Designing Encryption Scheme Using AES

Ejaz Bakhsh
School of Computer Science and Engineering, Galgotias University, Greater Noida, India

***Abstract*— Advanced Encryption Standard (AES) algorithm is one on the foremost common and widely symmetric block cipher algorithm utilized in worldwide. In this paper we will do key expansion has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to urge the important data when encrypting by AES algorithm. AES has the ability to deal with three different key sizes such as AES 128, 192 and 256 bit and each of these ciphers has 128-bit block size. In this paper will provide an summary of AES algorithm and explain different features of this key expansion details and class some previous researches that have done there on with compared to other process such as DES, RSA. This project will explain some modification of key modified in their frequency because AES contains different types od data. The new one key modified make more encrypted and also more secure as existing key expansion. Their will such operation as Substitute bye, Mix column, Sub byte and Add Round Key. Mix column operation is done on Mat lab.**

INTRODUCTION

Internet communication having the important role to transfer large amount of data in several fields. Some of data might be transmitted through insecure channel from sender to receiver. Different techniques and methods have been using by private and public sectors to protect sensitive data from intruders due to the safety of electronic data is crucial issue. Cryptography is one among the foremost significant and popular techniques to secure the info from attackers by using two vital processes that's Encryption and Decryption. Encryption is that the process of encoding data to stop it from intruders to read the first data easily. This stage has the power to convert the first data (Plaintext) into unreadable format referred to as Cipher text. To perform this process cryptography applies on mathematical calculations along with some substitute and permutations with or without keys. Modern cryptography provides the confidentiality for more secure, integrity, nonrepudiation and authentication from unauthorized authentication. These days, there are variety of algorithms are available to encrypt and decrypt sensitive data which are typically divided into three types.

First is symmetric cryptography which uses the same key for encryption and as well as decryption for data. Second one is Asymmetric cryptographic. These sorts of cryptography rely on two different keys for encryption and decryption. Finally, cryptographic hash function using no key instead key it's mixed the info. The symmetric key is more efficient and faster than Asymmetric key.

Some of the common symmetric algorithms is Advance Encryption Standard (AES), RSA, Simplified Data Encryption Standard (S-DES). The main importance of this paper will provide a details about Advanced Encryption Standard algorithm for encryption and decryption of data then also making a comparison between AES and DES algorithm to point out some idea why replacing DES to AES algorithm. This paper is organized as follows: In this paper presents a brief history of AES algorithm. Related work discussed and also provides the evaluation criteria of AES algorithm. Basic structure of AES algorithm describes Encryption process of AES algorithm presents here. And the most important expanded key of AES. Satellite communication has the advantaged of large coverage, wide bandwidth, huge capacity, flexibility in different business, stable and reliable performance and no geographical restrictions. What's more, the cost has nothing to do with the distance. It is now widely used in military communications, emergency communications and the field of radio and television. It will become a focus in mobile also communications research. In satellite communications, because of fading, noise and interference, the signal will come through more

serious distortion. A strong error correction method should be applied to scale back the bit error rate within the case of limit power. Meanwhile, the printed satellite communication links lack effective safety feedback, so a safer encryption algorithm should be adopted. Therefore, how to improve the reliability and security of the data transfer is one key issue in research of satellite communications. Existing satellite communication technology divides encryption and error correction into two steps, that's to say, to encrypt the knowledge first, then to encode the encrypted data by error correction coding.

RELATED WORK

Hardware and software implementation of the AES algorithm is one among the foremost needy area to attractive researches to try to a search thereon . In current previous years a so many research papers have been publishing on AES algorithm to provide much more complexity and comparing the performance between the popular encryption algorithms to encrypt and decrypt data. In this paper evaluate the performance of three algorithms like AES, DES, and RSA to encrypt text files under three parameters like computation time, memory usage, and output bytes. Encryption time was computed to convert plaintext to cipher text then comparing these algorithms to find which algorithm takes more time to encrypt text file. According to the results they have obtained RSA takes more time compared to other algorithms. For second parameters RSA needs a bigger memory than AES and DES algorithms. Finally, the output byte of every algorithm has considered. DES and AES produce an equivalent level of output byte whereas RSA features a low level of output byte.

