Bijeta Sethet al. International Journal of Recent Research Aspects ISSN: 2349-7688,
Special Issue: Conscientious and Unimpeachable Technologies 2016, pp. 21-24

Analysis of cryptographic approaches

Bijeta Seth, Surjeet Dalal
Department of Computer Science & Engineering, SRM University Sonepat, Haryana, India

Abstract: **Security has always remained the greatest concern in any communication system. Cryptography is considered to be one of the main categories of computer security. Various cryptographic algorithms have been devised for providing security like DES,3DES,AES,Blowfish etc. The paper discusses the various types of cryptographic techniques applied to achieve security services. An efficient cryptographic algorithm named "Blowfish" is considered to be the most secured and fastest technique.**

Keywords:**cryptography, symmetric, asymmetric, AES, RSA, Diffie Hellmam, Blowfish**

I. INTRODUCTION

Security of information has been vital issue in modern era in case of communication. Security breaches in form of data loss, data leakage, data manipulation etc. must always be avoided. Cryptography has been widely used to provide security. Cryptography can be defined as the art of transforming plaintext (readable text) into ciphertext (unreadable text) which ensures data privacy and non alteration of data. If Alice and Bob send messages to each other, and they don't want others to read or change the content of their messages, then it means a secure communication channel is desired through transmission medium T. It is required to keep the secrecy of communications over transmission medium and to prove the authenticity of incoming messages.

II. TYPES OF CRYPTOGRAPHY

Cryptographic algorithms can be classified as shown in figure 1 below.

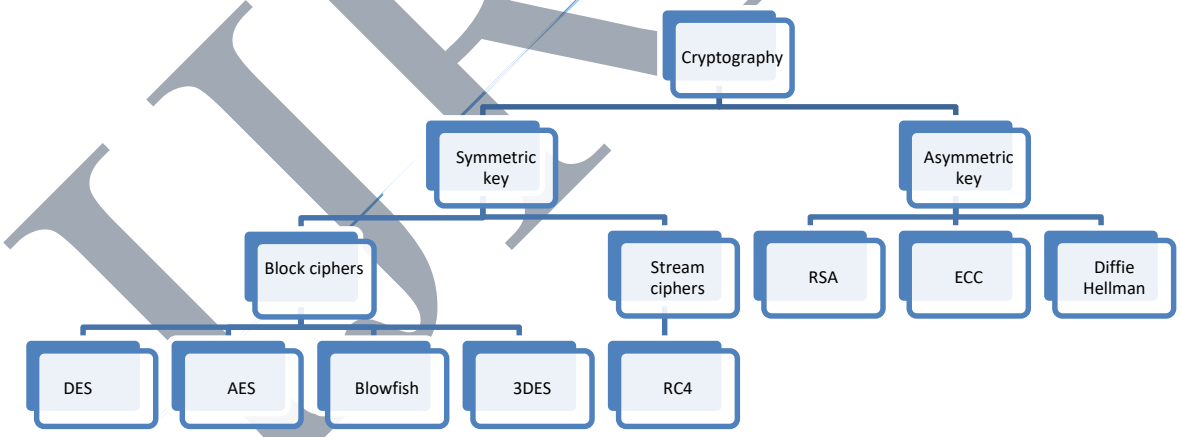

Figure 1: Classification of cryptographic algorithms

1) Asymmetric key cryptography or public key cryptography uses two keys namely public and private keys(one for encryption and other for decryption process). The sender uses public key to encrypt the message and the receiver uses his private keyto decrypt the message.
2) Symmetric key cryptography: same key is used for encryption and decryption.it can be categorized in two types:

a) Stream cipher: itencrypts one bit of plaintext at a time.

b) Block cipher: it encrypts one block at a time(typically 64 bits).

