International Journal of Trend in Research and Development, Volume 7(2), ISSN: 2394-9333
www.ijtrd.com

Analysis of AES and DES Algorithm

[1]Yash Shah, [2]Riddhi Rane, [3]Siddhesh Kharade and [4]Rutuja Patil,
[1]Assistant Professor, [2,3,4]Student,
[1,2,3,4]Department of Information technology, Vidyalankar Institute of Technology, Mumbai, Maharashtra, India

***Abstract*—**These days there is increased amount of digital data exchanged in every field, information security is becoming a crucial aspect of data transmission and storage. When we transfer multimedia data such as images, audio, video etc over the network the security of the data is provided by cryptography. Cryptography is the process in which the sender encodes the data and sends it in such a way that only the intended recipient could decode it and read it, for this process we use various cryptographic algorithms.AES and DES are the types of cryptographic algorithm which are more frequently been used because of their popularity. In this paper we had a brief study of different set of algorithms and its implementations and we did examine it on some parameters which is time consumed, bit independence criteria and avalanche effect.

Keywords*-AES, DES, Avalanche effect, Cryptography.*

I. INTRODUCTION

Although electronics documents have been greatly improved in the transferring speed and processing speed it would also result the electronic documents information is disclosed, counterfeited, tampered repudiated and so on. Therefore due to the rapid usages of data communication, security is becoming a more crucial issue. The fundamental requirements for security include authentication, confidentiality, integrity and non-repudiation..In order to achieve this security cryptography is needed. Cryptography is the process of securing information by converting it into and format which is not readable. In order to prevent some unwanted user or people to get access to the data cryptography is needed. Cryptography is a method to secure file by writing the hidden code to cover the original file. Therefore, if the people do not involve in cryptography, they cannot decrypt the hidden code to read. The most system uses two major classes of cryptographic algorithm namely private-key and public-key algorithms. In private key algorithm same key is used for both encryption and decryption. They usually operate at relatively high speed and are suitable for bulk encryption of messages. Public-key algorithm based on the idea of separating the key used to encrypt a message from the one used to decrypt it. They are relatively slow and therefore unsuitable for encryption of large bulky messages.

II. SECURITY PARADIGM

As the internet and other forms of electronic communication became more prevalent, electronic security is becoming increasingly important. The art or science encompassing the principles and methods of transforming an intelligent message back to its original form, to keep message secure is cryptography. Cryptography is used to protect email, messages, credit card information and corporate data within the context of any application-to-application communication, there are some security requirements, including:

- Authentication: The process of proving one's identity . Authentication is a process in which credential provided are compared to those on file in a database of authorized user's information on a local operating system or within an authentication server.
- Privacy/Confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

Cryptography is science and art of creating secrete code and cryptanalysis is art of breaking those codes. AES is the best and strongest cryptographic algorithm, because of three areas: Security, Cost and Implementation.

There are two types of cryptographic algorithms developed are as follows:

- Symmetric cryptography: It uses the same cryptographic key for both encryption of plain text and decryption of cipher text. If the same keys are used for encryption or decryption, we call it symmetric cipher.
    - Ek(M) = C
    - Dk(M) = M

  Those functions have the property that,
    - Dk(Ek(M)) = M

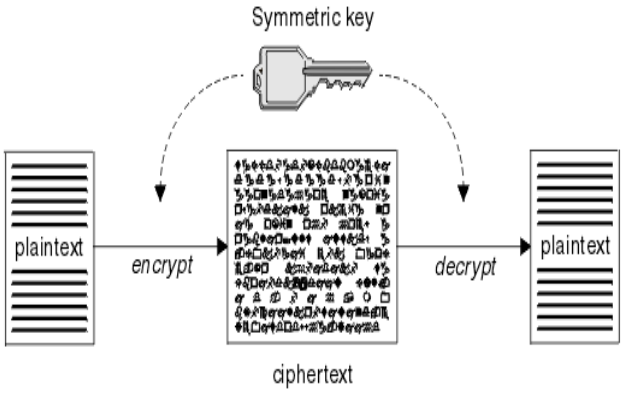

Figure-1 Symmetric key

- Asymmetric cryptography: Asymmetric cryptography or public key cryptography is cryptography in which a pair of keys (k1,k2) is used to encrypt and decrypt a message so that it arrives securely. In case of asymmetric cipher we have a key pair (k1,k2), k1 being public and k2 private, then
    - Ek1(M) = C
    - Dk2 (C) = M

