Symmetric Key Cryptography using Dynamic Key and Linear Congruential Generator (LCG)

Zeenat Mahmood
PG Research Scholar
Department
of Computer Science
and Engineering, RITS, Bhopal
(M.P.)

J. L Rana
Phd,Director Radharaman
Group of Institute, Bhopal
(M.P)

Prof. Ashish khare
Assistant Professor in
Department of Computer
Science and Engineering,
RITS, Bhopal (M.P.)

ABSTRACT
The present work deals with a new symmetric key cryptographic method using dynamic key. The demand for adequate security to electronic data system grows high over the decades. In the present work the authors have used the Linear Congruential Generator (LCG) for generating key. This is a block cipher technique. The advantage of the present method is that for every pair of encryption & decryption operation a new dynamic key is generated thus the process is very hard to break.The cryptography no longer relies on long term shared keys which are vulnerable under cryptanalysis attacks. It is impossible to detect patterns with which to perform cryptanalysis on the dynamic key.In the present work the authors have introduced concept of dynamic key with symmetric cryptography. Dynamic key is similar to one time pad. In this paper, a dynamic key theory is described and mathematically analyzed.In the present method author proposed a cryptography system in which four rounds of encryption & decryption are performed. In each round different parts of dynamic key are applied in order to make it hard against cryptanalysis attacks.

Keywords
Symmetric key cryptography, Encryption, Decryption, Dynamic key, Linear Congruential Generator.

1. INTRODUCTION
Cryptography is probably the most important aspect of communication security and is becoming increasingly important as a basic building block for computer security. The increased use of computer and communication systems by industry has increased the risk of theft of proprietary information.To avoid this one has to send the encrypted text or cipher. Cryptography is now an emerging research area where the scientists are trying to develop some good encryption algorithm so that no intruder can intercept the encrypted message. Symmetric encryption also referred to as conventional encryption or single key encryption, was the only type of encryption in use in 1970s. Symmetric-key (SK) cryptography can broadly be divided into three classes: stream ciphers, block ciphers and hash functions (including MAC algorithms). Stream ciphers and block ciphers are used to achieve data confidentiality. Hash functions and MAC algorithms are used respectively for integrity and authentication. This paper proposes a method for encryption & decryption using secret dynamic key. For every pair of encryption & decryption a new key is generated. The rest of the paper is organized as follows: Section 2 gives a brief introduction to cryptography, linear congruential generator, dynamic key, one time pad. Section 3 describes the proposed approach. Section 4 shows the comparative performance analysis. Section 5 concludes the work.

2. RELATED THEORIES AND CONCEPTS

2.1 Cryptography
There are two basic techniques to convert a plaintext message into unreadable message that is into Cipher text: (i) Symmetric Encryption: also referred to as conventional encryption or single key encryption was the only type of encryption in use prior to the development of public-key encryption in 1976. (ii) Asymmetric key Cryptography: where two different keys are used one for encryption and the other for decryption purpose. The advantage of symmetric key cryptography is that the key management is very simple as one key is used for both encryption as well as for decryption purpose and this key must be secret and it should be known to sender and the receiver only and no one else. On the other hand in public key cryptography there are two keys one key is called public key which may be available to anyone who wants to encrypt the message and the other one which is called secret key or the private key that must be kept only with the receiver. The problem of Public key cryptosystem is that one has to do massive computation for encrypting any plain text. Due to massive computation the public key crypto system may not be suitable to encrypt short message, in sensor networks, mobile networks etc. Furthermore, Blaze [3] stated that the asymmetric cryptography key size must be ten times or more that of a symmetric cryptography key in order to have a similar level of security.

2.2 Dynamic Key
The dynamic key cryptography is one of the advance technique in cryptography where either a long message is divided in to many part or there are many message in both case each message is encrypted with the help of different parts of key i.e sub keys, these all sub keys are not shared between the both parties but only very few information are shared and on the basis of these information both parties generated the dynamic key. [8][9].