Parameter	Symmetric key cryptography	Assymmetric key cryptography
Key	Uses a single key for both encryption and decryption	Uses one key for encryption process and second for decrption
Speed	Fast in speed	Slow speed
Security	Highly secure	Less secured ss compared to symmetric
Power	Less power required	More power required
Key exchange	It's a big problem	Not an issue
Usage	Used fo encryption and decryption	Used for encryption an decryption along with digital signature
Examples	AES,Blowfish	RSA,ECC,Eigamal,Diffie Hellman

Table 1:Comparison of cryptographic techniques

Parameter	Block cipher	Stream cipher
Encryption method	Encrypts one block of plaintext at a time	Encrypts one byte of plaintext at a time
Complexity	Computationally considered less complex	More complex
Load	Carries heavy load easily	Carries heavy load with difficulty
Cryptanalysis process	Difficult to perform	Easily performed
Example	AES,DES,Blowfish	RC4

Table 2: Types of symmetric key cryptography

III. OVERVIEW OF ALGORITHMS

Our paper focus on providing protection to data from any modification or malfunctioning by untrusted third party.To provide security to data,it must be stored in an encrypted format. This section describes a brief descrption of four chosen algorithms RSA,AES,Diffie Hellman and Blowfish algorithm.

1) Diffie Hellman

It was developed in 1776 and considered to be the first public key algorithm. It is a method for securely exchanging information between two parties ver an untrusted network.It is used by several protocols like Secure Sockets Layer(SSL),Secure Shell(SSH) and Internet Protocol security(IPSec).If Aice and Bob want to exchange message,they generate secret key for susequent usage,following the steps mentioned below [1].

Alice and Bob agree on two numbers "**p**" and "**g**"	"**p**" is a large prime number "**g**" is called the base or generator
Alice picks a secret number "**a**"	Alice's secret number = **a**
Bob picks a secret number "**b**"	Bob's secret number = **b**
Alice computes her public number $x = g^a \bmod p$	Alice's public number = **x**
Bob computes his public number $y = g^b \bmod p$	Bob's public number = **y**
Alice and Bob exchange their public numbers	Alice knows **p, g, a, x, y** Bob knows **p, g, b, x, y**
Alice computes $k_a = y^a \bmod p$	$k_a = (g^b \bmod p)^a \bmod p$ $k_a = (g^b)^a \bmod p$ $k_a = g^{ba} \bmod p$
Bob computes $k_b = x^b \bmod p$	$k_b = (g^a \bmod p)^b \bmod p$ $k_b = (g^a)^b \bmod p$ $k_b = g^{ab} \bmod p$
Fortunately for Alice and Bob, by the laws of algebra, Alice's "k_a" is the same as Bob's "k_b", or $k_a = k_b = k$	Alice and Bob both know the secret value "**k**"

Figure 2: Diffie Hellman algorithm

2) RSA

It was developed by Rivest Shamir Adleman in 1977 and is considered as one of the most popular and secure public key encryption method.it is widely used for key distribution and digital signature process.It is based on the concept of "integer factorization" in which one way function method is used which is easy to compute one way but is difficult to compute in reverse process.The algorithm works in three steps:

1)Key generation: Following are the steps involved in key generation[2]:

The key generation steps are:

Step 1: generate two different primary keys P and Q

Step 2: calculate the modulus n=p*q

Step 3: calculate the $\phi(n) = (p-1) \times (q-1)$

Step 4: select the public exponent an integer e such that $1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$

Step 5: calculate the private exponent a value of d such that $d = e^{-1} \bmod \phi(n)$

Step 6: public key = [e,n]

Step 7: private key = [d,n]

Figure 3: Steps of key generation in RSA algorithm

2) Encryption process: It involves conversion of a plaintext chosen as 'M' into a ciphrtext taken as 'C'. It takes 'e' as public key and 'd' as private key. It is formulated as

$C=M^e \bmod n$

3) Decryption process: It is the reverse process of encryption and can be generated usng the formula $M=e^d \bmod C$