  Those functions have the property that,
    - Dk2(Ek1(M)) = M

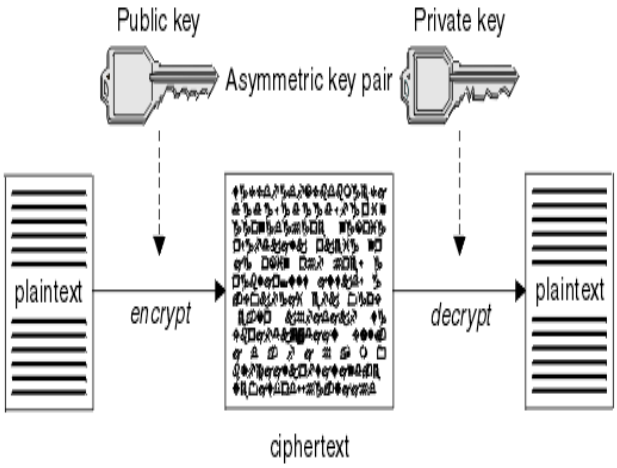

Figure-1 Asymmetric key

III. CRYPTOGHAPHIC ALGORITHM

A. DES Algorithm

The Data Encryption Standard(DES) is a block cipher algorithm which is designed to encrypt and decrypt data of 64-bit block size with a 64-bit key. In Encryption the data is being converted into cryptographic form which is not readable by the user this form is also called as cipher and in decryption the cipher text which is generated is converted back into its original form which is known as the plain text. Both the encryption and the decryption process are performed using a key which is a binary number. The authorized user must have the same key to decrypt the text which is been used to encipher the text. The DES algorithm makes used of 64-bit out of which only 56-bit are directly used by the algorithm and the remaining 8-bits are been used for error detection.DES performs 16 rounds series of substitution and permutation. In every round, data and key bit are shifted, permuted, XORed and then send through 8 s-boxes, a set of lookup tables that are mandatory for the DES algorithm. Unauthorized users cannot access the data even if they know the algorithm without the key.

B. AES Algorithm

The Advanced Encryption Standard (AES) was developed by the National Institute of Standard and Technology(NIST) with an intension to overcome the drawbacks of DES algorithm as it gets crack by Brute force attack.It is a symmetric block cipher cryptographic algorithm. It is one of the most popular algorithm which is been used to secure the data all over the world. AES has 128 bit block size which handles three different key sizes such as 128,192 and 256 bit. On the basis of the key size the execution round is 10,12 and 14 respectively. It has its own process for both encryption and decryption. AES algorithm performs a number of transformation on the data which is stored in array. The first step of the cipher is that data is stored into an array, after that cipher transformation are performed repeatedly in the number of encryption rounds. The first transformation in the AES algorithm is substitution using the substitution table, the second transformation performs shifting of data row and the third mixes the column. The last transformation performs operation in each column using a different part of the encryption key. It is very difficult to crack data encrypted using AES algorithm.

C. Comparison between AES and DES Algorithm

The table below specifies the comparison between AES and DES on various parameters.

Table 1

PARAMETER	DES	AES
Developed	1977	2000
Key length	56 bits	128,192 or 256 bits
Block size	64 bits	128,192 or256 bits
Possible keys	256	2^{128}, 2^{192} and 2^{256}
Structure	Based on feistel network	Based on substitution permutation network
Structure	Symmetric block cipher	Symmetric block cipher
Security	Proven inadequate	Considered secure
Attack	Brute force, Linear analysis	No crypt-analytical against AES

IV. METHODOLOGY

This project introduces hybrid approaches by combining two most important algorithms AES algorithm and DES algorithm. This hybrid encryption algorithm provides more security as compare to other security algorithm. The parameter on which this algorithm is analyzed was Avalanche effect, Bit Independence criteria and time consumed. In order to ensure more security the key which is given to this algorithm by the user in the beginning is given to a random function which generates more complex key which is then given to this hybrid algorithm. This provides more security.

