International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

A STUDY ON SYMMETRIC AND ASYMMETRIC KEY ENCRYPTION ALGORITHMS

S.Suguna[1], Dr.V.Dhanakoti[2],R. Manjupriya[3]

[1]*PG Scholar, Department of CSE, Valliammai Engineering College, Tamil Nadu, INDIA.*

[2]*Associate Professor, Department of CSE, Valliammai Engineering College, Tamil Nadu, INDIA.*

[3]*PG Scholar, Department of CSE, Valliammai Engineering College, Tamil Nadu, INDIA.*

Abstract- *Security plays a major role in internet and network application. Nowadays, internet and network application are emerging very rapidly. Today, the significant and the worth of the Transmitting or exchanging information over the internet or other communication medium are enlarging. Information Security plays a major role in the aspect of data transformation. The best way to give the security for our information is cryptography. Cryptography is the one, which plays a important role in computer security that translate the information from its original form in to an incomprehensible or unreadable form by using encryption and decryption techniques. The cryptography certifies that the information should be transmitted without any modification and only the official person can be able to uncover and read the information. There are large amount of cryptographic techniques are emerging to obtain secure communication. Fundamentally, there are two types of cryptographic techniques Symmetric and Asymmetric. The most secret data being transfer over electrical cable is very sensitive, that can be accessed for malignant purpose. The formal method of encryption can only maintain the information protection. Presently many cryptographic techniques have been found to improve the data protection effectively. So it is more significant to apply powerful encryption techniques to improve the information protection. This paper mainly focus on the different kinds of encryption techniques, the keywords are: cryptography, encryption, decryption, AES, DES, Triple DES , Blowfish, RC4, RSA ,ELGAMMAL ,Diffie – Hellman, Digital signatures.*

Keywords: - *AES, DES, Triple DES, Blowfish, RC4, RSA, ELGAMMAL, Diffie – Hellman, Digital signatures.*

1. INTRODUCTION CRYPTOGRAPHY

It is the art of secret writing [1]. Cryptography is the creativity of translating the original plain text in to cipher text. The sender translate the plaintext in to cipher text .This cipher text is then sends to the receiver. The authorized receiver gets the cipher text and then convert the cipher text back in to the original form. The main aim of the cryptography is to protect the information from illegal access. The data can be read in its original form is called plain text. The way of mask the plain text in such a way as to hide its original form is called encryption. The method of encrypting the plain text which results in unreadable form is called cipher text. The method of taking encrypted message or data and converting back into the text in to its original form is called decryption. An entity which provides encryption and decryption is called cryptosystems. [1]. Cryptography plays a vital role in security aspect. It provides many security goals to make sure the secrecy of data. Cryptography provides many advantages so it is widely used nowadays.

Cryptography is the art of sending the information in a protective way .And ensuring that the legitimate person can able to access the information. Because of the efficient usage of networking we can transmit the information from one location to another location over the internet.

For the secure communication we can hide the original information in to an unreadable form so that trespassers cannot able to read the information. Cryptography is mainly used for network security. The cryptography is an art of covering or hiding the data by encrypting the message or data by using algorithms. The encryption and decryption process is done by cryptography. By using keys the original message is converted in to cipher text it is called encryption process. The cipher text is converted back in to its original form by using keys is called decryption. Cryptography is categorized in to two techniques: Symmetric and asymmetric. In modern era, cryptography mainly deals in computer security and engineering [2].The encrypted form of plain text by using an algorithm is called as encryption algorithm. The decrypted form of cipher text by using an algorithm which is called decryption algorithm [2]. The key is used for both encryption and decryption process .By the time of encryption and decryption process, the security level at cryptography is identified by the size of key (key space).This paper contains some of the encryption and decryption techniques and security issues.

2. FOLLOWING ARE THE VARIOUS GOALS OF CRYPTOGRAPHY

A. Confidentiality

Data that resides in computer is transmitted and that is to be accessed only by the legal person and that data can't be accessed by anyone else.

B. Authentication

The data that is seen by any system has to check the identity of the sender, whether the data is appear from a legal person or illegal person.

C. Data Integrity

To verify the information has not been changed by illegal or unknown person. Only the sender and receiver can modify the message. No others have the rights to access the message (or) Data.

