A Review of Cryptographic Algorithms in Network Security

B.Nithya [#1], Dr.P.Sripriya [*2]

#Department of Computer Application, Vels University,
Pallavaram, Chennai, Tamil Nadu, India.
[1]nithyababu.rch@gmail.com
[*] Department of Computer Application Vels University, Pallavaram, Chennai, Tamil Nadu, India.
[2]sripriya.phd@gmail.com

***Abstract* - In the excellent growth of internet environment, there is a challenge to send data in secure. Security means sending information without any modification or hacking done by unauthorized users. The network security has the component of cryptography technique which acts like guard to the information. The general concept of cryptography is encryption and decryption. There are many cryptographic algorithms are used to send the information as cipher text which cannot be understand by the intruders. So experts have taken the existing algorithms to provide security over the network and they want to apply the benefits of those algorithms in the suitable places. First step of getting the help from algorithm is to be studied and compared their parameters. This paper presents a review that comparative study of algorithms taken by many authors.**

Keywords: Plain Text, Cipher Text, Encryption, Decryption, Attack, Security.

I. INTRODUCTION

When a computer is connected to a network, the connected systems meet many threats from the hackers. They affect the data transmission over the network. Security mechanisms should be given to the information which goes through the network. This mechanism is called cryptography. Cryptography allows the data to be sent through the network in unidentified format. This cannot be readable by the intruder. Only the sender of the information can understand the message, and the intended receiver can read the message by applying the key given by the sender. Cryptography has two concepts of encryption and decryption. Encryption is changing the plain information into unreadable form using *key*, called cipher text. The cipher text and the key will be sent to the receiver. At the receiving end the receiver will apply key on the cipher text and gets the actual information.

II. TYPES OF CRYPTOGRAPHY

Cryptography can be classified in two types,

- Symmetric key cryptography
- Asymmetric key cryptography

If there (Fig.1) is used only one key for encryption and decryption, the method is called symmetric key cryptography. The key is said to be private key. The algorithms which come under the symmetric key cryptography [18] are, DES, TDES, AES, RC4.

If two keys (Fig.2) are used for encryption that is one key is to encrypt the plain text and the other is to decrypt the cipher text, is called asymmetric key cryptography. The algorithms (Fig 4) are RSA, DHA, DSA, MD5, ECC.

