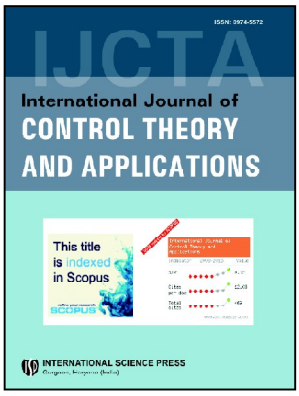


International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 49 • 2016

Implementation of AES Algorithm for High Security Applications

B. Raghavaiah[1] and Om Prakash[2]

[1] *Research Scholar, Department of Electronics and Communication Engineering, Jagdishprasad Jhabarmal Tibrewala University, India*
[2] *HOD, Department of Electronics and Communication Engineering, Jagdishprasad Jhabarmal Tibrewala University, India*
[1]*E-mail:raghavaece39@gmail.com,* [2]*om4096@gmail.com*

Abstract: It is an important responsibility of every federal organization is to select the applications of technologies and related safeguards in providing adequate security to its electronic data systems. The advanced encryption standard (AES) is one of the techniques that help for the federal organizations on providing security for their systems; the technique is explained in this publication. For maintaining confidentiality and integrity of the information represented, it is important to protect the data while transmission on while in storage.

The mathematical steps required to transform the data in cryptographic cipher and also to transform cipher back to original form are uniquely defined by the AES algorithm the federal agencies are provided with the AES, within the context of total security program containing the physical security procedure, with good information managing practices, and network access controls. For both transmitter and receiver the key must be provided simultaneously during the communication. Both encryption and decryption processes are explained in this presentation. The functionalities are verified by using ISIM simulator and synthesis is carried out by Xilinx ISE. 12.3I.

Keywords: AES, encription, decryprion, Xilinx

1. INTRODUCTION TO AES

The Advanced Encryption Standard which is shortly defined as AES which is a United states encryption standard defined in the federal information processing standard i.e., FIPS which is bit size of 128 bit and 192 bit size .In the year may 2002 it defined as federal standard. This Advanced encryption algorithm becomes as most recent for federal us in United States. One more algorithm is RSA which is a different way of cryptography process in this the bulk encryption of the information with RSA performed itself seldom. For use by Advanced Encryption Standard here we using RSA encryption keys let's take an example like Digital signature.

Whereas the AES i.e, Advanced Encryption Standard having the fixed size of blocks that is size of either r128 bit or 192 bit or else 256 bit of data in this way the data will perform different type of operation which are shown as below like byte substitution and the second one is mixed column and the third one is called add round here in this block the data perform the Xor function with the key which is brought from the key generation block, where in the key generation block 128 bit input key is expanded to different 128 bit key which are the number is

based on the number of rounds of operations which are performed over there by the key expansion operation in the fallowing below there is a clear explanation of each block of operation which is defined and repeated for different round it may be 10 or 15 rounds of these group of four operations.

The main operations performed in it are define as the byte substitution is the first operation in any round of this cryptography algorithm in this operation here we are using S-box data for the byte substitution of the data which is defined in matrix form for easy data of operations need to be performed in that way of process, whereas in the reverse process we are using an Inverse S-box For anti of this S-box operation. Whereas this S-box is the box which is defined in the matrix form for easy way bytes to be substitution by looking rows and column. The Shift Rows step operates on the rows of the state Whereas in this case the first row bits are unchanged and the second row of bits are performed one right shift operation and the third row of bits perform as two right shifts and this the shifting operation perform for the data which is shifting . For the block of size 128 bits and 192 bits the shifting pattern is the same. From each column of the input state in this way.

Whereas in this case the first row bits are unchanged and the second row of bits are performed one right shift operation and the third row of bits perform as two right shifts and this the shifting operation perform for the data which is shifting.

There must be no way to find the unencrypted clear text if the key is unknown, except brute force, i.e. to try all possible keys until the right one is found.

