ISSN No. 0976-5697

Volume 8, No. 4, May 2017 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review of Information Security using Cryptography Technique

Neha Sharma
MCA Scholar
Computer Science Applications
SBBSU
Jalandhar, Punjab, India
angleneha222@gmail.com

Prabhjot
MCA Scholar
Computer Science Applications
SBBSU
Jalandhar, Punjab, India
prabhjhim@gmail.com

Er. Harpreet kaur
Assistant Professor, CoD
Computer Science Applications
SBBSU
Jalandhar, Punjab, India
er.harpreetarora@gmail.com

Abstract- **Data security has become crucial aspect nowadays in every sectors. So in order to protect it various methods and algorithm have been implemented. It protects its availability, privacy and integrity. More companies stores business and individuals information on computer than ever before. Much of the information stored is highly confidential and not for public viewing. In this paper I have reviewed the cryptography algorithm which is based on block cipher concept.**

To write this paper I have study about information security using cryptography technique. After the detailed study of network security using cryptography. This paper is dividing in three sections. In section 1, I am presenting just basic introduction about in information security using cryptography. In section 2, I am presenting detailed description about cryptography algorithms like symmetric key algorithm like DES,AES ,blowfish and Asymmetric key algorithm like RSA , Diffie–Hellman key exchange algorithm. In section 3, I am presenting conclusion and references where I have completed my research.

Keywords-Information security, cryptography algorithm, Encryption , decryption, cryptography.

Section-I

INTRODUCTION

Cryptography is technique to provide message confidentiality. The term cryptography is Greek word which means “secret writing”. Now a days, cryptography commercial applications. If we are protecting confidential information then cryptography is to provide high level of privacy of individuals and groups. Cryptography is the methods that allow information to be sent in secure from in such a way that the only receiver able to retrieve the information[2].

Presenting continuous researches on the new cryptographic algorithm, are going on, however, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity. The main purpose of the cryptography is used not only to provide confidentiality, but also used in others security services like : data integrity, authentication , non repudiation[1]. Cryptography involves the process of encryption and decryption.

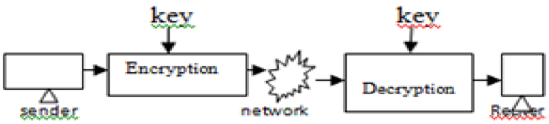

Fig. 1. Cryptography

The terms which are used in cryptography is given below:-

1. *Plaintext*: The original message or data that is fed into algorithm as input called as plaintext.

2. *Encryption algorithm*: Encryption is process of changing plaintext into cipher text.

3. *Cipher text*: Cipher text is encryption form the message. It depends upon plain text and key.

4. *Decryption algorithm*: The process of changing the cipher text into plaintext is known as decryption.

5. *Key*: It is also acts as input to the encryption algorithm. The exact substitution and transformation performed by the algorithm depends on the key [2].

Section -II

CRYPTOGRAPHY ALGORITHM

The cryptography algorithm are grouped into two categories as:-

1. Symmetric key or secret key Algorithm

2. Asymmetric key or public key Algorithm

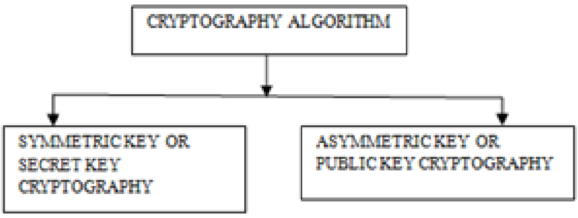
CRYPTOGRAPHY ALGORITHM
SYMMETRIC KEY OR SECRET KEY CRYPTOGRAPHY
ASYMMETRIC KEY OR PUBLIC KEY CRYPTOGRAPHY

Fig. 2. Types of cryptography algorithm

1. *Symmetric Key Or Secret Key Cryptography*: It is also called as single key cryptography. It uses a single key. In this encryption process the receiver and the sender has to agree upon a single secret(shared) key. Symmetric key algorithm are those algorithms in which both sender and receiver use the same key. Given a message (called plaintext) and the key , encryption produces unintelligible data, which is about the same length as the plaintext was. Decryption is the reverse of encryption , but uses the same key as encryption . in decryption , cipher text convert into plaintext using same key[5].

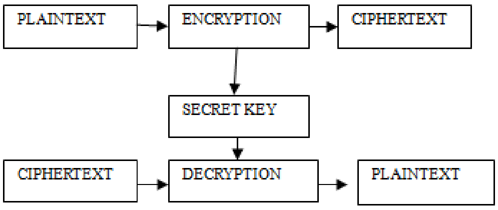

Fig. 3. Symmetric Key Cryptography Process

Examples of secret key algorithm are as follows:-

1. Data encryption standard(DES)

2. Advanced encryption standard(AES)

3. Blowfish

1. *Data Encryption Standard* (*DES*):- DES Is symmetric key block cipher published by NIST(National Institute of Standard Technology). It uses 64 bit plaintext with 56 bit key to obtain a 64 bit cipher[6].