2.3 Linear Congruential Generator (LCG)
In the proposed work the random number for dynamic key is generated using LCG. Linear methods are the best-known and most widely used algorithms to produce random numbers.
Their practical advantages are speed, ease of implementation, and the availability of portable code, parameters and test results. Linear Congruential generator is a classical random number generator. Where we have to choose the modulus m, a multiplier a, an additive term b, and an initial value y_0 [10]

$$Y_1=a*y_0+b \bmod m$$

We will denote this generator by LCG (m, a, b, y_0)

2.4 One Time Pad

The main idea of one time pad is to avoid long term shared cryptographic keys. In other words, when the one-time pad is truly random, it is unbreakable by analyzing successive messages [5]. In one time pad systems, the pads are shared between senders and receivers. To decrypt the messages, the decrypted pads at the receivers must be the same as the encrypted pads at the senders [5].

Therefore, these pads must be distributed between the parties. In practice, the distribution of pads between parties over networks is the weak point in one time pad systems. Similar to current security systems, symmetric cryptographic keys that are used to secure communication messages require secure key exchange among parties before the communication messages are sent. Normally, the key exchange can be performed via public key algorithms like Dife-Hellman [4] or MQV [12].

Every cryptographic key is only secure for a certain amount of time. In addition, larger keys often require higher computational resources, especially in asymmetric cryptography. In practice, excessively large keys may admit denial of service possibilities whereby adversaries can cause excessive cryptographic processing. However, the security of these algorithms relies on long term shared keys that contradict the original idea of one time pad. However, increasing the cryptographic key size is not always the best solution, since no matter how large the key is, its cryptography is still ultimately breakable [5].

3. PROPOSED ALGORITHM

In the present work we are proposing a symmetric key encryption method called "Symmetric Key Cryptography using Dynamic Key & Linear Congruential Generator". In the proposed work each message in encrypted using dynamic key only once after decryption the key is discarded.

A key discarding function is executed after every decryption in order to delete the key. For every encryption decryption operation a new key is generated. This concept is based on one time pad system. The proposed algorithm is simulated on MATLAB 7.5

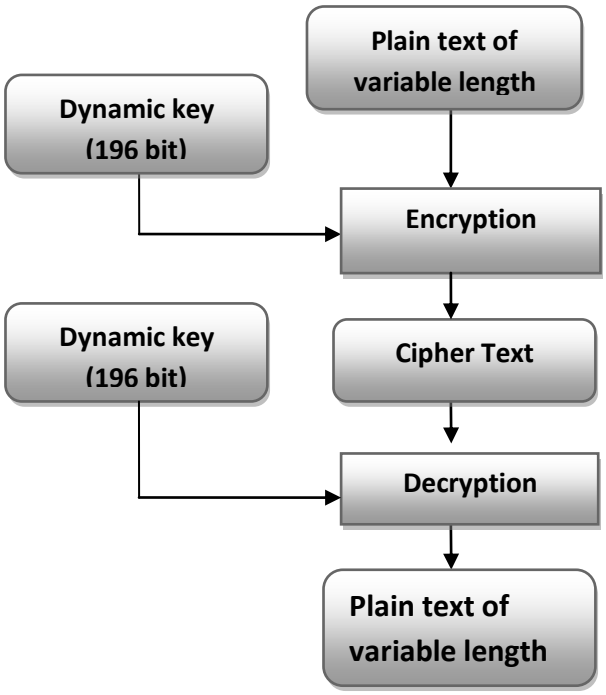

Fig 1: Proposed system

3.1 Dynamic Key Generation

In the proposed work the dynamic key is generated using Linear Congruential generator (LCG). User input a text key 'IK' .Minimum size of IK is 6 bits and it can have maximum 14 bits. Depending upon text key size a base value (y_0) is determined from base table i.e table 1. An inbuilt key 'IBK' is concatenated with the key entered by user to produce a matrix of size 14X14.A randomize function (F_r) is used to generate the key. The function F_r involves various matrix operations such as multiplication, shift operation, modulus etc .In which the random number y_0 is added to the final matrix to produce the dynamic key.

Algorithm 1: Key Generation Algorithm

Step1. User input key 'IK' of size (a) between 6 to 14 bit.
a=length (IK);

Step2. Determine corresponding base value (Y_0) of a from table 1.

$Y_{0=}\ Y_0(1,a)$;

Step3. Calculate Inbuilt key 'IBK'

IBK=rand 1,16);

B=a+IK;

Step 4 . Calculate Y1 using LCG.

$Y_1=a*Y_0+b \bmod m$;

Step5. Call Randomize function F_r to generate Dynamic Secret Key.

