Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

# Comparative Study Of Different Cryptoghraphic Algorithms

Maninder Kaur[1] , Navpreet Kaur[1] & Baldeep Singh[2]
PG Student of MCA[1], Assistant Professor[2]
SBBSU, Punjab, India
maninderminhas06@gmail.com, navitoor028@gmail.com, doad.baldeep@gmail.com

***Abstract*-- Due to development of network technologies it is easy to send and receive any type of information. The data or information may be related to banking system, government or military. This confidential information can be leaked or stole by unauthorized person. So foe this security is an impotent issue for confidential information. For security three aspect are required:- confidentiality, integrity & availability. ITUT recommended mechanism of encipherment. Encipherment refers to hiding or covering the data using key. Encipherment is classified into two categories:- cryptography and steganography. Cryptography is process of changing plaintext into cipher text which is not understandable by unauthorized or intruders. This paper is based on different algorithms used for cryptography and their comparative study. Cryptography uses two types of algorithms; symmetric key algorithm and asymmetric key algorithm.**

***Keywords:*** **network, security, cryptographic, algorithm**

## I. INTRODUCTION

The purpose of network security is essential to present loss, through misuse of data. Cryptography [1] is Greek word whose meaning is secret writing. Cryptography is process of converting text into another form that is not understandable by eve. Encryption [2] is process of converting plaintext to cipher text using key. Decryption [3] is process of converting cipher text to plaintext by using key which is given by sender. Encryption is done on sender side and decryption is done on receiver side.

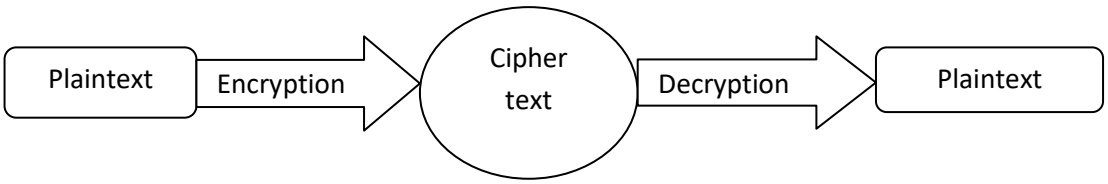


*Fig. 1: Process of cryptography*

Cryptography uses two types of algorithms:-

Symmetric key algorithm
Asymmetric key algorithm

### 1. Symmetric key algorithm

In this algorithm only one key which is private key is used on both sides that is sender and receiver. This is also called shared key algorithm because both sides use same key. The private key is generated by Alice and send to Bob for decryption. This key must be kept secret so that eve cannot stole the information. There are different symmetric[4] key algorithms.

**(a).DES :-** Data Encryption Standard is a symmetric key block cipher published by National Institute of Standard and Technology (NIST)[6]. DES[7] uses 64 bit plaintext and 56 bit key to generate 64 bit cipher text .Encryption is made by two permutations initial and final. DES uses feistelcipher[8],which divides a block into two equal halves.This uses 16 rounds for encryption. This main reason of failure of DES is: The key used in it is very small that is 56 bit which is easy to break by using brute force attack[9].

**(b).Triple DES:-** After DES IBM develop Triple DES[10] which works same as DES but main difference is that Triple DES use 3 keys, each key is of 64 bit and entire length of key is 192 bits. Although it is more secure than DES but it is also breakable by brute force attack.

**(c).AES:-** Advanced encryption standard[11] is a symmetric key block cipher was published by national institute of standards and technology in December 2001.AES is non festal cipher so it is not divide block into two equal parts. It encrypt and decrypt a block of 128 bits.AES convert plaintext into cipher text by using 4*4 array of bytes .the key size can brief 128,192 or 256 bits depend on no. of rounds which are 10,12 or 14 respectively.AES is more secure than DES.This algorithm use number of rounds for complete the process that's why it consume more time than DES.

### 3. Asymmetric key algorithm

In asymmetric[5] key algorithm two different key are used that is public key and private key public key is used on sender side for encryption and private key is used on



CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

receiver side for decryption. Asymmetric key algorithm is based on personal secrecy.

In asymmetric cryptography different algorithm are used like RSA,ElGamalcyptosystem and Elliptic Curve cryptosystem .

**(a).RSA:-**RSA[12] is the common public key algorithm invented by Ron Rivest ,AdiShamin and Len Adleman. In RSA two keys are used public key is used by Alice for encryption and this key is known to all, private key is used by Bob for decryption and is known to only Bob .in this two formulate are used for encryption and decryption.

$C=P^e \bmod n$

Where c is cipher text P and Q any prime no. and e is public key which must be greater than 1 and less than (p-1)(q-1) n is p*q and Pis plaintext decryption.

$P=C^d \bmod n$

P is plaintext , c is cipher text,d is private key which is known by only Bob and n is p*q where p,q is prime number.