A secondary criterion must also be met:

In this criterion number of keys must be large.The first criterion satisfied with Data Encrption standard, but no longer the secondary crietrion– computer speeds have trapped up with it, or soon will. AES meets both criteria in all of its variants: AES-128, AES-192 and AES-256.

2. ANALYSIS

The advanced encryption standard is one of the better way of algorithm used for cryptography compared with other cryptographic algorithms. We are using different methods that which are suitable for dissimilar situations in cryptographic processes. The AES is very easy to implement but for obtaining good results much experience and skills are required. AES makes the system itself secure with the protected good and strong key, having hammer and saw cannot make some a good carpenter. The short introduction that describes the methodology to apply AES for the system for verifying purpose out of scope.

By doing the encryption with AES which is based on the secret key of 128, 192 or 256 bits. But AES is not that much secure when the key is easy to guess. For applying the AES the must be sufficiently strong and good. The strong and good keys are produced by unpredictability and randomness. The passwords and pass phrases are with fixed length of 128 bits which is much less than 256 bits. At least 10 passwords of the kind are used in day to day work are used for 128 bit pass phrase approach.

The amount of computation necessary to break keys can be somewhat strengthened by using some special computational steps. The weak keys are no way unique for AES and are risks of incorrect usage, implementation of these shared keys by all encryption algorithms. The key implementation to a relatively simple about how many bits the chosen key, password and pass phrase is. The estimation is somewhat tricky, when the key is not produced by a true haphazard generator.

The question is how long the encryption should be pretensed in provisions of time. Security depends on the amount of time and cost spent by the attacker to break the key.An aggressive estimation on the rate of technological progress is to assume that technology; this doubles the speed of computing devices every year with unchanged cost. The demonstrated systems today within the commercial budget of 1 million dollars to handle a key of length 70 bits. Then for 128 bit keys , in theory be in the range of a military budget within 30-40 years.

The illustration for the current status of AES is given as the following example, a system that tries keys at a rate of 1 billion keys per second, where the attacker with capability to build. This is at 1,000 times faster personal computer in 2004. By this assumption the intruder needs 10,000,000,000,000,000,000,000 years to try all possible keys for the weakest key of AES- 128. The length of the key determines the time and cost the spent by the intruder to break it. In other cases a lifetime is not long enough to break an AES-128.

3. PROPOSED MODEL

The AES is developed by to cryptographers namely Joan daemen and Vincent Rijimen. The name Rijndael Dutch pronunciation is a play on the names of two inventers, ADVANCED ENCRYPTION STANDRD is the name of the algorithm described by variant of Rijndael. In practice the algorithm is also referred as AES. it is fast in both hardware and software . Unlike DES, AES don't use feistal networks. The AES uses 128 bit fixed block and a key of 128,192 or 256 bit length. The block size has a maximum of 256 bits, but the key size has no theoretical maxima. The version of Rijandal with a larger block size have additional columns in the state of AES operates on the 4x4 column _ major order matrix of bytes, termed the state. The AES calculations are done in special finite fields.

Whereas the AES i.e., Advanced Encryption Standard having the fixed size of blocks that is size of either r128 bit or 192 bit or else 256 bit of data in this way the data will perform different type of operation which are shown as below like byte substitution and the second one is mixed column and the third one is called add round here in this block the data perform the XOR operation with the key which is brought from the key generation block , where in the key generation block 128 bit input key is expanded to different 128 bit key which are the number is based on the number of rounds of operations which are performed over there by the key expansion operation in the fallowing below there is a clear explanation of each block of operation which is defined and repeated for different round it may be 10 or 15 rounds of these group of four operations.