Step6.Exit

A	6	7	8	9	10
Y_0	16	15	14	13	12

A	11	10	09	08
Y_0	11	12	13	14

Table 1: Base Table

MATLAB Code for Randomize function (F_r):

1. A[sk][1]=Text entered by user i.e IK

2. B[1][sk]=Text entered by user

3. C[14][1]=First 14 char of IBK

4. D[1][14]=Last 14 chat of IBK

5. E[14][sk]=A[14][1]*B[1][sk]

6. F[sk][14]=A[sk][1]*D[1][14]

7. G[14][14]= E[14][sk]*F[sk][14]

8. M[14][14]=G[14][14]+y_1

9. DSK = M[14][14]

% DSK is Dynamic Secret Key

3.2 Encryption process

This work proposes an encryption scheme which constitutes of four rounds as shown in fig 2. In each round various parts of dynamic key that is sub keys are applied and operation like XOR, Transpose ,Shifting are performed in order to produce cipher text. The size of plaintext block is 49 bits.

Initially the variable length plaintext is divided into blocks of fixed size i.e 49 bits. Size of dynamic key is 196 bits (matrix of 14X14). The dynamic key is divided into four parts: DKP1 (49 bits), DKP2 (49 bits), DKP3 (49 bits) & DKP4 (49 bits).

MATLAB Code of 'DetNB' (Determining Number of Blocks) Process to determine number of blocks:

S=size of variable length plaintext;
K= S mod 49;
I =49-K; % I=number of padding bits
NPT=(PT-K)/49;
%NPT=number of plaintext blocks of size 49 bits
B_{NPT+1}=find (PT, K, 'last') + 'I' number of padding bits;
If (K==0)
N=NPT;
% n= total number of blocks
Else
N=NPT+1;
For (j=1 to N)
Call process ENT;
%ENT is the encryption process of one Block.

The first part of dyamic key i.e DKP1 is applied to the first block of plaintext. The second part i.e DKP2 of the key is applied at the end of round 1.The series of operations performed on data contains ADD, Transpose, XOR, and Rotation operation. Rotation operation can be defined as **c(m)=mod((m+3),26)** This round generates a plaintext called Round1 partial plaintext (RPC1).

In the second round RPC1 is divided into three blocks. The dynamic key is divided into two parts: DKF (first 64 bits of dynamic key) and DKL (Last 147 bits of dynamic key). DKL is further divided into three parts of 49 bit each named DKL1, DKL2, DKL3. These three parts are separately applied on three blocks of RPC1 in order to perform XOR, Transpose, Shifting, Addition operation to produce round 2 partial cipher text (RPC2).

In the third round RPC2 is divided into two blocks. The partition of dynamic key performed in round two is reused and divided into three parts DKF1,DKF2 ,DKF3. Initially DKL2 is applied on the RPC2.At the end DKF3 is applied on RPC2.This round yield round 3 partial cipher (RPC3).

In the last i.e fourth round the DKF2 & DKF3 are applied on the RPC3 in order to produce round 4 cipher text (RPC4) that is the cipher text. A random matrix of size 5X1 is added to the RPC3 to produce cipher text of S+5)bits.

