Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/8845
DOI URL: http://dx.doi.org/10.21474/IJAR01/8845
ISSN NO. 2320-5407

RESEARCH ARTICLE

IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) FOR HIGH-SECURITY APPLICATIONS.

Badugu Nikhil Teja[1], Shweta Helchel[1], P.Sai Krishna Pratap Reddy[1] and V.SeethaRama Rao[2].
1. U.G. Student, Department of Electronics and Communication Engineering, SNIST, Telangana, India.
2. Assistant Professor, Department of Electronics and Communication Engineering, SNIST, Telangana, India.

Manuscript Info

Manuscript History
Received: 08 February 2019
Final Accepted: 10 March 2019
Published: April 2019

Key words:-
Encryption, Steganographic, Rounds, Symmetric key, Simulation.

Abstract

Advanced encryption standard is a steganographic algorithm that will be used to protect the confidential data. In this project we use a Symmetric key, i.e. same key expansion algorithm is used for both encryption and decryption. The AES can be programmed in software or built in with hardware implementations (like FPGA). The numbers of rounds that has to be performed depends on the size of the key. As we are using 128-bit key which consists of 10 rounds, this makes more complex to crack the information. As the key size increases, the number of rounds also increases and complexity also increase. So, it plays a major role in high-security applications. This algorithm is used in many high-security applications like Secure socket layer, OFTP, HTTPS, FTPS, SFTP, AS2, WebDAV, Online financial Transactions, E-Business Code.

Introduction:-

Communication through the networks around the world plays an enormous role in almost all the fields. But the data which are continuously transferred in the cloud server may at times get hacked as there exist few malicious people. Since there is an explosive growth of electronics and computer science the only process to store the huge amount of secured data is in the clouds. But now arises a doubt that is cloud safe? In order to clarify this doubt and side by side provide the best mathematical algorithm, there was the introduction to Cryptography. Cryptography is the process of hiding our secured and confidential data in different methods that will safeguard our information. Basically, there are two methods, namely Encryption and Decryption. Briefly speaking in encryption the original plain text is coded in such a way by using different algorithms (called as Block Cipher) while sending so that its secured and similarly on the reception side this encoded data is decoded by using the same algorithm but in an inverse process this method is called as Decryption. Since there is a heightened afraid that the data will be leaked either while transmission or in reception many of the highly esteemed and repudiated organizations prefer to follow this technique. As many of them are using there is an enormous number of developments in the field of cryptography and security of the network.

Hence this leads to the development of the higher versions of the advanced encryption standards by modifying the algorithm and making it far stronger to be hacked.

Corresponding Author:-Badugu Nikhil Teja.
Address**:-**U.G. Student, Department of Electronics and Communication Engineering, SNIST, Telangana, India.

Literature Survey

AES is originally known as Rijndael (name of the scientist), is the process of encoding the information which was found by US institute named the National Institute of Standards and Technology (NIST).Security of data and services plays a vital role in today's business world. Innumerable agencies want a strategic data protection technique for managing its data and avoid hacking of its highly esteemed secured information, because an unprotected data leads to a loss of millions of money when it gets in the hand of malevolent persons. Advanced Encryption Standard (AES), is one among the foremost digitalized secured technique that can be used for protecting the data in different techniques. AES does this by encrypting the data at the transmission as well as the reception side by introducing a symmetric key.

Generally, there are two ways of Encryption, They are: Symmetrical Encryption& Asymmetrical Encryption. AES uses only Symmetrical Encryption.

Symmetrical Encryption:

Symmetrical Encryption is an oldest and panoramic technique. This key either uses a string or a number. This key blends with the plain text and make the hacker unknown of our information. The important criterion to be remembered in this technique is that the Key which will be created in the Key expansion algorithm should be remembered by both the sender and the recipient. In case the receiver forgets the algorithm to expand the key, he can retrieve the key from the sender hence making it less difficult to memorize the techniques. The major point to be observed is that it makes use of a single key making the algorithm much simpler and easier for the lame person. This key can be of higher powers of 2. As the power increases the more secured data will be to get hacked.