3)AES

Advanced Encryption Standard or Joan Daemen and Vincent Rijmen algorihm works in blocks of 128 bits upto 256 bits. The key size has no maximum limit. It uses the same key for encryption and decryption process. It converts plainext to ciphertext in a number of repitions based on encryption key. The decryption method uses the same process to transform ciphertext to plaintext using the samr encryption key. The process of AES is shown in figure below:

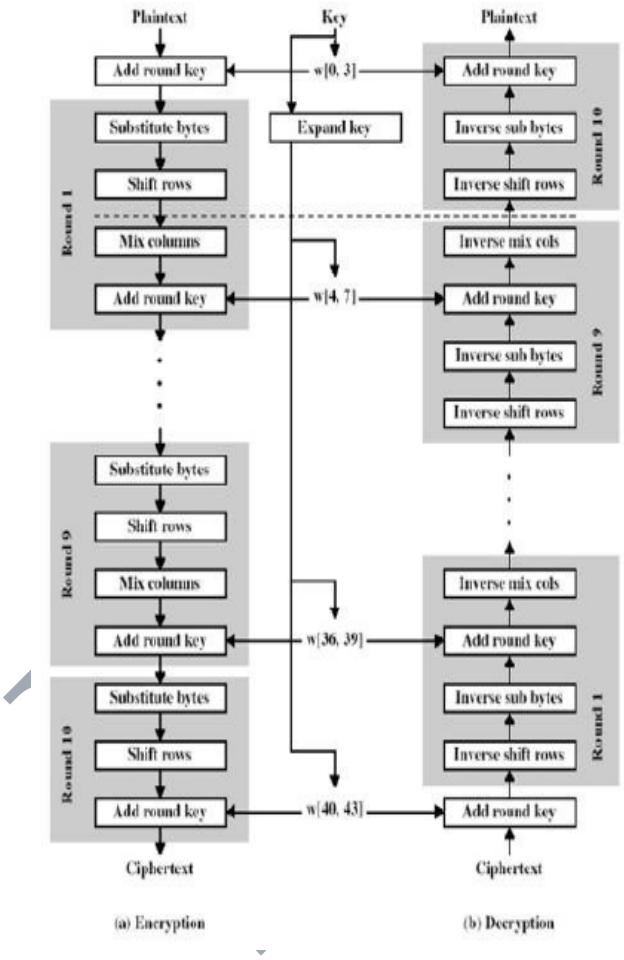

Figure 4: AES Algorithm[3]

4) Blowfish Algorithm

It is considered to be the fastest symmetric block cipher used in place of DES/IDEA.it was developed in 1993 by Bruce Schenier.it is a 16 rounds Fiestal structure wit changeable key length(32-448 bits). All operations are done as addition on 32 bitwords and XOR. Blowfish S boxes are key dependent.It operates in three phases:

1) Key expansion
2) Data encryption: Blowfish consists of 16 rounds.The input is a 64 bit data element 'x'.Following are the steps used in encryption:
   a) Divide x into two 32 bit halves:xL,xR
   b) For i=1 to 16:
      1) $xL=xL \text{ XOR } P_I$
      2) $xR=F(xL) \text{ XOR } xR$
      3) Swap xL and xR
   c) after the sixteenth round,swap xL and xR again to undo the last swap
   d) $xR=xR \text{ XOR } P_{18}$
      $xL=xL \text{ XOR } P_{17}$
   e) Finally recombine xL and xR to get the ciphertext
3) Data decryption: It is exactly same as encryption except that P1,P2..P18 are used in reverse order.