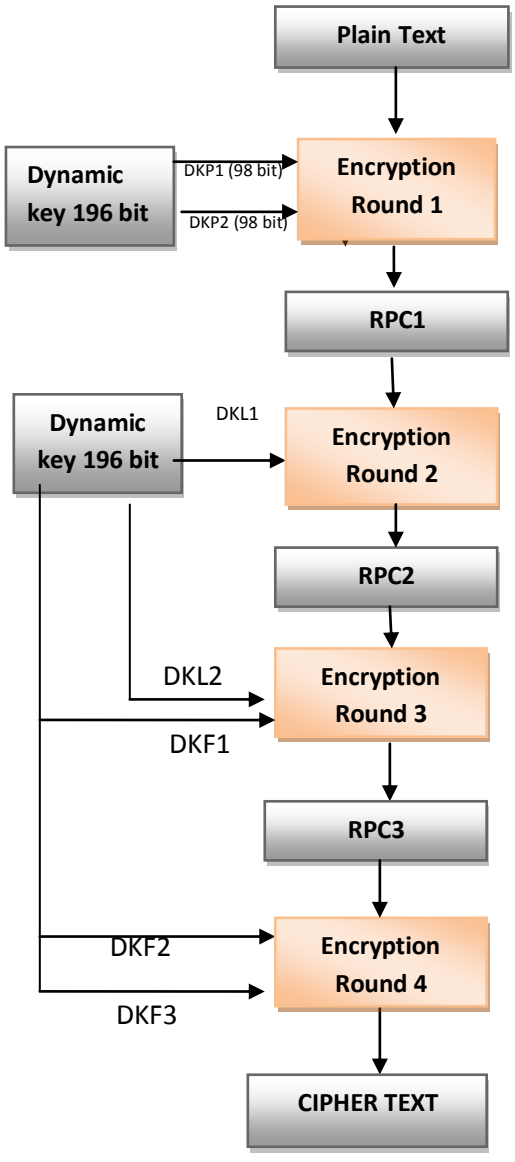

Figure 2: Encryption process

3.2 Decryption process

The Decryption process is just reverse of encryption process as shown in fig 3. Decryption process constitute of four rounds. Each round produces a partial plain text which is forwarded to the next round in order to the desired plain text.
In the first round of decryption process round 1 partial plain text (RPT1) is produced. Similarly RPT2 in the second round, RPT3 in the third round and RPT4 in the fourth round are produced.
A random matrix of size 5X1 is subtracted from RPT to produce Plain text of 'S' bits. Finally all the plaintext blocks are concatenated to produce desired plaintext.

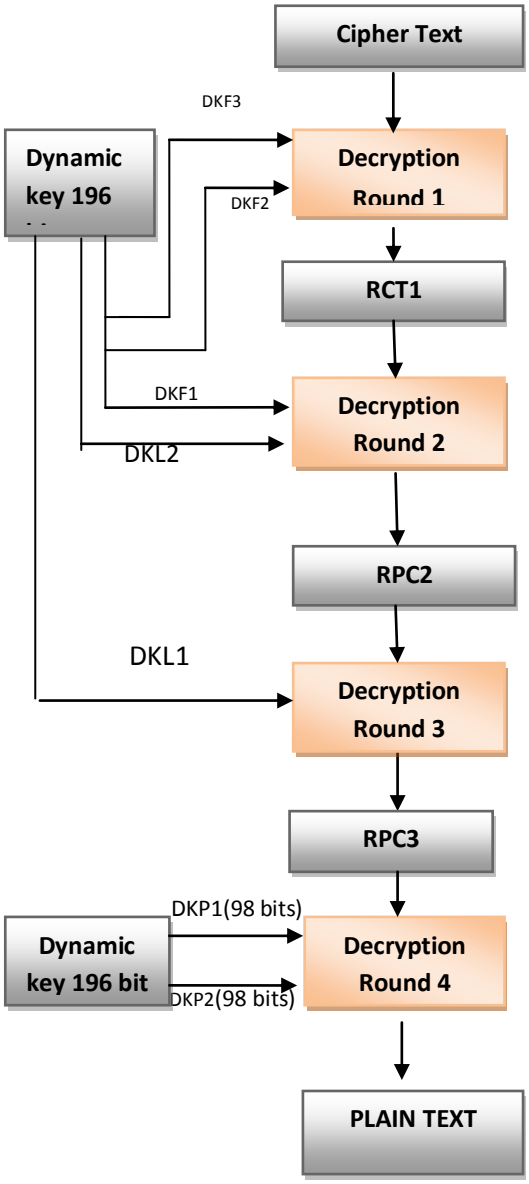

Figure 3: Decryption process

4. COMPARATIVE PERFORMANCE ANALYSIS

This section describes the key size, block size differences of various symmetric key algorithms. Time taken by various algorithms to perform encryption and decryption is also discussed. Table 2 contains key & block size description. Table 3 shows time taken by various algorithm & proposed algorithm.
The chief merit of this algorithm is that the key is dynamic that is different parts of key are applied on different round of algorithm. The secret key is used for only one pair of encryption, decryption. The key is generated by the algorithm is expected to be completely random and non deterministic in nature. Also as outlined earlier, it is computationally infeasible for the hacker to guess each and every key used. However the main merit of the algorithm is little amounting of computational time that one has to spend to encrypt a message. Encryption of very sensitive information the algorithm might prove to be useful. Suggested applications of the above algorithm are in banking systems, financial transactions through the internet and military applications.

