A Review Paper: The Effect of Cryptographic Techniques on Data Security over a Network

[1]Sa'idu Sani, [2]Ms. Prashansa Taneja, [3]Ms. Shreya Kalta

[1]Student, [2,3]Assistant Professor
Department of Computer Science and Engineering
Alakh Prakash Goyal University, Shimla, India

***Abstract*: Nowadays, communication plays vital roles that help in the growth of new technologies. In this juncture security is an essential part to be considered. A protocol and mechanism may beneeded to help in securing the data that is transmitted. The procedure of changing the original text/data into an unreadable representation is called encryption. The process of converting an unreadable format back to the original data is known as decryption. Decryption is the process of restoring the original information from an unreadable format. Decryption is the process of transforming the unreadable format back to the original information. The encryption and decryption of data are examples of cryptographic methods. This book covers a variety of cryptographic methods, as well as the concepts of encryption and decryption and an introduction to cryptography techniques. This paper provides a comprehensive overview of cryptography techniques as well as the RSA public key cryptographic algorithm.**

***Keywords*: Cryptography, Cipher text, Plain text, Algorithm, encryption, decryption**

Introduction

The importance and the uses of exchanged data over the network or other media types are increasing; therefore the provision for the optimum solution to offer the necessary protection over the data thieves, attacks along with providing these services in time is part of the most significant matters in the security related areas. A written text, also consider as plain text, that is sent over the network is first changed into a non readable text known as cypher text, allowing the sender and the recipient to use the information. Encryption is the technical word for the procedure of changing plain text transmissions to cypher text messages.

Decryption refers to the procedure of converting cypher text back to plain text. Encryption is the polar opposite of decryption. In this communications procedure, the computer at the sender's end normally performs encryption to convert plain text messages into cypher text messages. The message is then sent via the network to the intended recipient.

The recipient's computer receives the converted message and decrypts it.[1].

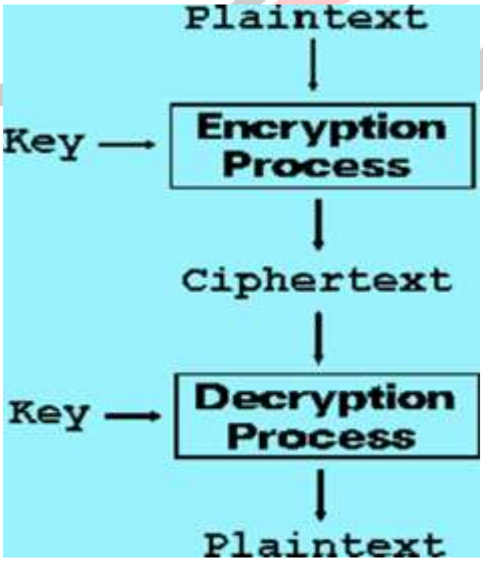

Figure1. Cryptography Process

When we think of cryptography as a form of secret coding, it performs some basic functions. Cryptography's most basic service is the capacity to permit communication between participants in such a way that prohibits others from reading it. Cryptography is important not just to ensure confidentiality, it can also solve other issues such as data integrity, authentication, and non-repudiation [2].

Another service given by cryptographic system is the provision of mechanisms that allow information to be delivered in a secure format with only the intended recipient having access to it. Continuous research into new system of cryptographic algorithms is now underway. However, it can be very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time difficulty and space complexity[3].

1. THE CRYPTOGRAPHIC PURPOSE

Cryptography is required in data transfer and telecommunications when connecting through any non-trusted channel, such as a network, particularly the Internet.
There should be some unique security considerations in the context of any application-to-application connection, including

1) Authentication: The procedure of getting one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address based, both of which are notoriously weak.)
2) Privacy/confidentiality: are uses to ensure that no one can read the message except the intended receiver.
3) Integrity: this is also the receiver ensure that the received message has not been altered in any way from the original.
4) Non-repudiation: this is another mechanism to prove that the sender really sent this message.

The cryptographic processes, are not only protecting data from theft or alteration by intruders, it can also be used for user authentication. In the field of cryptography, there are three types of cryptographic systems that are commonly employed to achieve these objectives. These types are:

1) Secret key cryptography

2) Public-key cryptography, and

3) Hash functions.

The above techniques are fully explained below. In these cases, the initial unencrypted data is referred to as plaintext. It is the conversion into cipher text, which will can simply decrypted back to usable original text.