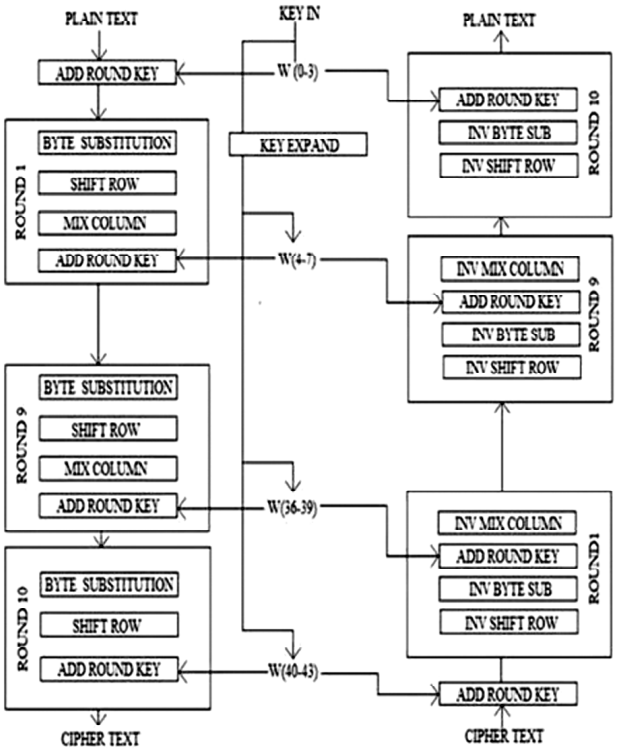


Figure 1: Block diagram of AES

(A) The Byte substitution Operation

The byte substitution is the first operation in any round of this cryptography algorithm in this operation here we are using S-box data for the byte substitution of the data which is defined in matrix form for easy data of operations need to be performed in that way of process, whereas in the reverse process we are using an Inverse S-box For anti of this S-box operation.

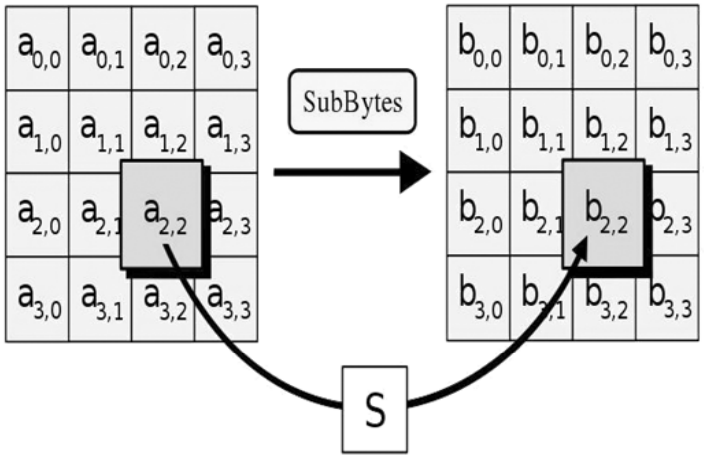


Figure 2: Byte Substitution operation

Whereas this S-box is the box which is defined in the matrix form for easy way bytes to be substitution by looking rows and column.

(B) Shift row Operation

The Shift Rows step operates on the rows of the state Whereas in this case the first row bits are unchanged and the second row of bits are performed one right shift operation and the third row of bits perform as two right shifts and this the shifting operation perform for the data which is shifting . For the block of size 192 bits and 128 bits the shifting pattern is the same. From each column of the input state in this way.

Whereas in this case the first row bits are unchanged and the second row of bits are performed one right shift operation and the third row of bits perform as two right shifts and this the shifting operation perform for the data which is shifting.

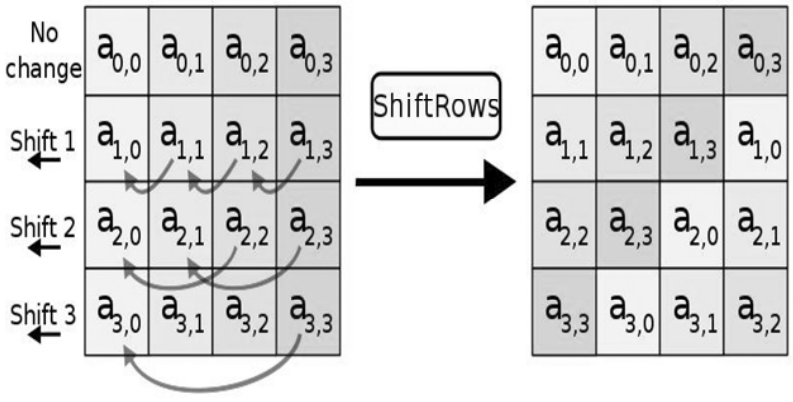


Figure 3: Shift rows information

(C) The Mix Columns step

In which here each column of the sate are combined using an invertible transformation operation in the mix column step. Whereas here the Mix Columns operation perform as like of 4 byte of operation as input and 4 bytes of operation as output

