A STUDY OF CRYPTOGRAPHIC TECHNIQUES IN DATA SECURITY

[1]S Thanga Revathi [2]Dr.N.Ramaraj
MNM Jain Engineering College, Vignan University,Guntur
thangarevathi84@gmail.com , ramaraj_gm@yahoo.com

***Abstract* - Today's networking world has made communication to be possible between all the systems that are widely spread. With this increase in communication ease, there is a requirement for the security of Data. Today Cryptography plays a major role in providing security in internet or any public network. Cryptographic techniques are widely used in all financial, governmental, official and intelligence agencies to provide security for all formats of data that can be transmitted through the network. A survey is done on major cryptographic algorithms that are widely used now and the results of various algorithms have been compared for different criteria.**

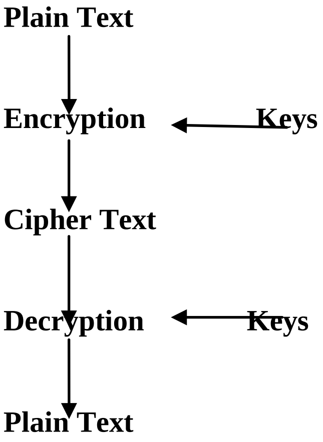
***Keywords:* Privacy, Symmetric Algorithm, Asymmetric Algorithm, RSA, DES, AES, Blowfish.**

I Introduction

Cryptography is a standard way of securing the electronic documents. Cryptography is the study of data hiding and substantiation [2]. It includes the protocols, algorithms and strategies to refuse the access of illegal users to use the secured data. Cryptography helps to store sensitive information or transmit it across insecure networks such as internet so that it cannot be read by anyone except the actual recipient. It is the method of securing the data by concealing the information to a different format is known as cryptography. It mainly depends on the Key which is used for the transformation. The Cryptography provides security by encrypting and decrypting the data.

A. Key terms used in Cryptography:

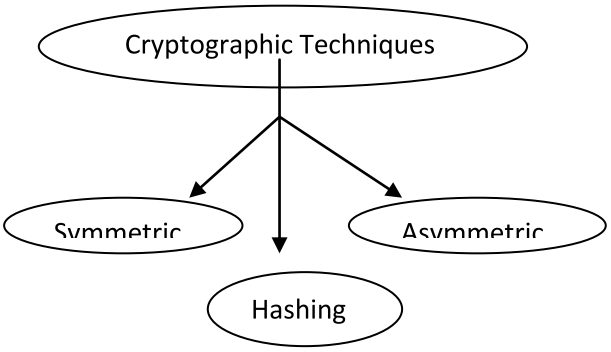
1. Plain Text: It is the original message or data.
2. Cipher Text: It is the transformed output of the original message.
3. Encryption: It is the technique which transforms the plain text to cipher text.
4. Decryption: It is the technique which transforms the cipher text to plain text.
5. Keys: The encryption and decryption process is done using the Keys.



The major categories of cryptographic algorithms fall into 3 categories.

1. Symmetric key based algorithm
2. Asymmetric key based algorithm
3. Hash algorithm

Symmetric algorithm: In this algorithm both the encryption and decryption are done with the same keys. In order to maintain a personal information link this algorithms uses a special key that represent a secret that is to be shared between more users [2] AES, DES, Blowfish are examples of symmetric algorithm.



Asymmetric Algorithm: In this one key is used for encryption and another key for decryption. This type is also known as Public Key Cryptography. In an asymmetric algorithm secret can be shared between many users who needs the particular data. RSA, Diffee Hellman, Elliptic curve are examples of Asymmetric algorithm.

Hash Algorithm: In this method computation is performed to get a hash value depending on the plain text and the key used. It is also known as on time encryption. In the receiver process the hash value is recalculated to evaluate the integrity of the data.

II Purpose of Cryptography

Cryptography is used to provide security at various levels because of these following reasons:[4]

Confidentiality : It is method to ensure that the data is read only by the intended recipient. If more people are in communication at the same instance it must be ensured that the data is not enclosed to any unauthorized users in the network. This is made possible by Encryption.

Authentication : It is necessary to provide the identity of the sender of the message. It is required to ensure the identity of the sender which is done by means of Authentication Process.

Integrity : It is a property which ensures that the message which is being transmitted is not modified by any unauthorised users intentionally or accidentally. This property is ensured by the mathematical calculation involved in the encryption process.

Non-Repudiation : This property is to prevent the sender to re transmit the messages repeatedly.
Access Control : It is the property to ensure that the swent message is viewed only by the actual receiver. This is ensured by the encryption and decryption process.

