International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-2, December 2020

Linear Congruential Pseudorandom Numbered Hybrid Crypto-System with Genetic Algorithms

Reddaiah Buduri, Srinivasa Rao Kanusu, Swetha Chinthakunta, Amruthavani Godina, Sivajyothi Siddavatam

Abstract: ***While using networks that may be in any form more and more problems related to securityrises within the network as well as outside the network. To resolve the security problems network security is the science that facilitatesto safeguard the resources and the quality of the network and data. At different workstations filters and firewalls are used in protecting the resources. But while the data is in transmission security services are needed to protect. These services are to be altered frequently to prevent from attacks. In developing such system, this work uses linear congruential pseudorandom number with multiple genetic algorithms. In small business applications these types of hybrid systems can be used to prevent from hackers.***

Keywords: ***Encryption, Decryption, Linear Congruential, Pseudorandom Number, Scramble Mutation, Uniform Crossover Functwion.***

I. INTRODUCTION

In present generation of electronic commerce securing the network is a tough task for the users as well as organizations. The main aim of the network security is to protect the recourses, integrity of the network. Along with these, data is to be protected that is travelling through the network. In the current situation as the networks are widely used, security became a difficult task to handle. As per the estimation on the cost of criminal activities carried out by means of computers, they are increasing very vastly and the loss that it may cause is very high. Due to this estimation, it is observed that there is every need to provide security to the network. To manage the resources, form different kinds of attacks, proper mechanism is needed that provides security and also prevents from damaging the network.

A. Attacks in Network

In present days due to the spread of internet, large numbers of users are connected and their information is stored in the servers of internet. Similarly, activities like social, personal and professional also depends on internet. Due to these reasons unauthorized users who do not have permissions to access may destroy the recourses and also may reduce the internet services. Keeping in mind all the irregularities, attacks and threats, providing security to the network becomes very important. As the attacks are the main sources of threats to the connected systems they are divided into passive attacks and active attacks. When it comes to passive attack it is merely examining the movement of data, analyzing the traffic, eavesdropping and monitoring [6]. As a part of active attack, it is blocking the data that is moving from source to destination and interrupting the data, modifying it and fabrication of data [7]. Anything which can cause harm to the user is known as threat. A threat may be an object or an entity or a program that represents a form of danger.

B. Threats for Network

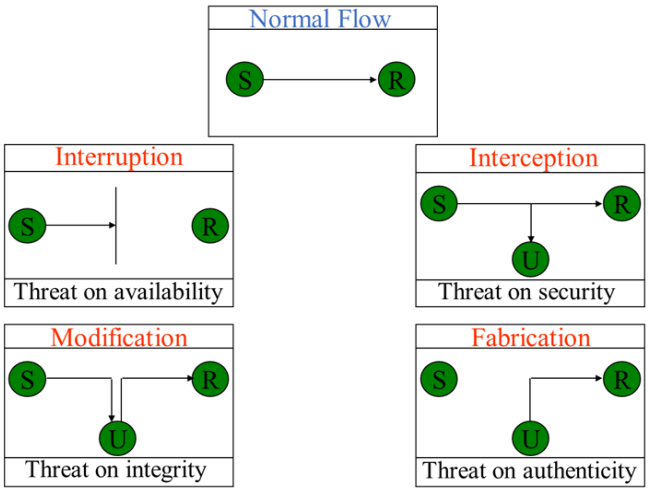

Fig. 1. Types of Threats

This section mainly deals with some of the general network security attacks that we typically encounter. We can classify attacks as Interruption, Interception, Modification and Fabrication. The classification of different types of attacks are shown in figure 1.

II. BACKGRUND STUDY

Marin in his work discussed by taking different issues into account about security in the network such as detecting penetrations, understanding network issues and examining privacy in network [1].