In the cipher text the Shift row and the mix column operation are makes diffusion.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Each Colum is by the known matrix it will perform the multiplication operation whereas here in this way 128 bit key of multiplication is performed whereas here multiplication by the value 1 means it is leaving unchanged and where it is multiplied the value of 2 is shifting to the left multiplication which is by the value 3 means shifting to its left and where it perform Xor operation with the initial un shifted value. When the shift operation completed the Xor operation with 0x1b will performed if incase the shifted value is more than 0xff.

Whereas here each of the polynomial is treated as the GF (2 power 8) and is the multiplied modulo x4+1 with the fixed value of the polynomial c(x) =0x03 and the equation is defined as x3 + x2 + x + 0x02. In their Hexadecimal pattern the coefficient are displayed of binary representation of the polynomials whereas this type of process ids defined as in article Rijndael Mix Colum operation.

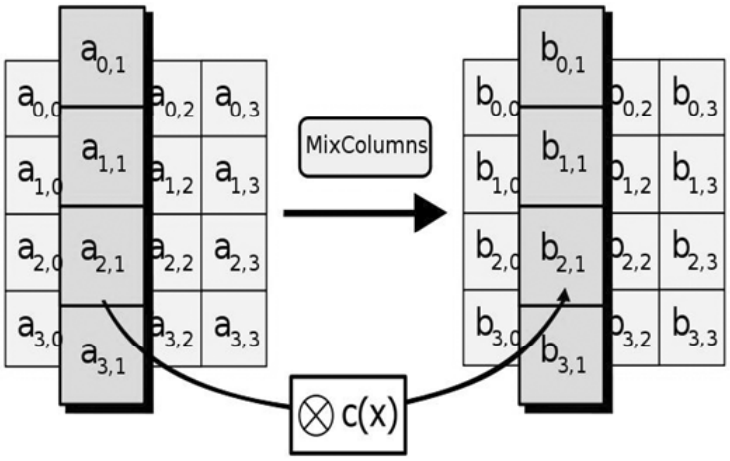


Figure 4: Mix Columns information

(D) The Add Round Key Operation

With the state in the Add round Key the sub key is pooled, where as for every round of operation the main key using Rijndel's key is schedule the same size as the state a sub key is derived. By combining each of the byte of the state using a XOR operation the sub key is added with sub key which is sub corresponding to it.

(E) Cipher Optimization

This cipher by merging Sub Bytes and Shift Rowables with MixColums having the 32-bit size word in this way it speed up the execution we have a possibility over here to convert them into the sequence of the Look Up

