A Hybrid Cryptography Technique to Support Cyber Security Infrastructure

Dr. Vivek Kapoor
Asst.Professor, Dept.Of Information Technology,
Institute Of Engineering & Technology,
Devi Ahilya University, Indore, India.

Rahul Yadav
Dept. Of Information Technology,
Institute Of Engineering & Technology,
Devi Ahilya University, Indore, India.

Abstract- **Cryptography is an art and science of achieving security by encoding message to make them non-readable. It converts the data from readable format that is known as plain text into unreadable format known as cipher text and vice versa. There are various types of cryptographic algorithms proposed over the years based on different techniques. These techniques use various approaches to implement the basic functionality of cryptography i.e. to hide the information from unauthorized user. This survey describes various aspects of cryptographic techniques and various issues related to cryptography. Along with it, a proposed work is there which addresses some of the core issues of cryptography along with their solutions.**

Key words- Encryption, symmetric and asymmetric cryptography, cryptanalysis, SH1 hash technique, DES, RSA.

.

1. INTRODUCTION

The given chapter provides the understanding about the basic overview of the proposed work and their involved work. In order to improve the cyber security, the key objectives and overview of the work is presented.

1.1 Overview

The art of preserving information by transforming it (encrypting it) into an unreadable format (for human eyes), called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking, although modern cryptography techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is Pretty Good Privacy because it's effective and free. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses [1].

There are a number of applications available now in these days by which the private and sensitive data is transmitted using untrusted network. Basically most of the time user sends the data from a trusted network to a trusted network. Bet between source and target host the network remains unsecure. Therefore, Most of the applications are consumes the cryptographic techniques for providing the security and confidentiality in data. In this presented work the main aim is to find the efficient and optimum solution for color image cryptography. Efficiency concerned with the minimizing the computational resources in terms of memory consumption and execution time and the solution optimization is leads to modifying the cryptographic technique using hybrid approach with their integrity check. Thus the desired cryptographic system required to work in less time and less memory consumption. In order to develop such approach simple mathematical techniques and lightweight cryptographic standards are required to employ with the system.

1.2 Data security aspects

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and soon. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography [2].

Confidentiality: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.

Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation: Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

Access Control: Only the authorized parties are able to access the given information

2. CRYPTOGRAPHY

This section of document contains the basic terminology that is used in encryption and decryption techniques [3].

Plain Text: The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send “Hello Friend how are you” message to the person Bob. Here “Hello Friend how are you” is a plain text message.

Cipher Text: The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, “Ajd672#@91ukl8*^5%” is a Cipher Text produced for “Hello Friend how are you”

Encryption: A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

Decryption: A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

- Decrypt – It is the process of converting cipher text into plain text.
- Cryptographic Algorithm – This is the algorithm which converts plain text into cipher text.
- Public key – This is public that means known to everyone.
- Private Key – It is only known to sender.

2.1 Characteristic of Cryptography

Although some important characteristics might not be quantifiable, it seems intuitively logical that it should be possible to identify some cryptographic algorithm characteristics that can be expressed either in objective, numeric values or subjective, adjectival values. Metrics might be used for evaluating and comparing cryptographic algorithms and the inferred confidentiality protection value of products containing cryptographic algorithms. Encryption algorithm may require some characteristics: [4]

Type - symmetric (secret key or one-key) or asymmetric (public key or two-key). While strictly speaking this may not be a metric, the type of key that an algorithm uses would be of sufficient interest to users to be worth specifying. (Because there are short-cut attacks that can be used on asymmetric algorithms, very long keys are required. With any meaningful key length, two-key algorithms are very slow when compared to one-key algorithms. This effectively limits their use to the management of keys for symmetric algorithms. It should be noted that some two key algorithms can provide a covert channel for traffic while masquerading as signatures.)

Functions. Message secrecy, message integrity, authentication, digital signatures, like the type of algorithm, may not be a metric per se but may be of interest to end users. An export criterion varies with the functionality, among other things.

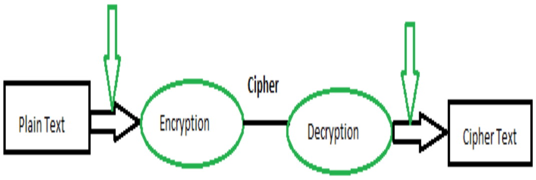
Key size. The Key Length Metric proposed in this white paper is intended to provide this comparative value.