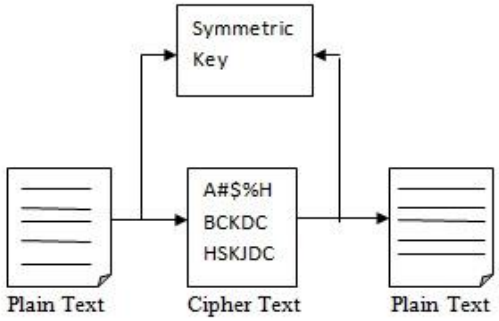

Fig 1:-Symmetric Encryption

ADVANCED ENCRYPTION STANDARD ALGORITHM

The Advanced Encryption Standard is specified as a iterative process that convert the input text (i.e. original text) into the output Cipher text. Each processing step depends on the key which is obtained from Key Expansion algorithm (which is explained below). This is a repetitive mathematical algorithm which uses four operations in each and every round; those are SubBytes, ShiftRows, and MixColumns and AddRoundKey algorithms in Encryption side. But in decryption side it uses four operations namely InvSubBytes, InvShiftRows, InvMixColumns and AddRoundKey.

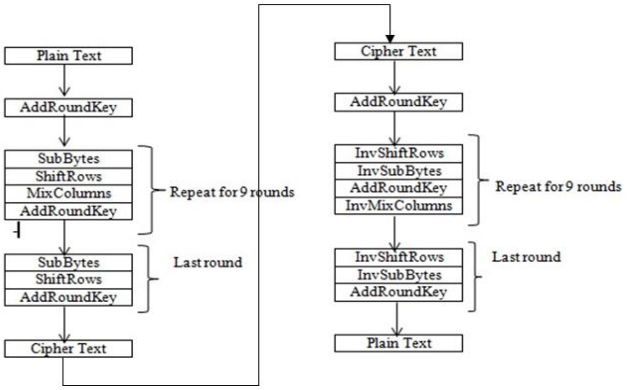

Fig 2:-Block Diagram Of Aes

Encryption:

Encryption is a miscellaneous process of hiding the confidential data in such a manner that in case if there is a loophole in the data it can't be known by the third person. In simple words the process of encoding the data by the mixture of various pseudorandom characters, digits randomly placed in differed notations (i.e. either in hexadecimal, decimal, octal or binary).More the mathematical operations are done the more secure the data will be. In this project we send the input data of 128-bit in the form of hexadecimal, and which is entered in the matrix of array called as State array and also a 128-bit Key is generated called as key array. Each array consists of 4 rows and each element is of 1 byte, where as one column forms a word.

SubBytes Transformation:

We use a predefined matrix called as S-box or Substitution box. This S-box will increase resistance towards specific attacks. If we give input as one byte it will match its corresponding substitute in the s-box and replace the particular data with the data present in the S-box.

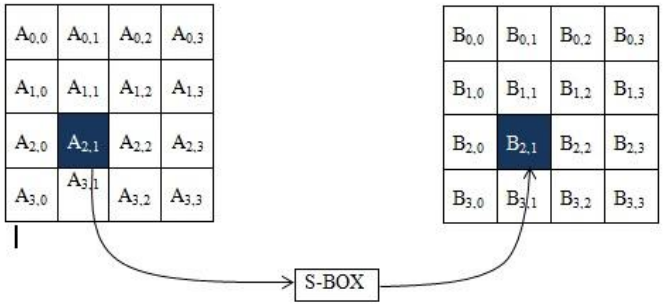

Fig 3:-SubBytes Transformation

ShiftRows Transformation:

The output from the Sub-bytes is given as input to this operation. This transformation depends mainly on the circular left shift operation. In the first row there is no change. In second row there will be one byte circular left shift. In third row there will be two byte circular left shift. In fourth row there will be three byte circular left shift.

