Comparative Analysis of various cryptographic algorithms on the basis of time and block size

Mithlesh Kumar Yadav[1]

[1]*Assistant Professor, Department of Computer Engineering, School of Engineering, PP Savani University*

ABSTRACT

Data encryption is the process of protecting information. It protects its availability, privacy and integrity. To write this article we have study about information security using cryptography technique. After the analyzing different techniques of encryption, we are proposing Advance Encryption Standard (AES). The AES has the better security compared others encryption algorithm and prevent data from Spoofing. It is very efficient in both hardware and software.

Keyword: *Cryptography, Information Security, Plaintext, Key*

1. INTRODUCTION

Data Encryption is the process of converting the plaintext into Encoded form (non-readable) and only authorized person/parties can access it. Data security is an essential part of an Individual/organization; it can be achieved by the using various methods. The encrypted data is safe for some time but never think it is permanently safe. After the time goes on there is chance of hacking the data by the hacker. Fake files are transmitted in the same manner as one can sends the encrypted data. There are many algorithms available in the market for encrypting the data. Encryption Key has the major role in the overall process of data [1].

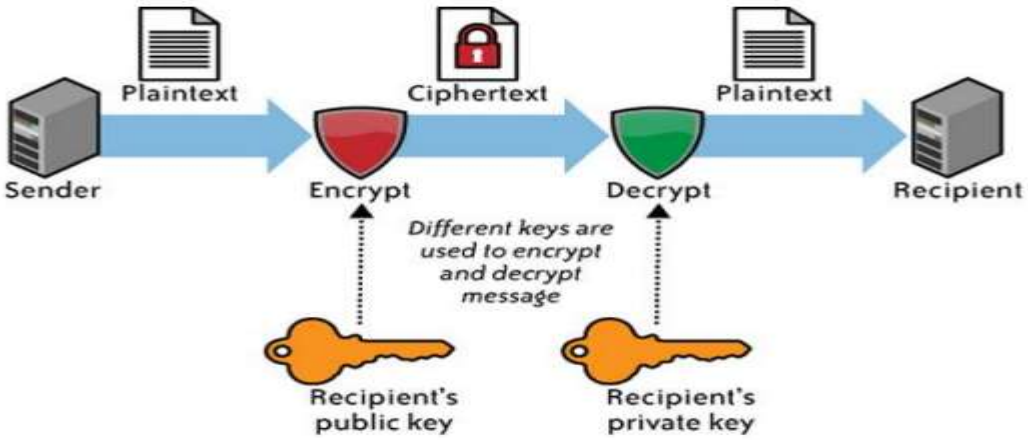

Figure 1. Encryption and Decryption

2. CRYPTOGRAPHIC APPROACHES

2.1 Data Encryption Standard (DES)

It is one of the most widely accepted, publicly available cryptographic systems today. It was developed by IBM in the 1970s but was later adopted by the US government as a national bureau of standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It uses a 56-bit key to encrypt the 64 bit block size data. It processes 64-bit inputs into 64-bit cipher-text and algorithm performs 16 iterations [1].

2.2 International Data Encryption Algorithm (IDEA)

IDEA is a block cipher designed by James Massey and Xuejia Lai and was first described in 1991. It uses 128 bit key length which operates on 64 bit blocks. It consists of a series of eight identical transformations based upon bitwise exclusive-or, addition and multiplication modules. It is based upon symmetric cipher and has very weak key design method therefore security level of the algorithm is very poor as compared to the DES. IDEA not becomes so much popular due to its complex structure [2].

2.3 Blowfish

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention [3].

2.4 Triple DES (TDES)

It was developed in 1998 and derived from DES. It applies the DES cipher algorithm three times to each of the data blocks. Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards: All keys being independent Key 1 and key 2 being independent keys All three keys being identical Key option #3 is known as triple DES. The triple DES key length contains 168 bits but the key security falls to 112 bits [4].

2.5 Twofish

It was derived from blowfish by Bruce Schneier in 1998. It is freely available in the public domain as it has not been patented. It is a symmetric key block cipher having key sizes 128,192 and 256 bits used to encrypt the 128 bit block size data in 16 rounds. The algorithm making use of S- Boxes and makes the key generation process very complex and secured [5].

