ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015

Comparative Study of Cryptographic Algorithms

Ms.Ebeena Paul
MSc Computer Science
BPC College, Piravom, Kerala, India

Ms.Shelja Sadasivan
MSc Computer Science
BPC College, Piravom, Kerala, India

Ms. Ceena Paul
Asst Professor
Dept of Computer Science
BPC College, Piravom, Kerala, India

Abstract— **Internet has revolutionized many aspects of our daily lives. Nowadays Internet is used for millions of applications. Huge amount of data travels over the network. The security of data is an important aspect and encryption algorithms play an important role to provide the security to the wireless networks. The main aim of the cryptography is to enhance the data confidentiality and privacy by making the information unintelligible. Hence the data cannot be interrupted by the intruders. The Encryption techniques and various algorithms are used to provide the needed security to the applications .This paper provides a fair performance comparison between the various cryptography algorithms such as the AES, RSA, DES within few factors achieving an efficiency and security.**

Keywords— ***Cryptography, Encryption, Symmetric key encryption, Asymmetric key encryption, DES, AES, RSA.***.

I. INTRODUCTION

Use of Internet is growing rapidly. So, providing security to the data over networks has become a critical issue nowadays. Data over networks is insecure; it should be disclosed only to the intended recipients not to everyone. Data is more prone to attacks while transmitting in the network. Cryptography came into existence to provide solutions to all the issues of network security. Cryptography provides security to data while it is in network. Cryptography is a word with Greek origins, means "secret writing", and it is the science and art to transform the messages to make them secure and immune against security attacks. 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. The process to convert ordinary information or the plain text into unintelligible text or the cipher text in cryptography is called encryption.

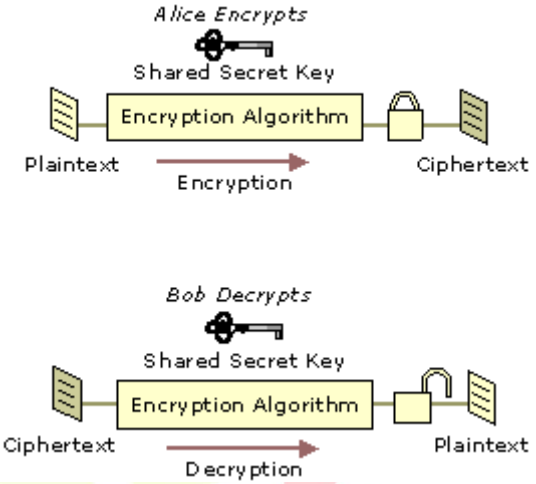


Fig.1. General Structure - Cryptography

The cipher text is understandable only to someone who knows how to decrypt it. The message or information is encrypted using an encryption algorithm. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm which usually requires a secret decryption key.

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

II. CLASSIFICATION

Cryptographic Algorithms can be classified into two Categories:

- Symmetric-key cryptographic algorithms
- Asymmetric key cryptographic algorithms

A. Symmetric-key cryptographic algorithms

Symmetric key algorithms are also known as private key algorithms. In symmetric key algorithms, encryption and decryption processes are performed using the same key.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015

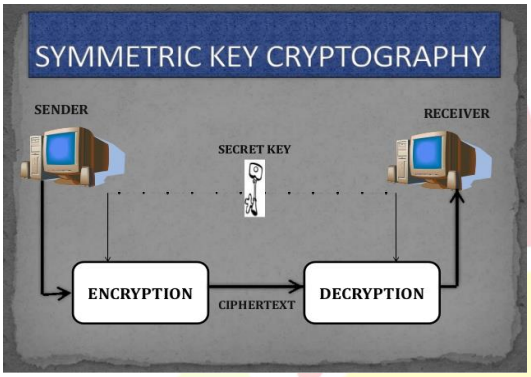


Fig.2. Symmetric Key - Cryptography

In private key algorithms, encryption and decryption keys are mathematically related (usually inverse of each other). Private Key algorithms are efficient and take less time to encrypt messages. These algorithms are used to encrypt and decrypt long messages because size of key is small [1]. It is generally categorized as being either stream ciphers or block ciphers. The ciphers of today are called round ciphers because they involve multiple rounds, where each round is a complex cipher made up of simple cipher. The main de-merits of Symmetric key cryptography are:

- Two parties must somehow exchange the key in a secure way.
- Public key is distributed in a non secure way.
- Easy for hacker to get the key as it is shared in unsecure way.

