Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 6, June 2017, pg.377 – 383

CRYPTOGRAPHY: THE SCIENCE OF SECURITY

Zaira Nazir[1], Snober Shahzadi[2], Miss. Taha[3]
Department of Computer Science, SSM College of Engineering and Technology Parihaspora Pattan Kashmir

ABSTRACT: Cryptography is where security engineering meets mathematics. Cryptography has often been used to protect the wrong things or used to protect them in the wrong way. Network and internet applications is becoming very popular. Security is the most challenging aspect in the internet and network applications. It can be provided by a technique called cryptography. It involves encryption and decryption of messages. Encryption means converting a plain text into cipher text and decryption means getting back the original message from the encrypted text. In addition to confidentiality cryptography also provides Authentication, Integrity and Non-repudiation. The beauty of cryptography lies in the key involved and the privacy of the keys used to encrypt or decrypt. Cryptography is a developing technology, which is important for network security. Currently, the range of cryptography applications have been expanded after the development of communication. Work in the field of cryptography is still in developing stages and a considerable research effort is still required for secured communication. This paper discusses about the state of the art for a various cryptographic algorithms that are used in networking applications.

KEYWORDS: Asymmetric encryption, cryptography, Network security, symmetric encryption

I. INTRODUCTION

In 1970s cryptography was primarily based on securing communication using a shared secret key. This key was helpful in both encrypting and decrypting communications. This type of encryption is called "symmetric" because the same key is used to encrypt and decrypt. Symmetric encryption is still used widely today. As computers grew in popularity and our reliance on secure communications became more and more necessary for everyday life, experts began to see a significant issue with symmetric encryption. Fortunately in 1977 a new era of viable cryptography was introduced what we know as public key cryptography. In public key cryptography two keys are used a private key and public key. Everybody in the world can get a copy of the public key, but only the user has a copy of his/her private key. It is only possible

due to private key that we can decrypt the encrypted message. Cryptographic algorithms play a major role for data user security. Since the complexity of algorithm there is high the risk of breaking the original plain text from that of cipher text .Greater complexity means greater security. Encryption is the process of encoding plain text into cipher text (secure data).Decryption is the revoking of the encryption process by which cipher text is converted to plain text.

II. LITERATURE SURVEY

The various methods for cryptography are as under.

A. Cryptography

1. Plain Text: It is the original form data that a sender wants to send to the receiver. It is an original understandable message that is input to the algorithm.

2.Ciphertext: Ciphertext is the scrambled content or message in its coded human unreadable form. The ciphertext is the output of encryption process and input of **decryption** process . If two different keys used for encryption of a message, then two different ciphertexts are produced.

3. Encryption Algorithm: It performs different techniques such as substitution and transformation on the plaintext to obtain ciphertext.

4.Decryption Algorithm: It is the exactly opposite procedure of encryption technique. To obtain original plaintext it uses ciphertext and secret key.

5:Secret Key: The secret key is input to an encryption process. The key value is independent of plaintext and algorithm. Depending on the key being used, the algorithm gives various output. The exact operation performed on that algorithm depend on the key.

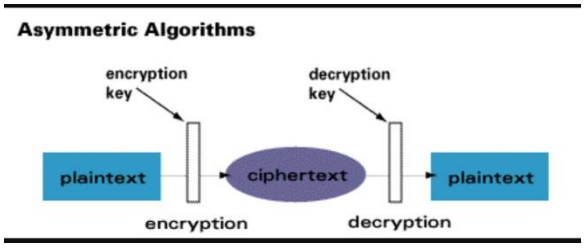

Figure1 (Asymmetric Algorithms)

B. Based on the key, cryptosystems can be classified into two categories:

Symmetric and Asymmetric: In Symmetric Key Cryptosystems, we use the same key for both Encryption as well as the corresponding decryption. i.e. suppose K is the key and M is the message, then DK(EK(M)) = M

Asymmetric or Public key or shared key cryptosystems use two different keys. One is used for encryption while the other key is used for decryption. The two keys can be used interchangeably. One of the keys is made public (shared) while the other key is kept a secret. i.e. let k1 and k2 be public and private keys respectively. Let M be the message, then Dk2(Ek1(M)) = Dk1(Ek2(M)) = M