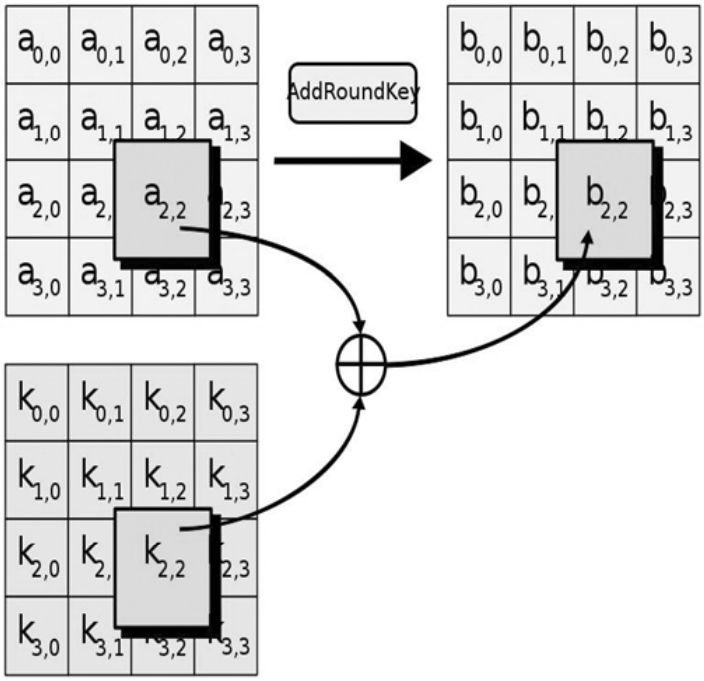


Figure 5: Add around key information

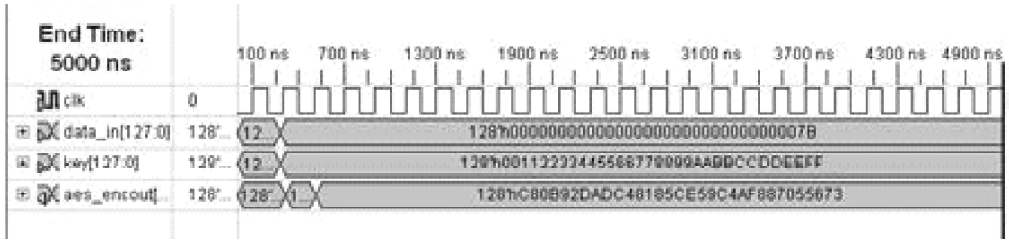
Tables which is define as technically as LUTs .In this way we need four 256 entries and 32-bit table format analysis for this it will occupy the space of 4096 bytes that is four kilo bytes memory for each one of the table.

Whereas with 166 tables of Lookups and twelve 32 bit exclusive OR operations which are pursued by the four 32 bit XOR operations.

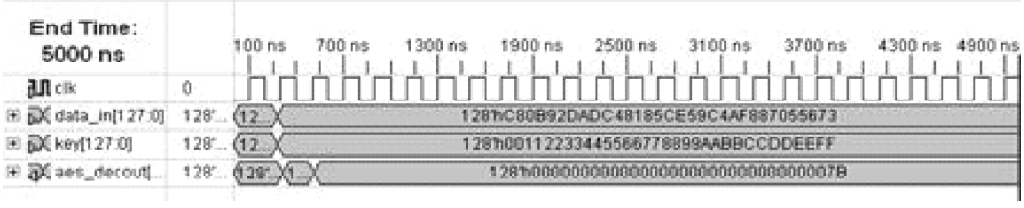
For the given target platform the $kb size memory is too large. By the use of the circle rotates the single 256 entries of 32 bit is like 1kb table.

