International Research Journal of Advanced Engineering and Science

ISSN: 2455-9024

A Recent Study of Various Encryption and Decryption Techniques

Sandip Thitme[1], Vijay Kumar Verma[2]

[1, 2]Dept. of CSE, Lord Krishna College of Technology Indore, India
Email address: [1]sandipthitme89@gmail.com

Abstract— *In the era of internet & smart phone every day terabytes of data are being generated. Data security over internet during communication is a great challenge. Cryptography is an integral part of data security mechanism over the internet. Cryptography makes information unintelligible to an unauthorized person. Cryptography provides confidentiality and maintains integrity to genuine users. In the past year there are various cryptographic algorithms have been developed. But every user needs a cryptographic algorithm which has highest level of security and performance. There are several algorithms with a cost performance trade off. User can choose any cryptographic algorithms which is best with requirements. In this paper we proposed a recent study of various encryption and decryption techniques. We also compare some of the existing algorithms based on certain parameters.*

Keywords— *Cryptography, encryption, decryption, confidentiality, security.*

I. INTRODUCTION

Fast development in the computer technology, smart phone and networking technology leads very fast communication and interchanging information, data among users. This causes a major concern for privacy, identity and theft. So some security mechanism must be required to ensure the security of the data. The information has to be secured and must be read or used only by people who are authorized. The data like texts, images are commonly used in communication through network. Cryptography is a standard way of securing the electronic documents. Cryptography provides data hiding and substantiation. It includes the protocols, algorithms and strategies to refuse the access of illegal users to use the secured data.

II. FUNDAMENTAL TERMINOLOGY

A. Plaintext: Plaintext is original message not formatted text to which sender wishes to communicate with the receiver.

B. Cipher text: Cipher text is generated by using encryption technique over plaintext using an algorithm. Cipher text is also known as encoded text or non-readable text.

C. Encryption: Encryption is a process of converting information into a form that is unreadable without a decoding key.

D. Decryption: Decryption is a reverse process of encryption. Decryption process converts a cipher text into a plaintext of original message.

E. Key: A key is a secret code and a value that is used to encrypt or decrypt a message. It is a numeric or alpha numeric text or may be combination of both.

III. NEED OF CRYPTOGRAPHY

In data and information are communicated over the networks cryptography is necessary. There are five primary objectives of cryptography today

1. *Privacy/confidentiality*: Ensuring that no one can read the message except the intended receiver.
2. *Authentication*: The process of proving one's identity.
3. *Integrity*: Assuring the receiver that the received message has not been altered in any way from the original.
4. *Non-repudiation*: A mechanism to prove that the sender really sent this message.
5. *Key exchange*: The method by which crypto keys are shared between sender and

IV. TYPES OF CRYPTOGRAPHIC TECHNIQUE

There are several ways of classifying cryptographic algorithms. We categorized based on the number of keys that are employed for encryption and decryption.

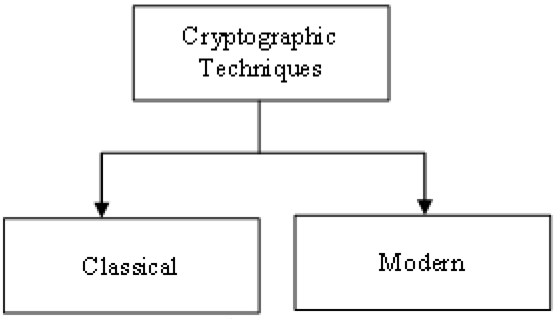

Fig. 1. Types of cryptographic techniques.

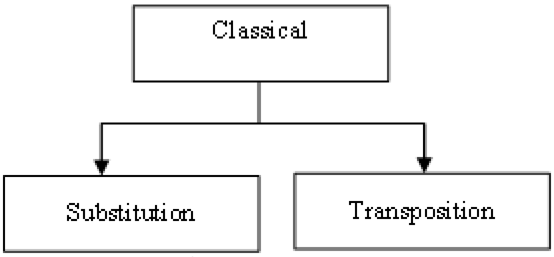

Fig. 2. Types of classical cryptographic techniques.

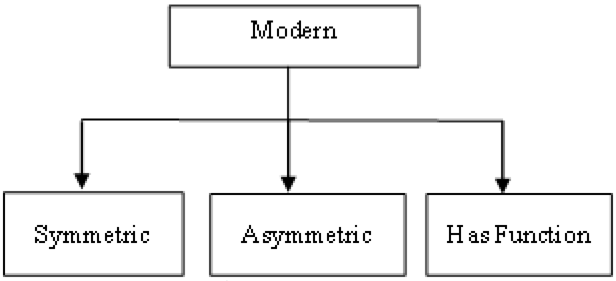

Fig. 3. Types of modern cryptographic techniques.

