GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Designing Encryption Scheme using AES

A report for the Evaluation 3 of Project 2

Submitted by

EJAZ BAKHSH

(1613101266/16SCSE101700)

in partial fulfilment for the award of the degree of

BACHELORS OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

Under the Supervision of

Dr. N.V. KOUSIK, MCA,M.Phil, Ph. D , Associate Professor

APRIL/MAY-2020

GALGOTIAS
UNIVERSITY

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report "**DESIGNING ENCRYPTION SCHEME USING AES"** is the bonafide work of "**EJAZ BAKHSH (1613101266)**" who carried out the project under the work under my supervision.

SIGNATURE OF HEAD

Dr. MUNISH SHAHARWAL.,
PhD (Management),
PhD (CS) Professor &Dean
School of Computer Science
& Engineering

SIGNATURE OF SUPERVISOR

Dr. N.V. KOUSIK**.,**
MCA, M. Phil, PhD (CS)
Associate Professor
School of Computer Science
& Engineering

TABLE OF CONTENTS

ABSTRACT

Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used 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 get the real 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. This paper will provide an overview of AES algorithm and explain several crucial features of this key expansion details and demonstration some previous researches that have done on it with comparing to other algorithms such as DES, 3DES, Blowfish etc. 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 Matlab.

LIST OF FIGURES

INTRODUCTION

Internet communication is playing the important role to transfer large amount of data in various 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 because of the security of electronic data is crucial issue. Cryptography is one of the most significant and popular techniques to secure the data from attackers by using two vital processes that is Encryption and Decryption. Encryption is the process of encoding data to prevent it from intruders to read the original data easily. This stage has the ability to convert the original data (Plaintext) into unreadable format known as Cipher text. To perform these process cryptography relies on mathematical calculations along with some substitutions and permutations with or without a key. Modern cryptography provide the confidentiality, integrity, nonrepudiation and authentication [1]. These days, there are a number of algorithms have been available to encrypt and decrypt sensitive data which are typically divided into three types.

1. Frist one is symmetric cryptography that is the same key is used for encryption and decryption data.
2. Second one is Asymmetric cryptographic. This types of cryptography relies on two different keys for encryption and decryption. Finally, cryptographic hash function using no key instead key it is mixed the data [2]. The symmetric key is much more effective and faster than Asymmetric.

Some of the common symmetric algorithms is Advance Encryption Standard (AES), Blowfish ,Simplified Data Encryption Standard (S-DES) and 3DES. The main purpose of this paper will provide a detail information about Advanced Encryption Standard (AES) algorithm for encryption and decryption data then make a comparison between AES and DES algorithm to show 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 have 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 communications research. In satellite communications, due to fading, noise and interference, the signal will come through more serious distortion. A strong error correction method should be applied to reduce the bit error rate in the case of limit power. Meanwhile, the broadcast satellite communication links lack effective safety feedback, so a more secure 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 information first, and then to encode the encrypted data by error correction coding. This step-by-step method not only increases the complexity of the system, but also leads to a longer delay. This will result in restrained system efficiency and limit the further miniaturization of the baseband chip. However, the credible and reliable data transfer method combined with encryption and error correction is at the forefront of research. When it applies in the satellite communications system, it can improve the transmission efficiency, reduce the system processing delay, and ameliorate the real-time nature of the business transfer. A preliminary study on the joint encryption and error correction method is being carried out among the national and international researchers. In 1978, based on the characteristics of the Goppa codes, Mc Eliece firstly made use of error-correcting codes to construct a class of public-key system--M public key system [1]. M public key system can encrypt and decrypt easily, but its key size is too large. Worse still, the security confronts a hidden danger. In 1991, the Korzhik and Turkin claimed that it had been broken through [2]. After a few years, researches on encryption and error correction algorithm were mainly around the improvement of the M public key system. During this period of time, a number of different types of M key systems were proposed. In 1984, Rao proposed a private key cryptography [3], the basic idea was to apply the McEliece public key in the private key cryptography. In 1986, Wang Xinmei put forward Ms public-key system [4] and MC packet encryption and error correction system [5] by a deep study on the M public key system. At the same year, Niederreiter utilized Goppa codes checked matrix to construct a new public-key system, referred to as N public key system [6]. To some extent, these M-alike key systems make a progress in security, the error correction capability and decoding time. In 2006, Mathur and Subbalakshmi proposed a high degree of diffusion codes (HD) in the literature [7]. This method is based on the SPN structure, which is used in the AES algorithm. It utilizes the HD codes as a diffusion layer of the SPN structure. Because the HD codes have the error correction capability, and it is also a byte-based encoding.