Complexity. (Algorithm complexity for encryption, decryption, and key setup.) These attributes for encryption, decryption and key setup probably could be specified as the number of operations such as bit operations, modular multiplications and modular exponentiations. The number of operations wouldn’t change, only the speed of implementation. (This could be complicated if the algorithm can be parallelized.)

Attack. Best known methods of attack such as brute force, factoring, linear and differential cryptanalysis (qualified with whether known or chosen plaintext is provided,) number of steps and time required for a successful attack.

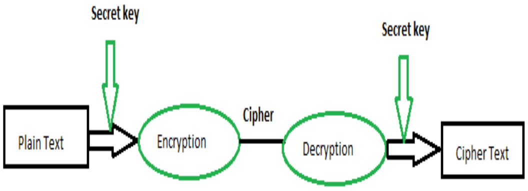
Strength. An assessment of the strength of the algorithm, based on key length, algorithm complexity and the best methods of attack. A subjective, adjectival cryptographic Algorithm Strength

2.2Cryptosystem



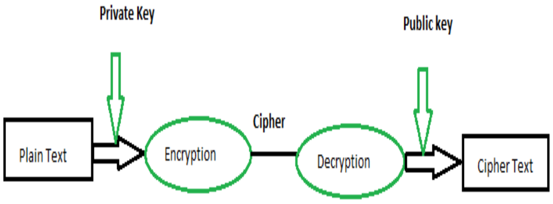
Cryptography can be broadly categorized into two different types depending on the nature of key being used i.e. symmetric key cryptography and Asymmetric key cryptography.

Symmetric key Cryptography –Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key. Process of symmetric key cryptography is shown in the following diagram.



Symmetric key cryptography

Asymmetric key Cryptography –The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. process of Asymmetric key Cryptography shown in the following diagram



Asymmetric Key Cryptography

3. CRYPTANALYSIS

It is an art of deciphering the cipher text without knowing the key or encryption. Some of the methods related to this are as follows:

□ Cipher text Only: In this type of attack an attacker can access only cipher text or decrypted data but cannot access plain text. This type of attack is done on simple cipher like Caesar cipher where frequency analysis can be used to break the code.

□ Known Plain text: In this type of attack a cryptanalyst have plaintext and their corresponding cipher text. Attacker tries to find out the relation between these two.

□ Chosen Cipher text: In this type of attack a attacker obtains the various types of plaintexts corresponding to an arbitrary set of cipher text.

□ Chosen Plain text: In this type of attack a attacker obtains the various cipher text corresponding to an arbitrary set of plain text.

□ Adaptive Chosen Plain text: This is similar to Chosen Plaintext, except in this type of attack a attacker chooses subsequent set of plaintext which is based on the information obtain from previous encryption methods.

□ Adaptive Chosen Cipher text: This is similar to Chosen Cipher text, except in this type of attack a attacker chooses subsequent set of cipher text which is based on the information obtain from previous encryption methods.

□ Related Key Attack: As the chosen plaintext attack in which attacker can obtain only cipher text encrypted with the help of two keys. These keys are unknown but the relationship between these keys is known. Example two keys differ by a single bit.

4. LITERATURE SURVEY

This section provides the study on the recent contribution placed in the domain of hybrid cryptographic data models.

According to ***Mohammad Reza Najaf Torkaman et al [6]*** exists a big demand for innovative secure electronic communications while the expertise level of attackers increases rapidly and that causes even bigger demands and needs for an extreme secure connection. An ideal security protocol should always be protecting the security of connections in many aspects, and leaves no trapdoor for the attackers. Nowadays, one of the popular cryptography protocols is hybrid cryptosystem that uses private and public key cryptography to change secret message. In available cryptography protocol attackers are always aware of transmission of sensitive data. Even non-interested attackers can get interested to break the ciphertext out of curiosity and challenge, when suddenly catches some scrambled data over the network. First of all, we try to explain the roles of innovative approaches in cryptography. After that we discuss about the disadvantages of public key cryptography to exchange secret key. Furthermore, DNA steganography is explained as an innovative paradigm to diminish the usage of public cryptography to exchange session key. In this protocol, session key between a sender and receiver is hidden by novel DNA data hiding technique. Consequently, the attackers are not aware of transmission of session key through unsecure channel. Finally, the strength point of the DNA steganography is discussed.

Information protection is one of the most important issues in every domain, especially when we are talking about enterprises. Information safety can be translated into three key terms: integrity, availability and data protection. There is a great number of means used in order to achieve the three objectives simultaneously. The most popular is cryptography because it offers a lot of techniques which nowadays are impossible to fail. In this paper ***Georgiana Mateescu et al [7]*** want to prove their efficiency by comparing the different types of crypto algorithms and by presenting their weaknesses and strengths. In order to maximize the benefits of the crypto techniques, we propose a hybrid approach that combines three crypto algorithms.

Mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client to overcome on the limitation of mobile devices and uses the main advantage of cloud computing. As mobile cloud computing continues to grow, so does the need for effective security mechanisms because data offloaded and moved from mobile to unknown destination. Encryption algorithms play good roles in information security systems (ISS). Those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. The present asymmetric encryption methods and symmetric encryption methods can offer the security levels but with many limitations. For instance key maintenance is a great problem faced in symmetric encryption methods and less security level is the problem of asymmetric encryption methods even though key maintenance is easy. To improve the strength of these algorithms, ***Hatem M. Abdul Kader et al [8]*** propose a new hybrid cryptographic algorithm in this paper. The algorithm is designed using combination of two symmetric cryptographic techniques and two Asymmetric cryptographic techniques. This protocol provides three cryptographic primitives, integrity, confidentiality and authentication. It is a hybrid encryption method where elliptical curve cryptography (ECC) and advanced encryption (AES) are combined to provide node encryption. (RSA) algorithm and (Blowfish) are combined to provide authentication and (MD5) for integrity. We applied this protocol on one type of wireless sensor network (Zigbee) to be evaluated and compared it with other four hybrid cryptography protocol. The results show that the proposed hybrid cryptographic algorithm gives better performance in terms of computation time and the size of cipher text.

Satellite based communication is a way to transmit digital information from one geographic location to another by utilizing satellites. Satellite as communication medium to transfer data vulnerable various types of information security threat, and require a novel methodology for safe and secure data transmission over satellite. ***Omar M.Barukab et al [9]*** a methodology is proposed to ensure safe and secured transferred of data or information for satellite based communication using symmetric and asymmetric Cryptographic techniques.

Cryptography is the technique to encrypt and decrypt the data for secure communication. The cryptographic mechanism enables the entities of network to transmit secure data through insecure channel. So that, only the intended users can access the transmitted data. Two public key cryptographic techniques are mostly used for secure transmission of data, namely Elliptic Curve Cryptography & RSA. Among this two cryptographic system, ECC is more first due to its small key size. DNA-cryptography is a new technique, which also used for secure data transmission in recent years. The DNA based cryptography technique, derived from DNA computing. It uses DNA nucleotide sequence for cryptographic purpose. To develop more secure and stable cryptography technique, ***Prokash Barman et al [10]*** propose a new hybrid DNA encoded Elliptic Curve Cryptography scheme in this paper. DNA encoded ECC cryptography uses smaller key size and less computation power with multilevel security. The main attraction of the proposed system is that it has two level of security. First is unknown DNA sequence based encoding and the second is Light weight ECC based encryption and decryption system.

5. ISSUES OF CRYPTOGRAPHY

There are several issues related to cryptographic algorithm such as time complexity, space complexity and its resistance to various types of attacks. In order to implement an effective cryptographic algorithm all these aspects needs to be considered in order to make it robust. Let's discuss these issues:-

Time Complexity: It is the amount of time required to encrypt and decrypt the data. The algorithm should be designed in such a way that it should take as less time as possible for its execution. Hence it is necessary to consider its time complexity while implementing a cryptographic algorithm.

Space complexity: It is the amount of space consumed by cipher text as compared with plain text. As more and more mobile devices with limited connectivity in terms of data rate are being used nowadays, it is very essential to keep the size of cipher text being produced as small as possible as to deal with variable data rates. Thus it is very important to device a way to reduce the size of cipher text as much as possible to increase data transmission efficiency.

Security: The very important purpose of cryptography is to secure the data being transmitted over the network from various types of attacks. The data being transmitted is always vulnerable to various types of attacks such as men in the middle attack, brute force attack etc. Thus in order to prevent the data from being compromised it is necessary to protect the data from unauthorized users.

Problem domain

Cryptographic techniques are a kind of art by which the data is transformed or manipulated using mathematical or logical models. Now a days the traditional cryptographic techniques have been replaces new and hybrid techniques of cryptography. These techniques promises to provide secure and efficient cipher generation, on the other hand the following complexities are observed during evaluation of different techniques.

1. Most of the cryptographic techniques are time consuming processes
2. Not includes the integrity checks on transmitted data
3. Required security in key exchange
4. The amount of cipher text is higher than the original text
5. During attack the cipher text is easily breakable with Men in the middle kind of attacks.