1. Symmetric Key Cryptography (SKC): Uses a single key for both encryption and decryption; also called symmetric encryption. Primarily used for privacy and confidentiality.

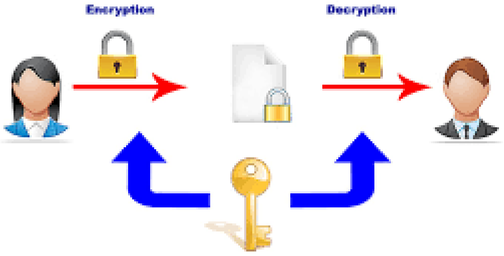

Fig. 2. Secret key cryptography techniques.

2. Asymmetric Key Cryptography (AKC): Uses one key for encryption and another for decryption; also called asymmetric encryption. Primarily used for authentication, non-repudiation, and key exchange.

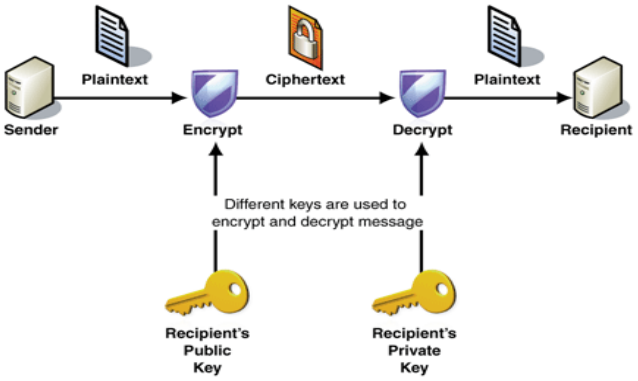

Fig. 3. Asymmetric key cryptography technique.

3. Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.

V. RELATED WORKS

In 2011 B. Ravi Kumar & Dr. P. R. K. Murti proposed "Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology". In the proposed method they stuff a new bit in the place of unused bit which is shifting from another printable character. In the proposed method after encryption, for every eight bytes of plain text it will generate seven bytes cipher text and in decryption, for every seven bytes of cipher text it will reproduce eight bytes of plain text. The proposed approach is very effective in complexity and security [1].

In 2012 Neha Jain & Gurpreet Kaur proposed "Implementing DES Algorithm in Cloud for Data Security". They showed that by using DES cipher block chaining eliminates the fraud that occurs today with stolen data. There is no danger of any data sent within the system being intercepted, and replaced. The system with encryption is acceptably secure, but that the level of encryption has to be stepped up, as computing power increases. Results in order to be secure the system the communication between modules is encrypted using symmetric key [2].

In 2013 Mansoor Ebrahim & Shujaat Khan proposed "Symmetric Algorithm Survey: A Comparative Analysis". They proposed performance study of the most popular symmetric key algorithms by using some parameter like Authentication, Flexibility, Reliability, Robustness, Scalability and Security. They also highlight the major weakness of the mentioned algorithms, making each algorithm's strength and limitation transparent for application [3].

In 2013 Sombir Singh & Sunil K. Maakar "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques". To improve the security of DES algorithm they add transposition technique before the DES algorithm to perform its process. By using an Enhanced DES algorithm the security has been improved. If the transposition technique is used before the original DES algorithm then the intruder required first to break the original DES algorithm and then transposition technique. So the security is approximately double as compared to a simple DES algorithm [4].

In 2013 Mini Malhotra & Aman Singh proposed "Study of Various Cryptographic Algorithms". They proposed a study over AES, DES, RSA, Diffie-Hellman, RC4, Blow Fish, El-Gamal, MD5 and Miller-Rabin. They provide a study of the research work done in the cryptography field and various cryptographic algorithms being used, through a literature survey between the years 2008 and 2013. They study provide a direction to the naive users and will allow many new future applications [5].

In 2014 K.B. Priya Iyer & R. Anusha proposed "Comparative Study on Various Cryptographic Techniques". They proposed a comparative study on different cryptographic algorithms such as AES, DES, clefia, speck and RSA etc. They show that RSA is found to be the best algorithm. In symmetric encryption technique throughput is increased, power is decreased and because of which the speed is fast and is viewed as a good technique [6].

In 2015 Jitendra Singh Chauhan & S. K. Sharma proposed"A Comparative Study of Cryptographic Algorithms". They proposed the performance of existing cryptographic methods like RSA, AES, Blowfish, DES, Elliptic Curve, MD5, SHA and RSA algorithms. Based on their experimental result they concluded that MD5 algorithm takes least encryption time whereas, RSA takes largest encryption time. They also found that Decryption of Blowfish algorithm is better than other algorithms, whereas, hashing based algorithms does not require decryption [7].

