IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Cryptography- A Secure Approach for Message Communication

Riya Grover
Dronacharya College of Engineering, Gurgaon, India

Abstract: *Cryptography The goal of cryptography is to provide an end-to-end secure communication. For instance, if Person A is talking to Person B, then the goal of cryptography is that to secure this communication so that only Person A and Person B can understand this conversation and hence, it is secured. Encryption and decryption are the most efficient way to achieve the goal of data security as well as data privacy. Data security and privacy are major concerns in the world of message communication. Encryption can be defined as a technique which follows an abstraction method and hides the original data and it can be only retrieved using a key known as decryption key and this process is known as decryption. Encryption and decryption can be achieved using different techniques and methods such as for symmetric encryption algorithms used are AES, 3-DES, SNOW. Cryptography plays an important part in securing the messages through encryption and decryption.*

Keywords: Cryptography, Encryption, Decryption, Encryption Algorithms, Secure Messaging

I. INTRODUCTION

In this digital world we need a really secure system so that not everything is visible to the world and here comes the role of cryptography it provides end to end security to our communication. The instant messaging tools such as WhatsApp, the messages are sent from the client to the server and after that to its destination. Hence, this data is at a high risk of getting eavesdrop anywhere throughout its journey. So the information that ideally should be private that means that it should be only understood or received by the destination client. But there are high chances that it could have been sent to someone else. So, to make it secure we need to use cryptographic techniques.

End-to-end encryption provides the gold-standard for protecting communication. In an end-to-end encrypted system, the only people who can access the data are the sender and the intended recipient(s) – and no one else. Neither hackers nor unwanted third parties can access the encrypted data on the server.

There are two terms that defines cryptography:

1. Encryption is an important privacy tool that secures your data (messages). It scrambles the text into a secret code kind of text that can't be interpreted by hackers, cybercriminals or any other unauthorised people. When that secret code or coded message reaches to its destination, the recipients have their personal key through which they unscramble the information back into normal text which is readable by humans.
2. Decryption: Decryption is the next step after encryption. After we have encoded the data or message we need to decode it too.

1.1 Goals of Cryptography:

There are three security goals that cryptography swear by:

1. Confidentiality: It means that only authorised person that see the message and hiding the information from the unauthorised people.
2. Integrity: It states that if the information needs some modification then only an authorised person is allowed to do that.
3. Availability: It simply states that the information should be readily available to the authorised people.

1.2 Mechanism

The job of cryptography is to provide security to the information. For achieving this goal we use cryptographic algorithms. The message that needs to be send is first encrypted using the key, basically on which the cryptographic algorithm relies.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

The key is nothing but a secret piece that helps in doing encryption and decryption. So, if any attacker need to crack the message, they would require the key.

There are two types of attacks that can happen:

1. Cryptographic Attacks: In this type of attacks, attackers usually apply mathematical techniques to crack the secret key rather that following the brute force technique
2. Non-Cryptographic Attacks: In this attackers does not exploit the mathematical weakness of cryptographic algorithms rather it majorly applies brute force methods that is trying all possibilities.

1.3 Cryptographic Algorithms

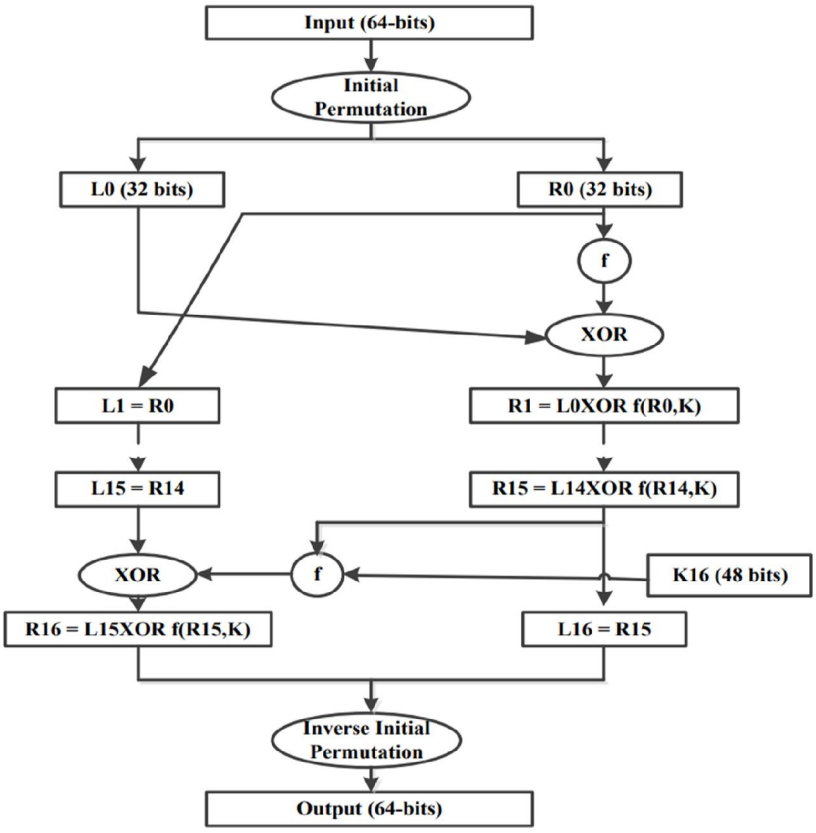
There are basically two types of encryption techniques. Those two types are the symmetric and asymmetric encoding algorithms. For example: AES, DES, 3DES, E-DES, BLOW FISH, SEAL, RC2, RC4 and RC6 which all have to do with bilateral algorithms. In contrast to RSA, ECC, EEE, DH, ELGAMAL ALGORITHM and DSA, which are relevant to unilateral algorithm.

