International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 2, March-April 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Implementation of Advanced Encryption System Algorithm

Mr. Parasurama[1], S. Nandheeswar[2], S. Anuradha[3]
[1] Associate Professor, [2,3]Student
[1,2,3]Department of Electronics Communication and Engineering, JNTUK University College, PPDCET, Vijayawada, Andhra Pradesh India

ABSTRACT
Moved Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an embraced cryptographic count that is used to make sure about electronic data. The tremendous and creating number of web and remote correspondence customers has incited an extending solicitation of security endeavors and contraptions for guaranteeing the customer data transmitted over the unbound framework with the objective that unapproved individuals can't find a good pace As we share the data through remote framework it should give data security, genuineness and approval.

The symmetric square figure expects a huge activity in the mass data encryption. A champion among other existing symmetric security computations to give data security is moved encryption standard (AES). AES has the advantage of being completed in both gear and programming. Gear execution of the AES has some portion of bit of slack such has extended throughput and better security level.

Keywords: *Encryption, Crypotography, Xilinx, Aes, Fpga*

How to cite this paper: Mr. Parasurama | S. Nandheeswar | S. Anuradha "Implementation of Advanced Encryption System Algorithm" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-2, April 2024, pp.839-843, URL: www.ijtsrd.com/papers/ijtsrd64771.pdf

IJTSRD64771

I. Introduction:
The more accommodating and amazingly monstrous got symmetric encryption estimation subject to be experienced these days is the Advanced Encryption Standard (AES). It is found at any rate six wrinkle snappier than triple Data Encryption Standard. An isolated from this for DES is required as its key size was thusly humble. With extending repeating power, With growing reenacting power, it had been thought of defenseless against complete key interest attack. Triple DES was proposed to beat this disadvantage in any case it had been found moderate. This secret creating procedure uses what's known as a square figure formula to avow that data is gotten a good deal on the secretively.

Rijndael count is symmetric square figure that can strategy data squares of 128 bits, using figure keys with lengths of 128, 192, and 256 bits, which is dictated by the flips standard. Rijndael was proposed to manage additional square sizes and key lengths; The figuring may be used with the three unmistakable key lengths appeared above, and in this manner these different flavors may be suggested as "AES-128", "AES-192" and "AES-256.

II. RELTED WORK
""Having an overview of important documents before every task helps bring forward fresh ideas for project implementation. For the purpose, it is very important to prepare a written summary of this particular task work that focused on the literature distributed up to that point and previous research in this field. The synopsis was completed using sources such as distributed articles, websites, and winners' records..

III. CRYPTOGRAPHY
"Cryptography is a system for securing information and communications using code, with the purpose of ensuring that only those who successfully receive the information can receive and process it." Prefix The word "mausoleum" means "hidden" and the suffix "graphy" means "form." In cryptography, the methods used to protect information are based on logical thinking, and many rule-based methods rely on realized numbers to convert messages into habits that make them difficult to decipher. Masu. These

numbers are used to ensure the validity period of encryption keys, electronic verification and confirmation to ensure data security, online verification over the Internet, and private transactions such as transactions with Visa and Platinum cards. will be done.

IV. IMPLEMENTATION

AES calculations are done using Verilog encoding in Model Sim Altera Web Elective 6.3g. First, we try to perform the computation by encoding and unscrambleing a single 128-bit square. Once a functional square shape is in place, the resulting step is to embed this square shape into a square movement strategy. The figure input (CFB) shown in Figures 4 and 5 was chosen because messages should not be embedded in the square size of another figure while preventing some control over the figure's content.

