



A Survey on Different Varied Data Communication Cryptography Methods

Dr. B. Lavanya * V.ThamizhThendral
Department Of Computer Science
University Of Madras
Chennai, Tamilnadu

Abstract: New technologies are developing rapidly and these technologies are playing vital role in our daily life. But technologies are facing a big issue on data security. In today world cryptography is keystone of computer and communication security. To provide secured data transaction or communication by using security algorithm. It is based on different concepts of mathematics such as number theory, computational – complexity theory, and probability theory. Cryptography algorithms are DES, Triple DES, AES, RSA, ECC, RC4, DSA, Hash algorithms etc., In this paper we study about various security algorithms used for data communication and their comparisons.

Keywords: Cryptography, Encryption, Big data

I. Introduction

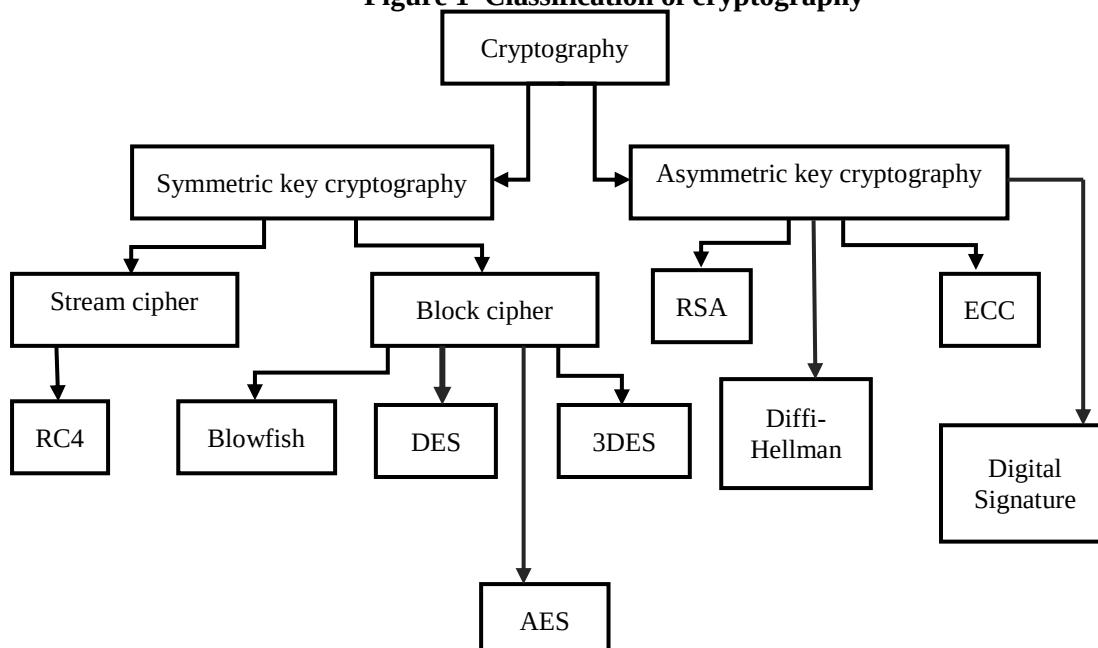
Today modern age is turning into technology age. We are transmitting information via technologies by using internet network. Some outsider or third party can attack or eavesdrop our sensitive information easily. So by using cryptography we can prevent such intruders. Cryptography is the heart of technologies for our data security. Cryptography performing two phases that is encryption and decryption [1].

Encryption: - Enciphering is the process of replacing data with unreadable code. That unreadable code also known as cipher text, encoded text, encipher text, encrypted text. Encryption is using key for encrypting the information.

Decryption: - Deciphering the cipher text into original text by using encryption key.

Key: - Key is important aspect in security algorithms. Strong encryption algorithm is built on the number of factors such as how key is created, managed, secured, size of the key and also depending on algorithm. Based on the key we categorized the cryptography into two types as shown in Figure 1.

Figure 1 Classification of cryptography



This Literature survey paper focuses on describing the encryption techniques and how it keeps sensitive information securely and comparisons of the techniques.

II. RELATED WORKS

A. DES(Data Encryption Standard)

In 1972, IBM was presented the DES security algorithm by Horst Fiestel for to prevent the sensitive data from attackers. In 1977, DES was improved as Federal Information Processing Standard (FIPS) by National Bureau of Standard [2] [3]. DES is block cipher method. DES using 64 bit key (2^{56} or 7.2×10^6) from that 56 bit used for key bit i.e. used for encode and decode the data. Another 8 bit is used as parity bit for error correction [3]. Initially carrying out permutation with 64 bit input. Next to encrypt the message performing the encoding operation 16 rounds. At final permutation output consists 16 round of the key and it is contains function of the input message and the key. Mostly used in military secret information transformation, banking industries, commercials and so on. DES cracking by using key exhaustion and brute force attack [3]. [4] To create an application for file security and in this application using **DES and LZW (Lempel- Ziv - Welch)** algorithm for secure the data. LZW is one of the data compression technique and this one is reduce the number of token reserve for 1 symbol. So level of safety is higher and data cannot be read easily by outsiders.

