Review on Improvised Imbricate Cryptography with Pseudo Random Number Generator using Linear congruentiality Algorithm.

Moditha Vasuki R, Pooja H D, Nikitha H M and A A Priyanka

UG Students, Department of Electronics and Communication Engineering, Rajeev institute of Technology, Hassan, India.

modithavasukir1999@gmail.com, poojahdhsn@gmail.com, nikithavishwa1998@gmail.com aapriyankahassan@gmail.com.

Abstract: Electronic-communications as internal communications tools are use by many organizations to enhance team work and to provide security. To provide a transaction in E-Business, it is important that the electronic-communication has high degree of security and privacy. Protection of the data is required during data transmission and thereby there is increasing utility of network security. Parties who are exchanging sensitive and important business information in secured manner find usage of Cryptography as highly reliable. Relationship between the randomness and Cryptography is going to be established here. If there is higher the randomness of predicting the next bit in Cipher, higher will be the secrecy and thereby increasing the efficiency. By combining imbricate Cryptography with the result of the linear Congruential Pseudo Random Number Generator an algorithm is generated. This algorithm involve layered approach. Layers of Encryption and Decryption provide security. In second layer key is used, which is implanted in the message. To recover the message correct key is used. Here the message and key are inwardly plaited. One of the advantage here is that the any of the user can choose key of variable lengths so that key cannot find with permutation and combination.

Keywords: Pseudo Random Number, Bitmap file, linear Congruential generator, Encryption.

I. Introduction

The electronic- communication is increasing day by day and its usage in E-business has increased phenomenally. To do transact transaction in Ebusiness, it is important that electronic communication has high degree of security and privacy. It is always important to provide data protection during data transmission and thereby there is increasing utility of network security measures

Cryptography involves converting a single desipherable message into an unintelligible message and then converting that message to its original form. In electronic-communication and electronic-business security and privacy are the critical areas. Here the algorithm used is symmetric

key cryptography or conventional cryptography. Since the sender and receiver use the same key. When the sender and receiver use different key, it is known as asymmetric key cryptography or public encryption .

Imbricate cryptography is a new technique that uses symmetric cryptography in which the key is implanted in the message, so if the correct key is not available then the message cannot be recovered. Thus the encrypted file can be sent across the network of interest. Here the message and the key are inwardly plaited. As the user can choose key of variable length . It is not possible to find the key by permutation and combination. It involves layers of encryption and decryption. Multiple layer of encryption and decryption provide security.

Algorithm is generated by combining imbricate cryptography with the result of the linear congruential pseudo random number generator. To generate pseudo random number, pseudo random

generator process is used, it involves usage of a deterministic process to generate a short random stream.

II. Literature Survey

Imbricated Cryptography follows layered approach providing security and confidentiality at various levels. It"s a type of symmetric key Cryptography

thereby using only single key which can"t be guessed using permutation and combination as the size of the key is unknown [1]. Output can baffle anyone as it comes in the combination of 0"s and 1"s. Thus its key provides

DOI : 10.18231/2454-9150.2018.0806

confidentiality. It is simple and can easily be computed. It provide layers of security. The incorporated key at layer 2 provides protection. Using random generator at the first layer makes it very fast and simple, it uses minimal amount of memory.

A. Imbricated Cryptography for network security

Imbricated cryptography involves layers approach and it has layer of encryption and decryption since the user can choose key of variable length hence key cannot be found by permutations and combination. After this, the output is transmitted as a bitmap file. Then the encrypted file can be sent across the network of interest.

To crack the system any one must know the following:

- The binary value in the bitmap has ASCII value of the encrypted character.
- Then read the binary values from the bitmap file and convert them into characters format.
- To break the second layer, it is important that the key is XORed with the characters. (The key should be known.) . The key is not possible to find out because it is transmitted to a protected channel.
- Then the last one is find the mapping characters to break the first layer. Here key cannot find the permutation and combinations method. Hence the system has good performance.

Advantage of Encrypted Cryptography for network security as follows:

- **Confidentiality**: If the user do not have correct key the user not able to access the message.
- **Simplicity:** By using a very simple „C‟ program the system can be implemented this is only for text messaging.
- **Security:** The key is not possible to find out because it is transmitted to a secure channel.
- **Protection:** Protection is provided by the key since it controls the access to the message .
- **incorporated key:** System integrates the key with the message, so the message can be separated from the key only if the correct key is produced.[2]

Encryption: It converts the plain text into ununderstandable cipher text. It has 3 layers, each having its own importance.