Revised Manuscript Received on December 25, 2020.
* Correspondence Author
ReddaiahBuduri*, Department of Computer Applications, Yogi Vemana University, Kadapa (Andhra Pradesh), India. Email: b.reddaiah@yogivemanauniversity.ac.in.
SrinivasaRao Kanusu, Department of Computer Applications, Yogi Vemana University, Kadapa (Andhra Pradesh), India. Email: kanususrinivas@gmail.com.
SwethaChinthakunta, Department of Computer Applications, Yogi Vemana University, Kadapa (Andhra Pradesh), India. Email: reddyswetha95@gmail.com.
AmruthavaniGodina, Department of Computer Applications, Yogi Vemana University, Kadapa (Andhra Pradesh), India. Email: amruthagodina@gmail.com
Sivajyothi Siddavatam, Research Scholar, Rayalaseema University, Kurnool (Andhra Pradesh), India. Email: ljyothi81@gmail.com.

Wuzheng proposed a framework that concentrates on wireless networks for public key infrastructures [2]. Flauzac proposed an advanced security system that provides security for grids [4]. As it deals with grid it is a distributed solution in providing security in an unbiased joint method. A model has been proposed by Wu Kehe that illustrates information security. The information that is considered is to provide security to business applications, network security and data security [3].

III. SECURITYAPPROACHES

Most of the business organization is moving towards electronic commerce and they are encouraging the users to go for electronic commerce. This is made possible by the large use of internet and networks. In this situation the foremost essential element for industry is to exchange secret data of people involved in business activities in a protected way by means of secure communication channel. To achieve this type of secure communication cryptography is a tool and science that helps to provide security. This is a series of events and actions that helps in providing security services in protected communication channel. Security services are needed in places where data is transmitted through networks. When data is moving, unauthorized users tries to gain control on the data. Once controlled is gained data confidentiality, authentication and integrity of data may be lost. To safeguard from such security attacks proper protection mechanism must be used to transmit the data safely.

Cryptography is the science that deals with providing security services from unwanted access on data while in transmission. This science encodes and decodes the data by using mathematical concepts. Any newly developed system's strength is based on the cipher that is generated while encoding. This science helps in studying and developing new cryptosystems that may assist in stopping the activities of unauthorized users [5]. In this research work, it is aimed to develop a new hybrid system that uses linear congruential pseudorandom number generation, uniform crossover function and scrambled mutation. These genetic algorithms and pseudorandom numbers help in developing a complex cryptosystem. Such kind of systems is very difficult to understand and take more time to break it.

IV. PROPOSED SYSTEM

In providing security any algorithm has to provide privacy to data that is transmitted, authentication, integrity to data, non-repudiation of data. The proposed hybrid algorithm uses, linear congruential pseudorandom numbers and different Genetic algorithms to provide better security and other security related features.

A. Linear Congruential Pseudorandom Number

Linear congruential generators are very old and familiar methods to generate random numbers. This familiarity is because they are easy to implement. These linear congruential pseudorandom numbers are fast and needs minimum memory to maintain current state. Because of this they are valuable for simulating multiple independent streams. This generator is known to be minimal standard random number generator. It is used in building random number function in compilers and other software packages. Linear congruential generators are a class of pseudorandom number generator algorithms used to derive sequences of random like numbers. In cryptography random number and generation has an important role. A recurrence relation is used to describe linear congruential generator.

$$Xi+1=(aXi+c) \bmod m$$

- *a* is called the constant multiplier;
- *c* is the increment
- *m* is the modulus

where X is the sequence of pseudorandom values and a, c, m are constants.

B. Genetic Algorithms

i) Uniform Crossover Function

In uniform crossover each bit is selected randomly from either parent with equal probability to produce a new child as shown in figure 2.

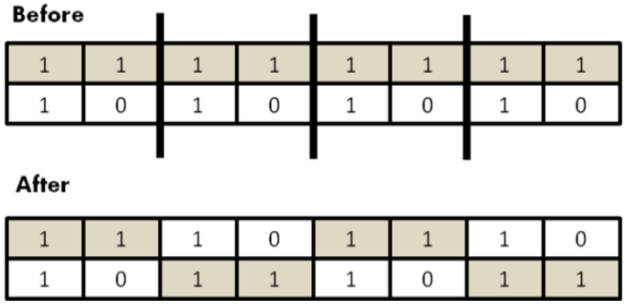

Fig. 2. Uniform crossover

ii) Scramble Mutation

It is a permutation representation in which subsets of genes are selected and their values are twisted up arbitrarily from the complete chromosome as shown in figure 3.