In symmetric key encryption different factors of the DES and AES algorithms are analyzed.

B. Asymmetric key cryptography algorithms

Public key algorithms are also known as asymmetric key algorithms. In asymmetric key algorithms two keys are used:

A private key and a public key. Public key is used for encryption and private key is used for decryption. The public key is announced to the public; whereas the private key is kept by the receiver.

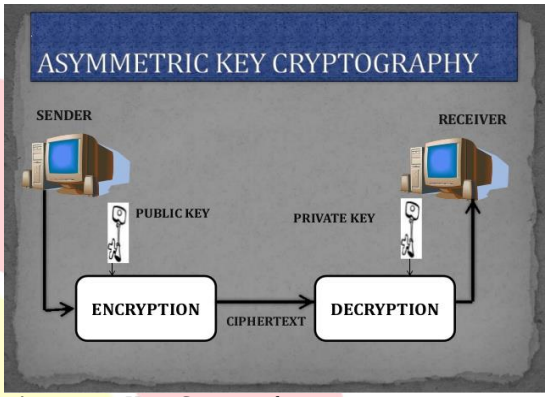


Fig.3. Asymmetric Key - Cryptography

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 this type of algorithms it is very difficult to derive one key from the other (means decryption key is very difficult to derive from the encryption key). The main de-merits of Asymmetric key cryptography are:

- Asymmetric encryption algorithms are comparatively complex.
- Time consuming process for encryption and decryption.

In asymmetric key encryption different factors of the RSA algorithm are analyzed

III. Overview Of Algorithms

Brief definitions of the most common cryptographic algorithms are given as follows:

A. Data Encryption Standard (Des) Algorithm

DES was designed by IBM in 1977 and is published by National Institute of Standards and Technology (NIST).It is a Private (symmetric) key cryptography algorithm. In DES, size of input block is 64 bits and key is 56 bits long. Same key is used for encryption and decryption. DES comprises various operations: mixing of bits, substitution, exclusive OR, S-boxes, straight permutation and expansion permutation [1]. Generally, the encryption process of DES is done in 16 rounds.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015

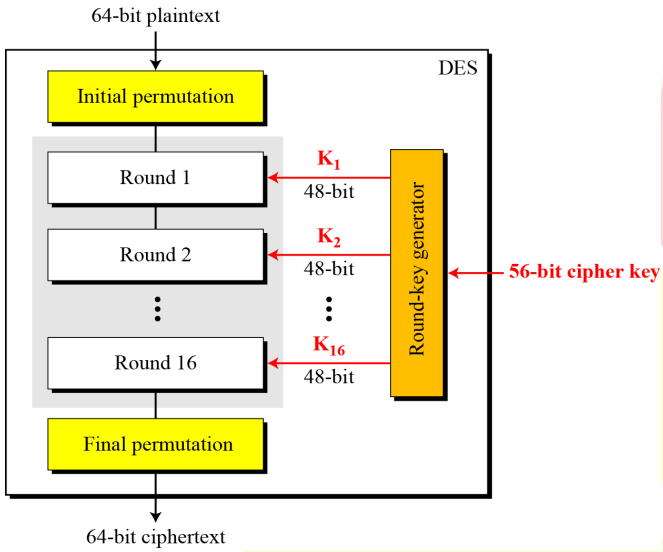


Fig.4 General Structure of DES

DES has two transposition blocks (P-boxes) and 16 complex round ciphers. The 16 iteration round ciphers are conceptually same and each uses a different key derived from the original key. The initial and final permutations are keyless straight permutations that are inverses of each other. The permutation takes a 64 bit input and permutes them according to pre defined values. Each round of DES is a complex round cipher, as shown below:

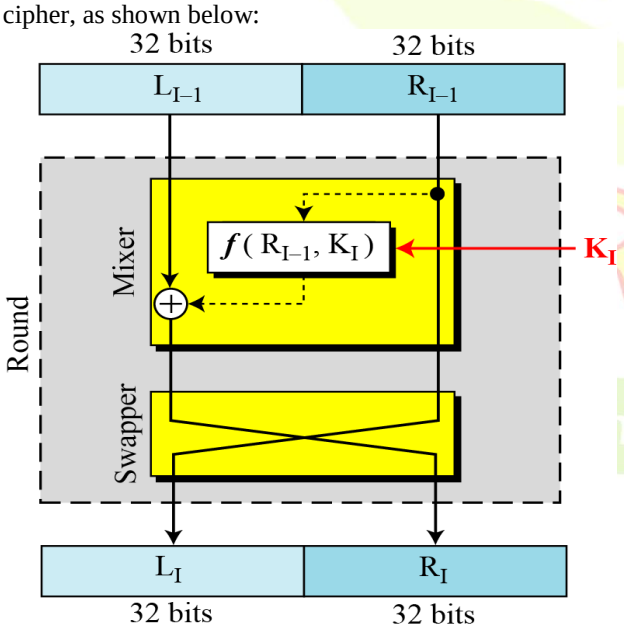


Fig.5 A round in DES (Encryption site)

The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output. This function is made up of 4 operations:

- An XOR function
- An expansion permutation
- A group of s-boxes
- A straight permutation as shown below.

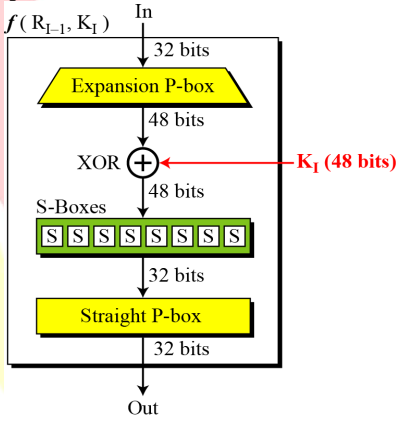


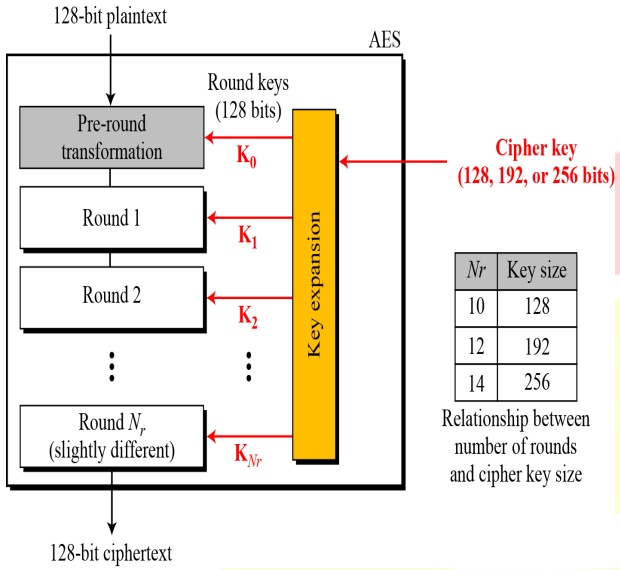
Fig.6 The DES function

DES is one of the most widely used types of cryptographic algorithm which provide confidentiality services.

B. Advanced Encryption Standard (AES) Algorithm

The US national Institute of Standards and Technology (NIST) indicated that DES encryption algorithm should only be used for legacy systems..With the modern technology and new encryption algorithms being developed, one problem restricting DES to be used widely is the slow process of encryption and decryption. In fact, 3DES is even three times slower than DES. Another drawback of thesewas the small block size of 64 bits,which is not secure any more. All these issues led NIST to call for proposals for a new Advanced Encryption Standard in 1997 [2]. General design of AES Encryption cipher is given below.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015



Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

Fig.7 General structure of AES

AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical. Generally, the working progress of AES can be divided into four main functions: Substitute Byte transformation, Shift Rows transformation, Mix Columns transformation and Add Round Key transformation. It contains 10 rounds of encryption iterations. The following is a brief explanation of AES encryption process: Then, the steps taken to encrypt are as follows:

1. Substitute Byte transformation: AES contains 128 bit data block, which means each of the data blocks has 16 bytes. In sub-byte transformation, each byte (8-bit) of a data block is transformed into another block using an 8-bit substitution box which is known as Rijndael Sbox.

2. Shift Rows transformation: It is a simple byte transposition, the bytes in the last three rows of the state,depending upon the row location, are cyclically shifted. For 2nd row, 1 byte circular left shift is performed. For the 3rd and 4th row 2-byte and 3-byte left circular left shifts are performed respectively.

3. Mix columns transformation: This round is equivalent to a matrix multiplication of each Column of the states. A fix matrix is multiplied to each column vector. In this operation the bytes are taken as polynomials rather than numbers.

