International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Cryptography Algorithms and Attacks

T.Ramya[1], Dr.V.V.Rama prasad[2]

[1]Scholar(M.tech),Dept.of CS,Sree vidyanikethan Enginnering College,A.P,INDIA
[2]Professor,Dept of CSE,Sree Vidyanikethan Engineering College,A.P,INDIA

ABSTRACT— In the modern period evaluation of wireless networks and networking has come in information and communication technology, there are so many things that gives facility to deal with these technologies by using internet. The important role to provide a security to the network is the main aspect of internet is email security and cryptography plays a major role to provide security to the network communication. Most email system adopt Public Key Infrastructure (PKI) as the mechanism to implement security and efficiency. The public key infrastructure based systems suffers from problems in scalability and expensive certificate management. The awareness of email security and its requirement to the common computer users is the is the main objective of this approach. For achieving secure communication a number of cryptographic techniques are developed. The proposed mailing system is secure against standard security model.

Keywords—Security Services, Cryptography, Encryption, Decryption, DES, AES, Blowfish, RSA.

1.INTRODUCTION

1.1. Information Security

Information Security Means protection of information ,it is protect the system data from those with spiteful intention. By using security services like Confidentiality, availability ,integrity protect the system data. The data can be thought of as benefit and like every other benefit, this data secured from third persons(or)attacks. To be ,Secured information need to be hide from unauthorized access(confidentiality),secured from third parties change(integrity),and available to authorized entry when it is needed(availability).the integrity, availability, confidentiality these are the most important security goals.

1.2. Security

Security defines protection against malicious attack by third parties. There are more attacks or threads from inside source. Security also involves Controlling the effects of mistakes and failures. The data that can protect or secured against an attack or failure will probably prevent random misfortunes, too.

1.3. Security Services

These are the security services described below

a) Authentication
b) Access control
c) Data confidentiality
d) Data integrity
e) Availability

a) Authentication: Authentication process help to establish proof of identities. This process ensures that the base of the messages or information is correctly identified.

b) Access Control: It specifies and controls who can access the process or information.

c) Data Confidentiality: Confidentiality defines the protection of information from third parties.

d) Data Integrity: The integrity technique ensures that the information remains the same when the destination reached as sent by the sender.

e) Availability: The Availability defines the resources should be available to authorized parties in every time.

1.4. Cryptography

Information Security is a secure communication of data or information become very important in information and transmission technology. To stop this, it is recommend to encrypt the data to provide information security. This type of protection is using in cryptography. The classifications of cryptography shown in fig.1

i. Plaintext:

Any communication is one type of language that we use in the human language, it takes the form of plain text. It is understand by the sender and the recipient and also anyone who get an access to that data.

ii. *Ciphetext:*

Cipher means a code or confidential message. When a plaintext is modified using any suitable technique

the result data is called as ciphertext. The plaintext is modified by unreadable format by using any suitable technique the result data is called as ciphertext.

iii. ***Key:***

An important facet of performing encryption and decryption is the key. The key used for encryption and decryption that generate the process of cryptography secure.

The process of converting from plaintext to ciphertext is called as **'encryption';**converting plaintext from ciphertext is called **'decryption'.** The many techniques used for encryption to establish the area of study knows as **cryptography.**

Cryptography Systems are divided into three independent dimensions:

a. The operations used for exchange plaintext to cipher text.

All encryption techniques are based on two principles: Change, an each element in the plaintext(bit, letter, group of letters)is mapped into another element or group and exchange ,in the plaintext all elements are rearranged.

b. The number of keys used.

The same keys is used in sender and receiver ,it is referred as secret key. If the sender and receiver use the contrary keys, it is referred as public key encryption.

c. The way in which the plaintext is processed.

Block cipher is processes the one block of input elements, at a time it generate an output block for each input block.

Stream cipher continuously processes the input elements, it produce at a time output one element.

1.5 Certificate less Public Key Cryptography

The Al-Riyami and Paterson [13] in 2003, introduce the concept of certificate less public key cryptography(CL-PKC),by using these concept to overcome the key escrow problem of Identity Based Cryptography. In CL-PKC, a trusted third party, called the Key Generation Center (KGC),supplies a user with partial private key. While compared to identity based public key cryptography (IDPKC),in this concept significantly reduce the trust

assumptions regarding the trusted third party .There placement of a public key of a user in the system by the KGC is equivalent to certificate by PKI system.