D. Non-Repudiation

It does not allow repudiation by the sender or receiver. The receiver proves the identification of the sender in case of denial by the sender. The sender proves the identification of the receiver in case of denial by the receiver.

E. Access Control:

It is ensure that only the authorized person can have the rights to access the transmitted information.

3. BASIC TERMINOLOGY USED IN CRYPTOGRAPHY

A. Plain Text

The data is in the original form is called plaintext. The sender sends the plaintext to the receiver. At the time of encryption process this plaintext is taken as input. Example: Seetha wants to send the message "How are you" to Priya. Then the message "How are you" is called plaintext.

B. Cipher Text

The data is in an understandable form is called cipher text. At the time of encryption process the plain text is converted into cipher text. The cipher text is can't be understand by anyone. It is the outcome of the encryption process. For example: The plain text "How are you" is converted into cipher text as "* @97k&A%L".

C. Encryption

The method of translating the plain text into cipher text with the help of algorithm and the encryption key is called encryption algorithm.

D. Decryption:

The method of translating the cipher text back in to its original form that is plain text with the help of decryption key and algorithm is called decryption algorithm.

E. Keys

The numeric, alpha numeric or special symbol are used as key. During the encryption and decryption process the key plays a major role. The information security directly depends on the selection of key.

4. CLASSIFICATION OF CRYPTOGRAPHY

Depending upon the key cryptography can be divided into two categories.

- Symmetric encryption(Private key)
- Asymmetric encryption(Public key)

A. Symmetric Encryption(private key Encryption)

During the encryption and decryption process the same key is used at the sender and receiver site. Before the Transmission of information starts the key distribution has to be made [2]. Example: DES, 3DES, BLOWFISH, AES etc.

B. Asymmetric Encryption(Public key encryption)

In Asymmetric encryption, two different keys are used for encryption and decryption process. At the same time the two keys are generated. In that one key is transferred to other side before the exchange of information begins [3]. Example: RSA, Elgamal, Elgamal signature Diffie Hellman key exchange, Digital signature

5. OVERVIEW OF ALGORITHM

SYMMETRIC KEY CRYPTOGRAPHY

1. DES- DATA ENCRYPTION STANDARDS

DES, Data Encryption Standards is a symmetric key block cipher. It was published by National Institute of Standard and Technology (NIST) . IBM designed the DES based on their Lucifer cipher. DES takes 64 bit plain text as input and produce 64 bit cipher text as output. The encryption process consists of the two permutation that is initial and final permutation and consist of sixteen fixed rounds.[4]The Round key generator takes 56 bit cipher key and gives the output as 48 bit cipher key. The 48 bit key is given to each round. In each Round the 64 bits is divided into two halves that is left and right. Every Round has two cipher elements (mixer and swapper). The left half of the 32 bits elements is directly given to the XOR and the right half of the 32 bit is given to the expansion D-box. The expansion D-box converts the 32 bits in to 48 bits .The expansion box output is added with 48 bit key and it is given to the XOR function. The XOR function performs its function and produces the result as 48 bits. These 48 bits are given to the group of s-Boxes and produce the result as 32 bits. These 32 bits are given to the straight D-Box and it performs its operation and gives the result as 32 bits. These 32 bits are then XOR with left half of the 32 bits. Then the swapper swaps the left and right halves. It is then given to the next subsequent Rounds. At the final 16^{th} round output is given to the final permutation. The reverse side of the encryption process is called Decryption process.

2. ADVANCED ENCRYPTION STANDARDS (AES)

The AES is a symmetric key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001.

AES is a non – fiestel cipher. It encrypts and decrypts data blocks of 128 bits. It consists of 10, 12 and 14 rounds. The key size can be 128,192 or 256 bits that depends on the number of rounds. It has three different AES version: AES-128, AES-192, and AES-256. Each round has sub bytes, shift rows, mix columns and add round key. In the

sub bytes, we interpret the byte as two hexa decimal digits. The row defines the left digits and the column defines the right digit. The function of the two Hexadecimal digits of the row and column are the new bytes. Shift rows are shifting to the left. Mix column is to mix the column matrix .In add round key adds a round keyword with each state column matrix

3. TRIPLE DES

Triple DES is a block cipher algorithm. For each block of data it is applied three times. To ensure additional security for our information, we increase the key size in triple when compared to other encryption algorithm. Triple DES has large key size. The original DES was affected by Brute Force attack. But, Triple DES protects against these kinds of attacks. Here, we use three different keys k1, k2, and k3. These three keys are independent of each other. The overall key length of Triple DES is 192 bits.

