ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms

Nivedita Bisht[1], Sapna Singh[2]

Assistant Professor, Department of Electronics and communication Engineering, SIT Pithoragarh, India[1]

Assistant Professor, Department of Electronics and communication Engineering, SIT Pithoragarh, India[2]

ABSTRACT: Data security is very important in wireless network and for this cryptography plays a crucial role which means "secret writing". In Cryptography encryption decryption of data is done by using secret key to provide data confidentiality, data integrity and data authentication. This paper provide a comparative study between various encryption algorithm like AES, DES, RSA and DIFFIE-HELLMAN .Here we compare the different factors of both symmetric key and asymmetric key encryption algorithm.

KEYWORDS: Cryptography, encryption, symmetric key encryption, asymmetric key encryption.

I. INTRODUCTION

Cryptography, a word with Greek origins, means "secret writing" is the science of devising methods that allow for information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient. The message to be sent through an unreliable medium is known as **plaintext**, which is encrypted before sending over the medium. The encrypted message is known as **cipher text**, which is received at the other end of the medium and decrypted to get back the original plaintext message. Hence a cryptosystem is a collection of algorithms and associated procedures for hiding and revealing information.

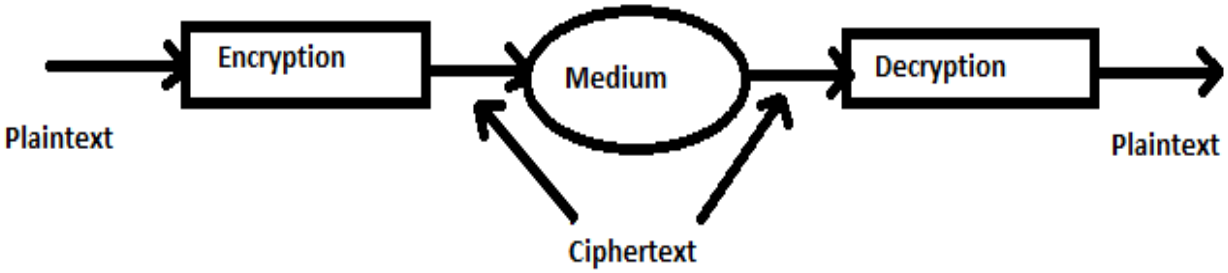

Fig .1 A Simple Cryptography Model

Cryptography algorithms can be divided into two broad categorizes - **Symmetric key cryptography** and **asymmetric key cryptography.**

II. SYMMETRIC KEY CRYPTOGRAPHY

In symmetric key cryptography, same key is shared, i.e. the one key is used in both encryption and decryption, hence also known as single key or secret key encryption. Symmetric key cryptography algorithms are simple requiring lesser execution time. As a consequence, these are commonly used for long messages. There are two types of symmetric key encryption modes one as block ciphers and other as stream ciphers. Block ciphers operate on groups of bits called blocks and each block is processed multiple number of times. The key applied in each round is in a unique manner. A stream cipher operates on one bit at a time i.e. The data is divided as small as single bits and then the encryption is done. In symmetric key encryption the AES algorithm and the DES algorithm different factors are analyzed.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

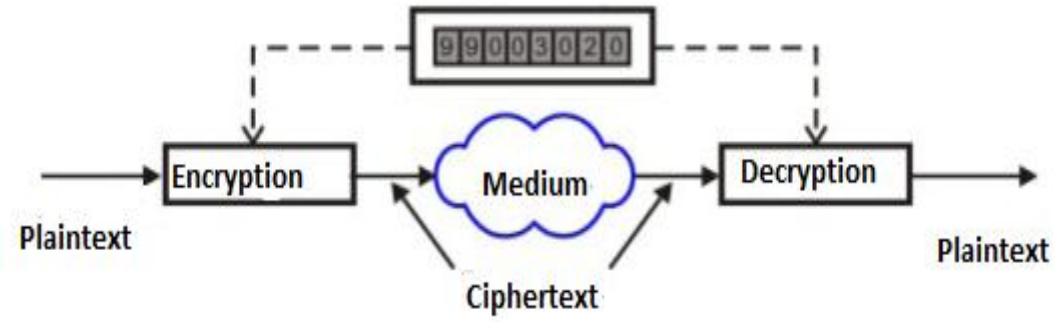

Fig.2 A Simple Symmetric Key Cryptography Model

III. ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

AES is a symmetric key algorithm which operates on two dimensional arrays of bytes known as state and the state consists of four rows of each bytes. AES has key size of 128,192 OR 256 Bits which protect against certain current and future attacks. Hardware and software both implementation are faster and can be implemented on various platforms.

IV. DATA ENCRYPTION STANDARD (DES) ALGORITHM

DES is a symmetric block cipher having 64-bits long input key but uses only 56-bits in length. The decryption is performed by same password as encryption only the stages are carried out in reversed manner.DES has 16 rounds so to produce cipher text the main algorithm is repeated 16 times. Des is more vulnerable to brute force attack because as the number of round increases the algorithm of security exponentially increases.

V. ASYMMETRIC KEY CRYPTOGRAPHY

In asymmetric key cryptography different keys are used for encryption and decryption, hence also known as public key encryption. The two keys are a private key and a public key. The public key is announced to the public; whereas the private key is kept by the receiver. The sender uses the public key of the receiver for encryption and the receiver uses his private key for decryption. Here the number of keys required is small but it is not efficient for long messages. In asymmetric key encryption the RSA algorithm and Diffie-Hellman algorithm different factors are analyzed.