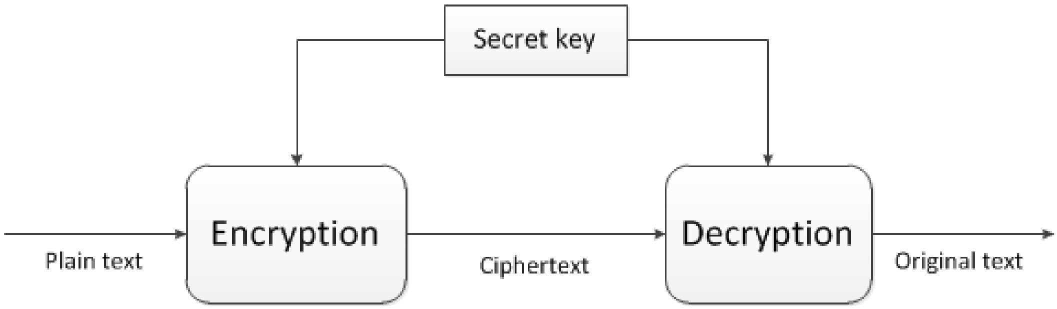

Fig 1: Symmetric Key Encryption

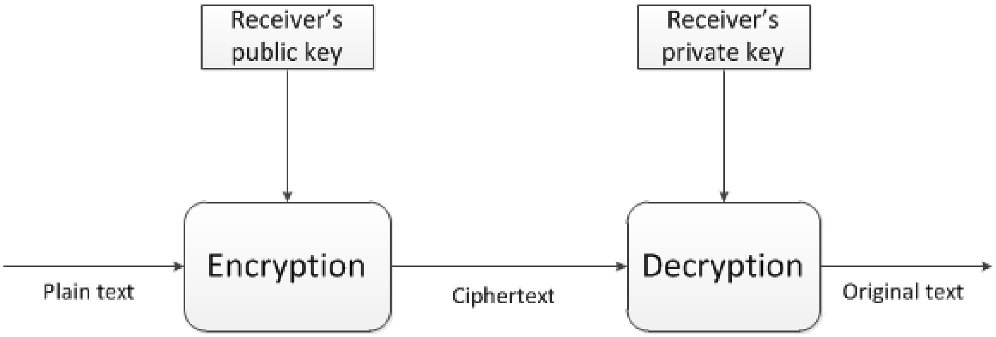

Fig 2: Asymmetric Key Encryption

III. TERMINOLOGY

A. *Plain Text:* The original message which is to be transmitted to the destination.

B. *Cipher Text:* The plain text is converted to the unreadable form. Consider the plain text "this is a cryptography technique" is converted as cipher text "Abhd&fh*vub%".

C. *Encryption*: The method converting the plain text to the cipher text is known as encryption.

D. *Decryption:* The reverse process of encryption that is converting cipher text to plain text is known as decryption.

E. *Key size:* To encrypt and decrypt, keys are important and the length of the key decides the level of security. If key length is high, security to the information is also high.

F. *Block Cipher*: The plain text is processed one block at a time, and produces output in the block of same size is known as block cipher.

G. *Stream Cipher:* The stream cipher processes plain text by continuously and output produces one element at a time.

H. *Encryption Time:* The time taken to encrypt the plain text to cipher text.

I. *Decryption Time:* The time taken to decrypt the cipher text to plain text.

J. *Throughput:* The throughput is calculated as diving the encryption time with the plain text in mega bytes.

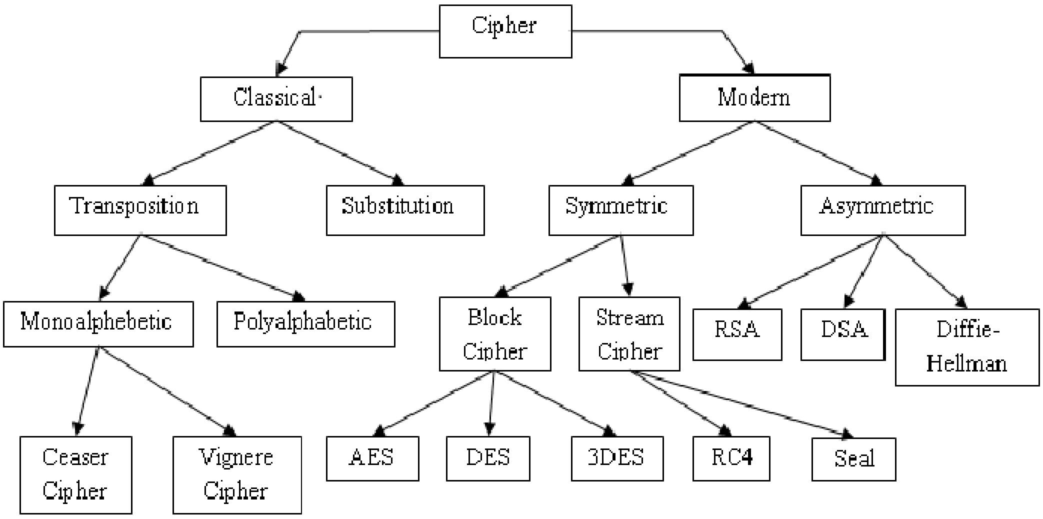

Fig 3.Existing Algorithms

IV. OVERVIEW OF THE EXISTING ALGORITHMS

This section discussed about the cryptography techniques, are used to provide security to the communication channel. The each algorithm has its own process, merits and demerits. This paper has given short description about the following algorithms (Fig.3),

- DES
- TDES
- AES

- RSA
- RC4
- MD5
- SHA
- ECC

A. DES (Data Encryption Standard)

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)

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)*

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 ($a_{i,j}$) of matrix is replaced with a sub byte ($s_{i,j}$), 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)

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)

It is a public-key cryptography system (Fig.2), 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.