It takes three 64 bit keys for a single round. In Triple DES the first key is encrypted with data, second key is used for decrypt the data and the third is used again for encrypting the data. It is more secure than DES. Even though it runs very much slower when compared to DES. The method for decrypting the data is same as the process for encryption but in reverse order. It is fully asynchronous. It uses only one clock cycle. It can be implemented in ASICS and FBGAS. It is delivered as Verilog RTC source code.

4. BLOW FISH

Blow fish is a symmetric block cipher. It is used for encrypting and protecting the data. It has a variable length key range from 32 bits to 448 bits, for safeguarding our data. It was designed in 1993 by Bruce schneier. It is a license for encryption method and it is freely available to all users. It is mainly used for applications, such that key does not change often, like a communication link [4].

Fiestel Network is a common method of converting any function into permutation. The working procedure of fiestel network:

- It split the block in two halves
- Now, the right half becomes new left half.
- If the left half is XOR'd with result of applying 'f' to the right half and the key, we have the new right half as the final result.
- Even the function f and not invertible the previous rounds can be derived.

BLOW FISH ALGORITHM

- It has large data blocks.
- It consists of 64 bit block size.
- The range of key scalable from 32 bits to 256 bits.
- It uses very simple operation which is efficient for microprocessors.
- It support for per computable sub key .For faster execution these sub keys are pre computed.
- It has a variable number of iteration.
- It uses sub key which is one way hash of the key.
- It has no linear structure.
- Its design structure is simple to understand. It increases the confidence in the algorithm. It is a fiestel iterated block cipher.

5. MULTIPHASE ENCRYPTION

Multiphase encryption is the process of encrypting the message multiple times by using same key or using two different keys in order to enhance the security of our data. Multiphase encryption provides more security when compared to other kinds of encryption techniques.

Example: plain text (p): HELLOWORLD Algorithm(c): ((p+1) +3) +2… (N times)

Cipher Text: IFMMPXPSME (After 1st cycle)

LIPPSASVPH (After 2nd cycle)

…….

…….

Encrypted N times

6.RC4

It was designed by Ron Rivest of RSA security in 1987. It was originally termed as "Rivest cipher 4"(RC4) and alternatively it is also called Ron's code. It is the stream cipher. Here, the same algorithm is used at the encryption and decryption site. It consists of variable size stream cipher which includes byte oriented operations. Pseudo random permutation the base for this algorithm. The stream data is XOR'd with the generated key sequence. The key size is independent of the plain text used. The key range from 1 to 256 bit to initialize the 251 bit state table. The plain text is XOR'd with pseudorandom stream to produce the cipher text.

ASYMMETRIC KEY CRYPTOGRAPHY

Asymmetric key cryptography is the technique which consist of different keys used for both encryption and decryption process. One key is called public key and another key is called private key .The public key is used for encrypting the original message, whereas the private key is used for decrypt the message. Both the public and private key are generated by the receiver. Later, the receiver distributes the public key to the sender through a public-key distribution channel. .Asymmetric key cryptography uses mathematical function for both encryption and decryption whereas in symmetric key cryptography uses substitution and permutation of symbols. Asymmetric key cryptography is used for authentication, Digital signature and secret key exchanges.

1. RSA

It is widely used public key algorithm. It was invented by Ronald Rivest, Adi Shamir and Leonard Adleman in the year of 1997. It uses two component e and d, where 'e' is public and'd' is private. Both encryption and decryption uses modular exponentiation. Modular Exponentiation

feasible in polynomial time by using fast exponentiation algorithm [5].

