USA.
[6] Adi Shamir Ronald Rivest and Len Adleman, "A method for obtaining digital signatures and public-key cryptosystem", Communications of the ACM, 21:120–126, 1978.
[7] AllamMousa, "Data Encryption Performance Based on Blowfish", 47th International Symposium ELMAR-2005.08-1 0, June 2005.
[8] IsraaTahseen and ShathaHabeeb, "Proposal New Approach for Blowfish Algorithm by Using Random Key Generator", Journal of MadentAlelemCollege,Vol. 4, No. 1, pp. 1-10, 2012.
[9] SIMMONS, G.J.: 'Symmetric and asymmetric encryption', ACM Comput. Surveys, 1979, **11,** pp. 305-330
[10] "Ms. Ramya G., Ms. Anita Madona M." "Enhancing DES and AES with 1024 Bits Key", International Research Journal of Engineering and Technology (IRJET), vol 2,issue 4, July2015, pp. 1008-1014.
[11] "Ms. Priya S, Ms. Anita Madona M" ,"Hybrid Data Encryption Standard", International Research Journal of Engineering and Technology (IRJET), vol 2,issue 4, July2015, pp.1024-1028.

BIOGRAPHIES

Bhawana Singh is a M.Tech student Of Computer Science& Engineering at Quantum School of Technology Roorkee. She is B.Tech in Information Technology and has five year of teaching experience in various engineering colleges. Her area of interest is Computer & Network Security.

Kamal Kant Verma is an Assistant Professor in Dept of Computer Science at Quantum School of Technology Roorkee. He is B.Tech and M.Tech in Computer Science and has ten year of teaching and research experience in various engineering colleges. He has published twelve research papers in various national and international journals/conferences. His areas of interest are Image Processing and Data Mining.

Rishi Kumar Sharma is a Senior Assistant Professor in Deptt. Of Computer Science and Engineering at the Quantum School of Technology, Roorkee. He is M.S. from University of Greenwich, London and B. Tech in Information Technology and has over 8 year of teaching experience, which includes 3 years of experience in the UK in different colleges. His areas of interest are Wireless Adhoc Network, Data Structure and Analysis of Algorithms.

DOI 10.17148/IJARCCE.2016.55137