V. LITERATURE SURVEY

Table 1: Study on Comparative Study of Existing Algorithms

S.No	Title	Algorithms Studied	Description	Conclusion
1	Anjula Gupta , et.al [1]	• DES • 3DES • AES • BLOWFISH • RC4 • RC2 • TWOFISH • SERPENT • IDEA • RC6 • RSA • DIFFE HELLMAN • MD5	• Compared algorithms – Key Size, Block Size, Round, Structure and Flexibility	• Blowfish - greater than all, better in performance. • Blowfish power consumption value is least
2.	Prerna Mahajan & Abhishek Sachdeva [2]	• AES • DES • RSA	• Algorithm steps • For each algorithm given process flowchart • Comparisons given in the basis of scalability, vulnerability, power consumption, security, rounds, stimulation speed • Comparison of encryption/decryption time	• AES encryption consumes least encryption time. • RSA consumes longest encryption time
3.	Mini Malhotra et.al [3]	• DES • AES • RIVEST CIPHER • BLOWFISH • RSA	• Summary of previous findings • Percentages given that research made on these algorithms.	• Last three years, research has been increased in this field • Found that RSA is widely used

		• DIFFIE – HELMAN • ELGAMAL • MD5		
4.	Gurpreet Singh, et al [4]	• DES • 3DES • AES • RSA	• Compared algorithm parameters like rounds, key length, security, speed.	• Each techniques has its own feature and used in real time applications. • AES is most efficient in speed, throughput
5	Rejani. R et.al. [5]	• DES • 3DES • AES • BLOWFISH	• Comparisons made on speed, power consumption, throughput • Simulation results for encryption decryption time	• Blowfish is best in speed • Symmetric is faster than Asymmetric • AES has more processing power
6	Shashi Mehrotra Seth et.al. [6]	• DES • AES • RSA	• Comparisons made on computation time, memory and output bytes • Experimentation taken on these algorithms with different file sizes	• DES algorithm consumes least encryption time • AES algorithm has least memory usage • RSA consume longest encryption time and memory usage is also very high
7	M.B.Nivetha, et.al. [7]	• DES • 3DES • AES • BLOWFISH • RC2 • RC6 • Hash Function (SHA-1, SHA-256, SHA-384 and SHA-512)	• Comparisons and analysis on these all algorithms • DES has no security • 3DES is more secure than DES	• SHA provided better security and less complexity due to less number of rounds.
8	Srinivas B.L et.al. [8]	• DES • BLOWFISH	• Comparisons made on speed, power consumption, throughput • Experiments made on Java Cryptography Extension and Java Cryptography Architecture. • Showed the chart of results and shown that encryption time depends on file size.	• DES and Blowfish are fastest
9	Chadi RIMAN et.al. [9]	• DES	• Explanation about new EDES	• The new E-DES

		• 3DES • AES • EDES	• Comparative analysis given on time for brute force attack, avalanche effect, time to encrypt	algorithm consumes least encryption time as compared to the other mentioned algorithms • Security is better if the key and data block size is long.
10	Nidhi singhal et.al. [10]	• AES • RC4	• Compared with different file size and made experiment on encryption time and decryption time, throughput, memory usage and CPU process time. .	• Experiments show that the RC4 is fast and RC4 is better than AES
11	Depavath Harinath et.al. [11]	• DES • TDES • AES • Blowfish	• Tests are made in JCE and JCA environment. • Evaluated by means of encryption and decryption time, throughput, and memory usage	• Triple DES needed more time to encrypt/decrypt, used less memory, and has low throughput • AES need more memory than blowfish
12	Alese, B, et.al. [12]	• RSA • ECC	• Run-time comparison made between – RSA and ECC • Test taken for key generation time, encryption/ decryption time	• RSA is better than ECC • RSA used in today’s applications like smartcards, cell phones
13	Piyush Gupta, et.al [13]	• MD5 • SHA	• Provided performance chart, similarities and compared these two with different parameters	• SHA is more secure than MD5 • MD5 is more faster than SHA on 32 bit machines
14	Gunjan Gupta et.al. [14]	• DES • TDES • BLOWFISH • AES • RC4	• Key size & Flowchart given for 1 and 16 rounds • Explained AES that performs DES trice, and given flowchart of AES steps	• Blowfish cipher is excellent • RC4 is a fast stream cipher
15	SumedhaKoushik et.al.[15]	• AES • DES • TDES • BLOWFISH • MD5 • RC4	• Using different microcontrollers done performance comparison between AES,DES,TDES, Blowfish	• AES is the best and has computer cost, better security, strongest & efficient when compared to others. • Blowfish is the fastest technique.
16	JyotiAttri et.al [16]	• DES • TDES	• Advantages and disadvantages of algorithms	• Rounds and block size not

