International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Review on Imbricate Cryptography

Bhangale Snehal Ananda[1], P. B. Bhalerao[2]

[1]Department of Computer Science and Engineering Marthawada Shikshan Prasark Mandal‟s Deogiri Institute of Engineering & Management Studies, Aurangabad Maharashtra state, India 2015-16

[2]Assistant Professor Department of Computer Science and Engineering Marthawada Shikshan Prasark Mandal‟s Deogiri Institute of Engineering & Management Studies, Aurangabad Maharashtra state, India 2015-16

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, Imbricate cryptography, Encryption

1. Introduction

The electronic communication is increasing day by day and its usage in E-Business has increased phenomenally. To do transact 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.

Cryptography involves converting a simple decipherable 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 Encryption. Since the sender and receiver use the same key. When the sender and receiver use different keys, 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 can not 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.

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.

To generate pseudo random number pseudo Random Number Generator process is used. It involves usage of a deterministic process to generate a short random stream.

2. Literature Survey

Imbricate Cryptography follows layered approach providing security and confidentiality at various levels. It‟s a type of a 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. Output can baffle anyone as it comes in the combinations of 0‟s and 1‟s. Thus its key provides confidentiality. It is simple and can easily be computed. It provides layers of security. The incorporated key at layer two provides protection. Using random generator at the first layer makes it very fast and simple. It uses minimal amount of memory. [1]

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 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.

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 network 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.

The algorithm has three layers of encryption, each having its own importance.

Layer-1:
Layers 1 is called as mapping layer and misrepresent the cracker by jumbling characters. At this layer each of the characters is replaced with another one character present in the same set of characters. There are two types of sets of characters those are repeated characters and non-repeated characters. Maximum English words consist of alphabets, those have maximum probability of occurrence of some characters such as ‚a‟‚e‟‚i‟‚o‟ and ‚r‟ because of this these characters are called repeated characters. Those characters whose occurrence are occasionally are called as non-repeated characters.

Layer-2:
Layer 2 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 layer-1 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. 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 obtain at the layer 2 into the equivalent binary value 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 is the reverse order of encryption. It also has three layers like encryption. Following are the each layer of the algorithm.

Layer-1:
Layer 1 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 that ASCII value is noted.

Layer-2:
Layer 2 is as 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.

Layer-3:
Layer 3 is called as the re-mapping layer and works same as layer-1 of encryption in the reverse direction.

2.2 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 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 KSXZR 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 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 the ideal value, and adjacent bits may be correlated. The expectations and correlations of various combinations of the random bits using the XOR operator under a variety of assumptions about the means and correlations of the original variables. Specifically, interested in the effectiveness of the XOR operator for reducing bias and if the successive bits are correlated then what will be happened.

The symbols X, Y, Z etc. are the random bits. [8]

2.4 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 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 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 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. [9]

3. Random Generator Processes

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.

Relationship between the Randomness and Cryptography is going to be establish here. If there is higher the Randomness of predicting the next bit in cipher, higher will be the secrecy and thereby increasing the efficiency.

A new algorithm is being formed by using Linear Congruential Pseudo Random Number Generator‟s result to circularly shift the characters in the input.

There are two broad categories of Pseudo Random Number Generators which are Congruential Generators and Generators using Cryptographic ciphers.

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

4. Linear Algorithm for Imbricate Cryptography

The Iinear 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 three layers are Pseudo Shifting Layer, Core Encoding Layer and Bitmap Conversion Layer.

4.1 Encryption Algorithm

Layer 1: Pseudo Shifting Layer:
This layer is called as Pseudo Shifting Layer. Each character in the given input is shift 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 the generator. [10]

Layer 2: Core Encoding Layer:
This layer is called as core encoding layer.It uses bitwise logics (0, 1) and ASCII format to encode the characters obtained after first level of encipherment. The characters that are 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
Character New = (Character Old) XOR (~Character of K). [11]

Layer 3: Bitmap Conversion Layer:
This layer is called as 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. [11]

4.2 Decryption Algorithm

This is decryption algorithm. The Bitmap Image is transmitted to the receiver by the sender.
1) Getting input Message say M from the user.
2) Generating pseudo random number say N by Pseudo Random Number Generator.

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.
3) The above step produces the ciphered text that was produced at Level 2 of Encryption.
4) Right shift the characters of produced cipher text with pseudo random number generated value „N" to obtain 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. [12]

5. Application

Identification and Authentication
Authentication and 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 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. Manytimes 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.

6. Acknowledgement

I would like to place on record my deep sense of gratitude to **Mr. S. B. Kalyankar**, HOD-Dept. of Computer Science and Engineering, Deogiri Institute of Engineering and management Studies Aurangabad, for his generous guidance, help and useful suggestions.

I express my sincere gratitude to **Mr. P. B. Bhalerao**, Dept. of Computer Science and Engineering, Deogiri Institute of Engineering and management Studies Aurangabad, for his stimulating guidance, continuous encouragement and supervision throughout the course of present work.

References

[1] Murali Kumar R "Imbricate Cryptography for network security" electronics for you, MAY 2006.
[2] Johan Hastad, Russell Impagliazzoy, Leonid A. Levinz, Michael Luby "A Pseudo random generator from any one way function", SIAM Journal on computing.
[3] Goldwasser, S., Micali, S. and Tong, P., \Why and how to establish a private code on a public network," 23rd IEEE Symposium on Foundations of Computer Science, 1982, pp. 134-144.
[4] Yao, A.C., \Theory and Applications of Trapdoor Functions", 23rd IEEE Symposium on Foundations of Computer Science, 1982, pp. 80-91.
[5] Alexi, W., Chor, B., Goldreich, O., Schnorr, C.P., \RSA Rabin Functions: Certain Parts Are As Hard As the Whole", SIAM J. on Computing, Vol. 17, 1988, pp. 194-209.
[6] Parts Are As Hard As the Whole", SIAM J. on Computing, Vol. 17, 1988, pp. 194- 209.
[7] Levin, L.A., \One-way Function and Pseudorandom Generators", Combina- torica, Vol. 7, No. 4, 1987, pp. 357{363
[8] Ambarish Karole, Nitesh Saxena, and Nicolas Christin, "A Comparative Usability Evaluation of Traditional Password Managers"

[9] Robert B Davies, "Exclusive OR (XOR) and hardware random number generators, feburary28, 2002..
[10] Blaze, Matt, Diffle Whitefield, Rivest, Ronald L. Schneier, Bruce; Shimomura, Tsutomu, Thompson, Eric; Wiener, Miachel (January 1996). "Minimal key lengths for symmetric ciphers to provide adequate commercial security".
[11] Behrouz. A Forouzan and Debdeep Mukhopadhyay "Cryptography and Network Security" second edition, TMH. Chapter and concept pg607
[12] Rohit Rastogi, Shashank Mittal, Shashank Shekhar "Linear Algorithm for Imbricate Cryptography Using Pseudo Random Number Generator"2015