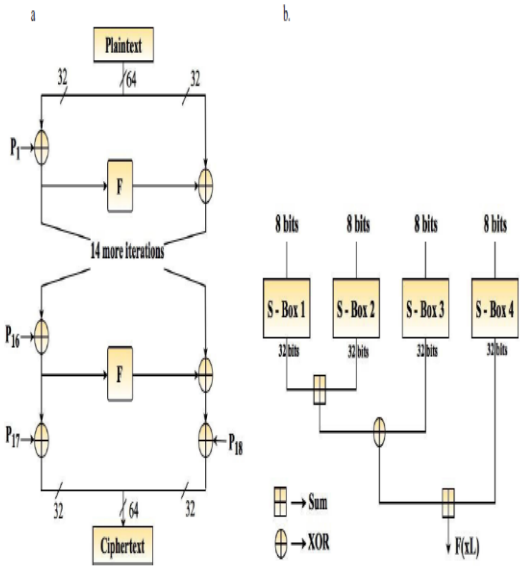

Figure 5: (a) Blowfish algorithm (b) Function module (F)[4]

Graphical representation of Blowfish Algorithm is shown in figure 5(a) taking into account Fiestal structure. The F function is shown ing fgure 5(b) . The function divides 32 bit input into four bytes and uses them as indices into an S-array. The lookup results are XORed together to produce output. P taken is an array of eighteen 32-bit integers. S is a two-dimensional array of 32 bit and stored as 4*256. P and S array are not recomputed unless the key changes.

IV. COMPARISON TABLE

Following table 3 provides a comparison of the various algorithms studied. It can be concluded that Blowfish is considered to be the most secure and fastest secret key algorithm.

Algorithm	Year	Key size	Block size	Encryption speed	Developed by	Level of security	Attacks
AES	2001	128,192 ,256 bits	128 bits	faster	Joan Daemen and Vincent Rijmen	Excellent security	Key recovery,side channel attack
RSA	1977	1024,248	<=$\log_2(n)$ In practice, block size is 2k bits with $2k < n \leq 2k+1$.	average	Rivest Shamir Adleman in	Adequate secure	Brute force attack,timing attack
Diffie Hellman	1976	variable	variable	Depend on key and block size	Whitfield Diffie and Martin Hellman	Good security	Man in the middle attack
Blowfish	1993	32-448	64 bits	Very fast	Bruce Schenier	Highly secured	No attack found suuccessful

Table 3:Comparison of different algorithms

V. SUMMARY

In this paper,we have analyzed various encryption algorihms.The basic parameters on which strength of each algorithm lies is key management,number of keys and bits used in a key.It is found that Blowfish algorithm is having highest security leveland faster encryption speed.

VI. REFERENCES

[1]. David A.Carts,"A review of the Diffie-Hellman Algorithm and its use in secure Internet protocols",SANS Institute Information Security Reading Room November 5,2001.

[2]. V Masthanamma,"An efficient Data security in cloud computing using the RSA encryption process algorithm",International Journal of innovative Research in Science, Engineering and technology,Vol 4(3) March,2015.

[3]. Isha Chawla,"Three way mechanism to enhance the dat security on cloud",International Journal of current Engineering and scientific research IJCESR Vol 2(6) 2015

[4]. Manju suresh,"Hardware implementation of Blowfish Algorithm for the secure data transmission in Internet of things,RAEREST Procedia Technology 25 pp 248-255 Sciencedirect 2016.

[5]. Rajdeep Bhanot,"A review and comparative analysis of various encryption algorithms",International Journal of Security and its applications,Vol 9(4) pp 289-306 2015.

[6]. Gurbind Kaur,:Enhancing Daa security of data on rest in cloud using RSA and Blowfish algorithm,International journal of science and research (IJSR) Vol4(10) pp 1106-1110 2013.

[7]. Randeep Kaur,"Analysis of security algorithms in cloud computing",IJAIEM,Vol 3(3) pp 171-176 March 2014.

[8]. K.Suganya," Performance study on Diffie Hellman Key Exchange Algorithm", International Journal for research in Applied Science and engineering Technology(IJRASET) pp 68-75 Vol2(3) march 2014 .

[9]. Kashish Goyal," Modified Caeser Cipher for better security enhancement",International journalof computer applications Vol73(3) July 2013.

[10]. Keiko,"An analysis of security issues for cloud computing",Journal of Internet services and applications,SpringerOpen Journal 2013.

