Performance Analysis of Data Encryption Algorithms for Secure Data Transmission

D. Asir Antontony Gnana Singh[1] , R.Priyadharshini[2]
[1, 2]Department of Computer Science and Engineering
[1, 2] Anna University, BIT-Campus, Tiruchirappalli – 24.

Abstract-*Data security is the most challenging issue in the world and the various security threats in the cyber security has to be avoided and to give more confidentiality to the users and to enable high integrity and availability of the data. Data encryption algorithm is the primary methodology to make the system more secure and to prevent the data from third party access. So, the selection of the suitable data encryption algorithm is very essential to make the data transmission more useful and secure. The selection of the suitable data encryption algorithm is based normally on its key length, data size and its performance criterias. The encryption of the data by using the various data encryption algorithms will provide the additional security to the data being transmitted. In this paper, we analyzed the various data encryption algorithms such as DES,AES, RSA, MD5 and SHA algorithms on the basis of the various parameters and made a comparision of these algorithms.*

Keywords-Data security, Key length, Encryption algorithms, confidentiality

I. INTRODUCTION

The cryptography algorithm technique will make the data in the network secure by improvising security to them. It allows only the intended person to view the data that is sent. The cryptography is normally said to be the art of hiding the message by encryption i.e., the conversion of the message into an unreadable format (encrypted text)called the cipher text and the conversion of the message from the cipher text back to the original format is called the decryption. The data before it is decrypted is called the plain data and the data comes after it is decrypt is called the cipher text.

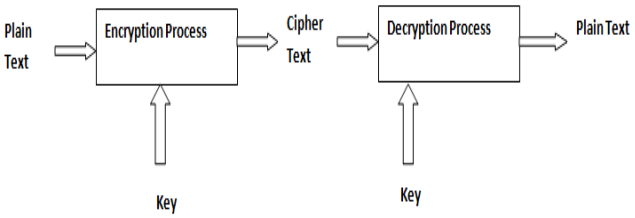

Figure1: Process of Encryption

Normally the cryptographic algorithms comes under the two broad classifications

- Symmetric encryption algorithms
- Asymmetric encryption algorithms

The Symmetric algorithms uses a single key to perform both the encryption and the decryption process. This secret key can be known only to the sender and the receiver, whereas the Asymmetric encryption algorithm or the public key systems used two keys namely the private key and the public key.. i.e., private key can be known only to the receiver and the public key can be known to everyone as it is kept public. The Asymmetric encryption is suitable in case of the security features, but the symmetric encryption is suitable in the perspective of computational strategies. The main objectives of cryptography is to provide the users Confidentiality, Integrity, Non-repudiation , Authentication , Access Control.

II. LITERATURE REVIEW

Rajdeep Bhanot and Rahul Hans developed a system to demonstrate the various data encryption algorithm to check for its security and the other performance related metrics for the symmetric key cryptographic algorithms [1].

Norman D. Jorstad conducted a survey on the various cryptographic algorithms and its metrics based on the performance and the security provided by them in a detailed manner [2].

Milind Mathur and Ayush Kesarwani designed the comparison between the six different most powerful encryption algorithm such as DES, 3DES, AES, RC2, RC6 and BLOWFISH and the performance of these algorithms are calculated based on the data loads provided to the systems [3].

Ranjeet Masram also made a comparison study on the various cryptographic algorithm which is symmetric based on the various file features like data types, data size, data density and key sizes [4].

Md Imran Alam and Mohammad Rafeek Khan aso discusses the performance and Efficiency analysis of the

various block cipher algorithms DES, 3DES, CAST-128, BLOWFISH, IDEA & RC2 of the symmetric encryption system [5]. By using the block cipher value along with its throughput, it is said that if the throughput value of the particular block cipher value increase then the power consumption value of that particular cipher is decreased and can be made vice-versa. It is proved by using the experimental results and values.

III. VARIOUS DATA ENCRYPTION ALGORITHMS

DES(Data Encryption Standard): Data Encryption Standard (DES) was initially designed by IBM and it later be adopted by the US government as the non-military and non-classified use standard encryption standard. The DES can work with the 64- bit plain text by using the 64- bit key. The DES imposes 16 complex rounds and two transposition boxes called P-boxes. The 16 rounds are iterated and the ciphers are same, but it uses a different key derived from the original key. The first and last permutations are keyless straight permutations and an inverse of each other. The Permutation takes a 64- bit key input and processes accordingly.

RSA (Rivest-Shamir-Adleman Algorithm)

The RSA (Rivest-Shamir-Adleman) algorithm is the most important public-key cryptosystem and the best known and widely used public key scheme that uses large integers like 1,024 bits in size. It has only one round of encryption and is a asymmetric block cipher. RSA is an algorithm used by modern computers to encrypt and decrypt messages. RSA is an asymmetric cryptographic algorithm that uses two different keys for encryption and decryption process. The system as asymmetric posses two large prime values namely P and Q as their product (P * Q) as an auxiliary value(I) as their public key. The auxiliary value must be kept secret. The RSA can be used as a primary algorithm for both the encryption process and the digital signatures.

The steps involved in the RSA process to perform the encryption and the decryption process.