DATA SOURCE

AES is an iterative instead of Feistl cipher. It is based on two common techniques to encrypt and decrypt data known as substitution and permutation network (SPN). Substitution and permutation is a number of mathematical operations that are carried out in block cipher algorithms. AES has the ability to deal with 128 bits (16 bytes) as a fixed plain text block size.
These 16 bytes are represented in 4X4 matrix and

A. AES operates on a matrix of bytes

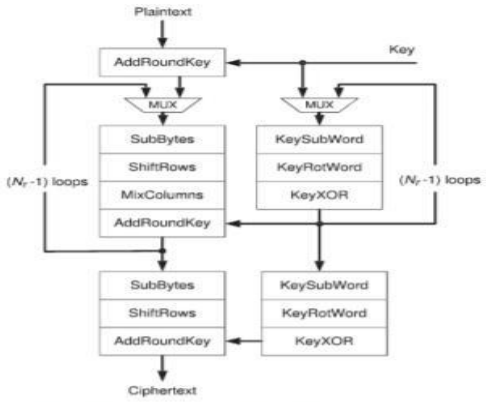

Fig. 1. Block diagram of AES encryption.

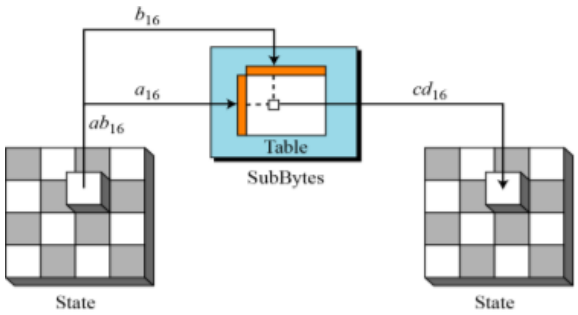

Fig 1.1: Substitution

The first step of each round is starts with Sub Bytes transformation. This stage is depends on nonlinear S-box to substitute a byte within the state to a different byte. According to diffusion and confusion Shannon's principles for cryptographic algorithm design it's important roles to get far more security.

B. Shift Rows Transformation

After the Sub Byte that perform on the state is Shift Row the next step is this. The main idea behind this step is to shift bytes of the state cyclically to the left in each row instead of row number zero.

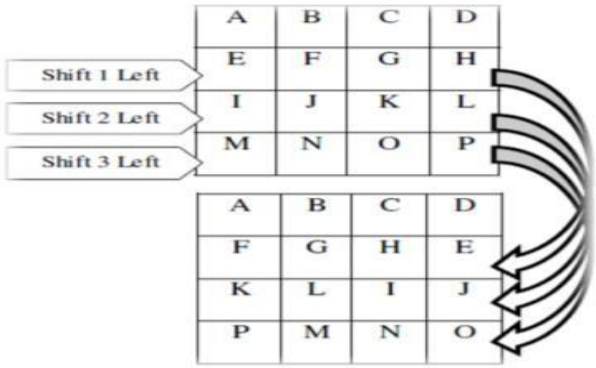

Fig 1.2: Shifting Rows

In this process the byte of row number zero remains and does not carry out any other permutation. In the first row just one byte is shifted the circular to left. The second row is shifted two bytes to the left. The last row is shifted three bytes to the left. The size of new state is remain unchanged that have the same original size 16 bytes but shifted the position of the bytes of state.

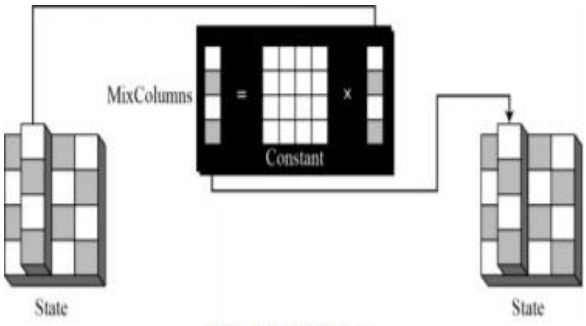

Fig 1.3: Mixing

C. Mix Columns

This is one of the deciding step occurs of the state is mix Column. The multiplication is carry out of the state. Each byte of one row in matrix transformation multiply by each value of the present state column. It means that each row of matrix transformation must multiply by each column of the state for result.

The results of this multiplication are used with XOR to produce a new four bytes for the next state. Here the size of state is not changed.

D. Add Round Key Transformation

Add Round Key is the most active stage in AES algorithm. Both the key and the input data are structured in a 4x4 matrix of bytes

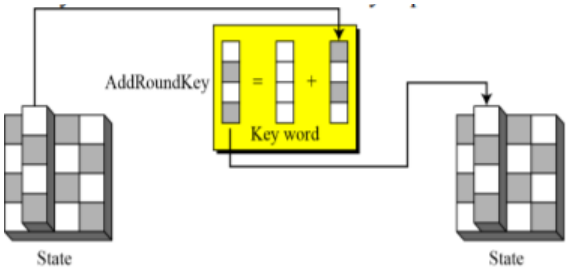

Fig 1.4: Adding Key

Then shows how the 128-bit key and input data are distributed into the byte matrices. Add Round Key has the ability to provide much more security during encrypting data. This operation is predicated on creating the connection between the key and therefore the cipher text.

