2021 International Conference on Emerging Smart Computing and Informatics (ESCI) | 978-1-7281-8519-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ESCI50559.2021.9396926

Analysis of Encryption Techniques for Secure Communication

S. D.Sanap
Maharashtra Institute of Technology
Aurangabad, India
saritawagh1@gmail.com

Vijayshree More
Jawaharlal Nehru Enginerring College
Aurangabad, India
vijayshreemore@gmail.com

***Abstract*-The process of digitization observed among various industries has led to significant amount of collection, processing, sharing and alteration of data. The rapid continuous increase in exchange of data over networks and cloud has encouraged activities such as unauthorized access, illegal usage, alteration of transmitted and stored data. Data security issues are now becoming important as society is moving towards digital age. To get over this problem encryption techniques plays vital role. Modern encryption techniques provides solution to these problems. This paper provides an overview of encryption techniques through which data security can be enhanced. In this paper analysis of security features and steps involved in designing of most broadly used symmetric encryption algorithms like DES, 3DES, AES is done. Furthermore analysis and comparison of these encryption process according to entropy, floating frequency and histogram is done.**

Keywords— Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES)

I. INTRODUCTION

The fast progress of current information technology cause more unauthorized users to attack and misuse the information .In addition some intruders with secret intentions can do alteration of data as the target which causes enormous threats for data security. Critical data belonging to consumer is under constant threat. Lack of adequate controls on private and confidential data also rises many theft issues [19]. Encrypted communications is indeed the evaluation of data protection correspondence framework. It is helpful to analyze those standards which have different perspectives on data security, such as verification, classification and uprightness of such information.

According to the finding as per fig 1. “Data breaches are going to become expensive and results in more customer data being misused every year” [18].This global overview was released by IBM security and Ponemon Discussions with even more than 2200 IT, information security and complying experts from 477 companies were undertaken.

As per study between year 2014 to 2019, the share of breaches caused by attacks grew by 21%[21].So employment of encryption techniques is recommended for secure communication. The design of encryption algorithms should be reliable and optimized in terms of memory, power and cost. The correct assortment of algorithm is significant to gain more security necessities which protect the data to cryptanalysis. This paper explores various factors associated in the evolvement of encryption methods.

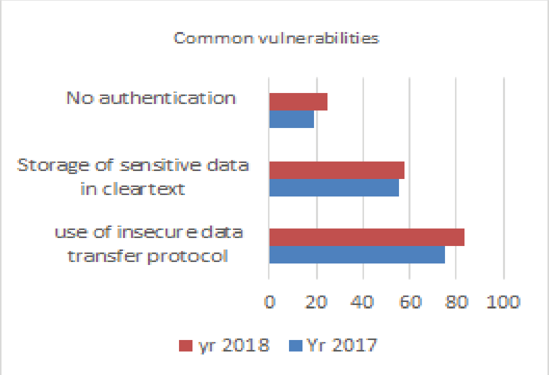

Fig. 1. Most common vulnerabilities on the network perimeter (percentage of systems)

II. LITERATURE REVIEW

A. *Encryption of Symmetric Key*

For encryption and decryption of a message, symmetric key encryption is used with an alike key. Keys are confidential and only approved senders and receivers who wish to connect are known to them. Encryption strength relies on the confidentiality of the keys. This algorithms are categorized as block and stream ciphers. Stream ciphers works on single bit at a time and incorporate feedback process to continuously alter the key [1, 3].

In block ciphers, the same key is used to encrypt a block at a time. The block cipher can work in four ways [1, 9].

1) Electronic Codebook (ECB) mode: Using the secret key to encrypt the plaintext block to form a ciphertext block, the same cipher text block will always be generated by two equivalent plaintext blocks. This is given by

$$Ck=f(\,Pk, Key) \tag{1}$$

2) Cipher Block Chaining (CBC) mode: The encryption adds a feedback mechanism. As seen in equation 2, the plaintext is Ex-ORed with the previous ciphertext block before encryption. Two similar plaintext blocks cannot encrypt the same ciphertext in this mode.

$$Ck=Pk\oplus C_{k-1} \tag{2}$$

3) Cipher Feedback (CFB) mode: The cipher is provided in this mode as feedback to the next encryption block with a new specification.

