International Journal of Engineering, Science and Mathematics
Vol. 6 Issue 8, December 2017 (Special Issue)
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Implementation of AES Architecture Design In High Level Cryptography

Ch.SantoshiKumari*
P.K.Suresh**
K.Pradeep***

Abstract

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in giving sufficient security to its electronic data systems. This publication explains a cryptographic algorithm, the Advanced Encryption Standard (AES) which can be utilized by Federal organization systems to save sensitive information. Safety of data during transmission or while in storage may be compulsory to keep up the confidentiality and integrity of the information provide by the data.

The algorithm clearly explains the mathematical process needed to send the data into a cryptographic cipher and also to transform the cipher back to the original position. The advanced Encryption Standard is being made available for use by Federal organizations within the situation of a total security program consisting of physical safety procedures, fine information management practices, and computer system/network access controls. In this the key should be available at the transmitter and receiver simultaneously during communication. In this project both encryption and decryption procedures are executed. The functioning is observed using ISE simulator and the synthesis is carried out using XILINX ISE 12.3i.

Keywords:

AES,

ENCYPTION,

DECRYPTION,

XILINX12.3i.

Author correspondence:

Chinta. santoshikumari,

P.G.Scholar,

BABA Insistute of Science And Techonlogy,BakkannaPalem,P.M.palem,Madhurawada,

1. Introduction

* Doctorate Program, Linguistics Program Studies, Udayana University Denpasar, Bali-Indonesia (9 pt)
** STIMIK STIKOM-Bali, Renon, Depasar, Bali-Indonesia
*** English Language Specialist, Oller Center, Carriage House, 2nd Floor, California, USA

AES is stands for Advanced Encryption Standard and is a United States encryption standard defined in Federal Information Processing Standard (FIPS) 192, printed in November 2001. It was considered as a federal standard in May 2002. AES is the most latest of the four current algorithms approved for federal us in the United States. We should not match AES with RSA, another standard algorithm as RSA is a different category of algorithm. Huge encryption of information itself is rarely performed with RSA.RSA is utilized to transfer other encryption keys for use by AES for example, and for digital signatures.

A symmetric encryption algorithm processing information in block of 128 bits is known as AES. The values zero and one will be taken a bit. In effect a two digit with two possible values as rejected to decimal digits that may take one of 10 values. A 128-bit blockis encrypted by sending it in a single way into a new block of the similar size, Under the effect of a key. AES is symmetric since the same key is utilized for encryption and the reverse transformation, decryption. The compulsory to keep for safety is the key. AES will be calculated to utilizes different key-lengths, the standard describes three lengths and the benefit algorithms are called AES-128, AES-192 and AES-256 in the same way to express the length in bits of the key. Every extra bit in the key effectively doubles the strength of the algorithm, when explained as the time compulsory for an attacker to perform a brute force attack, i.e. an exhaustive search of all possible key combinations in order to get the correct one.

In 1997 the US National Institute of Standards and Technology ended a call for candidates for a replacement for the ageing Data Encryption Standard, DES. 15 persons were allowed for further consideration, and after a whole public process and three open international conferences, the number of candidates was reduced to five. The last person was declared and comments were approved in FEB 2001. 21 organizations and candidates submitted comments None had any reservations about the suggested algorithm.

AES is established on strong and well-published mathematical ground, and appears to resist all known attacks well. It has been published for a long time has there’s a strong suggestion that impact no back-door or known weakness exist. It has been the subject of severe examination by researchers in the world, the whose accounts of economic value and information is already successfully protected by AES. It is clear that there are no unfamiliar factors in its design. The Belgian researchers developed it initialization. United state government developed the conspiracy. Therefore sometimes voices concerning the encryption standard. There is a fact that a solid encryption algorithm is necessary to meet only single main criteria.

- There is no way to get the unencrypted clear text if the key is unfamiliar except brute force, i.e. to try all possible keys until the right one is found.

A secondary criterion must also be met:

- Two stage a successful brute force, The number of possible keys should be so large that it is computationally easy for attacked in short enough a time.

The DES or Data Encryption Standard joins the first criteria, in fact no longer the secondary one. The speeds of computer were caught up with or soon will all of its variations of AES-128, AES-192 and AES-256 are met by AES.