PROPOSED SYSTEM

A. Security: one among the foremost crucial aspects that NIST was considered to settle on algorithm it's security. The main reasons behind this was obvious due to the most aims of AES was to enhance the safety issue of DES algorithm. AES has the best ability to protect of sensitive data from intruders and is not allowed them to crack the encrypt data as compared to other proposed methods. Cryptography and Network Security achieved by doing several of testing on AES against theoretical and practical attacks.

B. Cost: Another criterion that was emphasis by NIST to gauge the algorithms it's cost. Again, the factors behind this measure was also clear thanks to another main purpose of AES algorithm was to enhance the low performance of DES. AES was one among the algorithm which was nominated by NIST because it's ready to have high computational efficiency and may be utilized in a good range of applications especially in broadband links with a high speed.

C. Algorithm and Implementation Characteristics: This criteria was very significant to estimate the algorithms that were received from cryptographer experts. Some important aspects were measured in this stage that is the flexibility, simplicity and suitability of the algorithm for diversity of hardware and software implementation length of key. There are three different key sizes are used by AES algorithm to encrypt the data such as 128, 192 or 256 bits. The key sizes decide to the number of rounds such as AES uses 10 rounds for different size of key.

AES KEY EXPANSION

```
% Module 2: Shiftrow operation implemented in Matlab
%

state=zeros(4,4);
staten=state;
% Read the input data 4*4 into state
disp('Enter hex values:')
% format = 'hex-value'
for i=1:4
    for j=1:4
        disp('state----- Rowno  / Column no')
        disp(i)
        disp(j)
        temp=input('Enter hex value:')
        state(i,j)=hex2dec(temp);
    end
end
```

Key Size (bytes)	Block Size (bytes)	Expanded Key (bytes)
16	16	176
24	16	208
32	16	240

DECRYPTION PROCESS

Decryption is the process to get the original data which was encrypted before. This process is based on the key that was received from the sender of the data. The decryption process of an AES is analogous to the encryption process within the reverse order and both sender and receiver have an equivalent key to encrypt and decrypt data. The last round of a decryption stage consists of three stages such as Inverse Shift Rows, Inverse Sub Bytes, and Add Round Key.

CONCLUSION

Using internet and network are increasing rapidly. In daily basis there so many use with so many data are exchange with other user .Among them of data can be sensitive then it required to protect from several attackers. Encryption scheme play several roles to protect of original data from unauthenticated access. Several types of algorithms are present to encrypt data. AES algorithm technique is one of the most effective algorithms and it is worldwide supported and accepted on hardware and software. This algorithm able to deal with different key sizes such as 128, 192, and 256 bits with 128 of bits cipher block. Here explains so many of important features and quality of AES algorithm and also mention some previous researches that have done before on it to know the performance of AES to encrypt data under different parameters such as required memory and time etc.

REFERENCES

[1] Abdullah, A. M., & Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).

[2] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

[3] Gaj, K., &Chodowiec, P. (2001, April). Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using Field Programmable Gate Arrays. In Cryptographers' Track at the RSA Conference (pp. 84-99). Springer Berlin Heidelberg.

[4] Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India.

[5] Yenuguvanilanka, J., &Elkeelany, O. (2008, April). Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. In Southeastcon, 2008. IEEE (pp. 222- 225).

[6] Lu, C. C., & Tseng, S. Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on (pp. 277-285).

[7] Mohamed, A. A., &Madian, A. H. (2010, December). A Modified Rijndael Algorithm and it's Implementation using FPGA. In Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference on (pp. 335-338).

[8] Pramstaller, N., Gurkaynak, F. K., Haene, S., Kaeslin, H., Felber, N., &Fichtner, W. (2004, September). Towards an AES crypto-chip resistant to differential power analysis. In Solid-State Circuits Conference, 2004. ESSCIRC 2004. Proceeding of the 30th European IEEE (pp. 307-310).

[9] Deshpande, H. S., Karande, K. J., &Mulani, A. O. (2014, April). Efficient implementation of AES algorithm on FPGA. In Communications and Signal Processing (ICCSP), 2014 IEEE International Conference on (pp. 1895-1899).

[10] Nadeem, H (2006). A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, (pp. 84-89).