A review of encryption algorithms

M.Rajalakshmi [1], Dr.C.Parthasarathy [2]

[1] Department of Computer science and Engineering, P.T.Lee CNCET, Kanchipuram,India

[2] Department of Information and Technology, SCSVMV, Kanchipuram,India

***Abstract*—**The communication is common now a day, so the security is a main issue during data transmission. There are many cryptographic algorithms were found out and used in many applications securely. Cryptography is used to convert plain text to cipher text. This ensures the confidentiality, integrity, availability and authentication which are primary in security. Many applications use different cryptographic algorithm depends upon the requirement. But there are some attacks to those algorithms to crack the passwords and stealing the confidential data. In this paper some of the encryption algorithm is reviewed and comparative analysis is done. This paper presents the symmetric and Asymmetric encryption algorithms based on the literature review and analysis is made by comparing key size, block size, rounds of encryption, security level and the speed of the algorithm.

Keywords*— *encryption,cryptographic algorithm,cipher text,plain text.

I. INTRODUCTION

Cryptography is a technique that is used to secure data or network through encryption and decryption. It is the art of achieving security for data or message by encoding messages to make them non-readable. It is derived from the Greek word ‘crypto’ means "hidden or otherwise secret" and ‘graphy’ means “writing" so it is called cryptography means secret writing. It is used to secure communication from the third parties to maintain information securities such as data integrity, confidentiality, authentication, and non-repudiation. It transforms the messages or data to receiver side to make them secure against security attacks. The transformation of readable format into an unreadable format is called cipher text is called encryption. The unreadable format is transformed in to readable format is called decryption. Cipher text is obtained from encryption and plaint text is obtained from decryption. The message is encrypted using an encryption algorithm, which specifies how the message is to be encoded. No attackers can read the original message. Only an authorized person is able to decrypt the cipher text which requires a secret key for decryption. It is not only used to protect the information but provides authentication to the user also.

Cryptography Goals

There are some goals of cryptography that are given below:

1) Authentication: Sender and data receiver must be authenticated before sending and receiving data.
2) Confidentiality: The user who is authenticated, can access the messages
3) Integrity: Data is free from any kind of modification between sender and receiver.
4) Non-Repudiation: The sender the receiver cannot deny that they had sent a message.
5) Service Reliability: Attackers can attack on secure systems, which may affect the service of the user.

There are two types of cryptography algorithm for security

The first one is Symmetric key cryptography algorithm
The second one is Asymmetric key cryptography algorithm

Symmetric Key Cryptography

In Symmetric key cryptography only one key is used for both encryption and decryption and this is known as symmetric key cryptography. The key which is used in both encryption and decryption is called private key in symmetric key cryptography. The algorithms DES, AES, RC4, TDES are comes under the symmetric key cryptography.

Asymmetric Key Cryptography
In Asymmetric key cryptography one key is used for encryption and another key is used for decryption process and this is known as Asymmetric key cryptography. The algorithms DHA, RSA, MD5, ECC and DSA are come under the Asymmetric key cryptography.

The following terminologies were used in the cryptography
Plain text: The actual message or data that is to be transmitted to the receiver side.
Cipher text: The plain text which is converted to the unreadable format.
Encryption: The process in which plain text is converted to cipher text is known as encryption.
Decryption: The encryption process is reversed in decryption process that is the cipher text is converted to plain text.
Key: The key used in encryption and decryption are known as private keys and public keys.

II. EXISTING ALGORITHMS OVERVIEW

A. DES (Data Encryption Standard)

It was developed in the early 1975 at IBM labs by Horst Fiestel. The DES was approved by the NBS (National Bureau of Standards, now called NIST -National Institute of Standards and Technology) in 1978. The DES was standardized by the ANSI (American National Standard Institute) under the name of ANSI X3.92, better known as DEA (Data Encryption Algorithm). DES is developed in 1970s and it uses the Fiestel Structure. It is a symmetric and block cipher algorithm that is DES uses the same key for both encryption and decryption. So the sender and receiver must know the private key. The key length is 64 bits, where 8 bits are taken for parity check. It has 16 rounds of permutation process to encrypt a message. Almost the encryption and decryption process is same except, the decryption is done in reverse order.
The possible attack to DES is brute-force attack. Also there are three fast attack is possible to DES algorithm. Those are,
a) Differential Cryptanalysis
b) Linear Cryptanalysis
c) Davies Attack
DES is considered as less security, and this algorithm is not used much since this has been broken very easily.