EXITING SYSTEM

The Advanced Encryption Standard is the current United States standard symmetric block cipher. It was published in Federal Information Processing Standard (FIPS) 197 (see: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf). AES uses 128-bit (with 10 rounds of encryption), 192-bit (12 rounds of encryption), or 256-bit (14 rounds of encryption) keys to encrypt 128-bit blocks of data. AES is an open algorithm, free to use, and free of any intellectual property restrictions.

AES was designed to replace DES. Two- and three-key TDES EDE remain a FIPS-approved standard until 2030, to allow transition to AES. Single DES is not a current standard, and not recommended.

Choosing AES

The United States National Institute of Standards and Technology (NIST) solicited input on a replacement for DES in the Federal Register in January 1997. They sought a public symmetric block cipher algorithm that was more secure than DES, open, and fast and efficient in both hardware and software. Fifteen AES candidates were announced in August 1998, and the list was reduced to five in August 1999. Table 4.12 lists the five AES finalists

Rijndael was chosen and became AES. The name, pronounced “Rhine Dahl” in English, is a combination of the Belgian authors’ names: Vincent Rijmen and Joan Daemen. Rijndael was chosen “because it had the best combination of security, performance, efficiency, and flexibility.”[23]

Table 4.13 shows the “State,” which is the block of data that is being encrypted via AES. Each smaller box in the State is a byte (8 bits), and there are 16 bytes (128 bits) in each block. Data is encrypted and visualized in literal blocks. The algorithm that AES is based on was called “Square” for this reason.

AES Functions

AES has four functions: SubBytes, ShiftRows, MixColumns, and AddRoundKey. These functions provide confusion, diffusion, and XOR encryption to the State.

ShiftRows

ShiftRows provides diffusion by shifting rows of the State. It treats each row like a row of blocks, shifting each a different amount:

Row 0 is unchanged

Row 1 is shifted 1 to the left

Row 2 is shifted 2 to the left

Row 3 is shifted 3 to the left

MixColumns

MixColumns also provides diffusion by “mixing” the columns of the State via finite field mathematics.

SubBytes

The SubBytes function provides confusion by substituting the bytes of the State. The bytes are substituted according to a substitution table (also called an S-Box).

To use the table, take the byte of the State to be substituted (assume the byte is the letter “T”). ASCII “T” is hexadecimal byte “53.” Look up 5 on the X row and 3 on the Y column, resulting in hexadecimal byte “ed;” this replaces “53” in the State. Figure 4.28 shows the AES substitution table directly from FIPS-197, with the byte 53 lookup overlaid on top:

AddRoundKey

AddRoundKey is the final function applied in each round. It XORs the State with the subkey. The subkey is derived from the key, and is different for each round of AES.

PROPOSED SYSTEM

This paper proposes a physical-layer encryption method based on AES and LDPC, which is suitable for satellite communication. Compared with the LDPC-based error correcting cipher that is also based on AES and LDPC mentioned in literature [9], the SEEC method has a better performance. This paper will provide an overview of AES algorithm and explain several crucial features of this key expansion details and demonstration some previous researches that have done on it with comparing to other algorithms such as DES, 3DES, Blowfish etc. 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 Matlab. Three important criterions were used by NIST to evaluate the algorithms that were submitted by cryptographer experts.

A. *Security:* One of the most crucial aspects that NIST was considered to choose algorithm it is security. The main reasons behind this was obvious because of the main aims of AES was to improve the security issue of DES algorithm. AES has the best ability to protect sensitive data from attacker sand is not allowed them to break the encrypt data as compared to other proposed algorithm. This was Cryptography and Network Security achieved by doing a lot of testing on AES against the oretical and practical attacks.