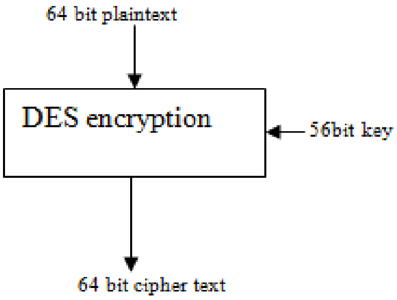

Fig. 4. Basic Diagram of DES encryption

DES encrypt 64 bit block of Plaintext using 64 bit key. The key actually contains 56 usable bits as the last bit of each of 8 bytes in the key is a parity bit for those bytes i.e. 8 out of 64 bits are parity bits. DES can also encrypt the messages larger than 64 bits.

DES structure is as follows:-

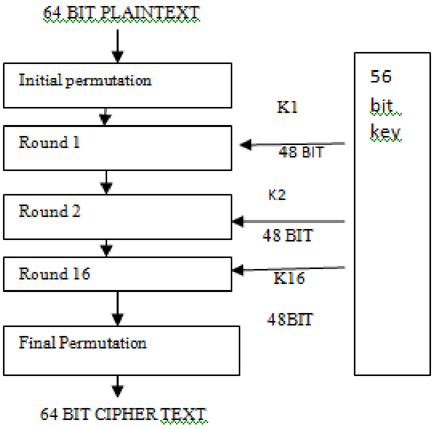

Fig.5. DES structure

In this figure, DES has three distinct phases:-

1. The 64- bit in the block are permuted or shuffled.

2. Sixteen rounds of identical operations are applied to the resulting data and the key.

3. The inverse of original permutation of step 1 is applied to the resulting data to get the ultimate cipher text.

4. In the initial permutation the various bits are shuffled with each other and is not dependent on key.

5. During each round the 64 bit block is broker into halves, the left half and the right half, each of 32 bit.

6. The key used in each round is of 48 bits and is derived from 56 bits key by rotating the bits [7].

DES has 56 bit key which is prone to brute force attack due to small bit size its criticism start from its beginning of evolution.

2. *Advanced Encryption Standard*(AES)**:-** AES is symmetric key block cipher that may replace DES and was published by NIST(National institute of Standard technology) in December 2001. AES also known as the Rijndael. AES is non festial cipher that encrypt and decrypt a data block 128 bits. Its uses the 10 ,12, or 14 rounds. The key size can be 128, 192 or 256 bits Depends upon numbers of rounds. AES versions are as:-AES 128,AES 192,AES 256[8].

TABLE 1

AES VERSIONS

Nr	Key Size
10	128
12	192
14	256

General Design of AES Encryption cipher:-

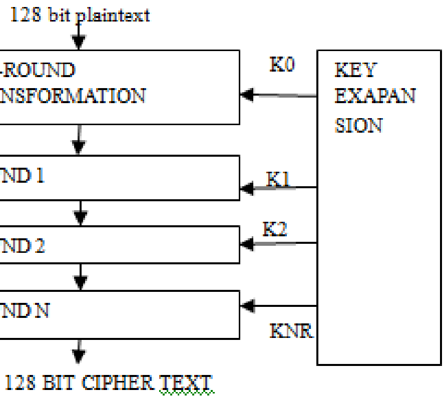

Fig. 6. AES Diagram

Number of Round:- Nr+1

AES was introduced to replace the DES. Brute force attack is the only effective attack known against this algorithm.

3.*BlowFish*:-Blowfish is symmetric block cipher that uses a variable length key up to 448 bits in length. It was designed in 1993 by bruce schneier as drop in replacement for DES . it is fast and well-tested algorithm. It is also unpatented and license free. Though it suffers from weak keys problems, no attack is known to be successful against it[10].

2. *Asymmetric Key Or Public Key Cryptography*:**-** Asymmetric algorithm are those algorithm in which sender and receiver uses the different keys. Public key encryption algorithm are asymmetric in the sense that the encryption and decryption keys are different . Each user is assigned a pair of keys- public and private key[12].

