International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

An Analysis of Cryptographic Techniques

Vishal Chelani[1], Deepak Moud[2]
[1]UG Scholar, [2]HOD, Department of CSE, Poornima Institute of Engineering & Technology, Jaipur, India
[1]2014pietcsvishal@poornima.org, [2]deepakmoud@poornima.org

Abstract: ***In recent scenario data is transferred from sender to receiver by some digital communication medium and data must be kept private. Data must be reached to that user who claimed for it using some credentials. So cryptography is a techniques which is used to hide the important data and to make the data transmission protected. Different techniques like AES, DES, RSA, Diffie Hellman are used to make data secure. In this review paper cryptography algorithms are implemented, analysed & compared based upon their response time or latency to convert the plain text into another form, their vulnerabilities by some attacks and complexities by their key size.***

Keywords: Cryptography, Techniques, AES, DES, RSA (Rivest Shamir and Adleman), Diffie Hellman.

I. INTRODUCTION

Cryptography is the technique through which one can convert the plain text into cipher text by using a secret code known as key so that the information or data can be secure and not used by any other invader. It allows the sender and receiver to send their private information end to end by encryption and decryption processes. An encryption process takes the input of plain text and a key which is passed to an encrypting function to convert the message into the unreadable form and transmit to receiver end through any medium. While at the receiver end decryption process starts to decrypt the cipher text and retrieve the message by using either the same or a different key. The key used for cryptography must be of good length or strong. The encryption and decryption is generally based upon the key which is to be used so users need to keep the key as private only. Sometimes it might be possible that an invader or an enemy hears the cipher text but until he does not know the decryption key he will not be able to get the information from it. Cryptography is a mechanism through a user can protect the consistency and integrity of data by implementing some encryption and decryption approaches.

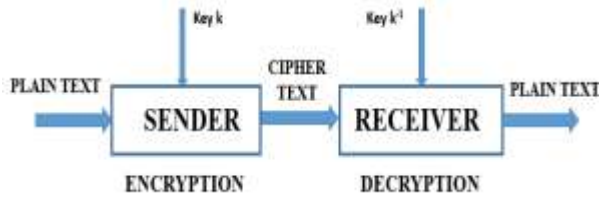

Fig. 1. Fundamental Model of Cryptography

Cryptography can be categorized into three sub-parts symmetric cryptography or private key cryptography, asymmetric cryptography or public key cryptography and hash function cryptography. Symmetric cryptography uses a shared common key between intended sender and receiver to encrypt and decrypt the message as shown in figure2. Therefore it is called symmetric key cryptography.

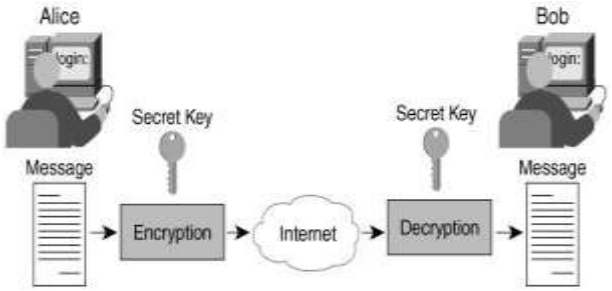

Fig. 2. Symmetric Key Cryptography

Secret key or symmetric key cryptography is divided into two components i.e. Stream cipher and Block cipher. Stream cipher encrypts and decrypts the message one bit or alphabet at a time where as Block cipher encrypts and decrypt the message into blocks.

Asymmetric Cryptography deploy two different keys for both encrypting and decrypting processes. The sender uses a key known as public key to encrypt or encode the plain text and the receiver decrypts or decode the plain text using another key known as private key as shown in figure 3.