2. The Approach of Encryption

Considering the encryption system, the original data serve as plaintext, is encrypted using an encryption algorithm, resulting in cypher text that can be read only by authorized members. Encryption is currently widely utilized in the protection of data across a wide range of platforms. It can also be used to keep data safe while it's in transit. Data transfer via networks (the Internet), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices, and bank automated teller machines are just a few examples [4].

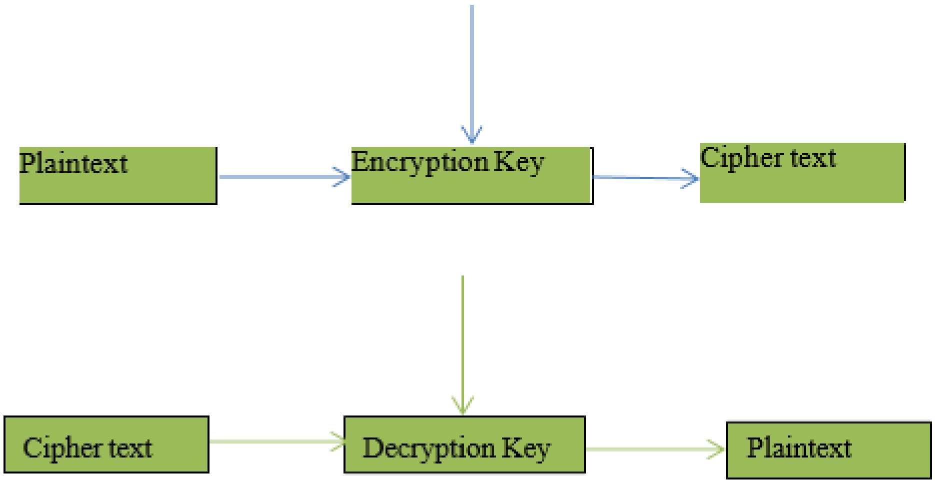

Figure 2: Encryption and Decryption Process

We have a commonly used key between the sander and the recipient the above technique is described as a private key. The private key concept is a symmetric key concept in which plain text is converted into encrypted text known as cypher text using a private key, and the cypher text is decrypted into plain text using the same as symmetric key. Both the encryption, decryption keys are frequently the same.

3. Common Techniques in Cryptography

We have two basic methods for encrypting information in cryptography: symmetric encryption (can be identify as secret key encryption) and asymmetric encryption (can also be identify as public key encryption). In one way or another, these two approaches operate differently [5].

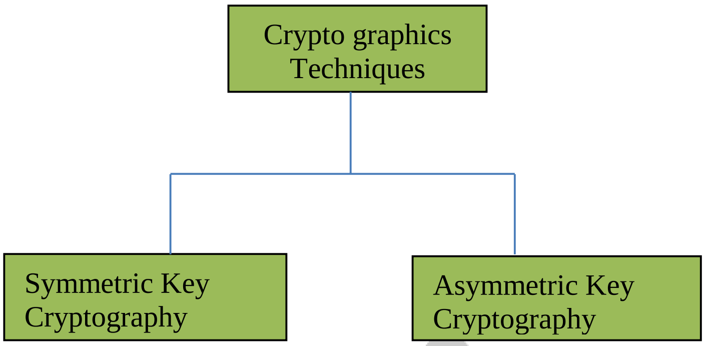
Crypto graphics Techniques
Symmetric Key Cryptography
Asymmetric Key Cryptography

Figure 3. Techniques

The symmetric encryption approach is the earliest and most well-known. It entails the use of a secret key, which can be a number, a word, or just a string of random characters that can be applied to the text of particular messages to alter its content or appearance. There are two related keys in public key encryption. The first key is a public key that anyone who wants to send you a message can use. A second is private key is kept secret, in such a way that only the sender can be able to view it[5].

a. Symmetric Key Cryptography

Private key cryptography can be consider as an encryption method in which both the sender and the recipient utilize the same key will be apply to encrypt and decrypt data. Ciphers are implemented as either block cyphers or stream cyphers in this technique. A stream cypher can use the input in cipher block format, which are blocks of plaintext rather than individual characters. This method is effective. than asymmetric cryptography.