ALGORITHM

{

- Select two large prime numbers p and q.
- Compute n=p*q.
- Then compute Ǿ (n) <------ (p-1)*(q-1).
- We have to select 'e'. e in the range 1<e<Ǿ(n) and e is cop rime toǾ (n).
- D←-----e^{-1} mod Ǿ(n)
- Public key←--e(n)
- Private key←---d
- Then return public and private key

}

2. ELGAMAL CRYPTOSYSTEM

It was invented by Tahar Elgamal in the year of 1984. Elgamal cryptosystem is based on discrete logarithm problem. It was originally developed by Diffie and Hellman. It requires the interaction between both the parties needs to calculate a common private key.[6]

It creates a problem that if the cryptosystem is applied to communication system where both the parties can't be able to communicate in the reasonable amount of time due to delay in the transmission (or) unavailability of the receiving party. This Elgamal system overcomes the problem of Diffie-Hellman key exchange algorithm by introducing a random Exponent k. This random Exponent is a replacement for the private exponent of the receiving entity. Because of the simplification it can be encrypted in one direction, without the compulsion of the second party to participate. This algorithm is mainly used for encryption of electronic message.

3. KEY GENERATION

In asymmetric key cryptography, we need two keys to encrypt and decrypt the messages. The Receiver is responsible for generating two keys. Then he sends the public key to the sender to encrypt the message and keeps the private key with him.

4. ENCRYPTION PROCEDURE

To encrypt a message Alice needs to receive his public key triplet from the receiver bob via unencrypted electronic mail. This encrypted message is safe because it is infeasible to compute the discrete logarithm.

5. DECRYPTION PROCEDURE

After receiving the encrypted message, bob uses his private key to decrypt the message that has been sent by the sender.

6. ELGAMAL SIGNATURE

This Elgamal algorithm not only supports encryption and decryption but it is also support electronically signing off the message. This signature technique has three main characters. [6]

- Alice finds the signature from M by using her private key.
- Bob has to verify the signature by using the public key.
- Forgery prevention.

7. DIFFIE HELLMAN KEY EXCHANGE

It is also a popular asymmetric key encryption Technique. It was invented by Whitfield Diffie and Martin Hellman in 1976. It is mainly used in transport layer security. It solves the following problem. Ram and priya wants to share a secret key, to use a symmetric key cipher. But their communication is insecure. Even a single piece of information exchange is observed by third party, so Diffie and Hellman provides a possible solution.[6]

8. DIGITAL SIGNATURES

It ensures the receiver that the message is send by a known sender. It is mainly used in financial Transaction, Banking etc.[1]

It consists of three algorithms:

- Key Generation Algorithm

  From a given set of possible private key, it picks a private key uniformly. It produces the result as private key and their Respective public key.

- Signing Algorithm

  It produces the signature by using a message and a private key.

- A signature verifying Algorithm

  It checks the message to accept or reject. It provides message authenticity.

6. CONCLUSION

This paper tells about the study of symmetric and Asymmetric key encryption algorithm like AES, DES, TRIPLE DES, RC4, Multiphase encryption, RSA, Elgamal cryptosystem, Digital signature and Diffie Hellman. Data security plays a vital role in network communication. Cryptography provides the security for data. Depending on the communication and channel we have to choose the best algorithm from the above one. Nowadays both symmetric and asymmetric play a major role in Network Security.

REFERENCES

[1]. W. Stallings, Cryptography and Network Security Principles and Practices Fourth Edition, Pearson Education, Prentice Hall, 2009.

[2]. Himani Agrawal and Monisha Sharma, "Implementation and analysis of various Symmetric Cryptosystems", Indian Journal of science and Technology Vol.3, No.12, 2012.

[3]. Manoj Kumar Pandey, et.all., "Survey Paper: Cryptography The art of Hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, Vol.2, No.12, 2013.

[4]. Tingyuan Nie, and Teng Zhang ,"A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.

[5]. "File Encryption and Decryption Using Secure RSA", Rajan.S. Jamgekar, GeetaShantanu Joshi, International Journal of Emerging Science and Engineering (IJESE)ISSN: 2319–6378, Vol.1, No.4, 2013.

[6]. "ElGamal Digital Signature Algorithm of Adding a Random Number", Xiaofei Li, Xuanjing Shen and Haipeng Chen, College of Computer Science and Technology, Jilin University, Changchun, China, Journal Of Networks, Vol.6, No.5, 2011.