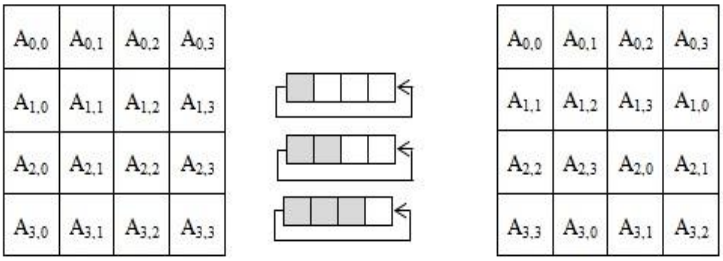

Fig 4:-ShiftRows Transformation

MixColumns Transformation:

The output from the shiftrow is given as input to this operation. In Mix Columns transformation, the columns of the state are considered as polynomials over GF (2^8) and multiplied by modulo of (x^4+1) with an already predefined polynomial c(x), given by: $c(x) = 3x^3 + x^2 + x + 2$.

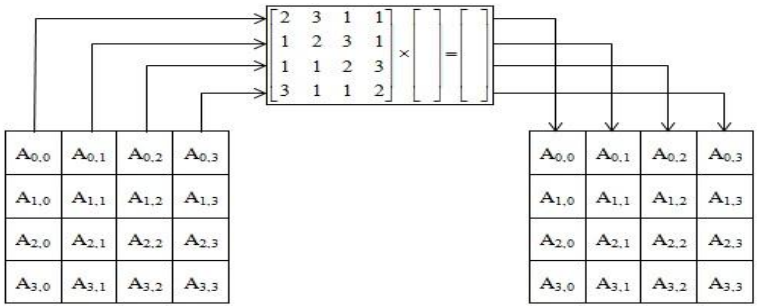

Fig 5:-MixColumns Transformation

AddRoundKey Transformation:

In the Add Round Key transformation, state array from the previous operation is given as a input. For every round a separate key is generated by using key expansion algorithm. This Key is generated from the original key that is given as input. This Round Key is performed bitwise ex-or operation with the input.

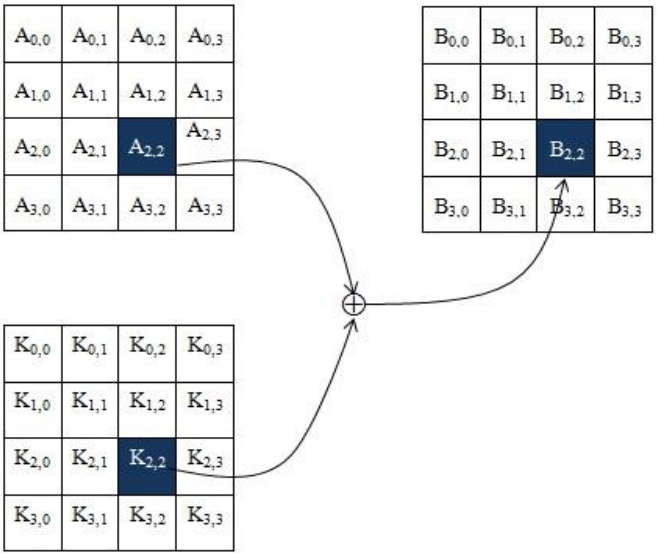

Fig 6:-AddRoundKey Transformation

KeyExpansion Transformation:

For every round there will be a round constant. After the substitution from the S-Box, bitwise ex-or operation is done with the round constant. The resultant word (one column consist of 32 bits) is performed bitwise operation with the previous round key's first column to generate the 1st column of new key. Then similarly bitwise operation is done with the previous round's second column to get the second word of new key. Next bitwise operation with the previous round's third column is done to get the third word for new key. Later, bitwise operation is performed on previous round's fourth word to generate the last word of new key. where Rcon is the Round Constant and RotWord is the Rotation of the word by one byte.