4) Output Feedback (OFB) mode: The output feedback mode is much the same as the Cipher Feedback mode, only that the encrypted output is sent as feedback instead of the actual XOR output cipher. Both bits of the block are sent instead of sending selected bits in this output feedback mode [13, 15].

B. Asymmetric key encryption:

This is generally referred to as public key encryption, in which varying encryption and decryption keys are used. The encryption key is also referred to as a public key and can be used to encrypt key messages. The decryption key is a hidden key [2].

C. Design and structures of algorithms

1) RSA: It is among best public key cryptosystem. A variable key size encryption block and variable size key are used [5]. To produce the public and private keys, it requires two prime numbers. In general, construction is carried out in following steps as follows [17]

- Randomly select two distinct p1 and q1 prime numbers.
- Compute n=p1 *q1
- Select a number such that 1<e<$\emptyset(n)$
- Calculate $\emptyset(n) = (p-1)(q-1)$ (3)
- Now calculate private key d=(k*<$\emptyset(n) + 1)/e$Where k is an integer
- Public key is formed by n and e
- Ciphertext C=p^e mod n where p is plaintext

2) Data Encryption Standard (DES)

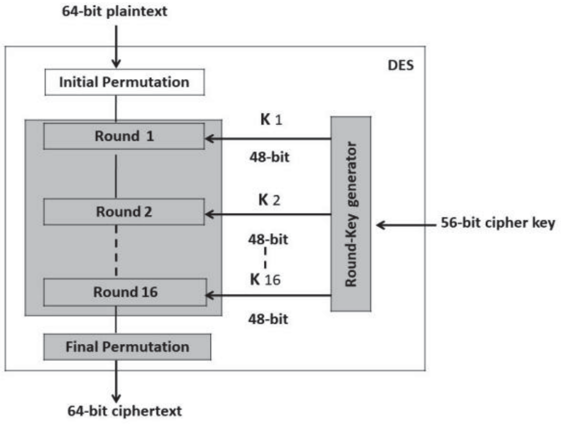

Fig. 2. DES

In DES mainly three steps are performed as Initial and final permutation, Round function and Key generation [9, 11].

3) Triple Data Encryption Standards (3DES): It is designed to improve protection with longer keys. Three keys are used for encryption process [12].

$$C=Eki3(Dki2(Eki1(P))) \tag{4}$$

$$Plaintext=Dk1(Ek2(Dk3(C))) \tag{5}$$

Keying options in 3DES

- k =3x56=168 bits
- ki1 and ki2 independent and ki3=ki1=2x56=112 bits
- ki1 =ki2=ki3=56 bits key+8 bits for error detection=64 bits

4) Advanced Encryption Standard (AES): Due to evolution in internet technology, highly secure algorithms are needed. As there are many weakness in RSA, DES and 3 DES replacement of these algorithm was needed .So AES was selected as more secure algorithm. AES is based on concept of substitution and permutation [4]. Three types of key options are available in AES as 128 bits, 192 bits and 256 bits with round set of 10,12 and 14 respectively[8,10].