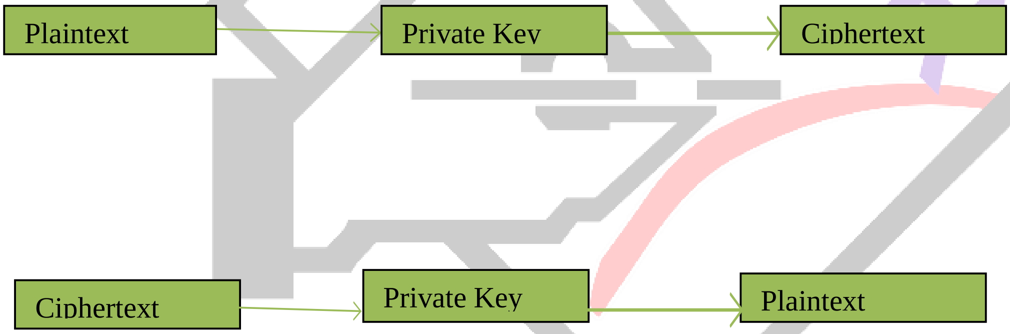

Figure 4. Symmetric key Process

b. Asymmetric Key Cryptography

Public/Asymmetric key encryption is a kind of encryption in which both the sender and the receiver utilize a separate key for encryption and decryption. One key can be used for encryption and the other can be used for decryption; the public key can be apply for encryption and the private key will be for decryption. This method is more acceptable than private/symmetric systems. [6].

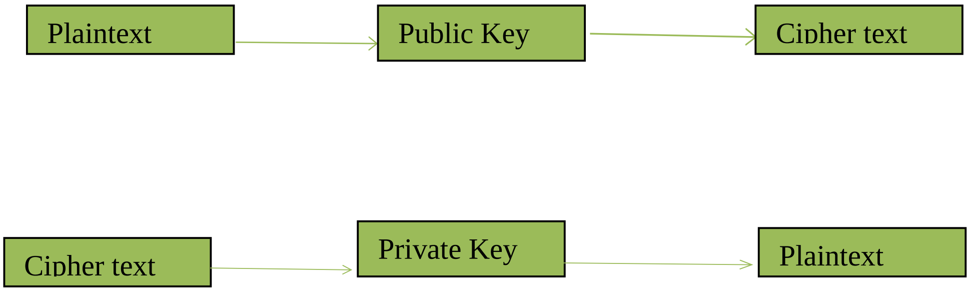

Figure 5: Asymmetric key Process

c. Hash Function

A cryptographic hash function is an algorithm that takes any amount of data as input and produces a fixed-size output of encrypted text called a hash value, or simply "hash." That encrypted text can then be saved in place of the password and used to validate the person later[7].

Cryptographic Hash is a Hash function that produces a fixed-size output from a random-size input. Calculating is simple, but retrieving original data is difficult. It's tough to duplicate the same hash with different inputs, and it's a one-way function, so reverting isn't an option. Hashing is sometimes referred to as Digest, Message Digest, Checksum, and so on[8].

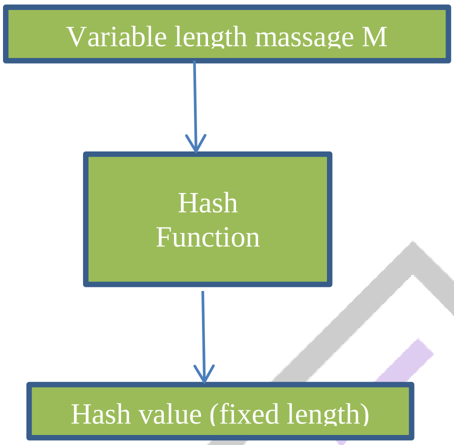

Figure 6: Hash function

4. Algorithms

For both private/symmetric and public/asymmetric key techniques in cryptography, many different types of algorithms can be employed to encrypt and decode a text. DES (Data Encryption Standard), AES (Advance Encryption Standard), Blowfish, and others are used for private (symmetric) keys, whereas RSA (Rivest, Shamir, Adlemen), Diffie-Hellman, and others are used for public (asymmetric) keys.

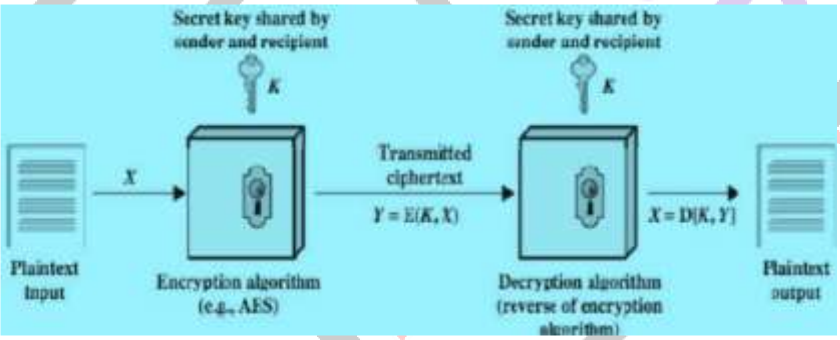
Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 6. Algorithm Method

5. AES Algorithm

The AES algorithm (which is known as Rijndael algorithm) is a private/symmetrical block cypher that converts original text in 128-bit blocks to cipher text utilizing keys of 128, 192, and 256 bits. Because it is considered secure, the AES algorithm has become a global standard.