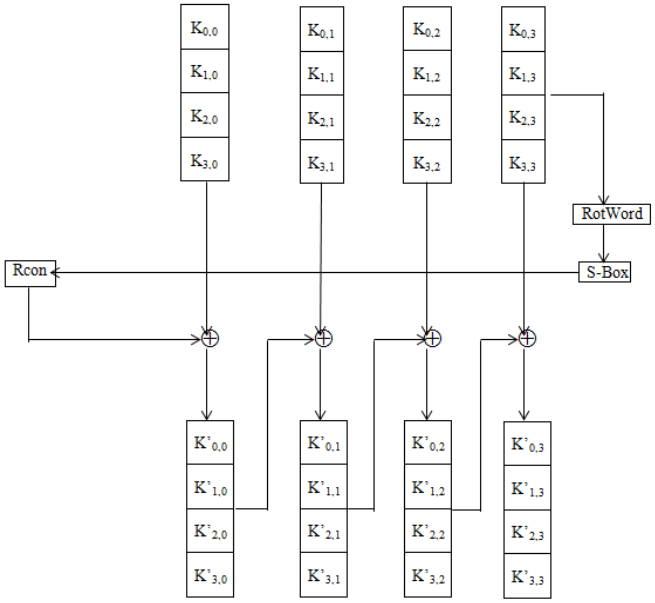

Fig 7:-KeyExpansion Transformation

Decryption

Decryption is the method of decoding the encrypted form of the data known as the cipher text in a way that only legalized persons can have access to retrieve the original data. The encrypted data, which is referred to as cipher text, is

decoded using an algorithm. An authorized receiver can easily decode the data with the key provided. Expect the AddRoundKey remaining transformations are different from Encryption.

InvSubBytes Transformation:

InvSubBytes Transformation is a non-linear transformation which uses a predefined matrix called Inv S-Box or Inverse Substitution Box. The output from the encrypted block is used as input, in this transformation the data is substituted similarly like the algorithm of sub-bytes of the encryption block.

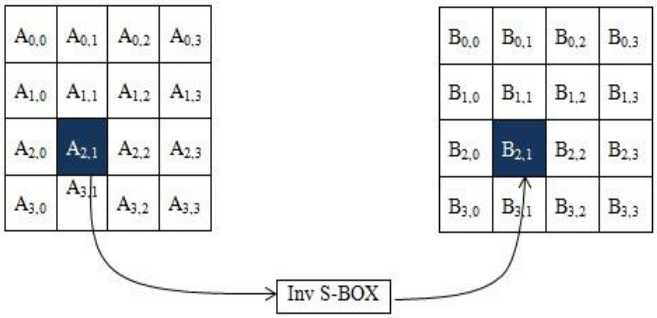

Fig 8:-InvSubBytes Transformation

InvShiftRows:

The input which is of 16×16 matrix is subjected to circular right shift operation. In the first row there is no change. In second row there will be one byte circular right shift. In third row there will be two byte circular right shift. In fourth row there will be three byte circular right shift.

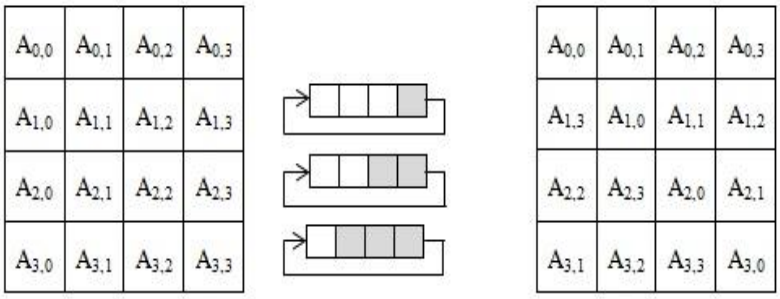

Fig 9:-InvShiftRows Transformation

InvMixColumns Transformation:

In Mix Columns transformation, the columns of the state are considered as polynomials over GF (2^8) and multiplied by modulo of (x^4+ 1) with an already predefined polynomial c(x), given by: $c(x)=11x^3+13x^2+9x+14$.