4. Addroundkey transformations: It is a bitwise XOR between the 128 bits of present state and 128 bits of the round key. This transformation is its own inverse.

These steps are repeated for 10 rounds (in 128 bits),and some minor functions will generate the encrypted text. The decryption algorithm is just the reversed steps of the above process.

C. RSA (RIVEST, SHAMIR, ADLEMAN) ALGORITHM

RSA is most widely used public –key algorithm. It provides secrecy and digital signature both. This algorithm is developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It uses the prime numbers to generate public and private keys based on mathematical calculations and multiplying large numbers together. Steps involved in RSA algorithm are generation of public and private keys, Encryption Process, Decryption Process:

Choose any two prime numbers say p & q. (p & q cannot be divided by any other number except 1 and itself). Calculate n, n = p x q. Calculate another number Ø also known as Euler's totient function. Value of Ø= (p-1) x (q-1). Now assume a number e such that d x e = 1 (mod Ø). The value of e should lie between 1 and Ø. Number e should be a prime number. Number e and Ø should be co-prime means e and Ø are not divisible by any other number except 1 or in other words g.c.d. of e and Ø should be 1. Now calculate the value of d by using extended Euclidean algorithm's table method. After calculating the value of d, public keys (e and n) are announced to the public and private keys (d and Ø) are kept secret.

Encryption process:

Now anyone can send a message by using public keys (e and n). Plain text (Original message) is converted into Cipher text (scrambled message) by using the following formula:

$$C = P^e \pmod{n} \qquad .(1)$$

Decryption process:

Cipher text is converted into Plain text by using private key d. Cipher text (scrambled message) is converted into Plain text (original message) by using the following formula:

$$P = C^d \pmod{n} \qquad (2)$$

Restrictions:

For RSA to work , the value of P must be less than the value of n. If P is a large number, the plaintext needs to be divided into blocks to make P less than n.

IV. THEORETICAL ANALYSIS

TABLE 1. Comparison of Algorithm

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue IV, December 2015 in association with BPC COLLEGE PIRAVOM
National Conference on Recent Trends in Data Mining (NCRTID-2015) - 10th & 11th December 2015

Factors	DES	AES	RSA
Abbreviation	Data Encryption Standard	Advanced Encryption Standard	Rivest-Shamir-Adleman
Developed	1977	2000	1977
Key used	Same key for encryption and deccryption	Same key for encryption and deccryption	Different key for encryption and deccryption
Algorithm	Symmetric	Symmetric	Asymmetric
Key length	56 bits	128,192 or 256 bits	Depends on number of bits in the modulus n where n=p*q
Speed	Slow	Fast	Slowest
Cipher type	Symmetric block cipher	Symmetric block cipher	Asymmetric block cipher
Tunability	No	No	Yes
Power consumption	Low	Low	High
Security	No secure enough	Excellent security	Least secure
Cost	Costly	Cheaper	costly
Implementation	Complex	Simple	complex
Encryption ratio	High	High	High
Rounds	16 rounds	10- 128 bit key, 12 – 192 bit key, 14 – 256 bit key	
Block size	64 bits	128 bits	variable

V. CONCLUSION

This paper presents a detailed study of the popular Encryption Algorithms such as RSA, DES and AES. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used. In this paper, a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which might be suitable for different applications and has its own advantages and disadvantages. According to our study it can be found that AES algorithm is most efficient in terms of speed, power consumption, security, cost etc.

References

[1] Priti Bali, "Comparative study of private and public key cryptography algorithms: a survey", International Journal of Research in Engineering and Technology

[2] Ali Makhmali, Hajar Mat Jani," Comparative Study On Encryption Algorithms And Proposing A Data Management Structure" international journal of scientific & technology research

[3] Behrouz Forouzan, "Cryptography and network security"

[4] Gurpreet Singh , Supriya "A Study of Encryption algorithm(RSA, DES , 3DES and AES) for Information Security" ,International Journal of Computer Applications

[5] AL .Jeeva, Dr .V. Palanisamy, K. Kanagaram ," Comparitive analysis of performance efficiency and security measures of some Encryption algorithms" International Journal of Engineering Research and Applications

[6] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh, " Comparative analysis of cryptographic algorithms" , International Journal of Advanced Engineering Technology

[7] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors ",Journal of computing.