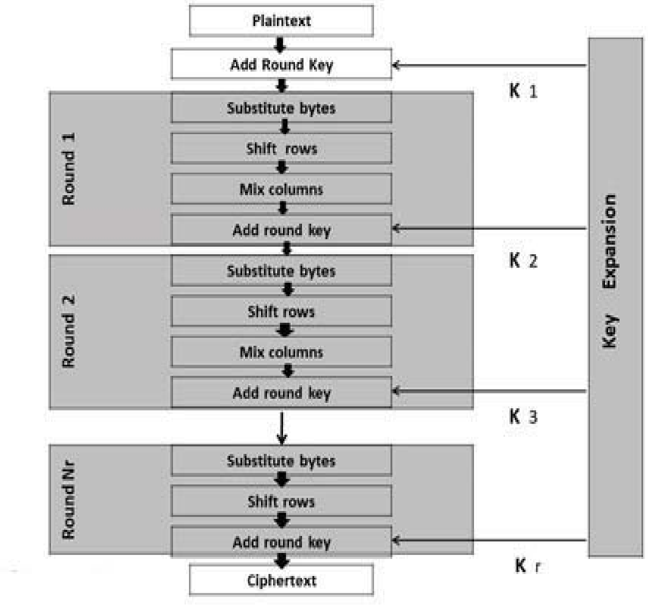

Fig. 3. Rounds of AES

Each round function consists of four transformation as

- Substitute byte: A byte substitution is done using a nonlinear table called S-box. This is done for achieving resistance against differential cryptanalysis. In first part multiplicative inverse in GF(2^8)is calculated with fi(x)=xi8+xi4+xi3+xi+1.In second part affine transformation is applied [16].
- Shift rows: SR transformation is a cyclic shift of each row by different byte offsets. No change in first row, while second is one shifted. The third row shift by twice and fourth row is shifted thrice [14].

- Mix columns: Each column of four is transformed by mathematical function. The columns are taken as polynomials over GF(2^8) and multiplied modulo x^4+1 with polynomial a1(xi).

$$a1(xi)=\{03\}xi3+\{01\}xi2+\{01\}xi=\{02\} \qquad (6)$$

- Add a round key: In this transformation, an XOR operation attaches a round key to the state. Each round key is made up of Nb words added in the state [7].

III. PROPOSED METHODOLOGYY FOR ANALYSIS

Entropy, histogram and floating frequency are important parameters for comparison of above elaborated algorithms .Tests are executed on intel core i3 8130U CPU,2.20Ghz machine using Cryptool. The modern symmetric and the asymmetric encryption algorithms, and the key management functions are based on the Secude toolkit. [20] The methods available include both classic methods and modern cryptosystems. The text files of various sizes are used to conduct experiments, where a comparison of three algorithms RSA, DES including its modes and AES is carried out. Performance evaluation based on cryptanalytical measurement is done. The details can be interpreted as a message source from the information theory point of view. The probability allocation of these source files is analyzed to calculate the information quality. The individual messages are believed to be stochastically independent of each other and to be distributed with a uniform probability by the source.

IV. IV. RESULTS AND DISCUSSION

A. Entropy:

The entropy of a text is an index of the content of its knowledge. The entropy is calculated per character in bits. It is a distinctive distribution that calculates the average volume of data that can be collected by observation. [20]

“E (pt[1], pt[2],..., pt[r]):= - [pt[1] * log(pt[1]) + pt[2] * log(pt[2]) +... + pt[r] * log(pt[r])]” (3)

Where pt[i] is probability with which data is generated. It is an index of its data content in a document. For same input text file entropy achived is as per table I.From observation it is conluded that AES has highest entropy.High entropy gives more security as it less vulnerable.

TABLE I. ENTROPY

Encryption Technique	Entropy achieved (Maximum possible is 8)
RSA	5.99
DES (ECB)	5.83
DES(CBC)	5.89
3DES(ECB)	5.90
3DES(CBC)	5.93
AES	6.03

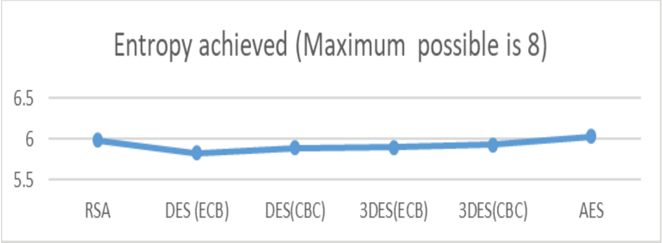

Fig. 4. Entropy

B. Histogram:

It gives the frequency distribution of the characters.If histogram is uniform that means algorithm is robust. The histogram displays the distribution of frequencies of the characters. Histogram observed for same input text for all mentioned algorithm is as follows. This parameter plays important role in healthcare information system. In ECB mode of DES and AES gives variation in frequency of occurrence.