1.6.Types of Cryptography

a. Secret Key Cryptography:

In an encryption and decryption same keys is used, the technique is known as secret key cryptography.

b. Public Key Cryptography:

In an encryption and decryption two contrary keys are used, the technique is known as public key cryptography. The types of cryptography is shown in fig.2.

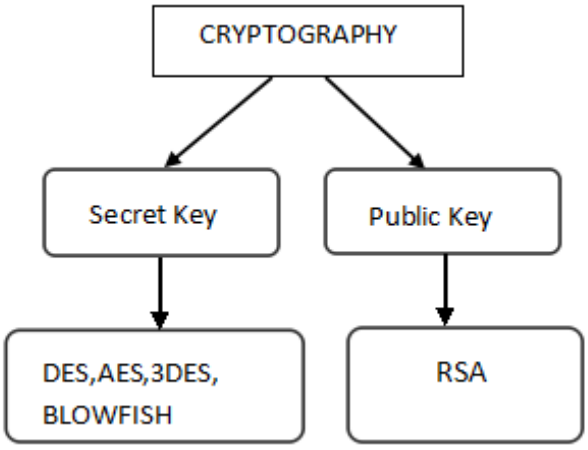

Fig:1 Classification of Cryptography

2. RELATED WORK

2.1. Symmetric and Asymmetric Cryptography

In symmetric cryptography (e.g., Data Encryption Standard (DES), Advanced Encryption Standard (AES)similar keys (i.e., $K1 = K2 = K$) is used in encryption ($C = EK(P)$) and decryption algorithm ($P = DK(C)$).

In asymmetric cryptography (e.g., Rivest -Shamir-Adleman (RSA) algorithm)two contrary keys are used (i.e., $K1 = K2$), the public key is used to encrypt a message ($C = EK1(P)$),and secret key is used to decrypt the cipher text into plain text ($P = DK2(C)$).

a). Symmetric Cryptography

In symmetric cryptography (e.g., Data Encryption Standard (DES),Advanced Encryption Standard (AES) similar keys (i.e., $K1 = K2 = K$) is used in encryption ($C = EK(P)$) and decryption algorithm ($P = DK(C)$) [1].

i).Data Encryption Standard (DES)

The most extensively used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Institute of Standards and Technology (NIST).