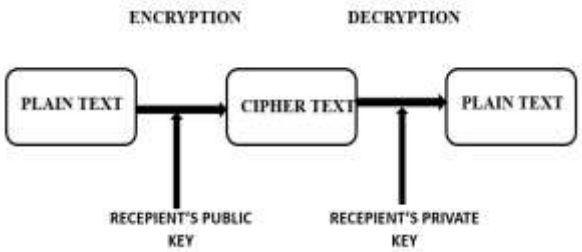

Fig. 3. Asymmetric Key Cryptography

Classification of Cryptography Algorithm:

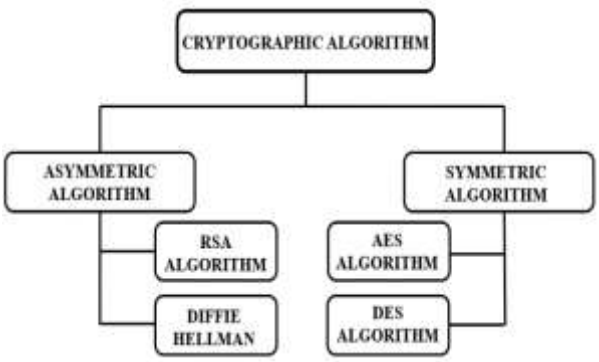

Fig. 4. Classification of Cryptography Algorithm

International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

II. ENCRYPTION ALGORITHMS

Asymmetric Algorithms: Asymmetric Cryptography Algorithm are those algorithm which uses two different keys i.e. a public and a private key for both encryption and decryption of a message or plain text. Asymmetric algorithms can be categorized into following algorithms:

1. RSA (Rivest Shamir Adleman) Algorithm
2. Diffie Hellman Key Exchange Algorithm
3. DSA (Digital Signature) Algorithm

Here we just discuss about RSA and Diffie Hellman Algorithm and its execution time and vulnerabilities.

A. RSA Algorithm:

RSA Algorithm is a most commonly used asymmetric public key cryptography approach invented by three MIT scholars Ronald Rivest, Adi Shamir and Leonard Adleman in 1978. RSA is generally used in different software's, digital signatures and for key exchange services. RSA uses a variable size encryption block and a variable size key. RSA technique uses two keys i.e. a public key and a private key. A public key is known to everyone but a private key is known to only that person who claims for it. The security of RSA is based upon the two prime numbers which are very large. RSA is safe as it has a proficiency to prevent concerted attacks.

It is essential that before encrypting and decrypting the data key must be generated by the following steps: -

- Select two dissimilar large unique prime numbers p and q.
- Calculate n by product of p and q i.e. n=p*q.
- Find the value of totient ϕ (n) = (p-1)*(q-1).
- Find value of e such that 1 < e < ϕ (n) and e must coprime to ϕ (n) it means e and ϕ (n) don't have common factors i.e. gcd (e, ϕ (n)) = 1.
- Calculated e will be act as public key for encryption.
- Generate an integer d with a congruence relation ed $\cong$ 1 i.e.

  e*d = 1 + k*ϕ (n) where 1 < d < ϕ (n)
- Generated integer d will act as a private key.

After generating public and private keys now encryption can takes place. Suppose a person 'A' disclose her public key to 'V' and keeps her private key secret. 'V' wants to send a message to person 'A' then,

$$C = M^{e} \pmod{n}$$

Now 'A' can retrieve her message by using her private key by following method: -

$$M = C^{d} \pmod{n}$$

B. Diffie Hellman Algorithm:

Diffie Hellman is an asymmetric key exchange cryptography algorithm over a public channel. It was initially developed by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. Diffie Hellman key exchange technique allows two users that have no prior information of one another to share a secure key upon an insecure channel. It is used to protect a wide range of internet services. The major issue of this algorithm is that communication is done itself made insecure due to man-in-the- middle attack.