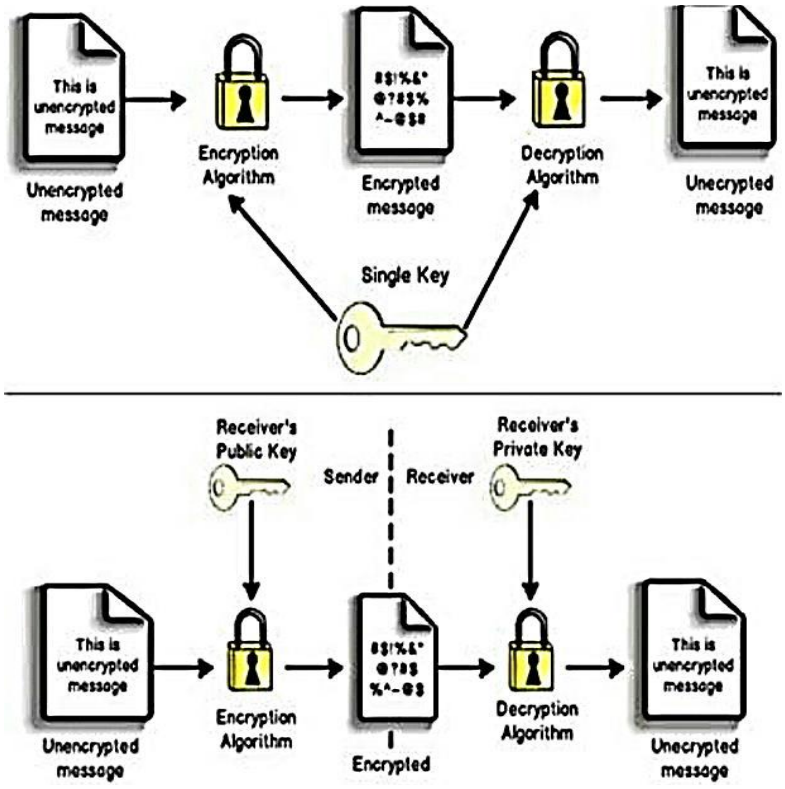

Figure2 (Symmetric key Cryptography and Asymmetric key Cryptography)

In general, symmetric key cryptosystems are preferred over public key systems due to the following factors:

1. Ease of computation

2. Smaller key length providing the same amount of security as compared to a larger key in Public key systems.

Hence the common method adopted is to use a public key system to securely transmit a "secret key". Once we have securely exchanged the Key, we then use this key for encryption and decryption using a Symmetric Key algorithm.

III.OBJECTIVES

Cryptography encounters following objectives.

1) Confidentiality : The information cannot be understood by anyone for whom it was not concerned. It remains private.

2) Integrity : The information cannot be modified in storage or transit between sender and intended receiver without the change being detected.

3) Non-repudiation : The creator/sender of the message cannot deny at a later stage his or her intentions in the creation or transmission of the message.

4) Authentication : The sender and receiver can acknowledge each others identity and the original destination of the information .

IV. TECHNIQUES USED

A. DES

The Data Encryption Standard (DES) is popular encryption technique and used by a large number of persons. The DES is block cipher technique in which it uses the same key for to encode and decode. The Block size and Key size DES is 64-bits and 56-bits respectively. It consists of 16 identical stages (Rounds), Initial Permutation (IP) and Final Permutation (FP). The DES consist of following steps:

STEP1. In the first step 64-bit, the plaintext is given as input to the IP and IP is performed on plaintext and to obtain the Permuted Input it rearranges the bits.

STEP2. The second step includes of 16-rounds of the same function, and it also contains permutation and substitution methods.

STEP3. The last round (sixteenth) output contains 64-bits, and they are a function of input plaintext and key

STEP4. Swap the output of left and right side, then preout is produced.

STEP5. At that point preout is gone through IP i.e. opposite **of** IP to create 64-bit ciphertext.