III SYMMETRIC KEY ALGORITHMS

Plain Text--→ ENCRYPTION--→ Cipher Text

KEY

Cipher Text--→ DECRYPTION--→ Plain Text

A. DES:

DES is a block cipher. It encrypts data in blocks of size 64 bits each. 64 bits of plain text is taken as input to DES, which produces 64 bits of cipher text. The key length is 64 bits [3]. DES results in a permutation among the 2^64 possible arrangement of 64 bits, each of which may be either 0 or 1. Each block of 64 bits is divided into two blocks of 32 bits each, a left half block L and right half R. The DES algorithm turns 64-bit messages block M into a 64-bit cipher block C. If each 64-bit block is encrypted individually, then the mode of encryption is called Electronic Code Book (ECB) mode. There are two other modes of DES encryption, namely Chain Block Coding (CBC) and Cipher Feedback (CFB), which make each cipher block dependent on all the previous messages blocks through an initial XOR operation. Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

B. AES:

AES is based on the substitution and permutation of the plain text . AES has 128-bit block size and a key size can vary as 128,192 or 256 bits [2]. AES operates on a 4×4 column-major order matrix of bytes, termed the state. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text.

Each round has 4 types of operation:

1. Substitution Bytes 2.Shift Rows

3.Mix Columns and 4.Xor with Round Key.

The number of cycles of repetition depends on the Keysize which are as follows:

10 cycles of repetition for 128 bit keys.

12 cycles of repetition for 192 bit keys.

14 Cycles of repetition for 256 bit keys.

Decryption is the reverse process of encryption and using inverse functions: InvSubBytes, InvShiftRows, InvMixColumns.

C. IDEA:

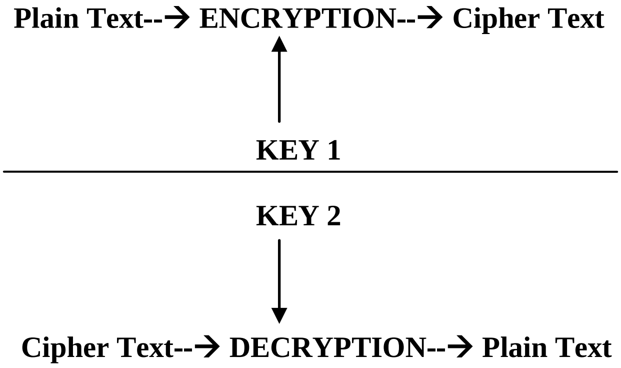
IDEA is one of the strongest cryptographic algorithms. Idea is a block cipher. It works on 64-bit plain text blocks. The key is longer and consists of 128 bits. IDEA is reversible of DES.[2]

The 64-bit plaintext block is partitioned into four 16-bit sub blocks. Four 16-bit key sub-blocks are required for the subsequent output transformation, and its generated from the 128-bit key. The key sub-blocks are used for the encryption and the decryption.[10] IDEA was used in Pretty Good Privacy (PGP).

D. BLOWFISH:

Blowfish is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data- encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes [8]. The data encryption occurs via a 16-round Feistel network . It is only suitable for application where the key does not change often, like communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

IV ASYMMETRIC KEY ALGORITHMS



Plain Text--→ ENCRYPTION--→ Cipher Text

KEY 1

KEY 2

Cipher Text--→ DECRYPTION--→ Plain Text

A. RSA

RSA is the most popular asymmetric cryptography algorithm. RSA is based on the selection of the Very large prime numbers which is used to compute the private and public keys[2] . Plain text is encrypted with public Key and the Cipher text is decrypted with the Private Key. Public Key of the users is available in public and know to all.

In Encryption process- compute *c = m^e mod n*, where the *e is* the public key, and *m* is the message block. The *c* is the encrypted message.

In Decryption process - The private key *d* is used to decrypt messages. Compute: *m = c^d mod n,* where *n* is the modulus and *d* is the private key.

Encryption and Decryption process depends on a variable ‘n’ which is computed based on the prime numbers.

RSA has three steps. 1. Key Generation 2 Encryption and 3. Decryption

B. Diffie Hellmann

Diffie-Hellman key agreement is not based on encryption and decryption. Diffe-Hellman (DH) is a method for securely exchanging a shared secret between two parties in real time untrusted network. Diffie– Hellman key exchange is a specific method of exchanging cryptographic keys [6]. It permits two parties that have no prior knowledge of each other to jointly make a shared secret key over an insecure communications channel. This key can then be used to encrypt posterior communications using a symmetric key cipher

The two parties will initially agree on a very large prime number and a generator function. Based on the agreed values both the parties will generate it s own public key and transfer it to the other party. On receiving the public key of the other party both the users will compute a function based on the received value which results in a common output. The Common value is the Shared Key for the two communicating parties.

V HASHING CRYPTOGRAPHY

A. MD5

MD5 (Message Digest5) is the commonly used cryptographic hash function with a 128-bit hash value. The input is converted into fixed length output of 128 bits. The input message is divided into fixed sized blocks of 512 bits. The algorithm depends on a

128-bit state which is divided in to 4 parts A,B,C and D. The 512 bit message block is used to modify the 128-bit state. The processing consists of 4 similar stages called rounds comprised of 16 operations which is based on the non linear functions.