The simple implementation of Diffie Hellman algorithm is use of multiplicative group of integers mod p, where p is a prime integer and g is primitive root to modulo p. These values could be obtained from 1 to p-1. Diffie Hellman algorithm works in following steps:

- Choose an integer 'p' which is prime and an integer 'g' which is primitive root of 'p'.
- Both 'p' and 'g' must be from 1 to p-1.
- Find 'a' and 'b' as a secret integers i.e. they must be kept secure.
- Calculate

  x = g^ a (mod p)

  y =g^ b (mod p)
- Now the secret key can be calculated as,

  k1 = y^ a (mod p)

  k2 = x^ b (mod p)
- Both k1 and k2 are secret keys to be exchange and are identical to each other.
- Therefore both users can use this common shared key to encrypt and decrypt the message without any other person intervention as shown in figure 6.

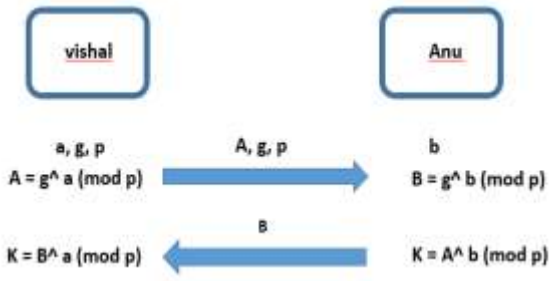

Fig. 5. Diffie Hellman Algorithm

C. DES Algorithm:

DES Algorithm is a block symmetric cryptography algorithm developed at IBM in 1970s. It means this technique uses only a single secret key for both encryption and decryption. DES is a Standardized method of securing the commercial information. DES Algorithm uses permutation and substitution operations while encrypt the data and vice-versa.

International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

DES Algorithm contains multiple steps in its procedure:

1. It uses 64-bit block of data as an input for encryption process.
2. 64-bits key is used for encryption and decryption, out of 64-bits 56-bits are used to encode and decode the data by initial permutation method and rest of the 8-bits are used for error detection (Parity bits).
3. The key is divided into two sub-parts of 28-bits each, then each half will be shifted as one or two bits based upon the number of round.
4. Now these two halves will be used to convert 56-bits key to 48-bit key by using permutation.
5. DES uses permutation and substitution method in a single round.
6. DES processes the data into 16-rounds for both encoding and decoding.
7. The data block of 64-bits are sub divided into two parts of 32-bit each.
8. One sub part of 32-bits will be used to expansion permutation to generate a 48-bit block of data as our key is also of 48-bit size.
9. In DES cryptography each round contains several sub processes like expansion of 32- bit data into 48-bit block and compress process using S-boxes and then the final permutation can be implemented.

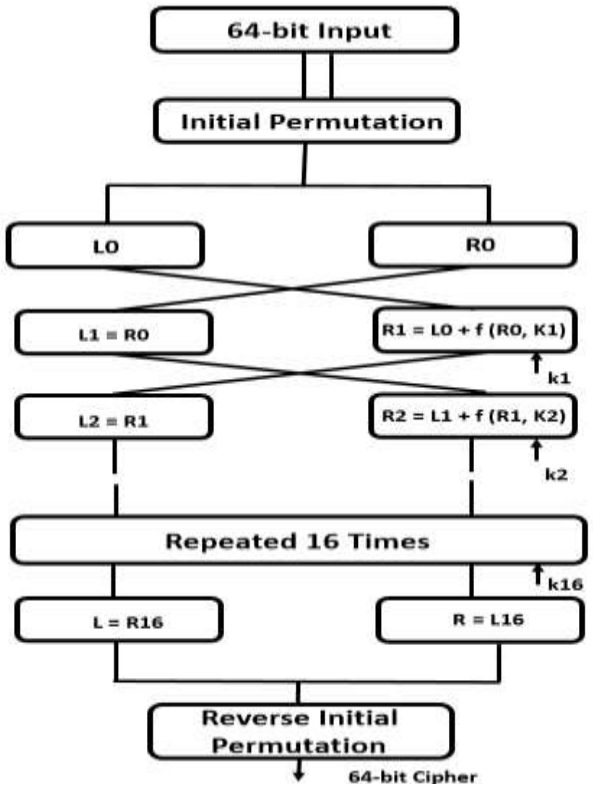

Fig. 6. DES Algorithm

A particular round of DES Algorithm contains an expansion operation to convert the 32 bit data block into 48 bit data block so that the XOR operation with a 48-bit key can be performed then the intermediate 48 bit output is transferred into a S-Box which compress the output data into 32 bit and after this permutation process can be implemented and a 64 bit output is generated.