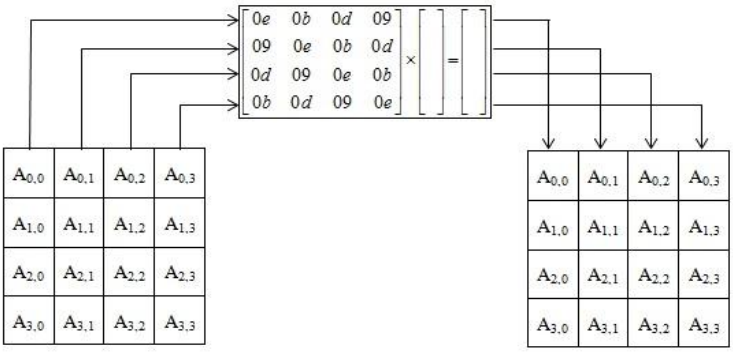

Fig 10:-InvMixColumns Transformation

Experimental Results:-

The programming is done in Verilog HDL. Synthesis and Simulation is done using Xilinx software. The following table shows the Design action and the following tools used for that design action.

Design Action	Tool Name
Design Entry	Verilog HDL
Synthesis Xilinx	Synthesis Tool(XST)
Simulation	Xilinx 2017.4

Encryption results:

Inputs to the encryption code are the Key[127:0],plaintext[127:0] and the output is ciphertext[127:0]. Given inputs in form of hexadecimal which is of 128 bits

1. **key**[127:0]=356893ff025686bbc9a68ce741cdaf3b.
2. **plaintext**[127:0]=52439da8f8daf08b8131681200c70ed4.
3. After undergoing 10 rounds of operation we get encrypted data i.e. **ciphertex**t[127:0]=c239afb5f19ac079bac c2ede6b7c18e1.

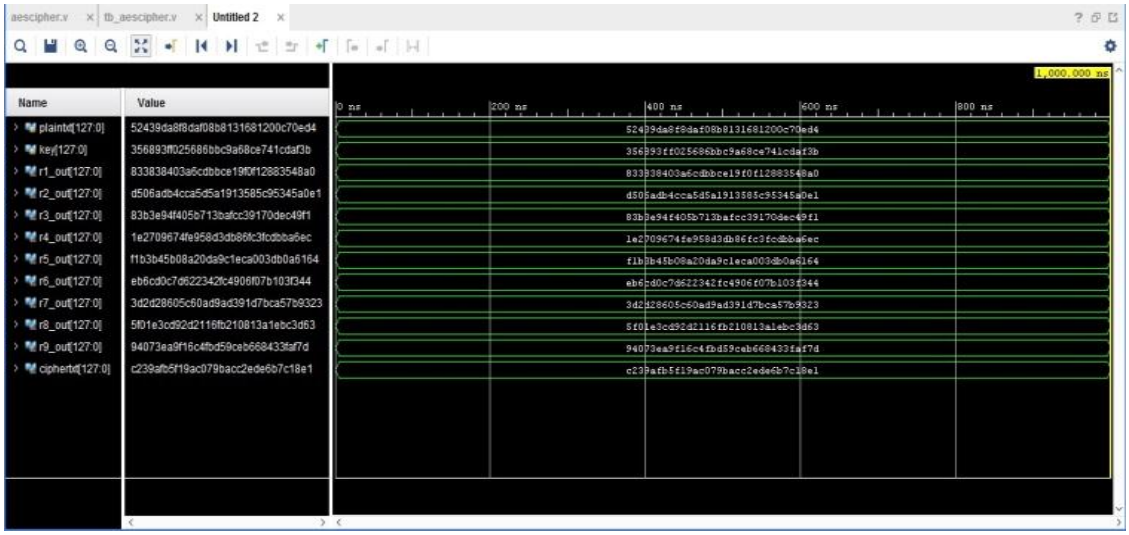

Fig 11:-Encryption Simulation Results

The above figure shows the inputs i.e. plaintext, key and it shows the output of every round (r1_out,r2_out,…). The final round output is the encrypted form of the plaintext which is the cipher text.

Decryption reults:

Inputs are key[127:0] and cipher text[127:0]. Outputs are plain text[127:0].

1. Let the value of key[127:0]=356893ff025686bbc9a68ce741cdaf3b.
2. The output of Encryption is given as input i.e. ciphertext[127:0]=c239afb5f19ac079bacc2ede6b7c18e1.
3. After undergoing 10 rounds of operation we get original data i.e. plaintext[127:0]=52439da8f8daf08b8131681200c70ed4.