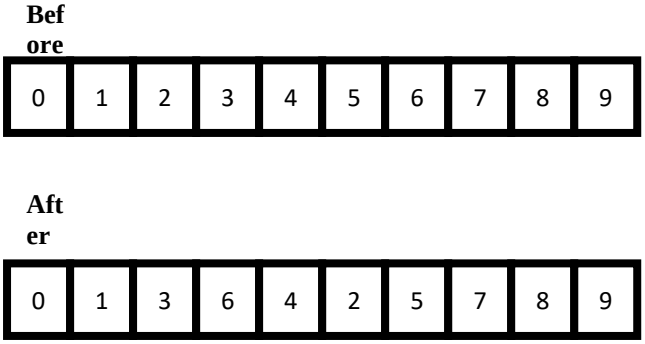

Fig.3. Scramble crossover

IV. PROPOSED HYBRID SYSTEM

A. Encryption Process

By generating linear congruential pseudorandom number, uniform crossover function from genetic algorithms and scramble mutation plain text is concerted into cipher text as shown in Figure 4 and the reverse process of decoding is shown in Figure 5.

B. Framework for Encryption

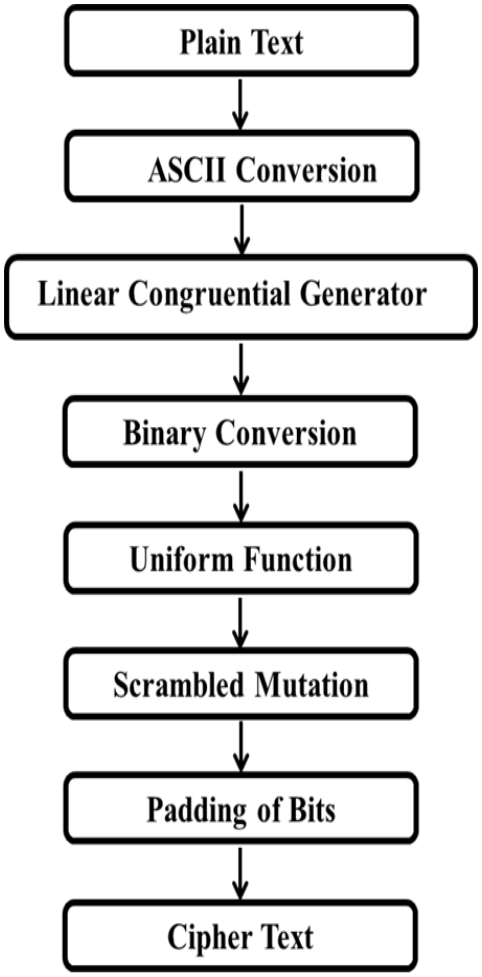

Fig.4. Overviewof Encryption Process

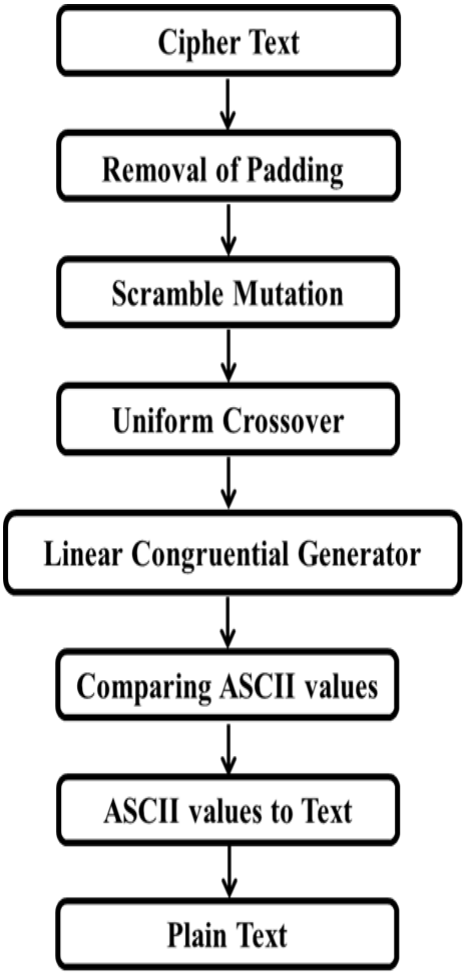

Fig. 5. Block Diagram of Decryption Process

C. Encryption Algorithm

Step 1: Initiate
Step 2: Read original data that needs to provide security.
Step 3: Changeoriginal data to ASCII format.
Step 4: DerivePseudorandom numberswith linear congruentfor ASCII values.
Step 5: Change derived pseudorandom numbers into binaryform.
Step 6: Split binary form to create parents noted as S1 and S2 blocks, each ofsize 18 bits.
Step 7: Parent blocks S1 and S2 are processed with uniform crossover function.
Step 8: Apply scramble mutation on the output of uniform cross over function.
Step 9: Add S1and S2 blocks to generate a sequence of 32 bits.
Step 10: If the given input text size is non-multiples of 4 or greater than 4, for every byte four multiples of dummy bits are to be added at the end.
Step 11: Divide 32 bits of S1 and 2 into 8-bit blocks and convert the blocks into equivalent characters.
Step 12: End

D. Frameworkfor Decryption

E. Decryption Algorithm

Step 1: Initiate
Step 2: Read secured data or cipher that need to be changed tooriginal data.
Step 3: Convert the given secure or cipher text into binary format.
Step 4: Eliminatethe padded bits if any that are at the end of Sequence of bits.
Step 5: Create parents noted as S1 and S2 blocks, each of size 18 bits.
Step 6: Apply scramble mutation for the parent blocks S1 and S2.
Step 7: Apply uniform crossover function to the output of scrambled function.