B. 3DES OR Triple DES

Triple DES is invented by IBM in 1988 and standardized in ANSI X9.17 and ISO 8732. 3DES was alteration of DES because it is performing the DES technique 3 times for each and every block of the information and also the advancement of the key size. Instead of performing full process of block cipher 3DES just increment the key length. Since Triple DES overcomes the disadvantage of DES like Brute force attack. The important plus point of 3DES is key size 2^{168} . The encoding and decoding of Triple DES is:

Encode:-

$c = \text{Encrypt}_{k_3} (\text{Decrypt}_{k_2} (\text{Encrypt}_{k_1} (P)))$

Decode:-

$P = \text{Decrypt}_{k_3} (\text{Encrypt}_{k_2} (\text{Decrypt}_{k_1} (C)))$ Whereas, C= Cipher text, P- plain text, k_1, k_2 and k_3 – keys.

The major weakness of 3DES is slow in Softwares because it was developed in 1972 in hardware installation with no efficient software, slow process for that reason it has 3 more time and rounds [3]. **Mayes.M.Hoobi [1]** presented the strong 3DES through combine the Triple DES and N^{th} Degree Truncated Polynomial (TPR) for the reason is to improve the high level of security of 3DES. TPR is hang on embedding message in a polynomial ring R. The ring R contain of truncated polynomial of degree N-1 and it is having the integer coefficients with this help to reduced modulo of certain parameters. The ring is $R = Z[X]/X^{N-1}$, whereas Z- set of integers, N – 1 more that the degree of the polynomial. In the proposed 3DES-TPR algorithm using 2 functions intended for advance the 3DES algorithm.

The functions are:-

i) **Enckey()** - added at encode

ii) **Deckey()** - added at decode beforehand the first round of decryption

By adding this function to increase the complexity in a block cipher and brute forced attack is also difficult to do.

C. AES(Advanced Encryption Standard)

In 2001, NIST (National Institute of Standard and Technology) introduced the AES. NIST selected the Rijndael from out of 15 candidates. After Rijndael named as AES and it is developed by Vincent Rijmen and John Daemen. AES is currently using algorithm and day-to-day continuously improving the block size 128bits with key size 128bits, 192 bits, and 256 bits. AES performing operation rounds 10, 12 or 14 for the 128bits, 192bits, and 256 bits. Process of the round is performing based on the key size [3]. AES operation is combination 4 different action.

Those operations are:-

- **Sub-bytes** – substitute byte transformation is transforming the every bite of a data item into other piece. [2]
- **Shift rows transformation** – Shift-row shifting the byte current position to another position. First row is unchanged other rows shifted cyclically by a certain offset. [2]
- **Mix columns transformation** – Composed with shift row, Mix column provide diffusion in the cipher. [2]
- **Add round key transformation**- using key schedule to derive the sub key from main key for each round [2].

Shadi Aljawarneh, Muneer Bani Yassein and we'am Adel Talafha [5] proposed a multithreaded programming approach for multimedia big data: encryption system by combining 3 major components: Feistel

Network, AES with the S-box, and the Genetic Algorithm's mutation crossover operators. AES main issue is key generation and management. So to solve this problem by using the proposed method. Feistel network imply to building the block ciphers. GA techniques covers genetic operators for example selection, crossover, mutation and the fitness function. GA is used to resolving the constraint or unconstraint optimisation problem for better quality. In each block GA integrates and joint the ciphered text and the cipher key together depending on the actions of the crossover and the mutation operators. This process performed fixed number of iterations. [6] In this paper, using ARIA algorithm. ARIA is designed by South Korea and using AES for Hadoop. The user select between theses 2 algorithm after that encrypted based on decided algorithm and distributed into data nodes with 64MB unit of HDFS blocks

D. Blowfish Encryption

In 1993, Bruce Schneier introduced the Blowfish. Blowfish is fastest, license free, unpatented, and freely available and alternative for existing encryption algorithms. it is a robust block cipher technique [3]. Blowfish is 64 bit block cipher and performing 2 operations. First operation is key expansion and second is data encryption. Blowfish doing 16 rounds of encryption and decryption process [7]. **Anupam Baruah, Lakshmi Prasad saikia** [7] using blowfish encryption to provide information security for e-banking. [8] In the paper, associate the blowfish and DCA (Defacement of Colluding Attack) encryption algorithm for to improve the data security. DCA doing pre-process the data previously enter into input of blowfish algorithm and blowfish performing its encryption process. These algorithm is having less encryption and decryption so time consuming also reduced.