B. SHA

SHA (Secure Hashing Algorithm) is a hashing algorithm. The main objective of the Hash Function is to provide Authentication rather than encryption of the Data. Several versions of SHA have been proposed based on the length of the output hash value. Variants of algorithms are SHA-0, SHA-1 and SHA-2 (2002 – 224, 256, 385, 512).

VI PERFORMANCE COMPARISON

Experimental result for encryption algorithm AES, BLOWFISH, DES, RSA are shown in the following table which have been implemented several input file sizes: 329 bytes, 778 bytes and 2048 bytes.v[3][6]

Table 1 : Performance Table

Algorithm	**File Size(bit)**	**Encryption Time(ms)**	**Decryption Time(ms)**
DES	329	284	280
	778	292	282
	2048	303	317
AES	329	287	293
	778	299	304
	2048	300	297
Blowfish	329	293	290
	778	281	278
	2048	283	279
RSA	329	462	490
	778	541	450
	2048	488	491

VII CHARACTERISTIC COMPARISON

The Comparison of Various Algorithms on the basis of Different Parameters has been listed below. [6][7][8]

Characteristic Table:

Table 2 : Characteristics Table 1

Parameters	DES	AES
DEVELOPER	IBM	Vincent Rijmen and Joan Daemen in Belgium NIST
KEY LENGTH (Bits)	64(56 usable)	128,192, 256
ROUNDS	16	10,12,14
BLOCK SIZE (Bits)	64	18
ATTACKS FOUND	Linear cryptanalysis, Differential analysis	Key recovery attack, Side channel attack

Table 3 : Characteristics Table 2

PARAMETERS	IDEA	BLOWFISH
DEVELOPER	Xuejia Lai and James in 1991	Bruce Schneier
KEY LENGTH (Bits)	128	Variable key length i.e. 32 – 448
ROUNDS	8	16
BLOCK SIZE (Bits)	64	64
ATTACKS FOUND	Linear attack	No attack is found to be successful against blowfish.

Table 4- Characteristics of table 3

PARAMETERS	RSA	Diffie Hellmann
DEVELOPER	Rivest, Adi Shamir and Leonard adleman	whitfield diffie and martin hellman
KEY LENGTH (Bits)	Key length depends on no. of bits in the module	uses key exchange management
ROUNDS	1	14
BLOCK SIZE (Bits)	Variable block size	64
ATTACKS FOUND	Brute force attack, timing attack	Eaves dropping

VIII Conclusion

In this paper we have surveyed about the different types of existing cryptographic algorithms. The performances of the some selected algorithms have been presented in this paper. In an asymmetric encryption technique the RSA algorithm is more secure as the code is complex because of its key size, tenability and also because of its use of factoring of high prime number for key generation.RSA is considered to be the efficient in storing digital signatures that cannot be repudiated. [2]Hence, RSA is found to be the best algorithm in this technique. In symmetric techniques DES is considered to be the most secured because the most efficient attack on it is still now brute force attack and AES is proven to be fast in both hardware and software. If the overall performance is considered , AES is viewed as the better algorithm. We would like to conclude that each algorithm is unique on its own way and all are useful in the real time encrypting system. The user can select the suitable algorithm depending on the need of the application. In the future, encryption algorithms may be designed to satisfy all the requirements of the user.

References:

[1]Ritu Tripathi, Sanjay Agrawal, "*Comparative Study of Symmetric and Asymmetric Cryptography Techniques*", International Journal of Advance Foundation and Research in Computer (IJAFRC),volume 1,issue 6,june 2014, ISSN 2348 – 4853.

[2] Ms. Ankita Umale, Ms. Priyanka Fulare, " *Comparative Study of Symmetric Encryption techniques for Mobile Data Caching in WMN"*, The International Journal Of Engineering And Science (IJES) ,volume 3,issue 3,page 7-12,2014, ISSN (p): 2319 – 1805.

[3]S.Pavithra, E.Ramadevi, " *Study and Performance analysis of Cryptographic Algorithms*", International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012

[4]Atul Kahate, "*cryptography and network security"*, Tata McGraw-Hill publishing company, New Delhi, 2008.

[5]William Stallings "*Network Security Essentials (Applications and Standards)*", Pearson Education, 2004.

[6]S. Abdul. Elminaam, H. M. Abdul Kader, M.M.Hadhoud, ,"*Performance Evaluation of Symmetric Encryption Algorithms*" , International Business Information Management Association (IBIMA),2009.

[7]Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "*Comparative Analysis of Cryptographic Algorithms*", International Journal of Advanced Engineering Technology, EISSN 0976-3945.

[8]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, PP877882.

[9] Gurjeevan Singh, Ashwani Kumar Singla, K.S.Sandha " *Performance Evaluation of Symmetric Cryptography Algorithms*," International Journal of Electronics and Communication Technology Volume 2 Issue 3, September 2011.

[10] Shashi Mehrotra Seth, Rajan Mishra," *Comparative Analysis Of Encryption Algorithms For Data Communication*", IJCST, Vol. 2, Issue 2, June 2011 pp.192-192