Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

A Survey of Data Encryption & Data Decryption Methods

Vishwakarma Manila and Jain Sourabh*

Computer Science and Engineering, Institute of Engineering and Science,
IPS Academy, Indore, India. E-mail: manila27.mv@gmail.com

ABSTRACT

The backbone of the modern world is electronic communication. Data is transferred from one place to another in almost no time using the electronic medium. But it also exposes the confidential data to the intruder. RSA is the most common and efficient cryptography technique that is used for the purpose of encrypting the content and then sending it over the channel, then than at receivers end the content is decrypted and converted in to original form. Although there are many security mechanisms are available. But there is a continuous need to improve the existing methods. Cryptography is a security mechanism which caters the security services of world in perfect manner. This paper presents a review of cryptography based techniques for data encryption and data decryption.

KEYWORDS: Network security, cryptography, Elgamal cryptosystem, two key cryptography

***Corresponding author**

Mr. Sourabh Jain

Assistant Professor, Computer Science and Engineering

Institute of Engineering and Science, IPS Academy

Indore, India

E-mail: sourabhjain@ipsacademy.org

INTRODUCTION

Today, information[1] is one of the most valuable intangible assets. Due to this fact, information security had become an important issue. Cryptography is one of the methods used to protect data from unauthorized access and being stolen. There are two types of cryptosystem, which are symmetric cryptosystem and asymmetric cryptosystem. In Symmetric cryptosystem, the sender and recipient share the same key. It means the same key is used for encryption and decryption. In Asymmetric cryptosystem, different keys are used. A public key is used by sender to encrypt the message while the recipient used a private key to decrypt it. Both of these cryptosystem have their own pros and cons. For instance, Symmetric cryptosystem consume less computing power but it is less secure than Asymmetric cryptosystem. Currently, there are a few cryptosystem which are widely implemented such as Advanced Encryption Standard (AES), Twofish, River Cipher 4 (RC4) and Data Encryption Standard (DES). However, these modern cryptosystem have their origins. The classical cipher such as Caesar Cipher, Hill Cipher, Vigenère Cipher act as the foundation for the cryptology's world today.

However, there are other natural cryptographic problems to be solved and they can be equally if not more important depending on who is attacking you and what you are trying to secure against attackers. The cryptographic goals covered in this text (in order of appearance) are privacy, integrity, authentication, and no repudiation.

These three concepts form what is often referred to as the **CIA triad**. The three concepts embody the fundamental security objectives for both data and for information and computing services. FIPS PUB 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are:

Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

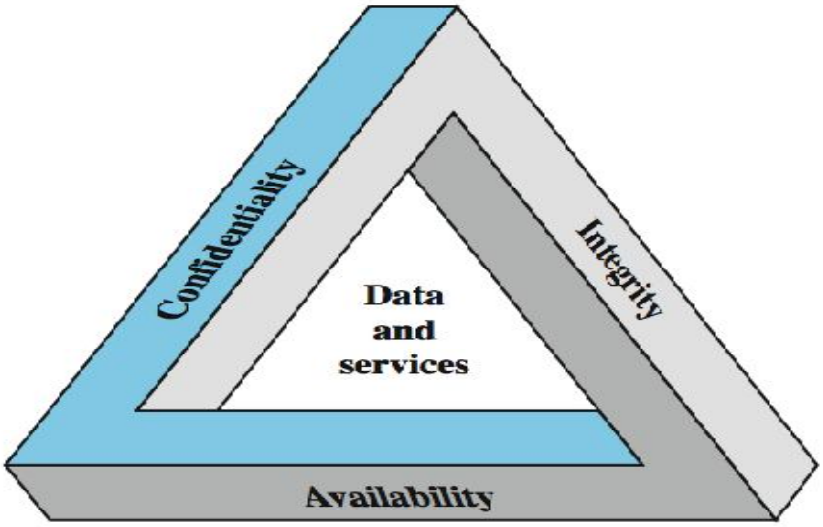

Figure 1.1 : Goals of Cryptography

LITERATURE SURVEY

The ElGamal system is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol.

After that there are many variances of ElGamal cryptosystem has been proposed till now some of them are: hashed ElGamal [3], twin ElGamal [6] proposed by cash in 2009 and show if there are groups where the Computational Diffie Hellman hold, but Interactive Diffie Hellman does not hold, in such groups twin ElGamal is secure where as classical ElGamal is not secure. But it is not known whether such groups exist or not. ElGamal-like cryptosystem proposed by Hwang in 2002 [4], use to

encrypt large message by breaking large messages into small messages, whereas original ElGamal PKC is use to encrypt single message and if multiple messages are encrypted using same parameters, system is vulnerable to known plaintext attack. With some merit in the new scheme, it comes with some demerit pointed out by Wang [5].