E. RSA(Rivest Adi Adleman)

Adi Shamir, Leonard Adleman and Ron Rivest introduced RSA in 1978. RSA is asymmetric encryption algorithm and it is based on two product of prime numbers (p and q). RSA consist of three actions and those actions are key generation, encryption and decryption [9]. In Key generation, choose q and p. Then work out $n=p*q$, calculate $\Phi(n) = (p-1)(q-1)$, take e from $1 < e < \Phi(n)$ and then $d*e=1 \text{ mod } \Phi(n)$ this is kept as private key exponent. And the public key is (n, e) and the private key is (n, d). Encryption is $C=M^e \text{ mod } N$ where $0 \leq M \leq N$ and decryption is $p=M^d \text{ mod } N$ [2] [9]. **MukeshKumar**[10] proposed a block based symmetric algorithm that is produce the initial key using a pseudorandom prime number and their exponential values were used, promote this key was used for encoding the given secret data using RSA algorithm. To encrypt a secret data, using 512 bit key size with some combination of alphanumeric method.

F. Digital Signature(DS)

In 1991, DSA was proposed by the National Institute of Standards and Technology (NIST). After that in 1993, adopted as FIPS 186 [9]. **Digital signature has 3 phases.**

- 1) **Key generation**– choice of 2 large prime number and generates 2 keys as private and public key.
 - 2) **DS generates** – by using message, keys, and modular arithmetic to form the signature.
 - 3) **Signature verification**- using verification equation to verify the message against the original message [11].
- [12] In this paper, authors generated the digital signature process based on the hash function. Enciphering the password by using SHA1 (Secure Hash Algorithm) and this converts the original text into as fixed length of encoded string. After compress the random hash to 16bytes, output turn into as key to the algorithm AES. Next choosing key from key-base to be signing the text using AES. Embedding the keyed with signed text and sent to the receiver. After receiver verify the text by mining the key ID from message and confirm the key Id in the Key base later applying AES for decryption

G. Hash Algorithm

Hash using any mathematical function for used to map data of arbitrary size. Hash algorithm is function that is converting data string to numerical string as output if fixed string using functions. That output string must be lesser then the input string. Hash function is collision resistance, pre-image resistance and second pre-image resistance. Based on the different hash functions are MD2, MD4, MD5, SHA1, SHA2, SHA3 etc. **Vikas Goyal and Chander Kant**. [13] Proposed the Hybrid Encryption Algorithm for Ensuring the Cloud Data Security by using 3 different algorithms are ECC, AES and SHA-1. first encoded the data with the help of AES to avoid the man-in-the – middle attack, insider job attack, etc., then to provide the data integrity for user side using SHA-1 to verify later on. SHA-1 is unidirectional. Even single change in the data we can easily detect by using this algorithm. For key generation purposed using ECC technique. Finally using OTP for user name and password. By this various technique prevent the data from lots of attacks such as brute force attack, authentication attacks,

dictionary attacks and man-in-middle attack etc., [12] In this paper authors, using digital functions based on the hash function (SHA1). And SHA-1 outcome becomes as key to the AES for encrypt the data. For deciphering, first verify the text by extracting the Key ID from the message after confirmed imply the AES for decrypting.

III. Overview of Security Algorithms

The below tables are overall information's of security algorithm. Discussing in this paper mentioned algorithms.

Table 1 Algorithms Complete Information

Algorithm name	Created by	Year	Key size	block size	Rounds	Type	Flexible	Features	Attacks
DES	IBM	1975	64 Bits	64 Bits	16	Block cipher symmetric key algorithm	No	Not strong enough	Exhaustive search, man-in-the-middle attack, Davies attack, differential cryptanalysis, linear cryptanalysis, differential linear cryptanalysis
3DES	IBM	1978	112 or 168 Bits	64 Bits	48	Block cipher symmetric key algorithm	No	Best security algorithm	Man-in-the-middle attack etc.,
AES	Joan Daeman and Incent Rijmen	1998	128,192,256 Bits	128 Bits	10,12 or 14	Block cipher symmetric key algorithm	Yes	Security is excellent.	Biclique attack, related – key attack etc.,
Blowfish	Bruce Schneier	1993	32-448	64 Bits	16	Block cipher symmetric key algorithm	Yes	Fastest encryption	Birthday attack, sweet32 attack, known-plain text attacked.
RSA	Rivest Shamir Adleman	1977	1024-4096	128 bits	1	Asymmetric key algorithm	No	Excellent algorithm	Timing attacks, Adaptive chosen cipher text attacks and side channel attacks
Digital signature	NIST	1997	variable	-	-	Asymmetric key algorithm	Yes	Good security and fast algorithm	Key only attack, known message attack, generic chosen message attack, directed chosen message attack etc.,

Hash algorithm has day-to-day updations and so it has lots of different algorithm types like SHA1, SHA2, and MD5. Some Hash attacks are collision attack, preimage attack, birthday attack.