Layer 1: It is also called „mapping‟ layer as it maps or replaces with every characters in the message with the other character from the same set. Ex: If source code is „kits‟, then equivalent mapping code is „ jsea ‟

Source file	**Equivalent mapping character**
a/e/i/o/s/t {repeated}	o/t/s/i/a/e
b/c/d/e/f/g/h/j/k/l/m/n/p/q/ r/s/t/u/v/w/x/y/z {non repeated}	h/f/b/d/g/c/l/n/j/k/m/u/y/p/z/q/v/w/x
0/1/2/3/4/5/6/7/8/9	4/6/9/7/0/8/1/3/2/5
Special character	Same character

Layer 2: It is called the core-encoding layer as it exploits the bitwise logics and ASCII format to encode each character. In this layer all those character formed by layer-1 is converted in to an ASCII character, which are not a usual symbol like alphabet, special character or number. After this the first character of the message obtained at the layer1 is XORed with negated ASCII character of the same first character of the password. Then this process is carried out for the rest of the message repeatedly. The password is of a small length, it is repeatedly applied to the message. Earlier „kits‟ was converted to „jsea‟ and if the key is „hai‟. Now the message will be converted as (j^ASCII(h), s^ASCII(a), e^ASCII(i), a^~ASCII(h)).this can be formulated as follows : new_char=(old_char)^(~key[i]).

Layer 3: This layer is called the bitmap-conversion layer as it converts ASCII characters that are obtained at the layer-2 into the equivalent binary value(8 bit representation) and then stores the obtained result as a bitmap file. This process is done by just gathering the binary equivalent value of the current ASCII characters of layer 2 and then writing it into a file that has a type bitmap.

Decryption: It is the reverse order of encryption. It also has three layers of encryption. Following are the each layer of the algorithm.

Layer 1: It is called as character-restructuring layer and it regroups the bits from the bitmap file to form ASCII characters. For each 8-bit data in the original bitmap file, find the equivalent ASCII value. Then character obtain by the ASCII value is noted.

Layer 2: It is called the core-decoding layer. One of the most important fact in bitwise XOR logic is that

if this bitwise XOR logic is applied twice then the original character can be reproduced. This proves that the algorithm used in encryption phase at layer-2 can also be used for decryption also. Thus the same bitwise logic is used here too. Here one thing to be noticed that is only the same key as used in encryption can retrieve the message back. This can be formulated as follow: ch=ch^~ASCII(k).

Layer 3: It is called as the re-mapping layer and works same as layer-1 of encryptionin the reverse direction.[3]

B. A Pseudorandom generator from any one-way function:

Here to construct pseudo random number one-way function is used. It is easy to construct a one-way function from a pseudo random generator, the result of this shows that there

DOI : 10.18231/2454-9150.2018.0806

is a pseudo random generator if and only if there is a one-way function. One of the basic primitives in the study of the interaction between randomness and computation is a pseudo random generator. Intuitively , a pseudo random generator is a polynomial time computable function g that stretches a short random string x into a long string g(x)that\looks "random toany feasible algorithm, called an adversary. The obtain adversary tries to distinguish the string g(x) from a random string the same length as g(x). The two string look the same as KSXZR to the adversary if the acceptance probability for both string is essentially the same. Thus, a pseudo random generator can be used to efficiently convert a small amount of true randomness into a much larger number of effectively random bits.

Random generator processes have some limitations. All the natural random generator processes are slow. It also suffers from the fact that if needed, random stream cannot be repeated. Alternatively, Pseudo Random Number Generator process is used. It involves usage of a deterministic process to generate a short random stream. This random stream of bits is used as the input. There are two broad categories of pseudo random number generators which is congruential generators and generators using cryptographic ciphers.

C. Exclusive OR (XOR) and hardware random number generators

The bias from those bits that are generated with the hardware random number generator can reduced with the operation called as exclusive or (XOR). Typically, the uncorrected bits generated by a hardware random number generator will have expectation different from ideal value, and adjacent bits various combinations of the random bits using XOR operator under a variety of assumption about means and correlation of the original variations. Specifically, interested in the effectiveness of the XOR operator for reducing biase and if the successive bits are correlated then what will be happened. The symbols X,Y,Zetc. are the random bits

D. Minimal key lengths for symmetric ciphers to provide adequate commercial security:

Encryption has an important role in protecting the privacy of electronic information against threats those are obtained from a variety of potential attackers. Now a days cryptography employs a combination of conventional or symmetric cryptographic system for the purpose of encrypting data and public key or asymmetric systems. And to have access to the strength that are required for the symmetric cryptographic systems is therefore an required step in cryptography for computer and communication security. Technologies that are readily available in market makes the brute force attacks again cryptographic systems that considered as adequate for the recent past several years both fast and cheap. General purpose computer used for this purpose, but an efficient approach is to employ field programmable gate array technology.[4]

III. Random generator processes

Random generator processes have some limitations. All the natural random generator processes are slow. It also suffers from the fact if needed, random stream cannot be repeated. Alternatively, pseudo random random number generator process is used. It involves usage of a deterministic process to generate a short random stream. This random stream of bits is used as the input.

Relation between the randomness and cryptography is going to be establish here. If there is higher the randomness of predicting next bit in cipher, higher will be the secrecy and thereby the efficiency. A new algorithm is being formed by using congruential pseudo random number generator"s result to circularly shift the characters in the input. There are two broad catagories pseudo random numbers generators which are congruential generators and generators using cryptographic ciphers.

Among the two methods of above linear congruential method is the most common technique for generating pseudo random numbers. In that when the adequate criteria is followed for selecting the co-efficient of the congruence equation and the value of the modules, then the sequence generated by a linear congruential equation delivers reasonable randomness.