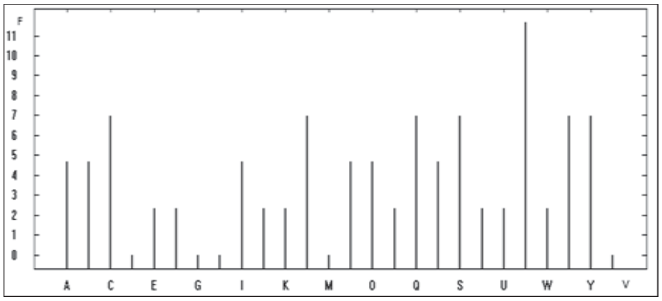

Fig. 5. Histogram of RSA

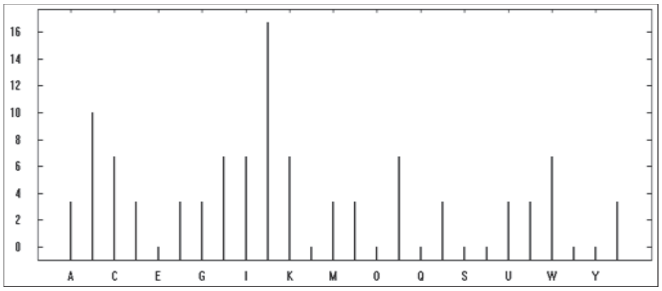

Fig. 6. Histogram of DES(ECB)

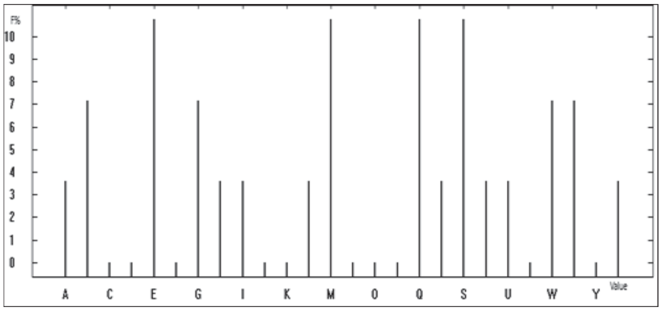

Fig. 7. Histogram of DES (CBC)

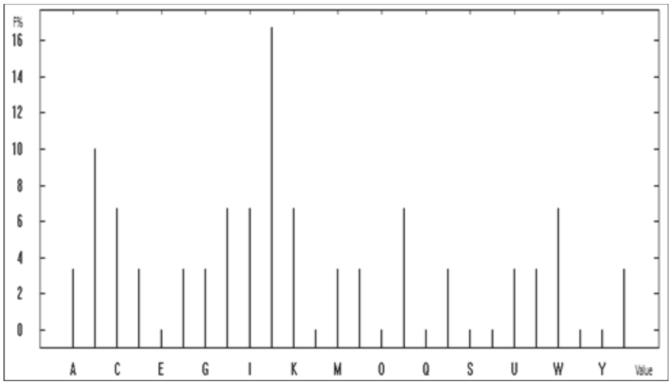

Fig. 8. Histogram of 3DES (ECB)

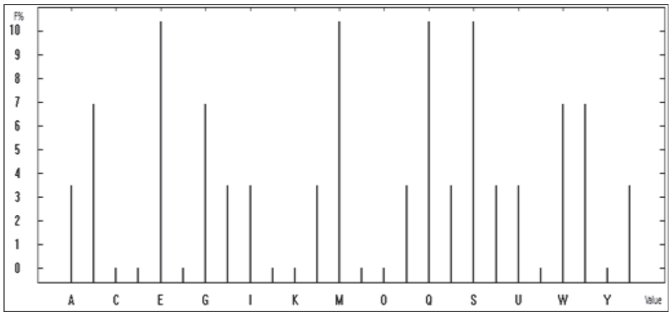

Fig. 9. Histogram of 3DES (CBC)

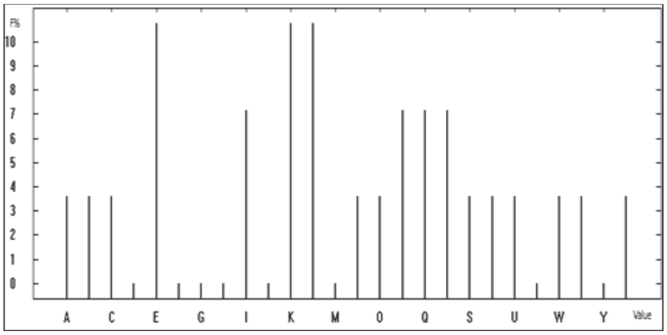

Fig. 10. Histogram of AES

C. *Floating frequency:*

The floating frequency at each point in the document is a feature of its local information material. The floating frequency determines numbers of different characters in any given 64-character section of the text can be found. Comparatively more number of different characters are found in AES.