**(b).ElGamalCryptosystem :-**ElGamal Cryptosystem[13] is another public key crypto system invented by TaherElgamal. ElGamal cryptosystem is based on the discrete logarithm problem[15]. The ElGamal key pair generation is simple than RSA. In ElGamal 2048 bits key size can also used. The main application of ElGamal cryptosystem is key exchange where two parties can exchange the keys, authentication and encryption and decryption of small message. It is new in market and is not widely used.

**(c).Elliptic Curve Cryptosystem:-**Elliptic Curve Cryptosystem[14] is more secure asymmetric cryptosystem then RSA and ElGamal,develop for more security and simplicity with smaller key size. This algorithm isdesigned on elliptic curves for security. The main benefits of elliptic curve cryptosystem are- It iseasy of key management and it has efficient computation.

**4. The comparison table is given below:-**

Table: Comparison Table

| Parameters | DES | Triple DES | AES | RSA | ElGamal Cryptosystem | Elliptic curve cryptosystem |
|---|---|---|---|---|---|---|
| Designers | IBM | IBM | Vincent Rijmen,JoanDaemen | Ron Rivest,AdiShamir,LeonardAdleman | TaherElGamal | Neal Koblitz,Victor S. Miller |
| Published Year | 1975 | 1998 | 1998 | 1977 | 1985 | 1985 |
| Type | Symmetric | Symmetric | Symmetric | Asymmetric | Asymmetric | Asymmetric |
| Rounds | 16 | 48 DES-equivalent rounds | 10,12,14 depend on key size | No rounds | No rounds | No rounds |
| Key size | 56 bits(+8 parity bits) | 168,112 or 56 bits | 128,192 or 256 | 1024 to 4096 | >1024 | >1024 |
| Block size | 64 bits | 64 bits | 128 bits | Depend on key size | Depend on key size | Depend on key size |
| Network type | Feistel cipher | Feistel cipher | Non-feistel | Common network | Common network | Common network |
| Speed | Fast | Fast than DES | Fast than triple DES | Very fast | Very fast | Very fast |
| Security | Breakable by brute force attack | Also breakable by brute force attack | Secure than DES | Secure | Secure | More secure |

**5. Conclusion:-**

This paper present different key algorithms of symmetric and asymmetric like DES,3DES,AES ,RSA,ElGamal and Elliptic curve algorithm. All algorithms have their own pros and cons. AES is symmetric is more secure and fast, although it needs more processing power. Also in asymmetric, RSA is secure but it use many large keys so its complexity increases that's why we use ElGamal asymmetric cryptosystem,Elliptic curve replaces ElGamal also but it is new in market and use discrete logarithmic problem.

**References:-**

[1]. Rivest, Ronald L. (1990). "Cryptography".In J. Van Leeuwen.Handbook of Theoretical Computer Science.**1**. Elsevier.





CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

[2]. Fouché Gaines, Helen (1939), Cryptanalysis: A Study of Ciphers and Their Solution, New York: Dover Publications Inc, ISBN 978-0486200972

[3]. Kahn, David, TheCodebreakers - The Story of Secret Writing (ISBN 0-684-83130-9) (1967)

[4]. Ayushi (2010). "A Symmetric Key Cryptographic Algorithm" (PDF).International Journal of Computer Applications.1-No 15.

[5].ChristofPaar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online cryptography course that covers public-key cryptography), Springer, 2009.

[6]. "2016 Appropriations Increase NIST Funding 166 percent". NIST. 2016. Retrieved 2016-01-13.

[7]. Biham, Eli and Shamir, Adi (1991). "Differential Cryptanalysis of DES-like Cryptosystems".Journal of Cryptology.**4** (1): 3–72. doi:10.1007/BF00630563. (preprint).

[8]. Menezes, Alfred J.; Oorschot, Paul C. van; Vanstone, Scott A. (2001). Handbook of Applied Cryptography (Fifth ed.). p. 251.ISBN 0849385237.

[9].Wiener, Michael J. (1996). "Efficient DES Key Search". Practical Cryptography for Data Internetworks. W. Stallings, editor, IEEE Computer Society Press.

[10]. Barker, William C. (May 2004). "NIST Special Publication 800-67 Version 1: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher" (PDF).Retrieved 2016-10-09.

[11]. ChristofPaar, Jan Pelzl, "The Advanced Encryption Standard", Chapter 4 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online lectures on AES), Springer, 2009.

[12]. Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF).Communications of the ACM.**21** (2): 120–126. doi:10.1145/359340.359342.

[13]. ElGamal, Taher (1985). "A public key cryptosystem and a signature scheme based on discrete logarithms" (PDF). Advances in cryptology: Proceedings of CRYPTO 84. Lecture Notes in Computer Science. **196**. Santa Barbara, California, United States: Springer-Verlag. pp. 10–18. doi:10.1007/3-540-39568-7_2.

[14]. ChristofPaar, Jan Pelzl, "Elliptic Curve Cryptosystems", Chapter 9 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online cryptography course that covers elliptic curve cryptography), Springer, 2009. (archivedhere as of April 20, 2016).

[15]. Shor, Peter (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer".SIAM Journal on Computing.**26** (5): 1484–1509. arXiv:quant-ph/9508027 . doi:10.1137/s0097539795293172. MR 1471990.