2 ANALYSIS

AES may as all algorithms, be used in different ways to perform encryption. Based on different situation many methods are suitable. This is crucial that the right method which is applied in the right manner for every situation or the outcomes might well be unsafe even if AES as such is safe. To implement a system using AES as its encryption algorithm is very easy. But we need better correct way for a prevalent situation. A Good Carpenter well need a hammer and a saw to prove his skill. In the same way AES make a system secure by itself. To explain correctly how to apply AES for varying goals is very much out of scope for this short introduction.

Encryption with AES is based on a secret key with 128,192 or 256 bits. Ease Encryption with basis as the key is simple to estimate it does not matter if AES is secure. To apply good and strong keys as it is to implement AES properly, AES must be secure and crucial. We need careful design to create better and stronger keys in difficult problem. Now a days the challenge is faced by that computers are dangerously deterministic, but what is needed of a good and key of opposite – unexpectedly and randomness. The keys which are derived into a fixed length must match for encryption algorithm from pass phrases typed by a human beings rarely correspond to 128 bits much less 256. At least the common phrase of same frequently applied in day to day work necessary because it mandatory to approach 128 bit equivalence in a pass phrase. Special techniques can strengthen weak keys by like computationally careful steps which is amount of computation necessary to break it. All encryption algorithm shared the risks of faulty utilize, and execution and weak keys for AES. If the implementation is right the security given minimizes a relatively simple questions about how many bits the chosen key, password or pass phrase really corresponds to. Sometimes the calculation is rather easy to calculate is the key is not produced by approved random generator.

Security is not an absolute; it's a relation between time and cost. It is necessary to posed any question about the safety of encryption in terms of how I thought are how much time will it need an attacks to get a key. Now a days, there are some speculations that military group possibly a technical and economic means to fight keys similar to about 90 bits, although no civilian researcher has actually seen or reported of such a capability. These days demonstrate system within limit cross the commercial budget about 1 million dollars are able to tackle key lengths about a 70 bits. To calculate the technology which may double that need of computing devices each year at the same cost, an aggressive calculation on rate of technological program is mandatory. If it is correct, 128-bit keys should be in theory in range of a military budget within 30-40 years. The following example gives an illustration on the present status for AES. We can calculate an attacker with the capability to make are by a system that the rate of one billion keys per second. It is almost 1000 times faster than the fastest personal computer in 2004. The attacker should need above 10 000 000 000 000 000 000 000 to find all possible keys for the weakest version, AES-128 under the example. It is necessary for us to choose the key length after decided for how much security is needed and the cost must be to brute force a safe key. In some military situations a few hours or days security is enough – one the war is ended and the information uninteresting and without value. In other example a lifetime may not be long enough.

3 Existing architecture:

In an existing system executed the safety strengthened near field communication tag with possible architecture supporting asymmetric cryptography by security purpose. In this existing system elliptic curve cryptography is used for security purpose.Heavily reusing hardware components like common 8-bit microcontroller or a memory achieved the low area goals. Mobile phones were enabled to allow understanding safety related NFC/RFID applications. The beginning low resource RFID tag that helps asymmetric cryptography.In this asymmetric cryptography two separate keys utilized for the encryption and decryption process. Public key is utilized at encryption process and secrete key is used at decryption process.

There are two separate keys utilized for the encryption and decryption of data in an asymmetric cryptosystem. The key which is utilized for encryption is made public key and so as called public key, and the decryption key is kept secret and known as private key. The keys which are produced in such a way that it is not possible to get the private key from the public.

Both the transmitter and receiver both have two keys in an asymmetric system. Generally, the private key is considered as private and not allowed over with the information to the receivers, although the public key is allowed.

In this existing system memory modules were not used.

Limitations:

- Computational burden: By its very nature, public key cryptography is not as fast or computationally efficient as symmetric cryptography.

- Communication overhead: PKI typically require significant communication overhead (frequent and large messages).

- In an asymmetric cryptography public key is used in encryption process and private key is used in decryption process. So everyone knows the encryption key so there is chance to hack the data.

- Memory modules were not used.

4 PROPOSED MODEL

AES is a specification for the encryption of electronic data. It has been adopted by the U.S. government and is now used worldwide. The algorithm described by AES is asymmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

The operating of AES is a 4×4 column-major order matrix of bytes, termed the *state* (the big block size have extra columns in the state versions of Rijndael). Generally we do maximum AES calculations in a special way with finite field.