B. TDES (Triple DES)

In cryptography techniques, Triple Data Encryption Standard (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) encryption algorithm three times to each data block. Triple-DES is also proposed by IBM in 1978 as a substitute to DES. So, 3DES is simply the DES symmetric encryption algorithm, used three times on the same data. It uses the simple DES encryption algorithm three times to enhance the security of encrypted text[1]. Triple data encryption standard is the next level of DES it was designed to break the attacks that DES met. To enhance the security, it processes DES in three times. 48 rounds are needed for TDES process and it has key length of 168 bits. By using this longer key, it applies to each block and encrypts the original text.

The TDES is also known as TDEA (Triple DES). There are three keying options. Keying option 1 is strongest and the three keys: K1, K2 and K3 are independent. In keying option 2, the two keys K1 and K2 are independent, and in keying option 3 all the three keys K1, K2 and K3 are identical.

C. AES (Advanced Standard Encryption)

In 1997, the National Institute of Standards and Technology (NIST) announced an initiative to choose a successor to DES; in 2001, it selected the Advanced Encryption Standard as a replacement to DES and 3DES. AES (Advanced Encryption standard) is developed by Vincent Rijmen, Joan Daeman in 2001. The AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in both software and hardware throughout the world for sensitive data encryption. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128 bits, 192 bits and 256 bits, respectively. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys[2]. It overcomes the drawback of DES algorithm, AES is also a symmetric and block cipher algorithm. The original name of AES is Rijindeal and published in 1977. It has 128 bit block size and key sizes are 128 (10 rounds), 192 (12 rounds) and 256 bits (14 rounds). The AES permutation process has four stages of substitute bytes, shift rows, mix columns and add round key.

1) Substitution bytes – In this step, each byte (ai,j) of matrix is replaced with a sub byte (si,j), that is Rijindeal S-Box. At the decryption end, the sub bytes are inversed to reach the original state.
2) Shift Rows - The shift rows operation, shift each rows with a certain constraint. That is first row of matrix is left same, the second, third and forth rows are shifted to one place left.
3) Mix Columns – In this step, the each column is multiplied with a fixed polynomial and the new value of the columns is placed.
4) Add Round Key – This sub key is derived from the main key and the sub key is added into this step by applying XOR to the matrix.

D. RSA (Ron Rivest- Adi-Shamir-Leonard Adleman)

The RSA (Rivest-Shamir-Adleman) algorithm is the most important public-key cryptosystem. It is best known and widely used public key scheme. This RSA algorithm uses large integers like 1,024 bits in size. It has only one round of encryption. It is asymmetric block cipher. RSA is an algorithm used by modern computers to encrypt and decrypt messages. RSA is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys are used in encryption and decryption process [3]. RSA algorithm is a public-key encryption method of having two keys called private and public keys. It is a block cipher encryption scheme and the key length of 1024 bits. RSA uses two prime numbers to generate public and private keys. These two prime numbers should be chosen randomly. The possible attacks on RSA are,

- The exponent of small number can be broken easily.
- If more receivers are getting encrypted message with same exponential, can be decrypted.
- Also the chosen-cipher text is possible.

E. RC4

RC4 is developed by Ron Rivest also known as Rivest Cipher 4. Here the stream cipher is used for encryption of the plain text. Pseudorandom stream of bits (key stream) are generated by the RC4 algorithm, and bit-wise encryption/decryption has been performed. The generation key system involves two stages,

- One is the permutation of all 256 bytes
- Another is two 8-bit index-pointers.

The key length for this RC4 is between 40-128 bits. If the common block ciphers are not used MAC strongly, bit-flapping attack is possible and the stream-cipher attack is also vulnerable if they are not correctly implemented.

F. MD5

The MD5 Message Digest algorithm is a cryptographic hash function used in many areas. Previous versions of MD5 are MD2 and MD4, and the next version to the MD5 is MD6. Here in MD5 the 128 bits that is 16 bytes of hash function is applied for encryption and decryption. In software field, MD5 is used to give assurance of the downloading files those are not met any intruder. That is the file servers provide a MD5 checksum, the user may compare this MD5 checksum with the downloading file, which confirms the file security.