B. *Cost:* Another criterion that was emphasis by NIST to evaluate the algorithms it is cost. Again, the factors behind this measures was also clear due to another main purpose of AES algorithm was to improve the low performance of DES. AES was one of the algorithm which was nominated by NIST because it is able to have high computational efficiency and can be used in a wide 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 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

BASIC STRUCTURE OF AES ALGORITHM

AES is an iterative instead of Feistel cipher. It is based on two common techniques to encrypt and decrypt data knowns as sub stitution and permutation network (SPN). SPN is a number of mathematical operations that are carried out inblock cipher algorithms [7]. 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 AES operates on a matrix of bytes. In addition, another crucial feature in AES is number of rounds.

A. *Substitute Bytes Transformation*

The first stage of each round starts with Sub Bytes transformation. This stage is depends on nonlinear S-box to substitute a byte in the state to another byte. According to diffusion and confusion Shannon's principles for cryptographic algorithm design it has important roles to obtain much more security. For example, in AES if we have hexa 53 in the state, it has to replace to hexa ED. ED created from the intersection of 5 and 3. For remaining bytes of the state have to perform these operations.

B. *ShiftRows Transformation*

The next step after Sub Byte that perform on the state is Shift Row. The main idea behind this step is to shift bytes of the state cyclically to the left in each row rather than row number zero. In this process the bytes of row number zero remains and does not carry out any permutation. In the first row only one byte is shifted circular to left. The second row is shifted two bytes to the left. The last row is shifted three bytes to the left [13]. The size of new state is not changed that remains as the same original size 16 bytes but shifted the position of the bytes in state

C. *MixColumns Transformation*

Another crucial step occurs of the state is Mix Column. The multiplication is carried out of the state. Each byte of one row in matrix transformation multiply by each value (byte) of the state column. In another word, each row of matrix transformation must multiply by each column of the state. The results of these multiplication are used with XOR to produce a new four bytes for the next state. In this step the size of state is not changed that remained as the original size 4x4.

D. *AddRoundKey Transformation*

AddRoundKey is the most vital stage in AES algorithm. Both the key and the input data (alsoreferred to as the state) are structured in a 4x4 matrix of bytes . shows how the 128-bit key and input data are distributed into the byte matrices. AddRoundKey has the ability to provide much more security during encrypting data. This operation is based on creating the relationship between the key and the cipher text. The cipher text is coming from the previous stage. The AddRoundKey output exactly relies on the key that is indicated by users [15].Furthermore, in the stage the subkey is also used and combined with state. The main key is used to derive the subkey in each round by using Rijndael's key schedule. The size of subkey and stateis the same. The subkey is added by combining each byte of the state with the correspondingbyte of the subkey using bitwise.

IMPLEMENTATION

Encryption method The idea of this algorithm is based on the classical SPN structure in block coding area.

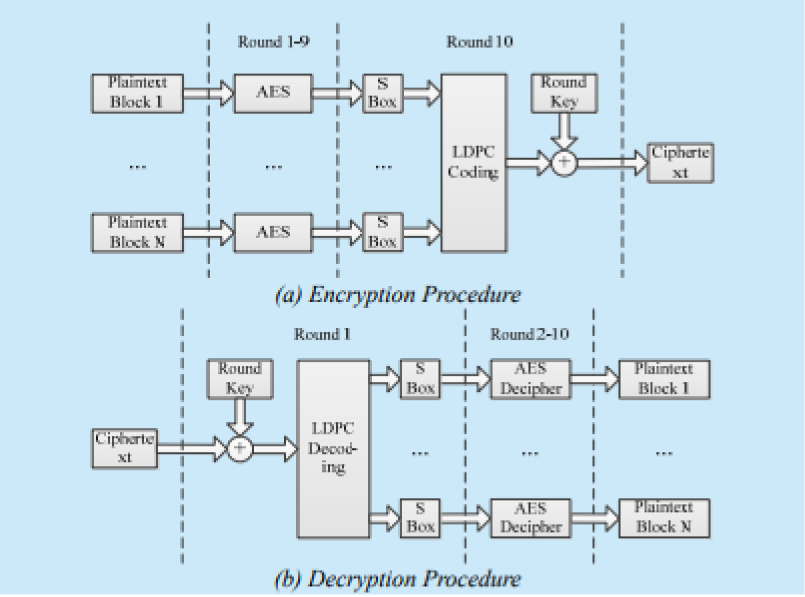


Figure 1 : Decryption Procedure

This method refers to the basic structure of AES algorithm. Both block length and key length are 128 bits. The computation of the former 9 rounds is same as the AES algorithm. In the final round, do the Sub Bytes (S-box) firstly, then, do the LDPC encoding by using the upper result as the information bit, in which the scale of LDPC check matrix depends on the corresponding standards of satellite communications. Because the good coding performance of LDPC can be only realized with long LDP codes, we take the encryption processing parallel in the anterior 9 rounds before the last round of the LDPC coding. At last, we obtain the ciphertext by XOR the result with the sub-key. So we get the encryption control of the LDPC encoding round. The encryption process is shown in figure.