The AES cipher is classified as a many of repetitions of transformation rounds that make the input plaintext into the last output of cipher text. Every turn contains several processing measures including one that supports on the encryption key. A group of reverse rounds are used to send cipher text back into the real plaintext utilized the similar encryption key.

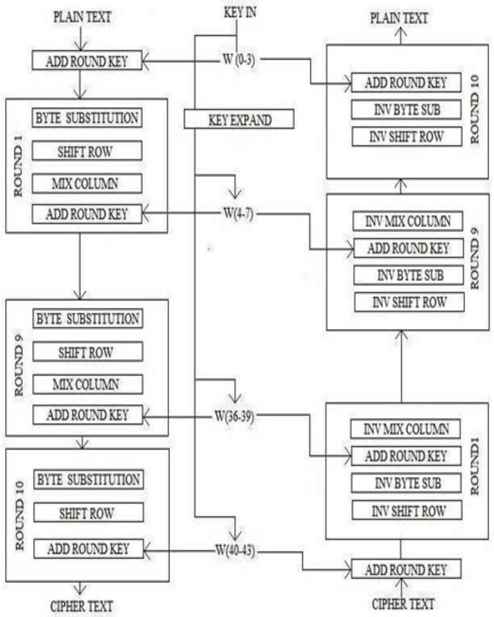
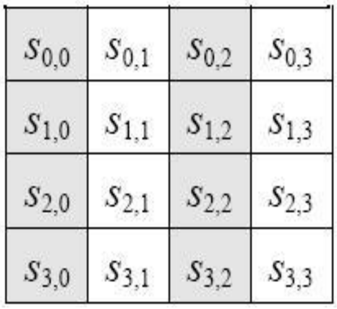


FIG 1 BLOCK DIAGRAM OF AES

AES algorithm consists of sequence of 128 bits of input and 128 bits of output. These bits are in the form of ‘0’s and ‘1’s.These sequences referred as blocks and the number of bits referred as their lengths. Internally the AES algorithm operations are performed on a two dimensional array of byte called the state. The state array diagram shown below. The state array consists of four rows and four columns of bytes, each row consisting of Nb byte. Nb is denoted as a block length. Here Nb=4, which reflects the number of 32-b words (number column) in the state array.



$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

Figure 4.2 State array

In AES algorithm, the length of the cipher key K is 128,192 or 256 bits. Nk = 4, 6, or 8 represents the key length which transforms the digit which 32-b words (number of columns) in the cipher key. Generally to perform AES the number of rounds to be performed during the execution of the algorithm which depend on the size of the key. The number of rounds which is recognized by Nr, where Nr = 10 when Nk = 4, Nr = 12 when Nk = 6 and Nr = 14 when Nk = 8. Here the designed architecture having Nr=10,and Nk=4.Figure shows the complete structure of AES algorithm .It performs both encryption and decryption process. Human beings depicts the FIPS 197 standard, as square matrix of bytes. The block which is transformed into state array that will be adjusted at every step of encryption or decryption process. In the same way we can depict the 128-bit key as a square matrix of bytes. Commonly a key can be extended into an array of key program words, every word is in order of 4-bytes and the total key programmed is 44 words for the 128-b key input.

Add Round Key: Encryption and Decryption Transformation:

In this add round key transformation, the 128-b of the state is bitwise XOR with128-bit of the round key. As explained in the figure, the operation can be considered as a column wise operation between the 4-bytes of a state column and one word of the round key; commonly we can view it as a byte stage program. The Add round key operation in decryption transformation is same, as XOR operation is its own inverse of encryption.