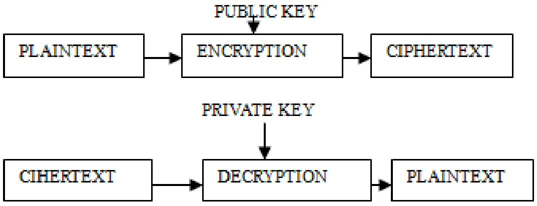

Fig. 7. Asymmetric Key Cryptography Process

Examples of public key encryption algorithm are as:-

1. RSA

2. Diffie -Hellman

1. *RSA Algorithm*: RSA was invented three scholar Ron Rivest Adi Shamir Lan Adleman , hence named RSA.

Steps are as:-

1. Generate RSA module,

A. select two prime number p and q.

B. calculate n=p*q.

2. Find derived number e

a. number e must be greater than 1 and less than(p-1)(q-1)($1<e<(p-1)(q-1)$)where(p-1) (q-1)=N

then $1<e<N$

b. there must be no common factor for e and N except for 1.

3. Form public key

a. pair of number n and e (n, e) from the public key.

b. interesting though n is part of public key , difficultly in factorizing a large prime number ensure that attacker cannot find in finite time the two prime (p and q) used to obtain n. This strength of RSA.

4. Generate private key

a. private key d is calculated from p , q, and e.

b. mathematical relationship between p, q, and e and d is given as:-

$e\ d \bmod (p-1)(q-1)=1$

5. The extended Euclidean algorithm p, q, and e input and given d as output.

6. Encryption: $C=P(e) \bmod n$

Where C= cipher text

P = plaintext

7. decryption : $P=C(d) \bmod n$

Where C= cipher text

P = plaintext [11].

2. *Diffie- Hellman Key Exchange Algorithm*:- Diffie – Hellman protocols is a public key cryptography method that is firstly implemented in 1976 over an in secured communication channel.

1. Alice and Bob agree on a prime number p and base g.

2. Alice choose a secret key number ‘A’ and send Bob ‘g’ with the power of g*A mod p.

3. Bob choose a secret number ‘B’ and send Alice ‘g*B mod p’.

4. Alice computes (g*B mod p)*A mod p.

5. Bob computes (g*A mod p)*B mod p[12].

Section -III

CONCLUSION

Many ciphers fail because they are used improperly, so we need a clear model of what a cipher does. Cryptography makes sure that the data when transferred over network is not modified. So in order to maintain data privacy cryptography algorithm are used to prevent the data altered while in transit state. Ours method is essentially block cipher method and it will take less time if the file size is large. The important things of our proposed method are that it is almost impossible to break the encryption algorithm without knowing the exact key value. We propose that these encryption methods can be applied for data. Encryption and decryption in any type of public application for sending confidential data.

REFERENCES

[1] Pawlan, m. (1998, February). Cryptography : the ancient art of secret messages.

[2] Charanjeet singh(Data communication and networks)

[3] Pranab Garg1, Jaswinder Singh Dilawari2, A Review Paper on Cryptography and Significance of Key Length, IJCSCE Special issue on “Emerging Trends in Engineering” ICETIE 2012.

[4] Gary C. Kessler, An Overview of Cryptography, 1998-2015 — A much shorter, edited version of this paper appears in the 1999 Edition of Handbook on Local Area Networks, published by Auerbach in September 1998., http://www.garykessler.net/library/crypto.html.

[5] Vishwa gupta,2. Gajendra Singh ,3.Ravindra Gupta, Advance cryptography algorithm for improving data security, www.ijarcsse.com, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[6] Siddharth Ghansela, Network Security: Attacks, Tools and Techniques, www.ijarcsse.com, Volume 3, Issue 6, June 2013 ISSN: 2277 128X. http://www.crypto-it.net/eng/theory/introduction.html.

[7] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518.

[8] Debasis Das1, U. A. Lanjewar2 and S. J. Sharma3, The Art of Cryptology: From Ancient Number System to Strange Number System, Web Site: www.ijaiem.org, Volume 2, Issue 4, April 2013 ISSN 2319 – 4847.

[9] Kartalopoulos, Stamatios V. "A Primer on Cryptography in Communications." IEEE Communications Magazine (2006): 146-151. EBSCOHost. Georgia Tech Library, Metz. 16 July 2006.

[10] Pratap Chnadra Mandal “Superiority of Blowfish Algorithm,” International Journal Of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.

[11] E. Thambiraja, G.Ramesh, Dr. R. Umarani, “A survey on various most common encryption techniques,” International Journal of Advanced Research in ComputerScience and Software Engineering, Vol 2, Issue 7, July 2012.

[12] Monika Agrawal, Pradeep Mishra,” A Comparative Survey on Symmetric Key Encryption Techniques,” International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882. Volume 2 Issue 3, September 2011. www.uscybersecurity.net/Pages/online_magazine.html.