G. SHA (Secure Hash Algorithm)

SHA is a set of cryptographic hash functions, have SHA-0, SHA-1, SHA-2, SHA-3. The hashing algorithms are most widely trusted and used in many applications for security. The usage of hash function is to provide index to the hash table. It is developed by NIST and published in 1993. The SHA-0 and SHA-1 are moreover same in block size (160 bits) and rounds (80). The SHA-2 has different block sizes of 224, 256, 384, 512 are denoted as SHA-224, SHA-256, SHA-384, SHA-512. The SHA-3 also has different block sizes of 224, 256, 384, 512 can be denoted as SHA3-224, SHA3-256, SHA3-984, SHA3-512.

H. ECC (Elliptic Curve Cryptography)

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller from IBM and Neil Koblitz from University of Washington as an alternative mechanism for implementing public-key cryptography. This ECC algorithm is based on algebraic structures of elliptic curves over finite fields i.e. elliptic curve theory. ECC Create Faster, Smaller and more efficient keys as compared to other encryption algorithm. In this, ECC encryption is done in elliptic curve equation form. ECC is that much efficient that it can yield a level of security with 164 bit key that other system require a 1,024-bit key to achieve that security level i.e.it givess the maximum security with smaller bit sizes which consumes less power[4] and hence, Elliptic curve cryptography is good for battery backup also. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005. It is a public-key cryptography system that is a pair of keys, one is public-key and another one is private-key. The public-key is a point (x,y) in the curve and the private-key is a random number chosen by user. The advantages of ECC algorithm is, it uses shorter key length, CPU consumption is low and memory usage is also very less.

I. BLOWFISH

Blowfish was developed by bruce schneier in 1993. It is basically a symmetric block cipher having variable length key from 32 bits to 448 bits. It operates on block size 64 bits. It is a 16-round Feistel cipher and uses large key dependent S-Boxes. Each S-box contains 32 bits of data.

Two fish

Two fish is also a symmetric block cipher having fiestel structure. It is also developed and explained by bruce schneier in 1998. Two fish also uses block ciphering like Blowfish. It is efficient for software that runs in smaller processor (smart cards) and embedding in hardware. It allows implementers to customize encryption speed, key setup time, and code size to balance performance. Two fish is license-free, un-patented and freely available for use. Two fish encryptiont uses 128, 192 and 256 bits as key size. It uses the block size of 128 bits and there are 16 rounds of encryption in this encryption algorithm.

J. IDEA (International Data Encryption Algorithm)

This algorithm is created by Xuejia Lai and James L and it was first used in 1991.The original algorithm went through few modifications and finally it got named as International Data Encryption Algorithm (IDEA)[5].IDEA is a Block cipher that operates with 64 bit plain text and 64 bit cipher text blocks and it is controlled by 128 bit key.

It has 64-bit plain text and cipher text block. For encryption purpose, the 64- bit plain text is divided into four 16 bits sub-blocks. In our discussion, we denote these four blocks as P1 (16 bits), P2 (16 bits), P3 (16 bits) and P4 (16 bits).

III. LITERATURE SURVEY

[1] Chia Long et al. paper shows a study of time and space-efficient, such as RSA and El-Gamal .RSA cryptography algorithm, encryption and decryption operations are accomplished by modular exponentiation. Fast modular exponentiation algorithms were often considered of practical significance in RSA cryptosystem. By using the technique of recording the common parts in the folded sub strings could improve the efficiency of the binary algorithm, thus can effective reduce the computational complexity of modular exponentiation.

[2] Qing Liu et al. aims at speeding up RSA decryption algorithm. EAPRSA (Encrypt Assistant Multi-Power RSA) was proposed to improve RSA decryption algorithm performance by transferring some decryption computations to encryption method. The experimental result shows that the speed of the decryption algorithm has been substantially improved.

[3] Mandal et al. designed an algorithm to combine both RSA algorithm and Diffie-Hellman Algorithm to provide a higher level of data security among other algorithms. Actually, their intent was to secure data of smaller as well as larger size by obtaining one randomly chosen key pair from set of RSA keys and one randomly chosen secret key using Diffie-Hellman algorithm and then applying RSA encryption to make even public components of Diffie-Hellman algorithm inaccessible for any eavesdropper freely.