Solution domain

In order to find an optimum solution for cryptographic processes the following solutions are suggested to incorporate.

1. Implementation of compression based cryptographic approach which reduces the cipher text in significant amount
2. Less number of cryptographic cycles for improving the time complexity of the cryptosystem.
3. Justifying the solution under authentic file transfer with man in middle case study
4. Apply the integrity check during recovery of data. For validating data it is not altered during the transmission it is required to validate the entire recovered data. Thus a additional method is required to incorporate that check the data for their intermediate modifications.
5. Improve security in key generation and key exchange

6. PROPOSED WORK

The proposed system is a cryptographic algorithm which accepts any kind of data for processing. In addition of that the simulation of the proposed methodology enables a user to send and receive data using the application. The proposed simulation first accepts the data from the user and then compresses it in order to reduce the data size. After doing that it uses the proposed cryptographic algorithm data to manipulate the data into cipher text. The generated cipher text is compressed again and using file splitter utility and then it is transmitted much efficiently on network. On the other end the receiver follows the same procedure in reverse direction to decrypt it.

1. Providing the simulation of secure file transfer utility by using hybrid cryptographic algorithm.

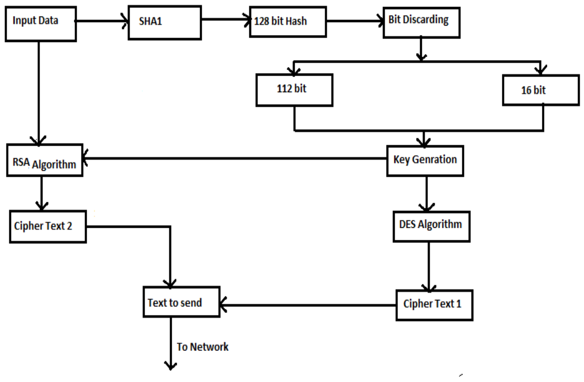
2. Designing and implementing the hybrid cryptographic technique in order to reduce the space and time complexity by compressing the data being sent in network.

3. Cross validating the data integrity using the MD5 hash function and secure hash function.

4. Reducing the size of cipher text so as to make data transmission more efficient.

7. PROPOSED METHODOLOGY

The overview of the proposed systems components and discussed in this section of document.



3.1 Encryption process

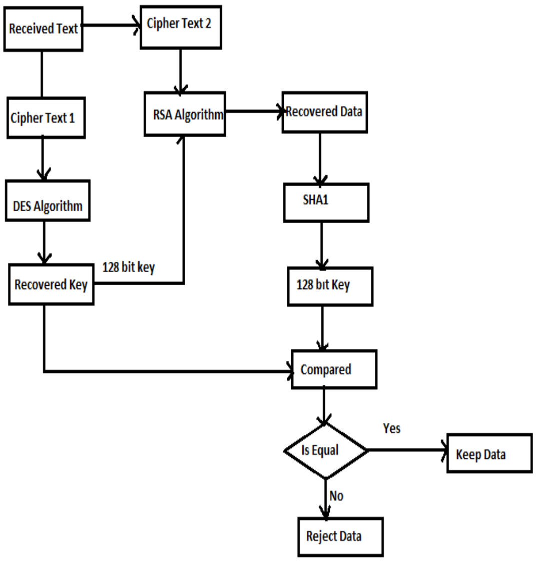
The proposed working hybrid model for data cryptography is given using figure 3.1 and figure 3.2. In figure 3.1 the encryption process of the system is described and the figure 3.2 reports the decryption process of the system. During the encryption process user need to encrypt the file using the hybrid cryptographic model, thus a input file is first produced to the system. The input file is first processed using SHA1 hash generation algorithm, the SHA1 algorithm generates the 128 bit hash code for the input data

Input file: This is the input file to be sent over the network.

SHA1: The compressed zip file is produced before the SHA1 algorithm to generate 128 bit hash. This hash is used to check the data validity at the receiver end. If the sender generated hash matched with the receiver end hash than the data is valid otherwise data is corrupt.

Key (16 bytes): This is SHA1 generated hash which is separately treated as key form encryption.

Over the produced 128 bit hash key the bit discarding process is taken place, in this process the 128 bit hash code is converted into 16 blocks of the 8 bit data. In each block of data the first bit is removed and placed separately for further processing. Thus the 128 bit hash code is converted into 112 bit of code and 16 bit of separated code. Both the bits 112 and 16 bit data is produced into a key generator where the 16 bit data is divided into 2 blocks of 8 bit and 112 bit of data converted into 14 blocks of data both the newly generated are combined to generate the complete 128 bit of key. For securing the key more the DES algorithm is used to encrypt the key which generates the cipher 1 which the encrypted key for decryption process. On the other hand the input original data is produced over the RSA algorithm with a 128 bit key generated by the key generator. This process generates the cipher 2. In further steps the cipher text 1 and cipher text 2 is combined and ready to prepare the text for transmission.