Step 8: Add S1and S2 blocks to generate a sequence of 32 bits
Step 9: Divide 32 bits into blocks of 6 bit each or multiples of 6.
Step 9**:**Derive numeric value for each 6-bit block.
Step10: GenerateASCII values for the numeric values derived above.
Step 11: Convert ASCII values into characters. The derived characters are the plain text.
Step11: End

V. RESULTS

For the above encryption and decryption algorithms the results are shown in Table I, Table II, Table III and Table IV. The example word considered for encryption process is **'google'.**

A. Encryption results

The text **"google**" is processed in the encryption algorithm with different methods and functions. The following results are derived. Table-I and in Table-II shows the transformation of data.

Table –I: Outcome of Encryption process

ORIGINAL TEXT	ASCII VALUE CONVERSION	LINEAR CONGRUENTIAL GENERATOR CONVERSION	BINARY CONVERSION	CREATING PARENTS
g	103	35	100011	
o	111	37	100101	
o	111	37	100101	S1=100011100101100101
g	103	35	100011	S2=100011100100100010
l	108	36	100100	
e	101	34	100010	

Table-II: Outcome of Encryption process continued

UNIFORM CROSSOVER	SCRAMBLE MUTATION	TOTAT BITS	ADDING NO OF BITS	CONVERTING BITS FOR BYTES (TOTAL/8)	EQUIVALENT CHARACTERS
S1= 100011100 100100000 S2= 100011100 101100111	S1= 101010010 110000000 S2= 100000011 101001111	S1&S2= 101010010 110000000 100000011 101001111	S1&S2= 1010100101100000010 00000111010011110000	10101001 01100000 00100000 01110100 11110000	® , <space> t ≡

When the secret text **'google', is** processed with linear congruential pseudorandom number generator, uniform crossover and scramble mutation from genetic algorithms,the derived secrete data is **"®,<space>t≡".**

B. Decryption

The cipher text **"®,<space>t≡"**is processed in the decryption algorithm. The following results are derived. Table-III and in Table-IVshows the transformation of data.