4. RESULTS

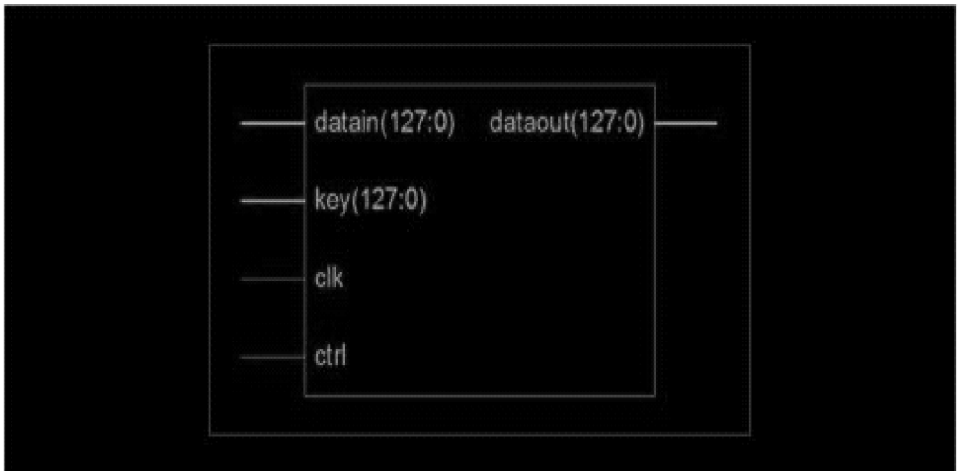
i) Encryption waveform



ii) Decryption waveform

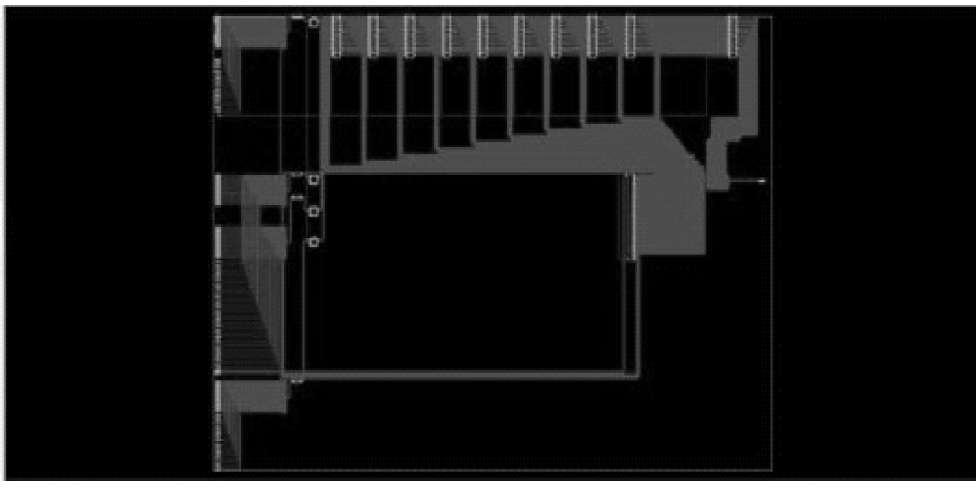


iii) Schematic



iv) RTL schematic of encryption

v) RTL schematic of decryption



5. CONCLUSION

In this paper, 128 bit security key is provided to convert the 128 bit plain text t and observed the cipher text. The original message can't be revealed to any intruder/ hacker. It is reveled for the sender and for the receiver by using key. So, the transmitted information is secure and safe by using AES. Modern features of AES cover a wide range of applications like secure internet that is defined as SSI, encrypted data storage, remote access servers,cable modems, secure videosurillance and electronic fianancial tansactions. The future scope of the research is to extend the input data from 128 bits to N bits, where N be any integer value over here.

REFERENCES

[1] J.Yang, J.Ding, N.Li and Y.X.Guo, "FPGA-based design and implementation of reduced AES algorithm" IEEE Inter. Conf. Chal Envir Sci Com Engin(CESCE).,Vol.02, Issue.5-6, pp.67-70, Jun 2010.

[2] A. M. Deshpande, M.S.Deshpande and D.N.Kayatanavar, "FPGA Implementation of AES Encryption and Decryption" IEEE Inter. Conf. Cont, Auto, Com, and Enter., vol.01, issue 04, pp.1-6,Jun. 2009.

[3] Hiremath S. and Suma. M. S. "Advanced Encryption Standard Implemented on FPGA" IEEE Inter.Conf. Comp. Elec.Engines.(IECEE), vol.02, issue.28, pp. 656-660, Dec. 2009.

[4] Abdelhafeez. S., Sawalmeh. A. and Bataineh. S. "High Performance AES Design using Pipelining Structure over GF (28)" IEEE Inter Conf. Signal Proc and Com., vol. 24-27, pp.716-719, Nov. 2007.

[5] Rizk. M. R. M. and Morsy, M., "Optimized Area and Optimized Speed Hardware Implementations of AES on FPGA", IEEE Inter Conf. Desig Tes Wor., vol.1, issue.16, pp.207-217, Dec. 2007.