3.2 Decryption Process

The transmitted text to the network is received by the end user, this text is termed here as the received text. In first process the received text is divided into two different ciphers, cipher 1 which is outcome of key data and seconds the cipher 2 that contains the encrypted data for security. The cipher 1 is treated first to generate the key for data recovery, therefore first the cipher text 1 is produced to DES algorithm for the recovering the original key by which the data is recovered. After recovering key using decipher of cipher text 1 the key is produced to RSA algorithm with the cipher text 2. The RSA algorithm decipher the original text and can be used with the other application but for authenticating the recovered data on receiver end the integrity check is applied for the data. Therefore first the recovered data is processed through the SHA1 hash key and 128 bit obtained from the data. In further the comparer is implemented, the comparer has two functionalities first using the SHA1 128 bit, regenerate the original key by which the encryption performed. Thus the same operation is performed over the 128 bit to generate key and second the comparison among generated key and the obtained key from network. In further is both the keys are found similar the data is accepted by the system else the data can be rejected.

Application domain

There is a rich verity of applications available for cryptographic approach some of the applications are listed in this section.

1. Network file transfer: due to less time complexity and space overhead the propose cryptosystem is helpful for secure data transfer utility
2. Reducing the disk utilization in host based applications
3. Improving the data transfer rate during network communication

Expected outcome

After implementation of the proposed cryptographic algorithm the following outcomes are expected.

1. Reduced amount of cipher text
2. Enhanced time and space complexity
3. Authorized with man in middle attack
4. An efficient and robust cryptographic technique.

8. CONCLUSION

Proposed algorithm is secure because which encrypt and decrypt message with secretly generated sender key and receiver key which is known to sender and receiver. Two level of security is implemented. Algorithm is based on hybrid cryptography as it uses asymmetric that is sender and receiver key and asymmetric key that is both sender and receiver uses same key pair for both process encryption and decryption.the DES and RSA hybrid cryptographic algorithm is relatively more secure and easier.

REFERENCES

[1] V Gampala, S Inuganti, S Muppidi, *"Data Security in Cloud Computing with Elliptic Curve Cryptography"*, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012

[2] D Elizabeth Rob, l Denning, "Cryptography and Data Security", http://faculty.nps.edu/dedennin/publications/Denning-CryptographyDataSecurity.pdf

[3] S J Lin and W H Chung, "A Probabilistic Model of Visual Cryptography Scheme With Dynamic Group", IEEE Transactions On Information Forensics And Security, Vol.7, No.1, February 2012

[4] N D. Jorstad, L T. Smith Jr, "Cryptographic Algorithm Metrics", Directorate for Freedom of Information and Security Review (OASD-PA) Department of Defense, January 1997

[5] E. Thambiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012

[6] Mohammad Reza Najaf Torkaman, Nazanin Sadat Kazazi, Azizallah Rouddini, "Innovative Approach to Improve Hybrid Cryptography by Using DNA Steganography", International Journal on New Computer Architectures and Their Applications (IJNCAA) 2(1): 224-235

[7] Georgiana Mateescu, Marius Vladescu, "A Hybrid Approach of System Security for Small and Medium Enterprises: combining different Cryptography techniques", Proceedings of the 2013 Federated Conference on Computer Science and Information Systems pp. 659–662, 978-1-4673-4471-5/$25.00 c 2013, IEEE

[8] Hatem M. Abdul Kader, Mohie M. Hadhoud, Salah M El-Sayed, Diaa Salama AbdElminaam, “Performance Evaluation Of New Hybrid Encryption Algorithms To Be Used For Mobile Cloud Computing”, INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH, VOL 2, ISSUE 4 63

[9] Omar M.Barukab, Asif Irshad Khan, Mahaboob Sharief Shaik , MV Ramana Murthy, “Secure Communication using Symmetric and Asymmetric Cryptographic Techniques”, I.J. Information Engineering and Electronic Business, 2012, 2, 36-42 Published Online April 2012 in MECS.

[10] Prokash Barman, Banani Saha, “An Efficient Hybrid Elliptic Curve Cryptography System with DNA Encoding”, International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842 Issue 5, Volume 2 (May 2015).