		• AES • RC4 • RSA • DHA	• Compared symmetric & Asymmetric algorithms in speed, security and key size	present in symmetric • Asymmetric require more computational power and slower than symmetric
17	Divya Sukhija [17]	• DES • AES	• DES explained with the length of keys, ECB,OFB,CBC • Given strength & weakness	• AES is efficient and secure and DES is very fast
18	Swati Kashyap et.al. [18]	• AES • DES • 3DES • RSA	• Comparisons between DES,TDES,AES,RSA in key size, block size & rounds.	• Performance depends on throughput of encryption scheme, if throughput increases power consumption is decreased • AES is better
19	RajdeepBhanot et.al [19]	• DES • TDES • RSA • AES • ECC • BLOWFISH • TWOFISH • THREEFISH • RC5 • IDEA	• Comparative analyses are given for all these algorithms. • Described how these algorithms differ in block size, key length, rounds, level of security, attacks and speed	• Keys having more no.of bits need more computation time • Blowfish has no attack, so ECC and blowfish are more secure
20	Mansoor Ebrahim et.al [21]	• DES • 3DES • Blowfish • IDEA • TEA • CAST • Rijindeal • RC6 • Serpent • Twofish • MARS	• All symmetric algorithms except IDEA has feistel structure. • Comparative of flexibility, scalability, security.	• AES is best in security, memory usage, flexibility and Encryption performance.

VI. RESULT AND DISCUSSION

From the above literature study of comparative analysis on existing algorithms, it can be discussed that how much the study made on each algorithms. Authors have taken repeatedly, some of the existing algorithms like DES, 3DES, AES, Blowfish, RC4, RSA and MD5 algorithms. But IDEA, TEA, CAST, RC2, RC5, RC6, Serpent, Twofish, Threefish, Mars, ECC, DHA, SHA are compared and read less. The comparisons of algorithms are in the basis of security, flexibility, encryption performance, speed and memory usage.

The comparative results said that the algorithms AES, Blowfish, RC4, DES, TDES are most fast in encryption time, speed, memory when compared to others.

VII. CONCLUSION

The day to day improving internet technology needs more and fast security for the communication channel, through which the information is passing. Even many algorithms are there to provide security to the network, almost of authors have studied and compared repeatedly the symmetric algorithms. This shows that symmetric algorithms have fastest than asymmetric algorithms.

The future work can be done in comparative study of symmetric algorithms on the specific or different parameters like flexibility, speed, encryption time, scalability and memory usage. This will lead to find which one is best in all the parameters to reach better security to the complicated or unsecured network.

REFERENCES

[1] Anjula Gupta , et.al. “Cryptography Algorithms: A Review “ International Journal of Engineering Development and Research, Vol.2 No.2, (2014).

[2] Prerna Mahajan & Abhishek Sachdeva,”A study of Encryption Algorithms AES, DES and RSA for Security”, Global journal of Computer Science and Technology, Vol.8,No.15, (2013) pp.15-22.

[3] Mini Malhotra et.al. “ Study of Various Cryptographic Algorithms”, International Journal of Scientific Engineering and Research, Vol.1, No.3, (2013), PP.77-88.

