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

Nandkishor Prakashrao Dasharathe¹, Dipak Choumwal², Ashruba Korde³
Assistant Professor³
Department of Computer Science and Engineering
Khurana Sawant Institute of Engineering & Technology, SRTM University, Nanded, Maharashtra, India

Abstract:
In this study paper we are going to establish the relationship between Randomness and Cryptography and also to generate an algorithm by combining the result of the Linear Congruentiality Pseudo Random Number Generator (LCPRNG) with Imbricate Cryptography. In this world Electronic communications as internal communications tools are used 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. The given algorithm is type of Symmetric Cryptography. It uses a layered approach. The first layer involves implanting a randomly generated number and by using this number we are creating a remapping matrix then use of this matrix for to transform text into cipher text at first layer. Second layer involves implanting the key to the cipher text which is obtained in the first layer thus making the security a two way approach. Therefore, the message can only be recovered by using the correct key and the correct Random number generated. The Random number generated is transmitted to the user with the key. Here the message and the key are inwardly plaited. It is not possible to find the key by permutation and combination. It involves layers of encryption and decryption provide security. In the third layer the message is converted into image format and the image is sent to other user. The advantage of the process is that it prevents cipher text only attack and known plain text attack. It is also easily computable and efficient.

Keywords: Bitmap Image, Linear Congruentiality Pseudo Random Number, Encryption, Decryption, Key, Representation Matrix.

1. INTRODUCTION

Cryptography or Cryptology is the practice and study of hiding information. It is called code, but this is not a correct name. It is the technology used to keep information secret and safe. Current cryptography is a mixture of computer science, electrical engineering and mathematics. Cryptography is used for computer passwords, shopping on Internet and ATM cards. When a message is sent in cryptography, it is coded or encrypted before it is sent. The method of changing text is called a coding or more precisely, ciphering. The changed text is called “ciphered text”. The change makes the message hard to read. Someone who wants to read it must have to decode it. How to change it back is a secret. Both the person that sends the message and the one that gets it should know the secret direction to change it, and others don’t know it. Studying the cipher text to discover the secret is called “Cryptanalysis: or “cracking” or sometimes “code breaking”. The electronic communication is increasing day by day and its usage in E-Business has increased phenomenally. To do transaction in E-Business, 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. There are two types of cryptography one is Symmetric key cryptography and the other is Asymmetric key cryptography. When the sender and receiver use the same key, it is known as Symmetric Key Cryptography or Conventional Encryption. When the sender and receiver use different keys, it is known as Asymmetric Key Cryptography or Public Encryption. Perfect secrecy can be achieved only if the key of encipherment is truly a random number. True random generator approach involves a natural random process, e.g., tossing of coin. Relationship between the Randomness and Cryptography is going to be established here. Algorithm is generated by combining Imbricate Cryptography with the result of the Linear Congruential Pseudo Random Number Generator.

2. LITERATURE SURVEY

Imbricate cryptography is a technique that used symmetric key cryptography in which the key is mixed in the message, therefore only if the correct key is available then and then only the message can 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 Layers of encryption and decryption provide security. Imbricate Cryptography follows layered approach providing security and confidentiality at various levels. The advantage of this new process is that it saves the input text from the „cipher text only Attack“ and „known plain text attack“. Thereby improving the performance of the generator. The first step of the algorithm doesn’t require the key. Apart from this, we have an advantage that mapping is done unpredictably as the key length being smaller than the message length. It is also easily computable and efficient. The
Linear Congruential Generator can only be used when the Encryption is taking places in layers else it would be like affine cipher and prone to frequency analysis. Moreover, Imbricate Cryptography is designed in layers make it long and slow. The advantage of this new process is that it saves the input text from the “cipher text only Attack” and “known plain text attack”. Thereby improving the performance of the generator. The first step of the algorithm doesn’t require the key. Apart from this, we have an advantage that mapping is done unpredictably as the key length being smaller than the message length. It is also easily computable and efficient. [5] The Linear Congenital Generator can only be used when the Encryption is taking places in layers else it would be like affine cipher and prone to frequency analysis. Moreover, Imbricate Cryptography is designed in layers make it long and slow. Now a days computer simulation are use everywhere, from the corporate office to the local video game play stations. Role of this simulation are the messages that to be transferred should be space insensitive to ensure more security, students should be completely aware of the limitations of Pseudo Random Number Generators. The fact that random number generators in use today are not truly random is no secret. Since there are many simulations that produce reasonable results, and produced random number is not truly random and produced random number is not truly random therefore it is problematic for students.

2.1 Imbricate cryptography for security
Imbricate cryptography involves layers approach and it has layers of encryption and decryption. Since the user can choose key of variable length hence key cannot be found by permutation and combination. After this, the output is transmitted as a bitmap file. Thus the encrypted file can be sent across the network of interest. [1] To crack the system any one must know the following:

1) The binary value in the bitmap has ASCII value of the encrypted character.

2) Then read the binary values from the bitmap file and convert them into characters format.

3) 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.

4) Then the last one is find the mapping characters to break the first layer. Here key cannot find by permutation and combination method. Hence the system has good performance.

Advantages of the Imbricate cryptography for network security are as follows:

1) Confidentiality: if the user do not have correct key then user not able to access the message.

2) Simplicity: By using a very simple 'C' program the system can be implemented this is only for text messaging.

3) Security: The key is not possible to find out because it is transmitted to a secure channel.

4) Protection: Protection is provided by the key since it controls the access to the message.

5) 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.