1. Choose p and q
2. Compute n = p * q
3. Compute φ(n) = (p - 1) * (q - 1)
4. Choose e such that 1 < e < φ(n) and e and n are co-prime.
5. Compute a value for d such that (d * e) % φ (n) = 1.
6. Public key is (e, n)
7. Private key is (d, n)
8. For encryption C=me(mod n) and decryption m =cd(mod n)

AES (Advanced Encryption Standard)

In 1997 the NIST tries to developed an algorithm to overcome all the deficiencies of both the DES and 3DES. AES (Advanced Encryption standard) is developed by Vincent Rijmen, Joan Daeman in 2001. The AES is the symmetric encryption algorithm that has three block ciphers namely AES- 128, AES-192 and AES-256. Each cipher text of 128-bits are processes using the keys of 128 bits, 192 bits and 256 bits respectively. The 10 rounds are done for 128-bit keys and 12 rounds for 192-bit key and 14 rounds for 256- bit keys are present.

Each and every round in the AES are identical except the last round.

Each encryption round are processed to complete each round till n. Each round possess four rounds i.e. Substitute byte, Shift rows, Mix Column and Add round key.

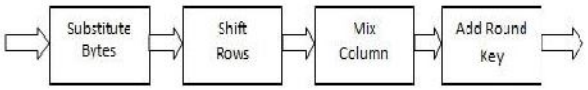

Figure 2: AES Round Steps

In AES encryption process, it uses different round keys called the state array of keys.i.e., the keys are processed to perform mathematical operations along with the arrary of keys. The data available in the AES blocks are of particular size. This encryption process includes following process:

1. First derive the different round keys from cipher key.
2. Initialize the state array with block data or plaintext.
3. Start with initial state array by adding round key.
4. Perform the process of state manipulation in nine rounds.
5. After tenth round of manipulation, we will get the final output as cipher text.

By following above process we get the final encrypted text or cipher text.

MD5(Message Digest5)

The Message Digest5(MD5) was developed by Ronald Rivest in 1992 by taking the block sizes as 512 bit and the digest size as 128 bit. The hash function producing the 128 bit hash value. The MD5 can be used as the best solution to impose the brute force attack to act against the extensive vulnerabilities and to provide excessive security.

SHA(Secure Hash Algorithm)

The Secure Hash Algorithm(SHA) is the most prominent hash algorithm used in the cryptographic systems.

It uses 160- bit which is also a resemblance of the MD5 algorithm. The SHA-1 was originally developed by th National Security Agency(NSA) to be part of the Digital Signature Algorithm.

RESULT AND DISCUSSIONS

ALGORITHM	BLOCK SIZE	KEY SIZE	SPEED	SECURITY
DES	64	56	SLOW	LESS
RSA	64	32-448	FAST	MORE SECURE
AES	128	128,192,256	FAST	MORE SECURE
SHA	512	160	SLOW	SECURE
MD5	512	128	SLOW	SECURE

Figure 3: Comparison table for the various Data encryption algorithm

The Figure and Figure represents the various data encryption algorithms and its related performance criteria to show that the various algorithm is not efficient not enough to sent the confidential encryption messages. The AES algorithm is considered among the best secure and efficient algorithm in the above mentioned all algorithms but the AES is limited to the particular key size and cannot extended above the level and it is necessary to accept the encryption algorithm that is proved to be highly secure and also it has higher key size is acceptable. So, we have to believe that the ABE is acts as an efficient algorithm in the data encryption standard and it is implemented in the next phase of the project.

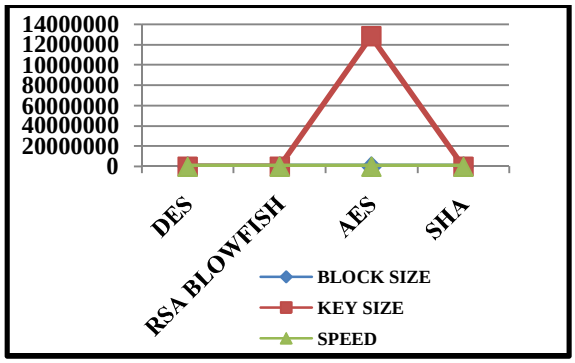

Figure 4: Graphical representation for the performance of Various Data Encryption Algorithm

IV. CONCLUSION AND FUTURE DISCUSSIONS

Form the above discussions it is proved that the AES algorithm is considered to be the most promising solution to all the data vulnerabilities present in the system and acts as an highly compromising data encryption standard for the data present in the network. By adding the higher block size to the system we can be able to increase the security and the integrity of the system.

REFERENCES

[1] D. Hakerson, A. Menezes and S. Vanston, “Guide to Elliptic Curve Cryptography”, Springer, Verlag, NY, 2004.

[2] M. Kumar and E. G. Dharma, “A comparative analysis of symmetric key encryption algorithm”, IJARCET, vol. 3, no. 2, 2014.

[3] I. Landge, T. Bharmal and P. Narwankar, “Encryption and decryption of data using two fish algorithm”, World Journal of Science and Technology, vol. 2, no. 3, pp. 157-161, 2012.

[4] J. W. Cornwell, “Blowfish Survey”, Department of Computer Science, Columbus State University, Columbus, 2002.

[5] E. Biham and A. shamir, "A differential cryptoanalysis of data encryption stamdard", Springer-verlag, 1993.

[6] Md Imran Alam*, Mohammad Rafeek Khan , “Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography ” , ISSN: 2277 128X, Volume 3, Issue 10, October 2013

[7] B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)”, [online] Available at: http://www.schneier.com/paper-blowfishfse.html.