IV. Results

From the above, comparisons of cryptography algorithms we are able to state that the best cryptographic methods are AES, TDES, Blowfish and the combination of DS and Hash provides the strongest algorithm. When we use DS and Hash for key generation and verification and encrypt using AES we can generate the strongest algorithm. Because compared to others still AES seemed to be strongest algorithm.

V. Conclusion

This paper performed survey about some important frequently using cryptography algorithms. These algorithms are studied and investigated well in order to help enhancing these algorithms in further to provide more security, integrity, confidentiality of the data. And the comparisons gave some idea about which is the strongest between the available security algorithms. When we combine symmetric and asymmetric algorithm it will give more accurate security features while using compression techniques to reduce the storage, bargaining on the time consumed.

References

- [1] Mayes M. Hoobi "Strong Triple Data Encryption Standard Algorithm Using Nth Truncated Polynomial Ring Unit", Journal of Science, 2017, Vol58, No. 3c.
- [2] Abood OG, Guirguis SK. A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications (IJSRP). 2018 Jul; 8(7).
- [3] Mushtaq, Muhammad Faheem, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad, and Mustafa Mat Deris Shakir. "A Survey on the Cryptographic Encryption Algorithms." Proceeding of (IJACSA) International Journal of Advanced Computer Science and Applications 8, no. 11 (2017).
- [4] Ida Bagus Ary Indraliswara, Ketut Sudarsana, Nurlaidy Joice Simamora, Vivi Novalia Sitinjak, Nurhayati Purba, Citra Kurniawan, Nurul Aziza, Dheasy Herawati, Dian Rianita, Hengki Mangiring Parulian Simarmata, Elita Modesta Br Sembiring, Ari Riswanto, Rosida Tiurma Manurung, Sofwan Hadi, M Mesiono, Andys-ah Putera Utama Siahaan, Wirda Fitriani, Diana Suita, Ramadhona Simbolon, Robbi Rahim "Application Of Data Encryption Standard And Lempel-Ziv-Welch Algorithm For File Security", international journal of engineering and technology, 7(3.2) (2018) 783-785.
- [5] Aljawarneh Shadi, and Muneer Bani Yassein. "A multithreaded programming approach for multimedia big data: encryption system." Multimedia Tools and Applications (2017): 1-20.
- [6] Song, Youngho, Young-Sung Shin, Miyoung Jang, and Jae-Woo Chang. "Design and implementation of HDFS data encryption scheme using ARIA algorithm on Hadoop." In Big Data and Smart Computing (BigComp), 2017 IEEE International Conference on, pp. 84-90. IEEE, 2017.
- [7] Anupam Baruah, Prof. (Dr.) Lakshmi Prasad Saikia "Information Security Using Blowfish Algorithm In E-Banking" International Journal of Computer Science and Mobile Computing, Vol. 6 Issue 3, March-2017, pg. 50-57.
- [8] Palak Jain, Nikhil Kumar Singh, Dr. Deepak Singh Tomar "Defacement of Colluding Attack Using Blowfish Algorithm" International Journal of Engineering and Technology, Vol 9 No.3 Jun-Jul 2017, DOI: 10.21817 /ijet /2017 /v9i3 /1709030233.
- [9] S. Nithya, Dr. E. George Dharma Prakash Raj "Survey on Asymmetric Key Cryptography Algorithms" Journal of Advanced Computing and Communication Technologies (ISSN: 2347 - 2804), Volume No. 2 Issue No. 1, February 2014.
- [10] Mukesh Kumar "Advanced RSA Cryptographic Algorithm for Improving Data Security" Part of the Advances in Intelligent System and Computing Book Series (AISC, volume 729), Cyber Security. Pp 11-15.
- [11] A. B. Nimbalkar, "The Digital Signature Schemes Based on Two Hard Problems: Factorization and Discrete Logarithm", Part of the Advances in Intelligent Systems and Computing book series (AISC, volume 729).
- [12] Asst.Prof.Dr.Shaimaa H. Shaker 1, Ghazw G. Jumaa2, "Digital Signature Based on Hash Functions" International Journal Of Advancement In Engineering Technology, Management and Applied Science (IAETMAS), Volume04 - Issue 01, January- 2017, PP. 88-99.
- [13] Goyal Vikas, and Chander Kant. "An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security." Big Data Analytics. Springer, Singapore, 2018. 195-210.