IV. Linear algorithm for the imbricate cryptography

The linear algorithm is comprises of three layers of encryption, each layer have its own contribution and thereby increasing the security of the new formed algorithm. The name of these layers are pseudo shifting layers, core encoding layer and bitmap conversion layer.

A. Encryption algorithm:

pseudo shifting layer: This layer is called as pseudo shifting layer. Each character in the given input I shifted by the total number of places those are generated by the pseudo random number generator method. The character to be replaced is present at the position which is at a place which is away from the current character by the number of places that is generated by pseudo random number generator. Here the difference between the repeated and non-repeated characters is omitted and thus completing the first level of encipherment. The XOR operation of input string with random generated value is cancelled out. There is no need to remember the probability of each alphabet. Thus each character in the input set is mapped according to the value obtained by he generator.

Layer 2:core encoding layer: This layer is called core encoding layer. It uses bitwise logics (0,1) and ASCII formats to encode the characters obtained after the first level encipherment. The characters that are obtained from the first layer can be a number, alphabet or symbol as

DOI : 10.18231/2454-9150.2018.0806

entered in the input seed, hence naming the layer as core encoding layer. [1] the first character as encipherment obtained by layer 1 is XORed with negated ASCII character of the first character of the password. The same process is repeated for the rest of the encipher text. The length of password is small due to it gets repeated to used. The number of times depending upon the lenth of the message.

Formulated has : character New=(character Old) XOR (~Character(K).

Layer 3: Bitmap conversion layer: This layer is called bitmap conversion layer. This is responsible for converting ASCII characters into their binary equivalents and this result is stored as a Bitmap file. Here each character is taken individually, and then its binary equivalent is obtained. The binary equivalent is then written in a file that is of type bitmap. Due to its bitmap nature, this layer is commonly referred as bitmap conversion layer

B. Decryption algorithm

This is description algorithm. The Bitmap Image is transmitted to the receiver by the sender.

[1] the random number generated by the pseudo random number generator i.e., N" and the key „K" is transferred to the receiver by the other means of secretly.

[2] Take 8 bits at a time from the input bitmap image and XNOR it with a key „k" i.e.

[3] Above step reduces the ciphered text that was reduced at level 2 of encryption.

[4] Right shift the characters of produced cipher text with pseudo random number generated value „N" to obtained the original message M at this step.

[5] The original text is obtained here.

Cryptography has an important role in providing security and confidential to data. Imbricate Cryptography is used to provide security to the data Sent to the other user through an insecure network. This is done in an efficient manner so as to obtain maximum benefit by utilizing minimum cost and resources. This paper establishes that the security of imbricate cryptography is enhanced by using pseudo random generator which increases the randomness of determining the cipher text. This method provides protection and confidentiality. Moreover it can be easily computed. Thus through this paper, it has been the endeavour to enhance the security of Imbricate Cryptography Encryption and Decryption algorithms for ensuring better security results in data transmission.

V. Application

A. Identification and Authentication

Identification and authentication are the important applications of imbricate cryptography. Identification verify someone"s or something"s identity. Authentication mainly determines whether the person or entity is authorised. Now a days E-banking is been used in rural areas, as it requires security, Imbricate Cryptography is used to control hacking.

B. Personal use

Privacy is the most important application of imbricate cryptography. To implement privacy by encrypting the information to remain private imbricate cryptography is used. Many times information cannot be accessed by person or entity, in that, the information is store in a way that reversing the process is virtually impossible.[5]

VI. Acknowledgement

I would like to place on record my deep sense of gratitude to **Dr. Aravind B N**, HOD-Dept. of Electronics and Communication Engineering, Rajeev Institute of Technology, for his stimulating guidance, continuous encouragement and useful suggestions.

I express my sincere gratitude to **Mr. Ravi L S**, Dept. of Electronics and Communication Engineering, for his generous guidance, help and useful suggestions.

References

[1] Bhangale Snehal Ananda, P B Bhalerao, review on Imbricate Cryptography, Index Copernicus value (2013):6.14/Impact factor (2014):5.61/vol 5 issue 6 january 2016, page no:916-920,2015-16

[2] Rohith Rastogi, Shashank mittal, shashank shekhar.Linear, Algorithm for Imbricate Cryptography using pseudo random number generator, 2015 2nd international conference on computing for sustainable global development(India Com),page no:89-94,2015.

[3] Nandkishor Prakash Rao Dasharathe, Dipak Chaunwal, Ashrubha Korde, Review on improvised imbricate cryptography with pseudo random number generator using linear congruentiality algorithm,volume 7 issue No.4,international Journal of Engineering Science and computing, page no:10703-10707, April 2017

[4] Prabhat k .Panda, Sudiptha Chathopadhyay, a hybrid security Algorithm for RSA cryptosystem,2017 4th international conference 361 full text.

[5] Mohammed Moizuddin, Joy Wingston, Mohammad Qayyaum, A comprensive survey: quantum cryptography, 297 2nd international conference, 763 full text.

DOI : 10.18231/2454-9150.2018.0806