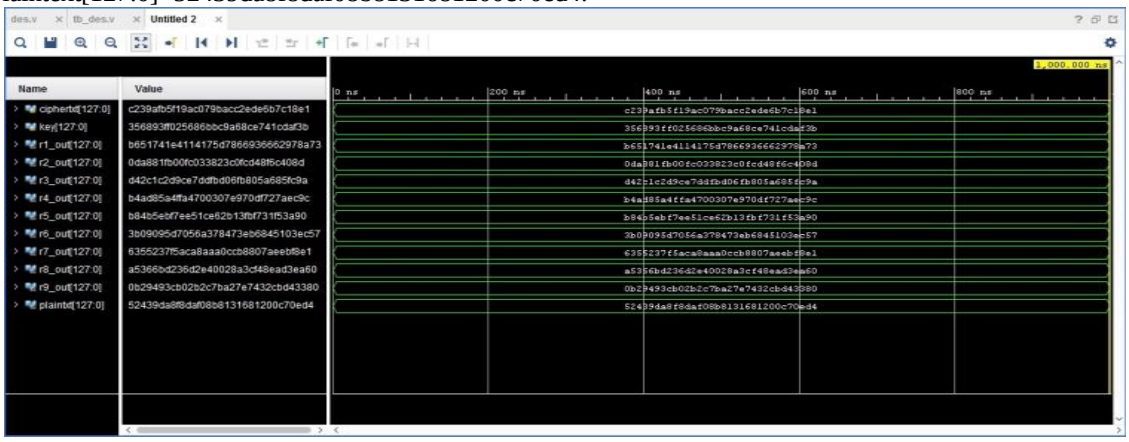

Fig 12:-Decryption Simulation Results

The above figure shows the inputs i.e. cipher text, key and it shows the output of every round (r1_out,r2_out,…). The final round output is the original data which is known as plaintext.

Conclusion And Future Scope:-

Advanced Encryption Standard (AES) is the advanced form of encrypting the data as it uses more rounds based on key size. It is difficult to hack the data as it requires 2^{128}(for 128bit key) trails to break the information. Since it is more accurate, so it is in many high security applications

This AES algorithm can be further implemented on the audio, video and image files. Further efficient way of using this algorithm is by using Fast Fourier Transform (FFT) i.e. converting the data into FFT and then undergoes AES transformations.

References:-

1. Ai-Wen Luo, Qing-Ming Yi, Min Shi, "Design and Implementation of Area-optimized AES Based on FPGA", 978-1-61284-109-0/11/2011 IEEE.
2. Yang Jun Ding Jun Li Na Guo Yixiong "FPGA-based design and implementation of reduced AES algorithm," 978-0-7695-3972-0/2010 IEEE DOI 10.1109/CESCE.2010.123.
3. M. Hasamnis, P. Jambhulkar and S. Limaye, "Implementation of AES as a Custom", Advanced Computing: An International Journal (ACIJ), vol.3, No.4, July 2012.
4. WANG Wei,CHEN Jie,XU Fei, "An Implementation of AES Algorithm Based on FPGA", 978-1-4673-0024-7/2012 IEEE.
5. Amaar, I. Ashour and M. Shiple " Design and Implementation A Compact AES Architecture for FPGA Technology", World Academy of Science, Engineering and Technology 59 2011.
6. J. Daernen and V. Rijrnen, "The Design of Rijndael", Springer-Verlag Berlin Heidelberg, 2002.
7. Jyrwa and R. Paily, "An Area-Throughput Efficient FPGA imple-mentation of Block Cipher AES algorithm", IEEE International Confer-ence on Advances in Computing, Control, and Telecommunication Tech-nologies, pp. 328-332, 2009.
8. William Stallings, " Cryptography and Nework Security", Third Edition, Pearson Education, 2003.
9. M. C. LIBERATORl and J. C. BONADERO "Aes-128 Cipher. Minimum Area, Low Cost FPGA Implementation"
10. Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).
11. Ritu Pahal Vikas kumar,"Efficient implementation of aes" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013 ISSN: 2277 128X.
12. Verilog HDL: A Guide to Digital Design and Synthesis, By Samir Palnitkar.