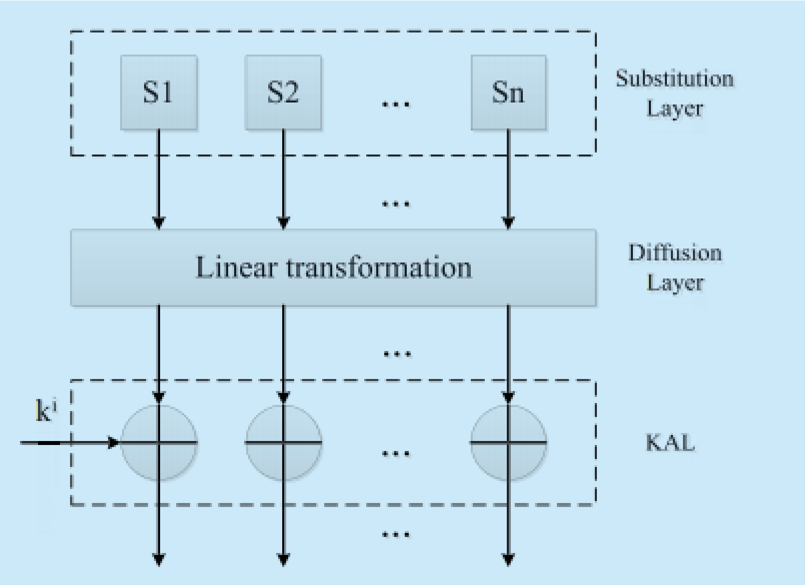
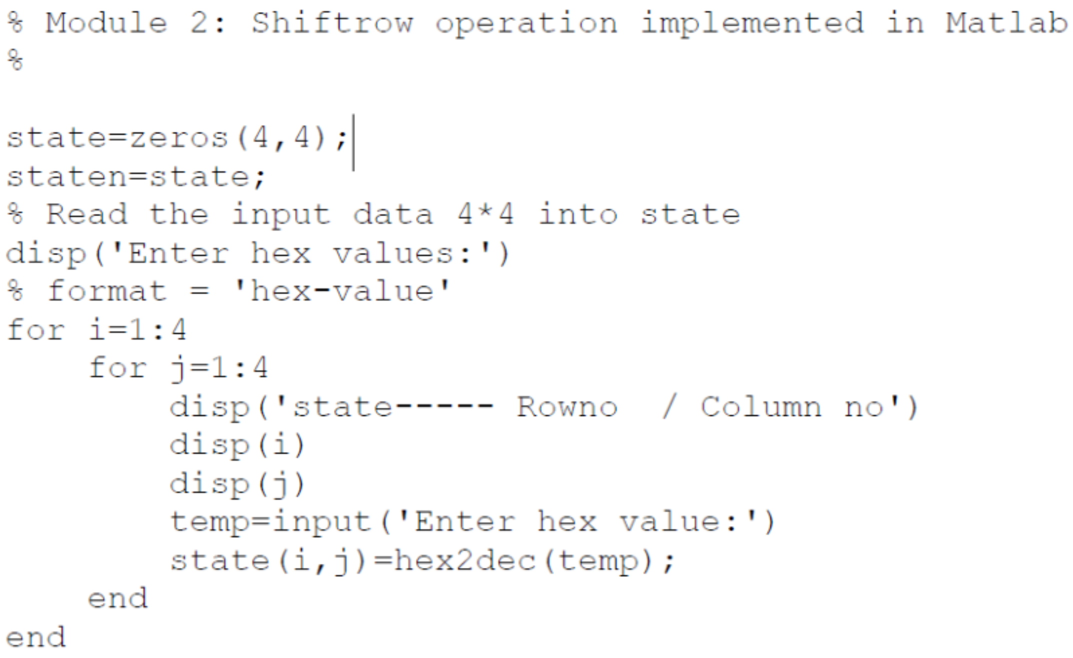