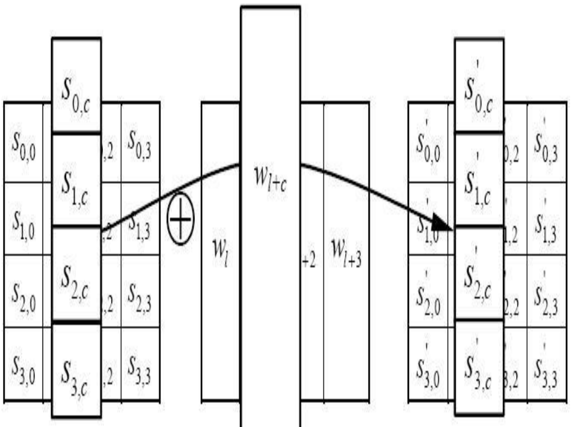
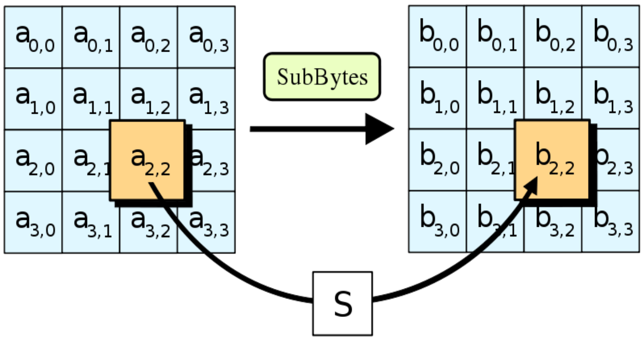


Figure3.3 Add Round Key Transformation for AES

The Sub Bytes step:

In the Sub Bytes step, we can updated every byte in the matrix by using an 8-bit substitution box, the Rijndael S-box. This program supplies the non-linearity in the cipher is utilized to derived S-box from the multiplicative inverse over **GF**(2^8),called to be a better non-linearity properties. The S-box is built to avid attacks related to a simple algebraic properties, By joining the inverse program with an invertible, we can also select the S-box. The S-box can also selected to avid all fixed points and all opposite fixed points.



$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

Fig 2 Information of Sub bytes

The Shift Rows step:

The Shift Rows every step function operates on the rows of the state; it also moves the bytes in every row by a certain offset. For AES, the first row is left unchanged. Every byte of the second row can be moved to the left in the same way the third and fourth rows can be transfer by offsets of two and three same order. The shifting pattern is the same for block of size 128 bits and 192 bits. Similarly every column of the output state of the Shift Rows step is composed by the bytes from every column of the input state. (Rijndael variations with a big block size also have a little different offsets). The first row is not changed and the transformation for second, third and fourth row is 1 byte, 3 bytes and 4 bytes same manner in the case of the 256-bit block respectively— when it is used with a 256-bit block, the change only applicable for the Rijndael's cipher as AES does not use 256-bit blocks.

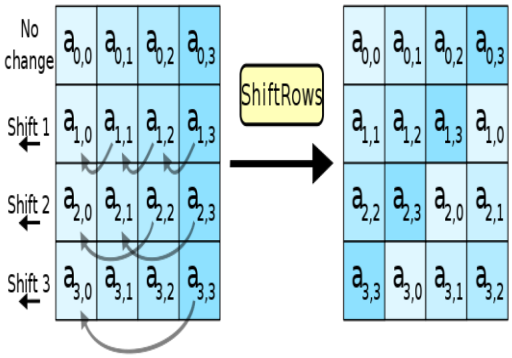

No change
Shift 1
Shift 2
Shift 3
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Fig 3 Information of Shift Rows

Mix Column:

Encryption and Decryption Transformation:

The mix column shifting works on the state column-by-column, considering every column as a four term polynomial. The column are considered as polynomial over GF (2^8) and multiplied with modulo x^4+1 with a fixed polynomial a(x), given by

$$a(x) = \{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$$

Let s\`(x) = a(x) x s(x):

$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c})$$

As a result of this multiplication, the four bytes in a column are replaced by the following

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

And the illustrates of Mix column transformation is shown here for the encryption process

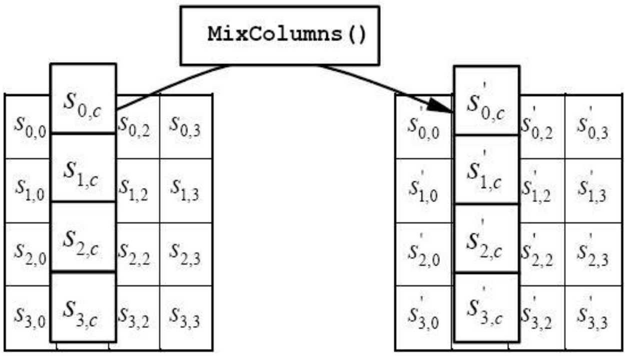

MixColumns()
$s_{0,0}$ $s_{0,c}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,c}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,c}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,c}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,c}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,c}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,c}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,c}$ $s'_{3,2}$ $s'_{3,3}$

Figure Mix Column Transformation of AES.