Basic Structure of AES Algorithm

AES is instead of Feistel cipher. It is based on two common techniques to encrypt and decrypt data known as substitution and permutation network (SPN). SPN is a particular number carried out in mathematical operations that are carried out in block cipher algorithms. AES can cope with plaintext blocks of 128 bits (16 bytes) which is a constant size. AES operates on a matrix of bytes, and these 16 bytes are represented in a 4x4 matrix. Another important element of AES is the number of rounds. The number of rounds is determined by the key's length. The AES method uses three different key sizes to encrypt and decrypt data, including (128, 192 or 256 bits). The number of rounds is dictated by the key size; for example, for 128-bit keys, AES uses ten rounds, twelve for 192-bit keys, and fourteen for 256-bit keys.

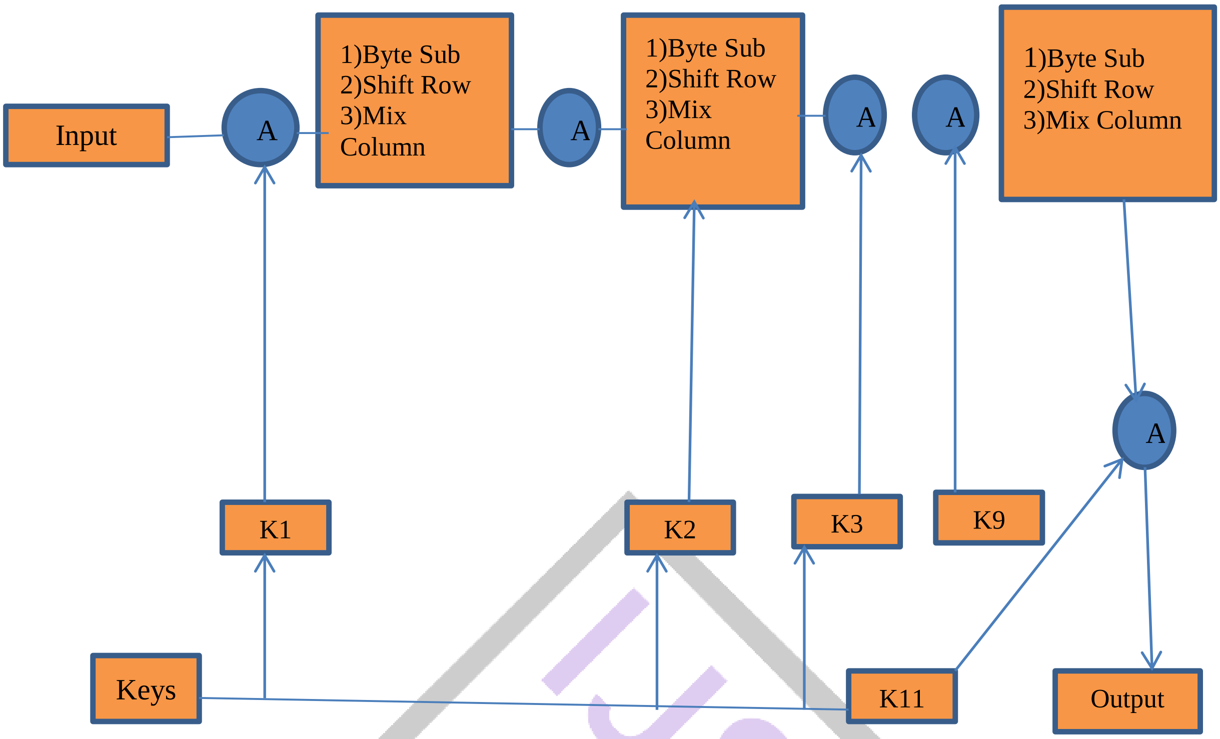

Figure 7: structure of AES algorithm

6. RSA Algorithm

In such a cryptosystem, the encryption key is made public, while the decryption key is kept private. The factoring problem, which is the practical difficulty of factoring the product of two large prime integers, is premised on this imbalance in RSA. In 1977, RSA was the first to openly describe the algorithm.