Figure 2 : Layers of encryption algorithm

The structure uses three functional modules, just as shown in figure 2. In these three layers, the substitution layer is for confusion achieving by the S-box, and it is the nonlinear part in block coding, Characteristics of the cryptography directly affect the security level. A good S-box can ensure the encryption algorithm to resist against different kind of attacks, such as differential cryptographic analysis attacks and linear cryptographic analysis attacks. The diffusion layer is for diffusion. Because of the limited storage and the speed requirements, we have to restrict the scale of the S-box, so diffusion layer is needed for diffusing the confusion effect of the substitution layer to a larger scale, and it is also for avalanche effect. So, we can conclude that, substitution layer has the capability to resist against differential and linear attacks, and diffusion layer propagates this capability to a larger scale. The Key Adding Layer (KAL) realizes the combination of data and key, using the key to control the round function. AES is a typical representative of the SPN structure cryptographic algorithm. This algorithm always completes the encryption in 10 rounds. Except for the final round, each round consists of four transformations: Sub Bytes, Shift Rows, Mix Columns and Add Round.

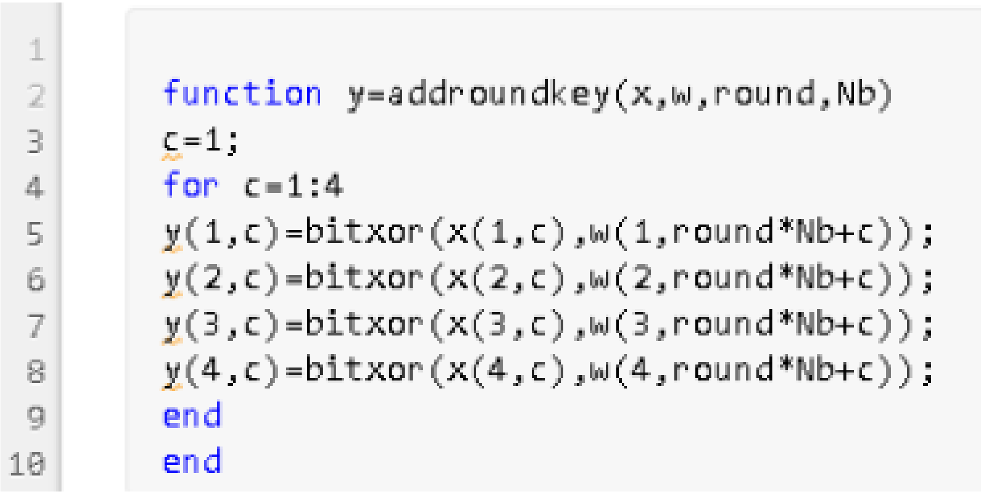
Screenshots of the code implementations:



```
% 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
```