[7] Jointly has done a Comparative Analysis of Encryption Algorithms for Data Communication. The authors analyze the performance of encryption algorithm is evaluated considering the following parameters like Computation Time, Memory usage and Output Bytes, RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm[7].

[8] Evaluate the Performance of Symmetric Encryption Algorithms like AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. Diaa Salama et.al jointly done a research work in the title "Wireless Network Security Still Has no Clothes" [9]. The above research work evaluates the performance of most common symmetrical encryption algorithms like AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6.

The Elliptic Curve Cryptosystem (ECC), whose security rests on the discrete logarithm problem over the points on the elliptic curve. The main attraction of ECC over RSA and DSA is that the best known algorithm for solving the underlying hard mathematical problem in ECC (the elliptic curve discrete logarithm problem (ECDLP) takes full exponential time. RSA and DSA take sub-exponential time. This means that significantly smaller parameters can be used in ECC than in other systems such as RSA and DSA, but with equivalent levels of security. A typical example of the size in bits of the keys used in different public key systems, with a comparable level of security (against hown attacks), is that a 160-bit ECC key is equivalent to RSA and DSA with a modulus of 1024 bits. The lack of a sub-exponential attack on ECC offers potential reductions in processing power and memory size. These advantages are especially important in applications on constrained devices [10]

Table1 : Literature Survey

Author	Proposed work	Conclusion
Abdalla M et al.[3] 2001	Hashed elgamal	It basically used for small messages.
wang M et al. [5] 2006	Elgamal PKC	It uses same parameters for encrypt multiple messages.
Cash D et al. [6] 2009	twin ElGamal	Encrypt large message by breaking large messages into small messages. Not secure.
Mehrotra Seth S et al. [7] 2011	RSA algorithm	It consume longest encryption time and memory usage.
Salama D et.al [8] 2011	AES, DES, 3DES, RC2, Blowfish, and RC6	Evaluates the performance of most common symmetrical encryption algorithms
G.V.S. Raju et.al [10] 2003	Elliptic Curve Cryptosystem (ECC)	Especially important in applications on constrained devices

PROBLEM DEFINITION:

- The main disadvantage of ElGamal is the need for randomness, and its slower speed (especially for signing).
- Another potential disadvantage of the ElGamal system is that message expansion by a factor of two takes place during encryption. However, such message expansion is negligible if the cryptosystem is used only for exchange of secret keys.
- Not secure against common modulus attack
- Not secure against known plaintext attack

CONCLUSION

We have elaborated the basic concept of cryptography and the key management schemes. A review of modern methods is also done in brief. The most of the modern data security techniques have been reviewed. Each of the method has been analyzed with the advantages and the disadvantages. Then a list of common problems in the current version has been identified. On basis of the research gap identified, the problem was formulated.

REFERENCES

1. Stallings William "Network Security Essentials", Pearson Education, 2004.
2. National Bureau of Standards, "Data Encryption Standard," FIPS Publication 1977; 46.
3. Abdalla M, Bellare M, and Rogaway P. "The oracle Diffie-Hellman assumptions and an analysis of DHIES." In David Naccache, editor, CT-RSA 2001; 20(LNCS):143–158. Springer-Verlag.
4. Hwang M.S., Chang C.C., and Hwang K.F. "An ElGamal like cryptosystem for enciphering large messages." IEEE Trans. Knowledge and Data Engineering, 2002; 14(2): 445- 446.
5. Wang M, Yen S, Wu C, and Lin C. "Cryptanalysis on an ElGamal-like cryptosystem for encrypting large messages." Presented at: Proceeding of the 6th WSEAS International conference of Applied Informatics and communications 2006; 418-422.
6. Cash D, Kiltz E, and Shoup V. "The Twin DiffieHellman problem and applications." 2009.
7. Mehrotra Seth S, Mishra R. "Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST , June 2011; 2(2):.192-192.
8. Salama Abd Elminaam D, Mohamed Abdual Kader H, and Mohamed Hadhoud M," Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, May 2010;10(3):213-219.
9. Salama D, Abdual Kader H, and Hadhoud M" Wireless Network Security Still Has no Clothes", International Arab Journal of e-Technology, June 2011 ; 2(2):112-123.
10. G.V.S. R and Akbani R. "Elliptic curve cryptosystem and its applications." IEEE International Conference on Systems, Man and Cybernetics, 2003; 2: 1540 – 1543.