.Table-III: Outcome of Decryption process

CIPHER TEXT	BINARY CONVERSION	REMOVING ADDING BITS	CREATING PARENTS	SCRAMBLE MUTATION
® , <space> t ≡	10101001 01100000 00100000 01110100 11110000	101010010110000000 100000011101001111	S1= 101010010110000000 S2= 100000011101001111	S1= 100011100100100000 S2= 100011100101100111

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

Table-IV: Outcome of Decryption process continued

UNIFORM CROSSOVER	TOTAL BITS	DIVIDING BITS INTO 6BIT BLOCK INTO DIGIT	CONVERTING 6 BITS BLOCKS INTO DIGITS	CONVERT ASCII VALUES FOR LCG	CONVERT ASCII VALUES INTO CHARACTERS
S1=	S1&S2=	100011	100011=35	35=103	g
100011100101100101	100011100101	100101	100101=37	37=111	o
S2=	100101100011	100101	100101=37	37=111	o
100011100100100010	100100100010	100011	100011=35	35=103	g
		100100	100100=36	36=108	l
		100010	100010=34	34=101	e

VI. CONCLUSION

With the increase of treats related to security organizations especially connected with e-commerce are developing different security mechanisms to protect their confidential data. But no single mechanism was developed that can be used for years together. There is every need to constantly change the security services and mechanisms. In this connection different mathematical functions and cryptographic methods can be used to develop new andstrongmechanism. This helps in providing security to the organizations. This proposed mechanism is developed by using linear congruential pseudorandom numbers and genetic algorithms. Genetic algorithms play a vital role in cryptography. In this workuniform crossover function and scramble mutation are used from genetic algorithms. These genetic algorithms are used to provide additional strength to entire process. Thistype of algorithms can be good for small business transactions.

REFERENCE

1. Marin, G.A. (2005), "Network Security Basiscs", In security & privacy, IEEE, Issue 6, Vol. 3, pp. 68-72, 2005.
2. WuzhengTan,Maojiang Yang,Feng Ye, Wei Ren, "A security framework for wireless network based on public key infrastructure", In Proc. Of Computing, Communication, Control and Management, 2009, CCCM 2009, Vol. 2, pp. 567 -570, 2009.
3. Wu Kehe, Zhang Tong, Li Wei, Ma Gang, "Security Model Based on Network Business Security", In Proc. Of Int. Conf. on Computer Technology and Development, 2009,. ICCTD'09, Vol. 1, pp. 577 – 580, 2009.
4. Flauzac. O, Nolot. F, Rabat. C, Steffenel. L. A, "Grid of Security: A New Approach of the Network Security", In Proc. Of Int. Conf. on Network and System Security, 2009. NSS'09, pp. 67 – 72, 2009.
5. ShyamNandan Kumar, "Technique for Security of Multimedia using Neural Networks", IJRETM-2014-02-05-020, Vol. 02, Issue. 05, pp. 1-7, Sep-2014.
6. NehaKhandelwal, Prabhakar. M, Kuldeep Sharma, "An Overview of Security Problems in MANET".
7. Stallings. W (2006), Cryptography and Network Security, Fourth Edition, Prentice Hall.

AUTHORS PROFILE

Reddaiah. Buduri is working in Department of Computer Applications, YogiVemana University. He Published 30 International papers and attended 10 National and International conferences. The areas of research are Software Engineering, Security.

SrinivasaRao Kanusu is working as Assistant Professor Department of Computer Applications, Yogi Vemana University since 2009. He is doing his Ph. D from Acharya Nagarjuna University. He Published International papers and attended 4 National and International conferences. The areas of research are Digital image processing, Cryptography and Network Security, Software Engineering.

SwethaChinthakunta is presently working in Department of Computer Applications, Yogi Vemana University. The areas of research are Software Engineering, Security for Cloud Computing.

AmruthavaniGodinais presently working in Department of Computer Applications, Yogi Vemana University. The areas of research are Network Security, Data Mining.

SivajyothiSiddavatamis a Research scholar at Rayalaseema University, Kurnool. Her research area is Digital Image Processing. She Published 2 International papers.