2.2 A Pseudo random Generator from any One-way Function
Here to construct pseudo random number one-way function is used. From a pseudo random generator it is easy to construct a one-way function, the result of this show that there 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 to any 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 strings look the same as KRXZ to the adversary if the acceptance probability for both strings 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 are Congruential Generators and Generators using Cryptographic ciphers [2] So many works that have to be contributed to the expansion of the conditions on one-way functions under which a pseudo random generator can be constructed. [3] [4] show how to construct a pseudo random generator based on the difficulty of factoring, and this was substantially simplified in [5]. When f is a one-way permutation, the task of inverting f(x) is to find x. In the case when f is not a permutation, the natural extension of successful inversion to finding any x0 such that f(x0) = f(x). The paper [6] introduces one-way functions which remain one-way after several iterations for the construction of a pseudo random generator. Construction of a pseudo random generator from any one-way function is given. [7]

2.3 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 day’s cryptography employs a combination of conventional or symmetric cryptographic systems for the purpose of encrypting data and public key or asymmetric systems for managing the keys that can get used by various types of symmetric systems. And to have access to the strength that is required for the symmetric cryptographic systems is therefore a required step in cryptography for computer and communication security. Technologies those are readily available in market makes the brute force attacks against cryptographic systems that considered as adequate for the recent past several years both fast and cheap. General purpose computers are used for this purpose, but an efficient approach is to employ Field Programmable Gate Array technology. [8]
2.4 Exclusive OR (XOR) and hardware random number generators

The bias from those bits which is generated with the hardware random number generator (RNG) can be reduced with exclusive operation or (XOR). Typically, the not corrected bits generated by a hardware random number generator (HRNG) will have expectation different from the ideal value, and adjacent bits may be co-related. The expectations and co-relations of various combinations of the random bits using the XOR operator under a variety of assumptions about the means and co-relations of the original variables. Specifically, it is interested in the effectiveness of the XOR operator for reducing bias and if the successive bits are correlated then what will be happened. [9]

3. SYSTEM DEVELOPMENT

3.1 Existing System

The algorithm being comprises of three layers of Encryption, each having its own contribution and thereby increasing the security of the new formed algorithm. The three layers are Pseudo Shifting Layer, Core Encoding Layer and Bitmap Conversion Layer. The three layers are described below.

\[ \text{Character New} = (\text{Character Old}) \oplus (\neg \text{Character of K}). \]

C. Layer 3: Bitmap Conversion Layer

This layer 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 it’s 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.

3.1.1 ENCRYPTION ALGORITHM

1. Getting input Message says M from the user.
2. Generating pseudo random number say N by Pseudo Random Number Generator.
3. Layer 1: Left shift the characters in M by N to generate cipher text say M2 i.e. \( M2 = M \ll N \)
4. Layer 2: Encoding the above generated cipher M2 using the key say K which is transferred to the receiver secretly by other means. The formula used to generate new cipher say M3: \( \text{Character New of } M3 = (\text{Character Old of } M2) \oplus (\neg \text{Character of } K) \)
5. Layer 3: The above generated cipher M3 is then converted into its binary equivalent and then placing the binary values in the Bitmap file. [1]
6. The bitmap file generated at the end of Layer 3 is transferred to the receiver which is then decrypted using the decryption algorithm to produce the original message M.

3.1.2 DECRYPTION 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 other means secretly.
2. Take 8 bits at a time from the input bitmap image and XNOR it with the key ‘K’ i.e. \( M2'[i] = (8 \text{ bits of bitmap}) \oplus (K[i]) \)
3. The above step produces the ciphered text M2 that was produced at Level 2 of Encryption.
4. Right shift the characters of M2’ with pseudo random number generated value ‘N’ to obtain the original message M at this step.
5. The original text is obtained here.
3.2 Proposed System

The new algorithm being formed comprises the same three layers but the main difference is that the new algorithm uses Remapping matrix which is created once the Pseudo number is generated for all the alphabets, numbers and symbols once and used when required. The three layers are described below.

**A. Layer 1: Pseudo Shifting Layer**
In this layer first of all the Pseudo random number is generated by using the Pseudo Random Number Generator. We have created a Matrix containing all the characters, numbers and symbols. Then each character in the Matrix is mapped according to the value of the generator. This new matrix is known as Mapping Matrix. When the user gives message to the system then each character in the text is mapped with the character in the matrix forming first layer of encipherment.

**B. Layer 2: Core Encoding Layer**
This layer uses the technique of the bitwise logics (0, 1) and ASCII format to encode the characters obtained after first level of encipherment. The characters obtained from the first layer can be a number, alphabet or symbol as entered in the input seed, hence naming the layer as Core Encoding Layer. [1] The first character of encipherment obtained by Layer1 is XORed with negated ASCII character of first character of the Password. The same process is repeated for the rest of the Enciphered text. The length of password is small due to which it gets repeatedly used. The number of times depending upon the length of the message formulated as,

\[
\text{Character New} = (\text{Character Old}) \oplus \overline{\text{Character of K}}.
\]

**C. Layer 3: Bitmap Conversion Layer**
This layer 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.

4. APPLICATIONS

Identification and Authentication:
Authentication and Identification and authentication are the important applications of imbricate cryptography. Identification verifies someone’s or something’s identity. Authentication mainly determines whether the person or entity is authorized.

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 is cannot be accessed by person or entity, in that, the information is store in a way that reversing the process is virtually impossible.

Passwords:
Passwords are not typically kept on a host or server in plaintext, but are generally encrypted using some sort of hash scheme. In the Windows NT case, all passwords are hashed using the MD4 algorithm, resulting in a 128-bit (16-byte) hash value.

5. REFERENCES:


[10]. Blaze, Matt, Diffie Whitefield, Rivest, Ronald L. Schneier, Bruce; Shimomura, Tsutomu, Thompson, Eric; Wiener, Michael (January 1996). “Minimal key lengths for symmetric ciphers to provide adequate commercial security”.