Algorithm	Key Size (Bits)	Block Size(Bits)
DES	64	64
3DES	192	64
Rijndael	256	128
Blowfish	448	64
Proposed Algo	196	49

Table 2: Key & Block Size Comparison

Algorithm	Megabytes processed	Time Taken	MB/Second
DES	**256**	**5.998**	**21.340**
3DES	**256**	**6.159**	**20.783**
Rijndael	**256**	**4.196**	**61.010**
Blowfish	**256**	**3.976**	**64.386**
Proposed Algo	**256**	**3.453**	**65.563**

Table 3: Comparison of Time complexities

5. CONCLUSION & FUTURE ENHANCEMENT

An algorithm using a dynamic key and linear Congruential Generator (LCG**)** to generate key for symmetric key cryptography is presented in the paper. The algorithm is shown to provide a high degree of security but requiring lot of computations. The important thing of our proposed method is that it is almost impossible to break the encryption algorithm without knowing the exact key value. We propose that this encryption method can be applied for data encryption and decryption in any type of public application for sending confidential data. A comparative study and security level are verified in this paper with other well known algorithms. More work on the key size and block size may be accomplished in future.

6. ACKNOWLEDGMENTS

We are very much grateful to Department of Computer Science to give us opportunity to work on symmetric key Cryptography. One of the authors (ZM) sincerely expresses her gratitude to Director RITS, Head of the dept CSE ,RITS , M. Tech In charge dept. of Computer Science & Engineering RITS, Bhopal for giving constant inspiration to carry out research work. ZM is thankful to faculties of Computer science & Engineering dept. RITS, Bhopal for their inspiration and support to finish this work.

7. REFE RENCES

[1] Wiliam Stallings," Cryptography and Network" , 3rd edition , Penntice Hall, ISBN 0-13- 111502-2, 2003.

[2] Behrouz A. Forouzan,"Cryptography & Network Security" Tata McGraw Hill, ISBN 13-978-0-07-066046-5.

[3] M. Blaze, W. Diffie, R. L. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Wiener," Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security",Report of Ad Hoc Panel of Cryptographers and Computer Scientists, Jan. 1996.

[4] W. Diffie and M. E. Hellman,"New directions in cryptography, " IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976

[5] Ayushi, " A Symmetric Key Cryptographic Algorithm "International Journal of Computer Applications (0975 8887) Volume 1 – No. 15

[6] Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, and Balasubramaniam Srinivasan "Dynamic Key Cryptography and Applications " International Journal of Network Security, Vol.10, No.3, PP.161{174, May 2010

[7] R. Divya & T. Thirumurugan, "A Novel Dynamic Key Management Scheme Based On Hamming Distance for Wireless Sensor Networks" , International Journal of Scientific & Engineering Research Volume 2, Issue 5, May-2011,ISSN 2229-5518

[8] Yunpeng Zhang, Fei Zuo, Zhengjun Zhai and Cai Xiaobin. 2008. A New Image Encryption Algorithm Based on Multiple Chaos System. International Symposium on Electronic Commerce and Security. 347-350.

[9] Xukai Zou, Yogesh Karandikar and Elisa Bertino, "A Dynamic key management solution to access hierarchy", International Journal of Network Management 2007; 17: 437- 450

[10] P. Hellekalek "Good random number generators are (not so) easy to find Mathematics and Computers in Simulation "46 (1998) 485±505

[11] Dr. Ranjan Bose and Amitabha Banerjee "IMPLEMENTING SYMMETRIC CRYPTOGRAPHY USING CHAOS FUNCTIONS"

[12] L. Law, A. Menezes, M. Qu, J. Solinas, S. Vanstone, "An effcient protocol for authenticated key agreement," Designs, Codes and Cryptography, vol. 28, no. 2, pp. 119-134, 2003

[13] F. Sun, S. Liu, Z. Li and Z. Lü., 2008. A novel image encryption scheme based on spatial chaos map. Chaos, Solitons and Fractals, 38 (3), 631 – 640.

8.AUTHOR'S PROFILE

Zeenat Mahmood has completed BE from TIT, Bhopal and pursuing M.Tech from RITS, Bhopal. Her research work includes one National paper and two International papers. She is a life time member of ISTE.

Dr. J.L Rana Director Radharaman Group of Institutes, Bhopal

Prof. Ashish Kumar Khare, HOD, Computer Science & Engineering dept. RITS, Bhopal has completed B.E from LNCT, Bhopal and M.Tech from SATI, Vidisha.