A. DES (Data Encryption Standard)

DES was introduced in IBM in the year 1972. The aim of the DES algorithm is to offer a strategy to keep safe a crucial financial database. The encipher instructions are:

- DES receives data of 64-bit long ordinary message and 56 bit key and comes up with 64-bit block.
- The ordinary text block needs to modulate the bits.
- The 8 similar bits are eliminated from the key through exposing the key to its key permutation.

There are several steps (as shown in the diagram) through which it will produce the readable message and the key :

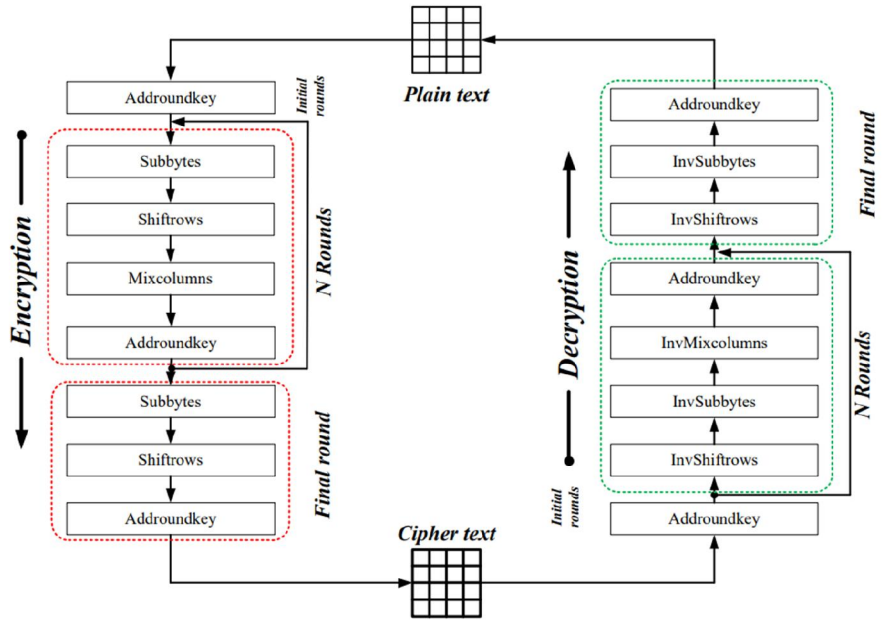


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

B. AES (Advanced Encryption Standard)

The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a128 bits block size. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the ciphertext.

During encryption-decryption, the AES process encodes 10 rounds for 128-bit keys. 12 rounds for 192-bit keys and 14 rounds to 256-bit keys to come out with the last encoded message. The following diagram shows the working of AES encryption algorithm:



II. CONCLUSION

This paper explains the concept of cryptography in the world of message communication. Further, it also explains the meaning of encryption and decryption. The result shows the techniques that are useful for real-time encryption. All encryption methods have proven to have their advantages and setbacks and have proven to be appropriate for different applications. In some previous studies, it has been indicated that AES algorithm is the most reliable one in terms of speed, encoding, decoding, flexibility etc.

REFERENCES

[1]. RIMAN, C., and Abi-Char, P. E.: Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey. Information Security and Computer Fraud, Vol.3, No.1, 1-7, (2015).

[2]. Elminaam, D. S. A., Kader, H. M. A., & Hadhoud, M. M.: Performance Evaluation of Symmetric Encryption Algorithms. International Journal of Computer Science and Network Security, Vol.8, No.12, 280-286, (2008).

[3]. Omar G. A., Elsadd, M. A., & Guirguis, S. K.: Investigation of Cryptography Algorithms used for Security and Privacy Protection in Smart Grid. In Power Systems Conference (MEPCON), 2017 Nineteenth International Middle East, IEEE, 644-649, (December 2017). 4- Sridevi, C.: A Survey on Network Security. Global Journal of Computer Science and Technology (2018).

[4]. B. A. Forouzan, "Cryptography and Network Security", TMH

[5]. A_Survey_on_Cryptography_Alalgorithms