[4] Gurpreet Singh, et al.” A Study of Encryption Algorithms (RSA,DES,3DES, and AES for Information Security” , International Journal of Computer Applications, Vol.67, No.19, (2013), pp.33-38.

[5] Rejani. R et.al, “Study of Symmetric key Cryptography algorithms” International Journal of Computer Techniques, Vol.2, No.2, (2015), pp.45-50.

[6] Shashi Mehrotra Seth et.al,” Comparative Analysis Of Encryption Algorithms For Data Communication”, International Journal of Computer Science and Technology, Vol.2, No.2 (2011) pp.292-294.

[7] M.B.Nivetha, et.al. “A Comparative analysis of Cryptography Algorithms”, International Journal of Innovative Research in Electrical Electronical and Instrumentation Control Engineering, Vol.2, No.10,(2014), pp.2102-2105

[8] Srinivas B.L et.al. “A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm” International Journal of Innovative Research in Computer and Communication Engineering, Vol 2, No.5, (2014), pp.77-88.

[9] Chadi RIMAN et.al. “Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey”, Information Security and Computer Fraud, Vol. 3, No. 1, (2015), pp. 1-7.

[10] Nidhi singhal et.al. “Comparative Analysis of AES and RC4 Algorithms for Better Utilization”, International Journal of Computer trends and Technology, (2011), pp.177-181.

[11] Depavath Harinath et.al. “Cryptographic Methods and Performance Analysis of Data Encryption Algorithms in Network Security” , International Journal of Advanced Research in Computer Science and Software Engineering, Vol.5, No.7 (2015), pp.680-688.

[12] Alese, B, et.al. “Comparative Analysis of Public-Key Encryption Schemes” International Journal of Engineering and Technology,Vol.2,No.9,(2012) pp. 1552-1568.

[13] Piyush Gupta, et.al “A Comparative Analysis of SHA and MD5 Algorithm”,) International Journal of Computer Science and Information Technologies, Vol. 5, No.3 (2014), pp.4492-449.

[14] Gunjan Gupta, Rama Chawla “ Review on Encryption Ciphers of Cryptography in Network Security”, International Journal of Advanced Research in Computer Science and Engineering, Vol 2, No. 7 (2012), pp.211-213.

[15] SumedhaKoushik, AnkurSinghal “Network Security using Cryptography Techniques”, International Journal of Advanced Research in Computer Science and Engineering, Vol 2, No. 12, (2012) pp.105-107.

[16] JyotiAttri, Aarti Devi, AnkushSharma&Pratibha Sharma “Study on Cryptographic Techniques in Computer Network Security”, Asian Journal of Basic Advanced Sciences, Vol 2, No. 3, pp.98-102.

[17] Divya Sukhija “Study A Review Paper on AES and DES Cryptographic Algorithms”, International Journal of Electronics and Computer Science Engineering, Vol 3, No. 4, pp.354-359.

[18] William Stallings, A Book of “Cryptography and Network Security Principles and Practice” Fifth Edition, 2006.

[19] Swati Kashyap, Er.NeerajMadan “A Review on: Network Security and Cryptographic Algorithm” International Journal of Advanced Research in Computer Science and Engineering, Vol 5, No. 4 (2015), pp.1414-1418.

[20] Rajdeep Bhanot, Rahul Hans “A Review and comparative Analysis of Various Encryption Algorithms” International Journal of Security and its Applications, Vol 9, No. 4, (2015) pp.289-306.

[21] Mansoor Ebrahim, “Symmetric Algorithm Survey: A Comparative Analysis”, International Journal of Computer Aplications” Vol.61, No.20, (2013), pp.12-19.

AUTHOR PROFILE

B.Nithya, is a research scholar in Computer Science at Vels University. Her area of interest is network security and doing research at various cryptographic techniques.

Dr.P.Sripriya, is working as associate professor at Vels University. Her area of interest is image processing. She published nearly 17 articles in scholarly journals and presented several papers in various national and international conferences.