Figure 3 : Shift Row Operation

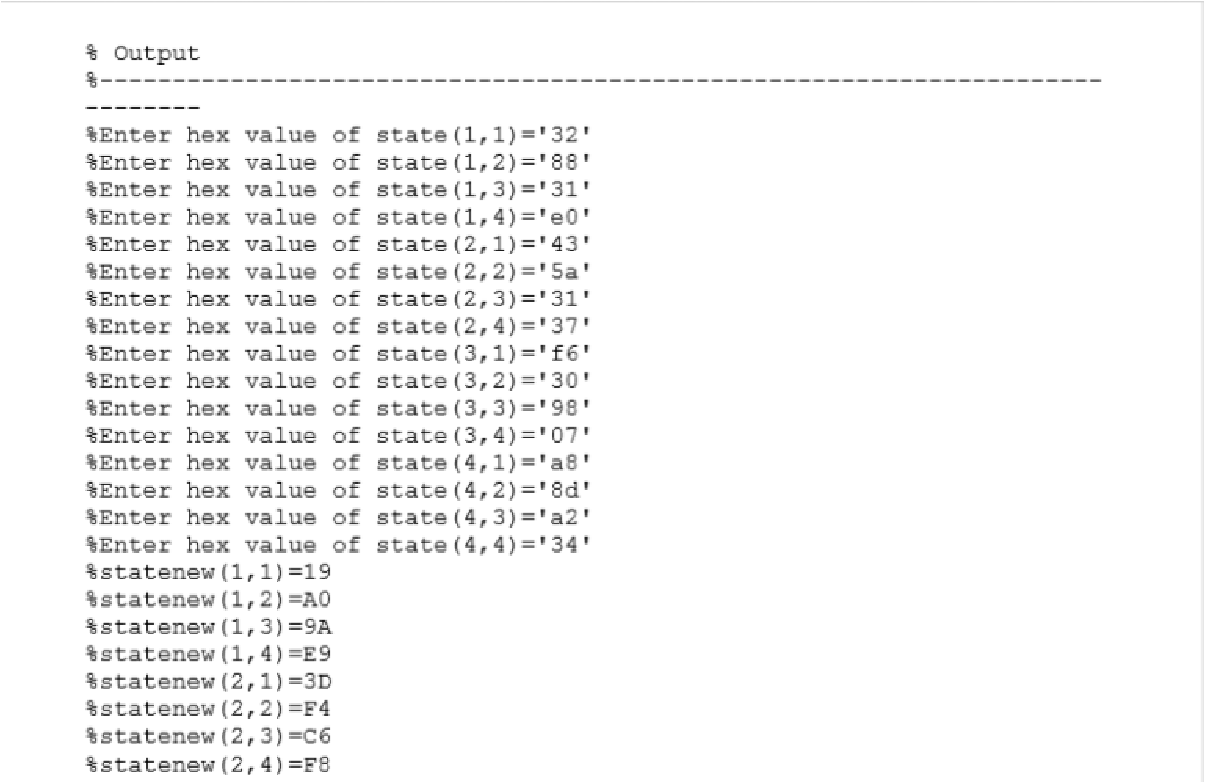


```
function y=addroundkey(x,w,round,Nb)
c=1;
for c=1:4
y(1,c)=bitxor(x(1,c),w(1,round*Nb+c));
y(2,c)=bitxor(x(2,c),w(2,round*Nb+c));
y(3,c)=bitxor(x(3,c),w(3,round*Nb+c));
y(4,c)=bitxor(x(4,c),w(4,round*Nb+c));
end
end
```

Figure 4 : Add Round Key operation

OUTPUT

Screenshots of the output:



```
% Output
%------------------------------------------------------------------------
--------
%Enter hex value of state(1,1)='32'
%Enter hex value of state(1,2)='88'
%Enter hex value of state(1,3)='31'
%Enter hex value of state(1,4)='e0'
%Enter hex value of state(2,1)='43'
%Enter hex value of state(2,2)='5a'
%Enter hex value of state(2,3)='31'
%Enter hex value of state(2,4)='37'
%Enter hex value of state(3,1)='f6'
%Enter hex value of state(3,2)='30'
%Enter hex value of state(3,3)='98'
%Enter hex value of state(3,4)='07'
%Enter hex value of state(4,1)='a8'
%Enter hex value of state(4,2)='8d'
%Enter hex value of state(4,3)='a2'
%Enter hex value of state(4,4)='34'
%statenew(1,1)=19
%statenew(1,2)=A0
%statenew(1,3)=9A
%statenew(1,4)=E9
%statenew(2,1)=3D
%statenew(2,2)=F4
%statenew(2,3)=C6
%statenew(2,4)=F8
```

Figure 5 : Output 1

CONCLUSION

In this paper, we propose a joint encryption and error correction coding method which applies to various communications domain. In this method the secret key of AES is adopted as the system key, the parallel encryption cod-ing is implemented in order to take advantage of excellent performance for long codes. At the same time, a new sub-key generation algorithm is proposed to keep the system more secure. Error correcting capability increases and it has more efficiency to secure the communications. Confidentiality of the message: only the authorized recipient should be able to extract the content of the cypher. In addition, obtaining information about the content of the message (such as a statistical distribution of certain characters) should not be possible, once the cryptographic analysis becomes easier. Message integrity: the recipient must be able to determine if the message was altered during transmission. Authentication of the sender: the recipient should be able to identify the sender and verify if it was him who sent the message. Irrevocability of the sender: it should not be possible to deny the authorship of the message.

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).