The Add Round Key step:

In the Add Round Key step, the sub key is joining every byte of the state. Every sub key is the same size as the state which the relevant byte of the sub key, For each round, a sub key is derived from the main key using Rijndael's key schedule: It is added by joining every; byte of the state with the corresponding byte of the sub key utilizing bitwise XOR.

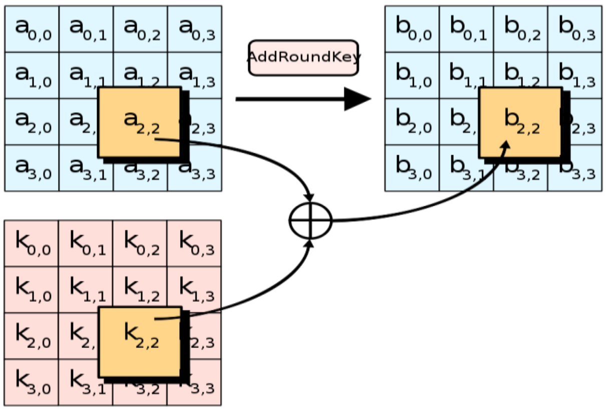

AddRoundKey
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

Fig. Add around key information

Optimization of the cipher:

It is easy to speed up implementation of this cipher by joining on systems with 32-bit are larger words which are done by the combination of columns, sub bytes, shift rows and sending then into a order of table observations. This may requires four 256-entry 32-bit tables that consume a total of four kilobytes (4096 bytes) of memory—one kilobyte for each table. A round completed with 16 table lookups and 12 32-bit exclusive-or operations, followed by four 32-bit exclusive-or operations which are followed by the Add Round Key step.

It result in four kilobyte table size which is too large for specified target. The table look up operation may be done with a single 256-entry 32-bit (i.e. 1 kilobyte) table by the use of circular rotates.

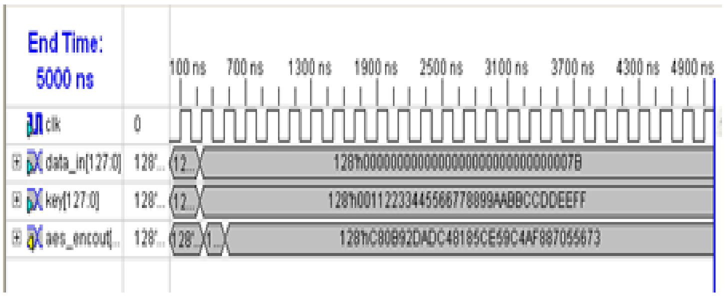
It is easy to join the Sub Bytes, Shift Rows, and Mix Columns stepby using a byte-oriented approach into a single round operation.

ADVENTAGES OF PROPOSED TECHNOLOGY:

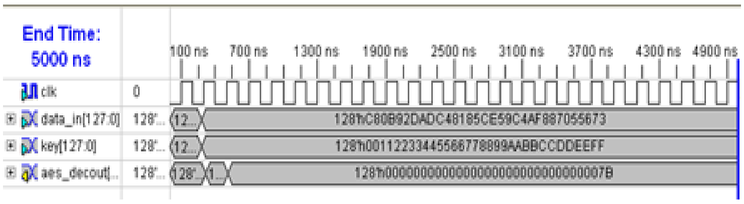
- It requires low space.
- Speed of operation is very high.
- Consumption of low power is required.
- Here we used memory modules to increase the security.

5 RESULTS

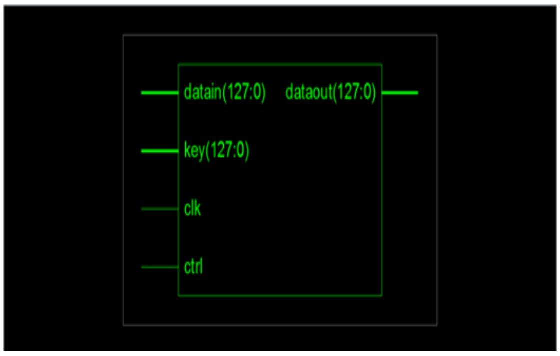
ENCRYPTION WAVEFORM


End Time:
5000 ns
100 ns
700 ns
1300 ns
1900 ns
2500 ns
3100 ns
3700 ns
4300 ns
4900 ns
clk 0
data_in[127:0] 128'... 12... 128'h0000000000000000000000000000007B
key[127:0] 128'... 12... 128'h00112233445566778899AABBCCDDEEFF
aes_encout[... 128'... 128'... 1... 128'hC80B92DADC48185CE59C4AF887055673