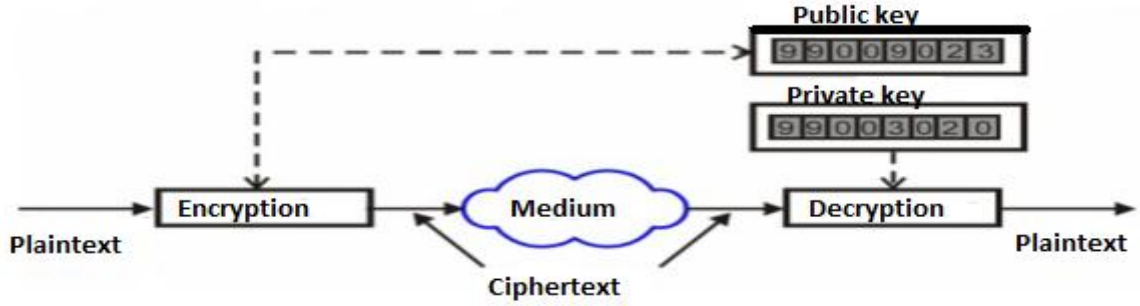

Fig.3 A Simple Asymmetric Key Cryptography Model

VI. RIVEST-SHAMIR-ADLEMAN (RSA) ALGORITHM

RSA is most widely used public –key algorithm. It provides secrecy and digital signature both. To generate the public and private key it uses a prime number and multiplies larger numbers together. In this it uses two different keys for encryption and decryption. For security purpose its key size should be greater than 1024 bits.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

VII. DIFFIE-HELLMAN (DH) ALGORITHM

It is the public key algorithm which uses discrete logarithms in a finite field. It is also known as key exchange algorithm. In this the protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. Hence this algorithm is vulnerable to a Man- in –the- middle attack. When an appropriate mathematical group is used then, only this protocol is considered to be secure.

VIII. THEORETICAL ANALYSIS OF ENCRYPTION ALGORITHM

FACTORS	AES	DES	RSA	DH
Key used	same key for encryption and decryption	same key for encryption and decryption	different key for encryption and decryption	different key for encryption and decryption
Algorithm	symmetric	symmetric	asymmetric	asymmetric
Key length	128,192 or 256 bits	56 bits key	1024 bits	key exchange management
Speed	fast	fast	fast	slow
Tunability	no	no	yes	yes
Power consumption	low	low	high	high
Security	excellent security	not secure enough	least secure	less secure than RSA
Cost	cheaper	costly	costly	depends on key
Implementation	simple	complex	complex	complex than RSA

IX. RESULTS

Here the study of symmetric and asymmetric key algorithms is done according to different factors. The key used is defined in terms of encryption and decryption either it is same or different. The algorithm used is defined according to its type symmetric or asymmetric. The key length is used according to bit value. The speed is defined in terms of fast or slow. The power consumption takes as low or high. The security is defined as excellent, not secure and least secure. The cost is defined as cheaper or costly. The implementation according to its algorithm used is simple or complex.

X. CONCLUSION

A comparative study of encryption techniques in terms of symmetric key and asymmetric key algorithms analyzed that symmetric key algorithms is viewed to be good in terms of speed and power consumption while asymmetric key algorithms in terms of tunability. In the symmetric key encryption AES algorithm is found to be better in terms of cost, security and implementation. In asymmetric key encryption RSA algorithm is better in terms of speed and security.

REFERENCES

1. Abdul D S, Eliminaam ,Kadar H M A and Hadhoud M M (2008), " Performance Evaluation of symmetric Encryption Algorithms," IJCSNS International Journal of Computer Science and Network Security , VOL.8 No. 12,December.
2. Gurjeevan singh, Ashwani single, K S sandha,"cryptography algorithm comparison for security enhancement in wireless intusion detection system, "international journal of multidisciplinary research, vol .1 issues 4, august 2011.
3. Neeta settia,"Cryptanalysis of modern Cryptography Algorithms" .In IJCST.2010.
4. A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, 2006.
5. Schneier, B. (1996), "Applied Cryptography", Wiley & Sons, p.399.
6. Monika Agrawal "A Comparative Survey on Symmetric Key Encryption Techniques" In International Journal on Computer Science and Engineering (IJCSE) Vol.4 No. 05 May 2012.
7. Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "comparative analysis of cryptographic algorithms" International Journal of Advanced Engineering Technology "/ IV/III/July-Sept., 2013/16-18.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

8. Idrizi, Florim,Dalipi, Fisnik & Rustemi , Ejup. "Analyzing the speed of combined cryptographyic algorithms with secret and public key" .International Journal of Engineering Research and Development,e-ISSN: 2278-067X, p-ISSN: 2278-800X,www.ijerd.com Volume 8,Issue 2 (August 2013), pp.45
9. Prashanti.G, Deepthi .S & Sandhya Rai.K. "A Novel Approach for Data Encryption Standard Algorithm ". International Journal of Engineering and Advanced Technology (IJEAT) ISS: 2249-8958, Volume -2 Issue-5, June 2013, pp.264.
10. Vishwa Gupta, Gajendra Singh, Ravindra Gupta."Advance Cryptography algorithm for improving data security "International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X Volume 2, Issue 1,January 2012 .
11. Behrouz A. Forouzan Debdeep M ukhopadhyay ,cryptography and network security,2e, Mc Graw Hill Education (India) Private Limited.