In 2015 Nivedita Bisht & Sapna Singh proposed “A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms” They provide a comparative study between various encryption algorithms like AES, DES, RSA and DIFFIE-HELLMAN. They used different factors of both symmetric key and asymmetric key encryption algorithm. In the symmetric key encryption AES algorithm is found to be better in terms of cost, security. In asymmetric key encryption RSA algorithm is better in terms of speed and security [8].

In 2015 Rajdeep Bhanot & Rahul Hans proposed “Review and Comparative Analysis of Various Encryption Algorithms”. They analyzed ten data encryption algorithms DES, Triple DES, RSA, AES, ECC, BLOWFISH, TWOFISH, THREEFISH, RC5 and IDEA. Among them DES, Triple DES, AES, RC5, BLOWFISH, TWOFISH, THREEFISH and IDEA are symmetric key cryptographic algorithms. RSA and ECC are asymmetric key cryptographic algorithms. They analyzed various encryption algorithms on the basis of different parameters and compared them to choose the best data encryption algorithm. They show that the strength of the each encryption algorithm depends upon the key management, type of cryptography, number of keys, number of bits used in a key [9].

In 2016 Ankita Verma & Paramita Guha , Sunita Mishra proposed “Comparative Study of Different Cryptographic Algorithms”. They classified Encryption Algorithm into Symmetric and Asymmetric Encryption and present a comparative survey on its types like AES, DES, RSA and BLOWFISH. Each algorithm has been compared on different set of parameters. From the results they found that among the symmetric encryption algorithm, AES and Blowfish are the most secure and efficient. In case of asymmetric encryption algorithm, RSA is secure and can be used for application in wireless network because of its good speed and security [10].

VI. Comparative Analysis

Technique	Description	Use
Symmetric	Single key to encrypt and decrypt data	Used for large amount of data
Asymmetric	Use mathematical related private /public key pair to encrypt and decrypt data	Commonly Used for Email message
Has Function	Use hash function to encrypt and decrypt data	Generally used in credit card encoding message

VII. Conclusion

They last decades several new and efficient symmetric encryption technique and asymmetric encryption techniques have been proposed. But the important factor for each and every techniques is depends on the four basis issue first one is strength of key used, second key management and third number of keys and fourth is number of bits used in a key.

References

[1] B. R. Kumar and Dr. P. R. K. Murti, “Data encryption and decryption process using bit shifting and stuffing (BSS) methodology,” *International Journal on Computer Science and Engineering*, vol. 3, no. 7, pp. 2818-2827, 2011.

[2] N. Jain and G. Kaur, “Implementing DES algorithm in cloud for data security,” *VSRD International Journal of CS & IT (VSRD-IJCSIT)*, Vol. 2, issue 4, 2012.

[3] M. Ebrahim and S. Khan, “Symmetric algorithm survey: A comparative analysis,” *International Journal of Computer Applications*, vol. 61, no. 20, pp. 12-19, 2013.

[4] S. Singh, S. K. Maakar, and S. Kumar, “Enhancing the security of DES algorithm using transposition cryptography techniques,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, issue 6, pp. 464-471, 2013.

[5] M. Malhotra and A. Singh, “Study of various cryptographic algorithms,” *International Journal of Scientific Engineering and Research*, vol. 1, issue 3, pp. 77-88, 2013.

[6] K. B. Priya Iyer and R. Anusha, “Comparative study on various cryptographic techniques,” *International Journal of Computer Applications, International Conference on Communication, Computing and Information Technology (ICCCMIT-2014)*, pp. 37-42, 2014.

[7] J. S. Chauhan and S. K. Sharma, “A comparative study of cryptographic algorithms,” *International Journal for Innovative Research In Multidisciplinary Field*, vol. 1, issue 2, pp. 24-28, 2015.

[8] N. Bisht and S. Singh, “A comparative study of some symmetric and asymmetric key cryptography algorithms,” *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 4, issue 3, pp. 1028-1031, 2015.

[9] R. Bhanot and R. Hans, “A review and comparative analysis of various encryption algorithms,” *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289-306, 2015.

[10] A. Verma, P. Guha and S. Mishra, “Comparative study of different cryptographic algorithms,” *International Journal of Emerging Trends & Technology in Computer Science*, vol. 5, issue 2, pp. 58-63, 2016.

[11] S. R. Shinge and R. Patil “An encryption algorithm based on ASCII value of data,” *International Journal of Computer Science and Information Technologies*, vol. 5, issue 6, pp. 7232-7234, 2014.

[12] S. A. Ubhad, N. Chaubey and S. P. Dubey, “Advanced ASCII based cryptography using matrix operation, palindrome range, unique id,” *International Journal of Computer Science and Mobile Computing*, vol. 4, issue 8, pp. 66-71, 2015.

[13] A. A. Milad and H. Z. Muda, “Comparative study of performance in cryptography algorithms (Blowfish and Skipjack),” *Journal of Computer Science*, vol. 8, issue 7, pp. 1191-1197, 2012.