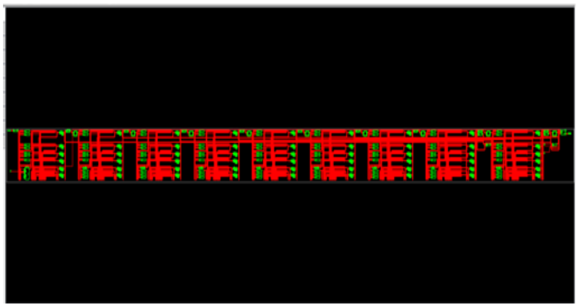
DECRYPTION WAVEFORM


End Time:
5000 ns
100 ns
700 ns
1300 ns
1900 ns
2500 ns
3100 ns
3700 ns
4300 ns
4900 ns
clk 0
data_in[127:0] 128'... 12... 128'hC80B92DADC48185CE59C4AF887055673
key[127:0] 128'... 12... 128'h00112233445566778899AABBCCDDEEFF
aes_decout[... 128'... 128'... 1... 128'h0000000000000000000000000000007B

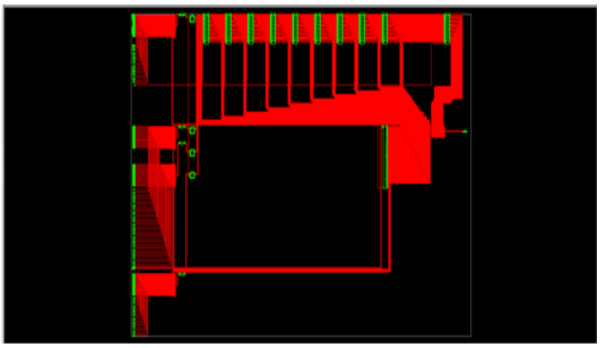
SCHEMATIC



RTL SCHEMATIC OF ENCRYPTION



RTL SCHEMATIC OF DECRYPTION



6 CONCLUSION

In this project, we have given 128 bits input and 128 bits security key and observed how it is delivered at the output with security. In this project there is no revealing of the original message to the hackers. The original message can be revealed to only sender and the receiver. So, in future, any propriety information can be transmitted securely by using this project (military or banking purposes) .

Modern applications of AES cover a wide variety of applications, such as secure internet (SSL), electronic financial transactions, remote access servers, cable modems, secure video surveillance and encrypted data storage. The future scope of our project is to extend 128 bits inputs to n bits(n is any integer value).

7 REFERENCES:

[1] J.Yang, J.Ding, N.Li and Y.X.Guo,“FPGA-based design and implementation of reduced AES algorithm” IEEE Inter.Conf. ChalEnvirSci 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”IEEEInter.Conf.Cont,Auto,Com,andEner., vol.01,issue04, pp.1-6,Jun.2009.

[3] Hiremath.S. andSuma.M.S.,“Advanced Encryption Standard Implemented on FPGA” IEEE Inter.Conf. Comp ElecEngin.(IECEE),vol.02,issue.28,pp.656-660,Dec.2009.

[4] Abdel-hafeez.S.,Sawalmeh.A. andBataineh.S.,“High Performance AES Design using Pipelining Structure over GF(28)” IEEE Inter Conf.SignalProc and Com.,vol.24-27, pp.716-719,Nov. 2007.

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

[6] Liberatori.M.,Otero.F.,Bonadero.J.C. andCastineira.J. “AES-128 Cipher.High Speed, Low Cost FPGA Implementation”, IEEE Conf. Southern Programmable Logic(SPL),vol.04,issue.07,pp.195-198,Jun. 2007.

[7] Abdelhalim.M.B., Aslan.H.K. andFarouk.H. “A design for an FPGAbased implementation of Rijndaelcipher”,ITICT. Ena Tech Soc.(ETNKS), vol.5,issue.6,pp.897-912,Dec.2005.