How key is generated in RSA

In RSA, a public key and a private key are utilized. Everyone may allow having access to public key, which is used to encrypt messages. Messages encrypted with the public key can only be decoded with the private key in a reasonable amount of time.[9].

The keys for the asymmetric algorithm (RSA) algorithm are generated using the following way:

i. Choose two distinct prime numbers p and q.

ii. For security purposes, the integer's p and q should be chosen at random.

iii. Compute n = pq.

iv. n is used as the modulus for both the public and private keys. The key length is its length, which is commonly given in bits.

v. Compute φ(n) = φ(p)φ(q) = (p − 1)(q − 1) = n - (p+ q -1), where φ is Euler's totient function. This value is kept private.

vi. Choose an integer e such that 1 < e < φ(n) andgcd(e, φ(n)) = 1; i.e., e and φ(n) are coprime.

vii. e is released as the public key exponent.

viii. Determine d as d ≡ e−1 (mod φ(n)); i.e., d is the modular multiplicative inverse of e (modulo φ(n)).

ix. d is kept as the private key exponent[10].

Encryption

Cipher text c corresponding to calculated as:

$$c \equiv m^e \pmod{n}$$

Decryption

Plaintext m can be calculated as:

$$m \equiv c^d \pmod{n}$$

7. Conclusion

The field cryptography is an interesting part in computer science field by considering the amount of work done to keep data/information secret. Various techniques and algorithm studied and different types of research have been done. Base on those research, the best algorithms are those which are well documented and well known and provided optimum security level. The research discussed the effect of cryptographic techniques such as symmetric, asymmetric and hash function. Each technique provided different security measure defending on the size of data apply. But asymmetric or public key cryptographic system may be seen as more scalable and provide more authentication and non-repudiation easily due to the double keys used. But there is also need to make a further study on an improved scheme such an algorithm that makes the encryption and decryption process more easily than RSA, AES and many more algorithms.

References

[1] A. Muhammad Abdullah and A. Muhamad Abdullah, “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data Call for papers View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data View project Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt,” no. June, 2017, [Online]. Available: https://www.researchgate.net/publication/317615794.

[2] S. Sharma and Y. Gupta, “Study on Cryptography and Techniques,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. © 2017 IJSRCSEIT*, vol. 1, no. 2, pp. 2456–3307, 2017, [Online]. Available: www.ijsrcseit.com.

[3] S. Vyakaranal and S. Kengond, “Performance Analysis of Symmetric Key Cryptographic Algorithms,” *Proc. 2018 IEEE Int. Conf. Commun. Signal Process. ICCSP 2018*, pp. 411–415, 2018, doi: 10.1109/ICCSP.2018.8524373.

[4] M. E. Haque, S. Zobaed, M. U. Islam, and F. M. Areef, “Performance Analysis of Cryptographic Algorithms for Selecting Better Utilization on Resource Constraint Devices,” *2018 21st Int. Conf. Comput. Inf. Technol. ICCIT 2018*, no. June 2020, 2019, doi: 10.1109/ICCITECHN.2018.8631957.

[5] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish,” *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.

[6] A. Arjunan, P. Narayanan, and K. Ramu, “Securing RSA Algorithm against Timing Attack,” *Int. Arab J. Inf. Technol.*, vol. 13, no. 4, pp. 3–8, 2016.

[7] U. Kiramat, A. Bibi, I. Farrukh, and T. Zeeshan, “Comparison of various encryption algorithms for securing data,” pp. 1–9, 2013.

[8] B. Preneel, “ECRYPT: The cryptographic research challenges for the next decade,” *Lect. Notes Comput. Sci.*, vol. 3352, pp. 1–15, 2005, doi: 10.1007/978-3-540-30598-9_1.

[9] U. Senthil Kumaran, M. K. Nallakaruppan, and M. Senthil Kumar, “Review of asymmetric key cryptography in wireless sensor networks,” *Int. J. Eng. Technol.*, vol. 8, no. 2, pp. 859–862, 2016.

[10] A. F. Mahdi, S. A. Taher, and M. R. Nsaif, “Modified Mathematical Method to Improve RSA Image Cryptosystem Algorithm,” *ARPN J. Eng. Appl. Sci.*, vol. 14, no. 2, pp. 464–469, 2019, doi: 10.36478/JEASCI.2019.464.469.