D. AES Algorithm:

AES Algorithm is also known as Rijndeal's Algorithm. It is a symmetric block cryptography. It was recognised that the DES algorithm was not much secure then two Belgian cryptographers developed AES algorithm. AES uses three different data block sizes i.e. 128 bit, 192 bit, 256 bit. Based upon the data block key size differs. It also uses some rounds i.e. 10, 12, 14 to process the data blocks for generating the cipher text. It consumes less time to process the data which makes its system much faster and efficient. In AES encryption process it uses different rounds: -

1. Usual Round: In a usual round there are certain operation which are to be implemented.

A. Sub Bytes

B. Shift Rows

C. Mix Column

D. Add Round Key

2. Final Round: In the final round only three operations are to be implemented.

A. Sub Bytes

B. Shift Rows

C. Add Round Key

i. The Sub Byte operation substitute the single byte into two hexadecimal digits.

ii. The Shift rows operation shifts the row according to their occurrence i.e. Row 1 is not shifted, Row 2 elements shifted by one position from left to right.

iii. The mix column is a kind of transformation applied to all columns. It transforms every column into a new state column.

iv. Add round key operation is a key adding operation to the column matrix.

AES also uses XOR operation of the plain text with round key and generates the cipher text.

Brute force attack might unlock the AES Algorithm, attacker uses English words dictionary and find the words that can hit the secret key to disclose the message.