The user needs to select a file which he wants to be encrypted then he needs to press the encrypt button and enter the key. Then the decrypt button is to be pressed and the same key which was entered before is to pressed which decrypts the file which is uploaded.

- Avalanche Analysis

The avalanche effect property is very important for encryption algorithm. This property can be seen when changing one bit in plaintext and then watching the change in the outcome of at least half of the bits in the cipher text. One purpose for the avalanche effect is that by changing only one bit there is large change then it is harder to perform an analysis of cipher text, when trying to come up with an attack.

$$\text{Avalanche Effect} = \frac{\text{Number of flipped bits in ciphered text}}{\text{Number of bits in ciphered text}}$$

- Bit Independence Criteria

A second property which would seem desirable for any cryptographic transformation is that, for given set of avalanche vectors generated by the complementing of single plaintext bit, all the avalanche variable should be pair wise independent. In order to measure the degree of independence between a pair of avalanche variable, we calculate their correlation coefficient, if its zero it mean that the variable are independent, if its 1 that mean stronger positive correlation and -1 is stronger negative correlation.

V. RESULT AND ANALYSIS

The comparison of AES and DES algorithm are shown below in the table no - using parameters such as avalanche effect and bit-independence criteria.

TABLE-II

Sr. No	Plaintext	Bit Change	Avalanche Effect
1	1101000110010 11111001 (hey)	38	59.3%
	1101000110010 11111000 (hex)		
2	1100101110111 0110001111100 1011110011110 0001110100 (encrypt)	32	57.14%
	1100101110111 0110001111100 1011110011110 0001110110 (encrypy)		
3	1100110110100 1110110011001 01 (file)	28	43.7%
	1100110111100 1110110011001 01 (fyle)		
4	1100011110100 1111000011010 0011001011110 010 (cipher)	28	43.7%
	1100011110100 1111000011011 0011001011110 010 (cipler)		
5	1100110110100 1110111011000 01101100 (final)	36	56.25%
	1100110110100 1111111011000 011101100 (fi~al)		
AVERAGE			**52.018%**

According to the analysis performed the avalanche effect calculated for AES algorithm is more than as compared to DES algorithm

CONCLUSION

Cryptography plays an important role in the security to maintain the confidentiality, integrity, availability, authentication and non-repudiation of the data. In this paper we have studied the cryptography algorithm such as AES and DES. They have been examined in terms of avalanche effect and bit change. The results are been stored in tabular form above in TABLE-II. Avalanche effect i.e. one bit variation is more in AES as compare to DES. Lastly, we concluded that AES algorithm is more secure that DES algorithm.

References

[1] Mohamad Noura, "DES: An efficient and secure DES Varient", 20188371019/

[2] Shady Mohameed Soliman,"Efficient implementation of the AES algorithm for security applications", 2017.

[3] Bawna Bhat,"DES and AES performance evaluation", 2015.

[4] Akash Kumar Mandal,"Analysis of Avalanche effect in plaintext using binary codes",2013.

[5] Seung-Jo Han, "The improved Data Encryption Standard algorithm(DES) ", 2012.

[6] B.Thiyagarajan, ”Data Integrity and Security in Cloud Environment Using AES Algorithm”,ICICES 2014.

[7] Takanori Machida, “Modifications to AES Algorithm for Complex Encryption”, IEEE transactions 2015.

[8] C. Giraud, “An Implementation of DES and AES,Secure against Some Attacks”, c Springer-Verlag Berlin Heidelberg.CHES, LNCS 2162, pp. 309–318, 2001.

[9] Shraddha Soni, "Analysis and Comparision between AES and DES Cryptographic Algorithm", December 2012.