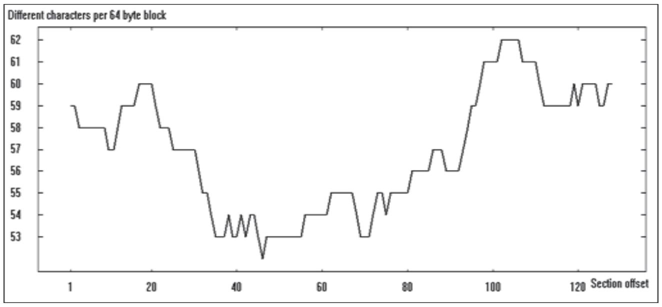

Fig. 11. Floating frequency observed in RSA

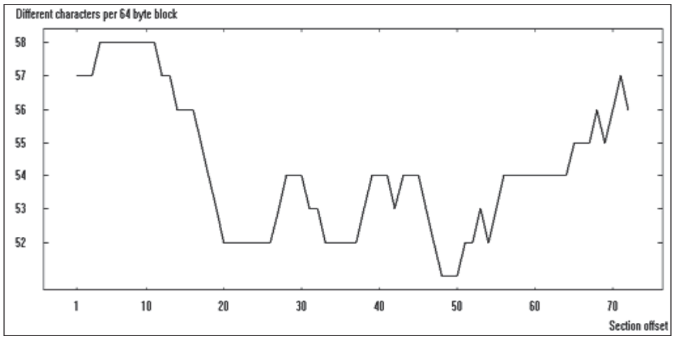

Fig. 12. floating frequency in DES (ECB)

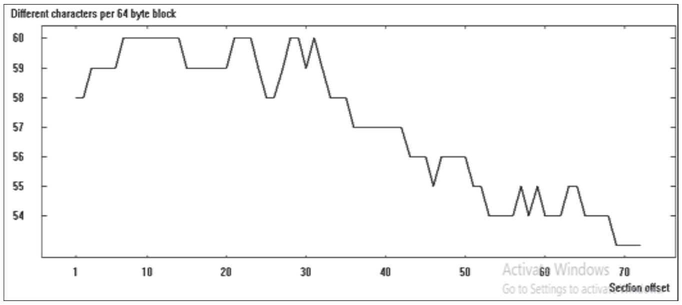

Fig. 13. Floating frequency in DES (CBC)

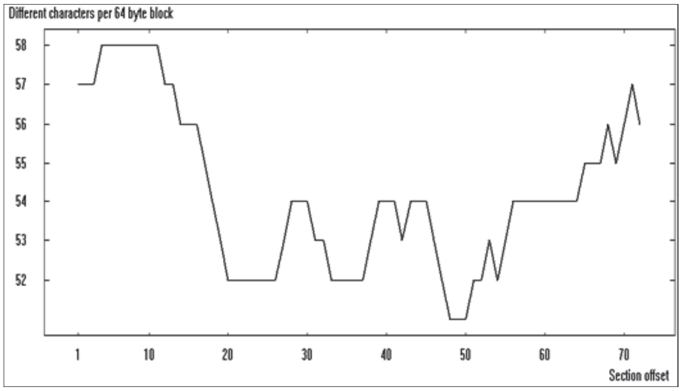

Fig. 14. Floating Frequency in 3DES

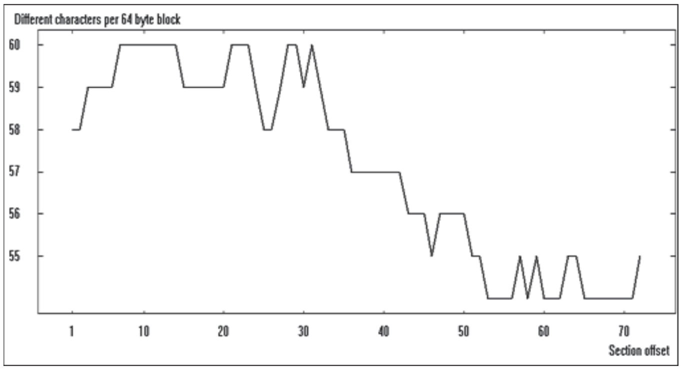

Fig. 15. Floating frequency in 3DES (CBC)