B. AES

It is a symmetric block cipher developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen in 1998.The AES stands for Advanced Encryption Standard and based on design method called as a substitution permutation network. The AES-128, AES-192, and AES-256 block ciphers are included in it. Every cipher encodes and decodes information in the block of 128-bits utilizing cryptographic keys of 128-bits, 192-bits, and 256-bits respectively.

The AES is a symmetric cipher and it uses the identical key to perform encryption and decryption on message. For 10 rounds, 12 rounds and 14 rounds AES use 128-bits, 192-bits and 256-bits keys are used respectively.

C. Blowfish

It is a designed by Bruce Schneier in 1993. It is symmetric block cipher technique. Its block size is 64-bit, and key length is variable. Its variable key length ranges from 32-bits to 448-bits. It is one of the fastest technique which has developed up to date [4]. This algorithm is unpatented and placed in the public domain due to which it can be used freely by anyone. Blowfish algorithm has two parts Key Expansion and Data Encryption. The keys involved for Blowfish calculation is 448 bits. Therfore, it requires 2448 combinations to look at all keys.

D. RSA

This algorithm was developed at MIT in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA). It is public key cryptosystem used for secure data transmission. This algorithm makes use of two keys, first to encrypt second to decrypt. The public key used for encryption of messages and decrypted by using the private key. In this method, any one key is kept secret. The following steps are performed to obtain the keys for RSA algorithm:

STEP1. Select two large prime numbers a and b.

STEP2. Calculate n=a*b; where n is modulus for both keys.

STEP3. Select e (public key) such that it is not a factor of (a-1) (b-1).

STEP4. Calculate d (private key) such that:

d*e mod (a-1) (b-1)=1.

STEP5. For encryption, calculate the ciphertext C from plaintext M as C= Me mod n.

STEP6. For decryption, calculate the plaintext M from the ciphertext C as M= Cd mod n

V. ADVANTAGES

A.DES

Advantages:

a) DES was introduced long time ago in 1977, so no real weakness was found.

b) A DES is similar to that of an ANSI and ISO standard so anybody can learn and execute it.

B.AES

Advantages:

a) This method is more secure as compared to other techniques.

b) It supports larger key size than DES and TDES.

C. Blowfish

Advantages:

a) It is symmetric block cipher and used as an option for DES

b) As it uses variable length key from 32-bits to 448-bits making it suitable for both residential and exportable use.

c) It was released in 1993 so the Blowfish code is not cracked up till now.

d) It has faster performance than other encryption algorithms.

D. RSA

Advantages:

a) The Public Key encryption and increased security is major advantage of RSA algorithm.

b) As it uses two keys, then public key is used for encryption and private key for decryption.

c) In RSA algorithm, the private keys are never transmitted nor revealed.

d) It gives a method for digital signature and that cannot repudiate.

From the above discussion, Blowfish algorithm is better than other algorithms regarding processing time

VI. CONCLUSIONS

In this wireless world nowadays the security of information is a more critical viewpoint. This paper shows the performance analysis of DES, 3DES, AES and Blowfish algorithms and above results demonstrate that

1. Blowfish algorithm has higher performance regarding encryption time and decryption time.

2. DES is less efficient as compared to other algorithms.

In Future work, our motive is to improve throughput and speed by using encryption and decryption methods. It can take low processing time and low power consumption. We will concentrate on the picture, sound and video for creating more grounded encryption algorithm with rapid, throughput, and less energy & less power consumption.

REFERENCES

[1] A William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] AtulKahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008.

[3] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha "Performance Evaluation of Symmetric Cryptography Algorithms," International Journal of Electronics and Communication Technology Volume 2 Issue 3, September 2011.7

[4] Pratap Chandra Mandal "Superiority of Blowfish Algorithm," International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.

[5] Mitali, Vijay Kumar and Arvind Sharma "A Survey on Various Cryptography Technique", International Journal of Emerging Trends & Technology in Computer Science, Volume 3, Issue 4, July-August 2014

[6] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[7] R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978.

[8] 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, Vol 2, Issue 7, July 2012.

[9] Monika Agrawal, Pradeep Mishra," A Comparative Survey of Symmetric Key Encryption Techniques," International Journal of Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