International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

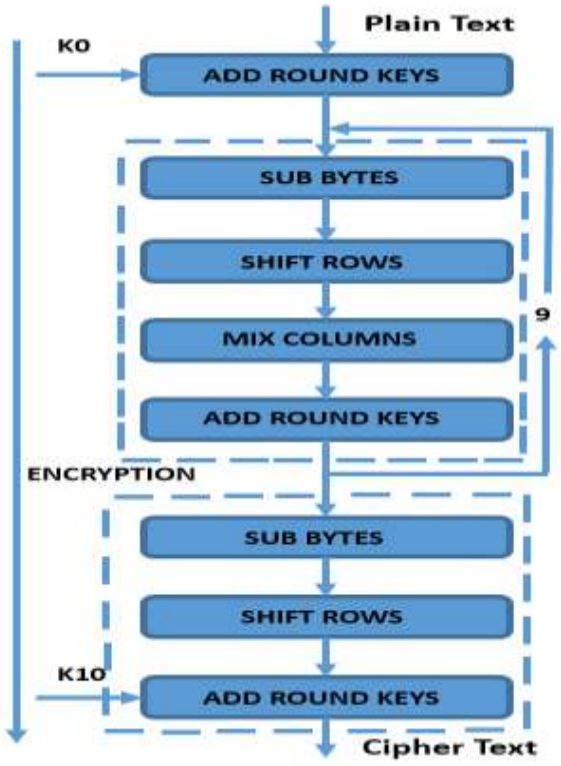

Fig. 7. AES Encryption

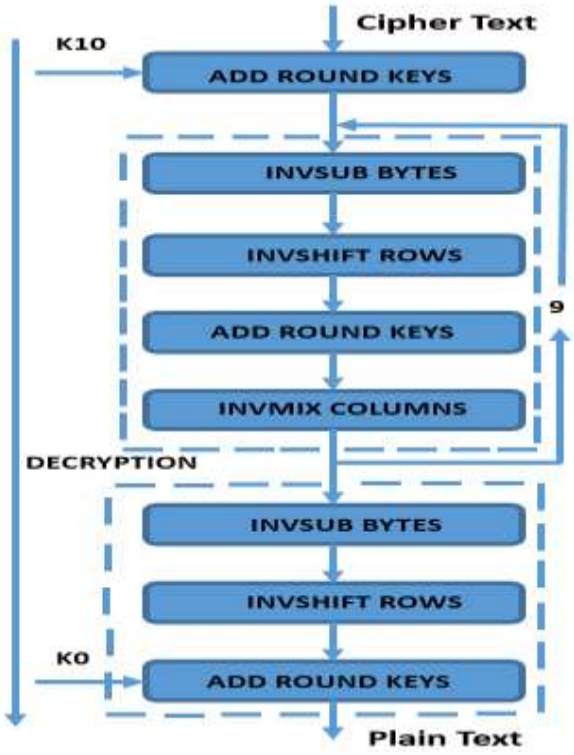

Fig. 8. AES Decryption

III. COMPARISION

We have implemented DES, AES symmetric and RSA, Diffie Hellman asymmetric algorithms on Codeblocks tool. The requirement of the system to run the above described tool is 2 GB Ram, more than 128 GB Rom and windows operating System. The algorithms are executed in the form of C language programs on a particular message i.e. "hellovishal". As we know that each algorithm has its merits and demerits so the below table can be used to illustrate the parameters like key size, block size, execution time, vulnerability to attacks, security, encryption, decryption, speed and number of rounds. Different Algorithms contains different-different execution time to encrypt and decrypt the data. The Graph of RSA, Diffie Hellman, DES and AES can be given as,

Fig. 9. Algorithm's Execution Time Graph

Table 1. Execution Time of Cryptography Algorithms

S.No.	Algorithm	Execution Time
1	RSA	5.481 Second
2	Diffie Hellman	7.614 Second
3	AES	12.558 Second
4	DES	9.561 Second

Table 2. Comparison Table of Asymmetric Cryptography

Parameters	RSA	Diffie Hellman
Key size	Greater than 1024	Minimum 2048 Bits
Block size	Minimum 512 Bits	2048 Bits
Power Consumption	High	Slightly Higher than RSA
Vulnerability of Attacks	Brute Force Attack & Oracle Attack	Man in the Middle Attack
Rounds	Single Round	Single Round
Security	Least Secure	Secure for Internet Services

Table 3. Comparison Table of Symmetric Cryptography

Parameters	AES	DES
Key Size	128, 192, 256 Bits	56 Bits
Block Size	128, 192, 256 Bits	64 Bits
Power Consumption	Low	Low
Vulnerability of Attacks	Brute Force Attack	Brute Force Attack, Linear and Differential cryptanalysis Attack
Rounds	10, 12, 14	16
Security	Highly Secure	Not Enough Secure

IV. CONCLUSIONS

Cryptography Algorithms are much important to protect the information while transferring from sender to receiver. Our work behind the research serves the efficiency of different algorithms based upon their execution time of encrypting and decrypting the data blocks. Based upon the text message it is concluded that RSA algorithm consumes less time to encrypt and decrypt the message but AES algorithm is also efficient because it resist some attacks which affects the RSA.

ACKNOWLEDGMENT

I am heartly thankful to Mr. Deepak Moud who gives me the guidelines to work upon my research and review. His guidance helps me a lot to know about the insight knowledge behind the cryptography techniques to secure the information which is confidential to each and every person.

V. REFERENCES

[1] A Study of Encryption Algorithms AES, DES and RSA for Security, Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013

[2] A Review Paper on Cryptography and Significance of Key Length, International Journal of Computer Science and Communication Engineering IJCSCE Special issue on “Emerging Trends in Engineering” ICETIE 2012.

[3] Review of Various Algorithms Used in Hybrid Cryptography, IJCSN International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013.

[4] Review and Analysis of Cryptography Techniques, International Journal of Scientific & Engineering Research Volume 4, Issue3, March-2013, ISSN 2229-5518.