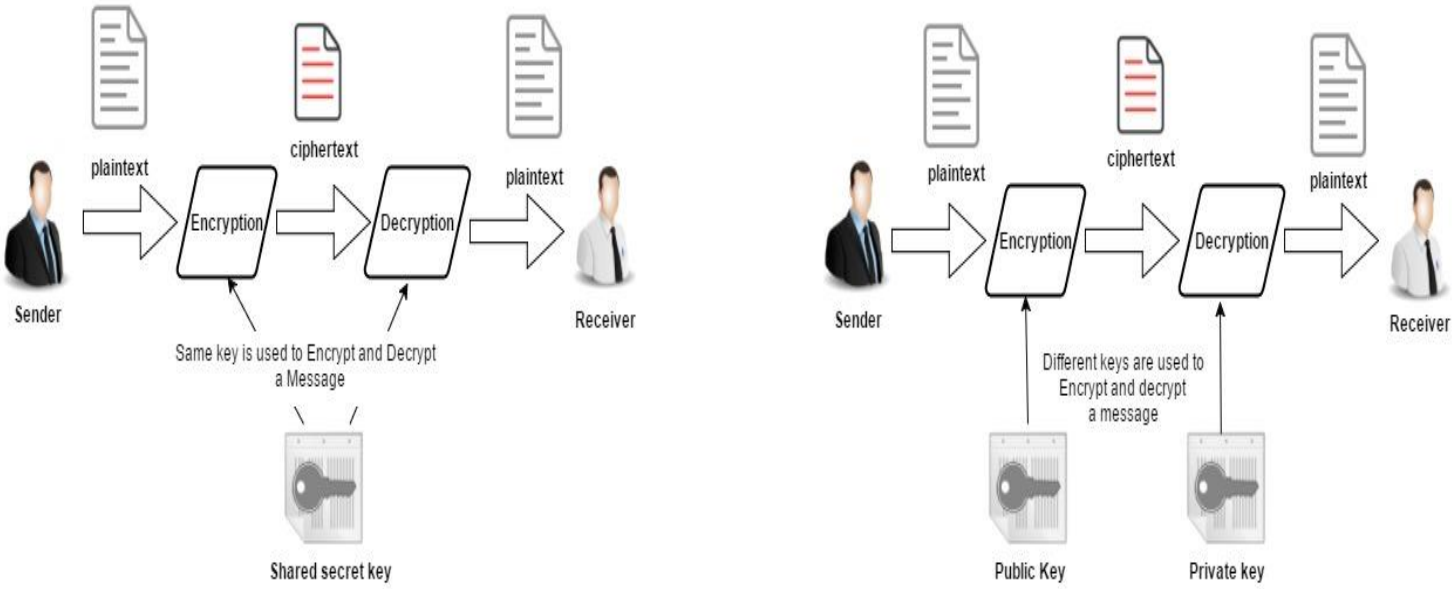

Fig.2: Secret key Cryptography and Public Key Cryptography

The algorithm itself is notice to as the Data Encryption Algorithm (DEA). For DES algorithm as explained by Davis R [12] , data are encrypted by using 56-bit key in 64-bit blocks .The algorithms transpose 64-bit input in a series of steps into a 64-bit output .The same steps, with the same key, are used to reverse the encryption.

The important two components that built up DES are:

- **Triple-DES (3DES):**A diversity of DES it makes three encryption/decryption passes over the block ,the DES uses the three 56-bit key.
- **DESX:** The Ron Rivest is invent by DESX, In an encryption by mixing 64 additional key bits to the plaintext ,increases the key length up to 120 bits.

ii).Blowfish

The one of the most known public domain encryption algorithm is Blowfish[2] is devised by Bruce Schneier , he is one of the most world leading cryptologists and the president of counterpane systems. The blowfish algorithm was first introduce in 1993.

The Blowfish technique encrypts 64-bit block cipher with verity length key and its contains two parts.

- **Data Encryption:** The data encryption involves a simple function of 16 times iterations .In an each round have key dependent permutation and data dependent substitution.
- **Sub key Generation:** The sub key generation convert the key up to 448 bits long to4168bits.

iii) *.Advanced Encryption Standard (AES)*

The Advanced encryption standard in 2001 was published by the National Institute of Standards and Technology(NIST).The Standard for wide range of application DES is approved. AES[3]is a symmetric block cipher that is deliberate to compensate to replace DES. Distinguish to public key cipher such as RSA, The AES[11] and most symmetric ciphers is quite complex and it is not easily explained as many other cryptographic algorithm.

b).Asymmetric Cryptography

In asymmetric cryptography two contrary keys are used (i.e., $K1 = K2$), the public key is used to encrypt a message ($C = EK1\ (P)$),and secret key is used to decrypt the cipher text into plain text ($P = DK2\ (C)$).

i).Rivest -Shamir-Adleman(RSA)

Two distinct keys(i.e.,K1=K2), used in symmetric cryptography(e.g.,Rivest-Shamir-Adelman (RSA)) algorithm , one key is public key is utilized to encrypt a message($C = EK1\ (P)$),and another key is private key is used to decrypt the ciphertext into plaintext ($P = DK2\ (C)$) .

The new technique is introduce in cryptography by the Diffie and Hellman and effect challenged cryptologist to come up with cryptographic algorithm that meet public key systems Requirement.

Table.1. Cryptography Algorithms_ A Comparison

Algorithm	Created By	Key Size	Block Size(in bits)
DES	IBM in the year 1975	56	64
3DES	IBM in the year 1978	112 (or) 168	64
AES	Joan Daemen and Vincent	256	128
Blow Fish	Bruce Schneier	32 (or) 448	64

2.2.Comparison of Cryptography Algorithms

The comparison of various cryptographic technique provided by Gurujeevan Singh, et al. [4]. A comparative survey on secret key encryption technique done by Monika Agrawal and Pradeep Mishra[7].Survey on most encryption techniques have done by E. Thambiraja et al. [6].The comparison of cryptography algorithm shown in Table 1.