2.6 Advanced Encryption Standard (AES)

It is a symmetric 128-bitblock data encryption technique developed by Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called Rijndael (pronounced Rhine Dahl or Rain Doll), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM. While the terms AES and Rijndael are used interchangeably, there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits [6]. It provides following services:

- ✓ It is a politically safe decision: the encryption standard of the US National Institute of Standards and Technology (NIST), and the US government reportedly approves AES with 192 or 256-bit keys for encrypting top secret documents.
- ✓ Nobody yet has (publicly) a full attack on AES, or a partial attack that is practical (though some impractical partial attacks exist5).
- ✓ AES is algebraically simpler than other block ciphers: effectively, it can be written as a series of mathematical equations.
- ✓ The NSA may have chosen Rijndael as they secretly know how to break it, or secretly estimated that they could develop a way to break it

3. COMPARATIVE ANALYSIS

We compare measured speed of encryption with various algorithms available as standard in Oracle JDK, using Eclipse IDE and then give a summary of various other characteristics of those algorithms. The encryption algorithms is consider here are AES (with 128 and 256-bit keys), DES, Triple DES, IDEA and Blowfish (with a 256-bit key). It's important to note right from the beginning that beyond some ridiculous point, it's not worth sacrificing speed for security. However, the measurements will still help us make certain decisions.

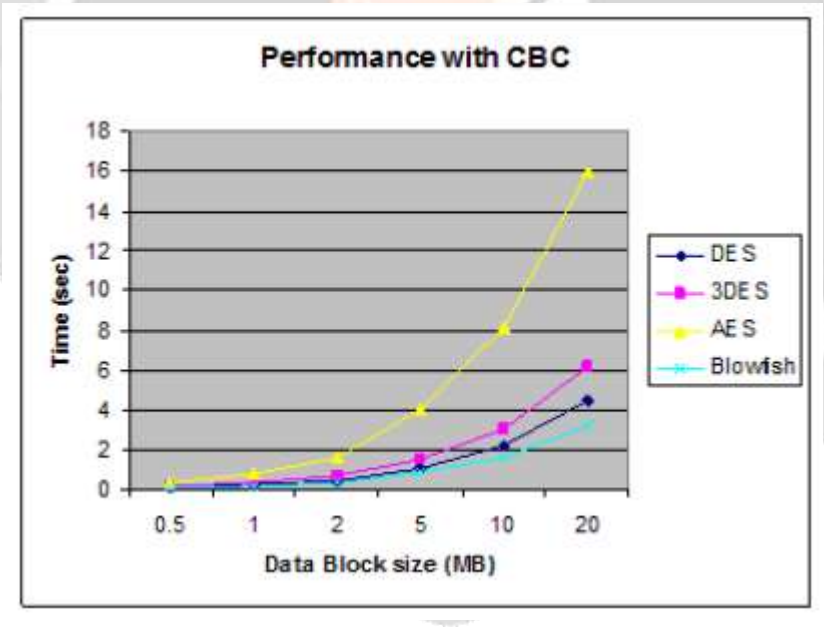

Figure 2. Comparative Analysis

4. CONCLUSION

The study of various algorithms shows that the strength of model depends upon the key management, type of cryptography, number of keys, number of bits used in a key. All the keys are based upon the mathematical properties. The keys having a greater number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data. AES data encryption is a more mathematically efficient and elegant cryptographic algorithm, but its main strength rests in the option for various key lengths. AES allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially strong. AES uses

permutation-substitution, which involves a series of substitution and permutation steps to create the encrypted block.

REFERENCES

[1] Ullah, K., Ayisha, B., Irfan, F., Illahi, I., Tahir, Z. Comparison of Various Encryption Algorithms for Securing Data. RCLIS (2020).
[2] Banerjee, B., Patel, J. A symmetric key block cipher to provide confidentiality in wireless sensor networks. Infocomp journal of computer science 15(1), 12-18 (2016).
[3] Banerjee, B., Jani, A., Shah, N. Traditional and quantum approaches against shor's algorithm: A review. International journal of research publication and reviews 2(2), 6 (2021).
[4] Banerjee, B., Jani, A., Shah, N. Post quantum security enhancement scheme for IoT blockchain framework. GIS Science Journal 7(6), 664-672 (2020).
[5] Banerjee, B. Avalanche effect: A judgement parameter of strength in symmetric key block ciphers. International journal of engineering development and research 7(2), 116-121 (2019).
[6] Banerjee, B., Patel, J. A survey on cryptographic approaches to provide privacy preservation in wireless sensor networks. International journal of Advance Engineering and Research Development 2(10), 6-9 (2015).
[7] Zeeshan Haider, Kiramat Ullah and T. Jamal, "DoS Attacks at Cooperative MAC", in Proc. of ArXiv, arXiv:1812.04935 [cs.NI], Dec. 2018.
[8] SA Butt, and T. Jamal, "Study of Black Hole Attack in AODV", in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.