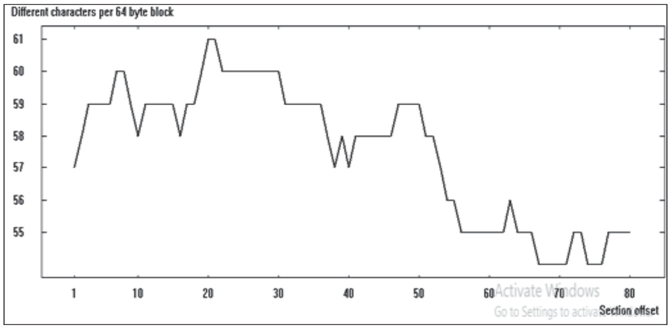

Fig. 16. Floating frequency in AES

V. CONCLUSIONS

A comprehensive analysis based on different evaluation parameters is done in this paper. The demonstration of results are mainly focused on entropy, histogram and floating frequency. Based on performance evaluation, AES provides more security. CBC mode of operation is more secure than ECB as it effectively uses chaining of previous block of data and initialization vector. In those applications where reliability and confidentiality are a high priority, AES can be used. Based on comparison, Due to significant advances in entropy, throughput and efficient encryption design, AES has the potential for further growth.

REFERENCES

[1] Behrouz Forouzan, “Data Communications and networking”, McGraw-Hill, 4th Edition.

[2] William Stallings, “Cryptography and network Security: Principles and Practice”, Pearson Education/Prentice Hall, 5th Edition.

[3] Michael Whitman, Principles of information security, CENGAGE Learning

[4] N. I. of Standards-(NIST), Advanced Encryption Standard (AES). Federal Information Processing Standards Publication197, 2001

[5] S. Burnett and S. Paine, RSA Security’s Official Guide to Cryptography. McGraw-Hill, 2001.

[6] “Economic impact of Data Encryption Standard (DES),” report prepared by NIST ,2001

[7] Daemen, J., & Rijmen, V. (2002). The Design of Rijndael.

[8] P. Hämäläinen, M. Hännikäinen, “Review of hardware architectures for advanced encryption standard implementations considering wireless sensor networks,” vol. 4599 LNCS, pp. 443–453, 2007

[9] ISO/IEC-18033-3, “Information technology - Security techniques-encryption algorithms - Part 3: Block ciphers,” International Standard ISO / IEC, 2012.

[10] Hoang Trang,Nguyen Van Loi,”An efficient FPGA implementation of the Advanced Encryption standard”,IEEE 2012

[11] Z. Hercigonja, D. Gimnazija, and C. Varazdin, “Comparative analysis of cryptographic algorithms and advanced cryptographic algorithms,” International Journal of Digital Technology & Economy, vol. 1, no. 2, pp. 1–8, 2016.

[12] J.G. Pandey” An Efficient VLSI Architecture for Data Encryption Standard and its FPGA Implementation”,IEEE 2016

[13] Eric Conrad,”Security Engineering CISSP study guide” Elsevier 2016

[14] Advanced Encryption Standard Algorithm Validation List.Retrieved http://csrc.nist.gov, NIST. (2017).

[15] Alfadel “Evaluating Time and Throughput at Different Modes of Operation in AES Algorithm”, IEEE 2017

[16] Soufiane Oukili “High speed efficient Advanced Encryption Standard implementation”,IEEE 2017

[17] Endroyono “Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm”,IEEE 2018

[18] “Cost of data breach study: global overview”, research sponsored by IBM security and independently conducted by ponemon institute LLC July 2018

[19] ”Protecting consumer data beyond organizations boundary, consumer data privacy” report by Data Security Council of India, 2018

[20] Berherd Esslinger,”The Cryptool bookLearning and experiencing cryptography with cryptool and SageMath”,2018

[21] “Cost of data breach study: global overview”, research sponsored by IBM security and independently conducted by ponemon institute LLC ,2019