3.TYPES OF ATTACK

3.1. Security Threats

The network security have number of security threats. The denial of service, distributed denial of service, viruses, Trojan horses, spy wares, malwares [8], illegal way in to the network property and data, accidental erasure of the records and the uncontrolled internet access these are the most security threats.

3.2. Virus assault

A program or an executable code is a computer virus, the executable code can executed and computer generated upon different undesirable and damaging functions for a systems and network. Virus is how to destroy your hard disk and processor ,use large scale at memory and over all performances can wipe out of a system and network.

A Trojan performs the complex actions but it cannot be replicated, it is capable of erasing all the important record. The computer worm is program ,it duplicate to all network and erase most important information. If you have a modernized antivirus program controlled the viruses, malware, adware and Trojan horses. The antivirus program with most up to date pattern files.

3.3.Unauthorized Access

An authorized person should be allowed to the network resources and records. only the sanctioned person(or) authorized person must have been accessed the resources and common folders in your network supposed to be scanned and monitored repeatedly.

3.4.Data stealing and cryptography attacks

If you have good encryption method loss can be prohibited in the network, i.e., encryption method use 128 bit security or 256 bit security encryption technique. In this manner the information when transferred during FTP protocol can be encrypted cannot be read.

3.5. Unauthorized application installations

In all servers and clients computers install only the certified software application to prevent the virus and security threats. The songs or video programs, gaming software or additional internet based applications no one should allow to install which can be source of security threat.

3.6.Application-Level Attacks

The attacker exploits the limitations in the application -example security restrictions in the web server. Examples malicious software attack [10] (viruses, Trojans, etc.), internet server attacks, and SQL injection .

4.CONCLUSION

This paper gives a detailed study of Cryptography Techniques or algorithms like AES, DES, 3DES, Blowfish, RSA. For selling and buying of products over the open network the data become most important, to provide security we use encryption algorithms and concepts. In this paper evaluated performances of symmetric algorithms. The AES ,DES ,Blowfish,RSA,3DES these are

the algorithms. The Blowfish has the better performing than other algorithms. In future we can use encryption techniques in such a way that it can consume less time and power of furthermore and high speed and minimum energy consumption.

REFERENCES

[1] W Stallings, "Cryptography and Network Security: Principles and Practice,"5th ed.,(Prentice Hall, 2010).

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

[3] Advance Encryption Standard (AES), Federal Information Processing Standards Publication 197. (United States National Institute of Standards and Technology (NIST), November 26, 2001).

[4] Gurjeevan Singh, Ashwani Kumar Singla and K.S. Sandha "Performance Evaluation of Symmetric Cryptographic Algorithms," International Journal of Electronics and Communication Technology ,Vol 2 Issue 3, Sep 2011.

[5] R.L.Rivest, A.Shamir and L.Adleman, "A Method for obtaining Digital Signatures and Public-Key Cryptosystem," Communication of the ACM, Vol No 21, Feb 1978.

[6] E.Thmbiraja, G.Ramesh and Dr.R.Umarani, "A Survey on Various Most Common Encryption Techniques," International Journal of Advanced Research in Computer Science and Software Engineering, Vol No.2, Issue 7, July 2012.

[7] Monika Agrawal, Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques," International Journal on Computer Science and Engineering (IJCSE), Vol No.4 ,May 2012.

[8] Siddharth Ghansela, Network Security: Attacks, Tools and Techniques, www.ijarcsse.com, Volume 3, Issue 6, June 2013.

[9] A. Joseph Amalraj, Dr. J. John Raybin Jose, "A Survey Paper On Cryptography Techniques," International Journal of Computer Science and Mobile Computing, Vol. No 5, Issue. 8, pp.55 – 59,August 2016.

[10] Rajesh R Mane,"A Review on Cryptography Algorithms, Attacks and Encryption Tools,"International Journal of Innovative Research in Computer and Communication Engineering,Vol.No.3, Issue 9, September 2015.

[11] Daemen.J and Rijmen, "The Advanced Encryption Standard," Dr. Dobb's Journal, Vol 26 Issue 3, pp. 165-188 ,July 2002.

[12] Davis.R, "The Data Encryption Standard in Perspective," Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978 .

[13] A. R. Sattam and P. Kenneth, "Certificateless public key cryptography a full version,",in Asiacrypt'03, LNCS 2894, Springer, 20,p.p. 452-473, 2003.