[4] Wang et al. described a complete set of practical solution to file encryption based on RSA. With analysis of the present situation of the application of RSA, they found the feasibility of using it for file encryption. The conventional RSA used C + + Class Library to develop RSA algorithm and realized Groupware encapsulation with 32-bit windows platform.

[5] Silva et al. proposed a very simple and direct cryptographic algorithm. The technique only applied to the product of two different but equal-sized primes and was based on reversing the decimal digits of the modulus. This algorithm required less memory and was easily parallelized.

[6] Geethavani proposed a new revised blowfish algorithm and resultant cipher text that was embedded into a cover audio file using discrete wavelet transform (DWT). The resultant stage audio was transmitted to the receiver and the reverse process was done in order to get back the original plain text. The proposed method presented a steganography along with the cryptography which increases the security of the algorithm.

[7] Nagar et al. aimed to speed up the implementation of RSA during data transmission between Internet and networks which was calculated to generate the keys and then save the values of keys in the databases. In this paper a new method was applied to exchange the values of keys between gateways that contain values of public and private keys that were stored in tables inside the database.

Table 1: Comparative analysis

Algorithms	Key size	Block Size	Rounds	Security Level	Speed
DES	64	64	16	Adequte	Very slow
TDES	168,112	64	TABLE I. 48	Adequete	Very slow
AES	128,192,256	18	10,12,14	Excellent	Faster
RSA	No of bits in the module	varaible	1	Highly secure	Average
RC4	varaible	40-2048	256	good	Fast
MD5	Series of MD	512	4	Adequte	Average
ECC	smaller	variable	1	High secure	Fast
BLOW FISH	32-448	64	16	Highly secure	Very fast
TWO FISH	128,192,256	128	16	Secure	Fast
IDEA	128	64	8	Secure	Fast

CONCLUSION

The security is a main issue currently in Internet. So is it difficult to provide security among several attacks. But there are many security algorithms were developed by many authors. So it important to know the details of those algorithms to use in various applications depends upon the security level of the applications. This paper presents some algorithms which provide security in various levels and the comparison analysis is given based on some of the papers. The comparative analysis shows the various algorithms key size, block size, rounds, security level and speed of the algorithm.

REFERENCES

[1] W. Stallings, "Cryptography and Network Security: Principles and Practice", (1999), Prentice-Hall, New Jersey.

[2] J. V. Shanta, "Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard) in IJCEM International Journal of Computational Engineering & Management", vol. 15, no. 4, (2012), pp.43-49.

[3] A. Kakkar and M. L Singh, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", Published in International Journal of engg, and technology(IJET), vol. 2, no. 1, (2012).

[4] Y. F. Huang, "Algorihtm for elliptic curve diffie-Hellman key exchange based on DNA title self assembly", Proceedings of 46th IEEE Theories and Applications, (2008).

[5] M. Thaduri, S. Yoo and R. Gaede, " An Efficient Implementation of IDEA encryption algorithm using VHDL", Elsevier, (2004).

[6] Chia Long Wu , Chen Hao Hu ,"Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application", Innovations in Bio-Inspired computing and Applications(IBICA), 2012, pp. 307 – 311.

[7] Qing Liu, Yunfei Li, Lin Hao, "On the Design and Implementation of an Efficient RSA Variant", Advanced Computer Theory and Engineering (ICACTE), 2010, pp.533-536.

[8] Mandal, B.K. , Bhattacharyya , Bandyopadhyay S.K. , "Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm ", Communication Systems and Network Technologies (CSNT), 2013, pp. 453 – 461.

[9] Wang, Suli , Liu, Ganlai , "File encryption and decryption system based on RSA algorithm", Computational and Information Sciences (ICCIS), 2011, pp. 797 – 800.

[10] Da Silva, J.C.L , "Factoring Semi primes and Possible Implications for RSA", Electrical and Electronics Engineers in Israel (IEEEI), 2010, pp.182–183.

[11] Geethavani, B. , Prasad, E.V. Roopa, R. "A new approach for secure data transfer in audio signals using DWT" , pp.1-6, Sept 2013.

[12] Nagar, S.A. , Alshamma, S. , "High speed implementation of RSA algorithm with modified keys exchange", Sciences of Electronics, Technologies of Information and Telecommunications (SETIT) , Page(s): 639 – 642 , 2010.