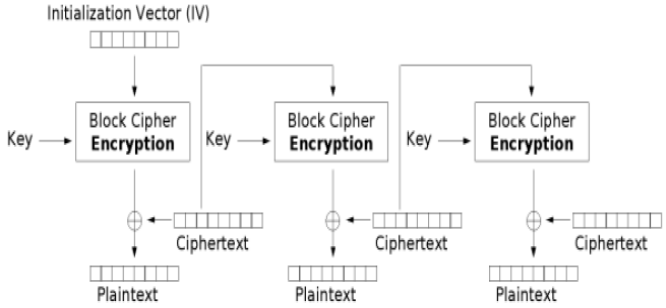


Figure-1: Decryption Using Cipher Feedback (CFB)

V. PROPOSED METHOD

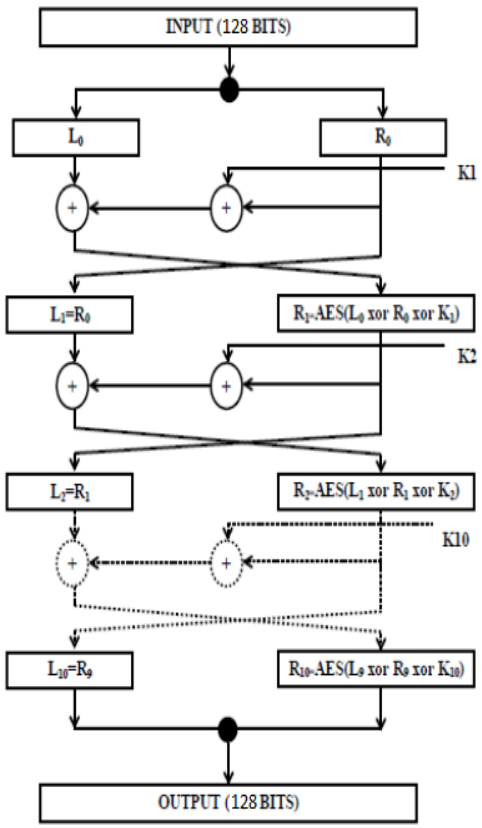


Figure-2: algorithm block diagram

``The basic idea of the proposed model is to integrate AES into all foci of the DES Fiesta network. Numerically, each round of the model can be communicated as follows: ``The above The set of conditions is emphasized over a total of 10 rounds, where the data square of 128 data is divided into left and right halves, and every round n, the left bit and right bit (Ln-1, Rn) of the last round. An XOR operation is performed between the three elements of -1) The key (Kn) created in this round was created as a commitment to the AES count.

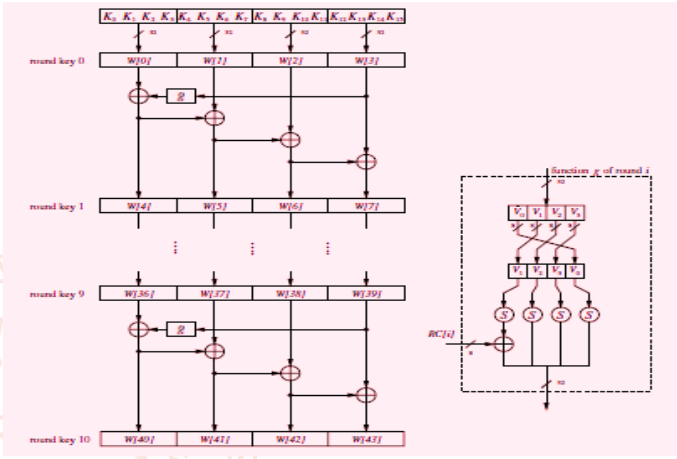


Figure-3: Synchronized Key Generation Algorithm

"AES systems process blocks of data that are 128 bits long using symmetric keys that are 128, 196, or 256 bits long. The exercise runs on 4 x 4 byte plans called states. The measurement includes dynamic steps. However, the teaching files contained in the state group are merged with the master key by the Add Round Key mod 2 extension. "The following steps are not repeatable changes." Each round performs four great tasks:

(1) ``byte sub byte replacement"

(2) ``row shift shift"

(3) ``section mixing, column mixing"

(4) "Add Round Key"

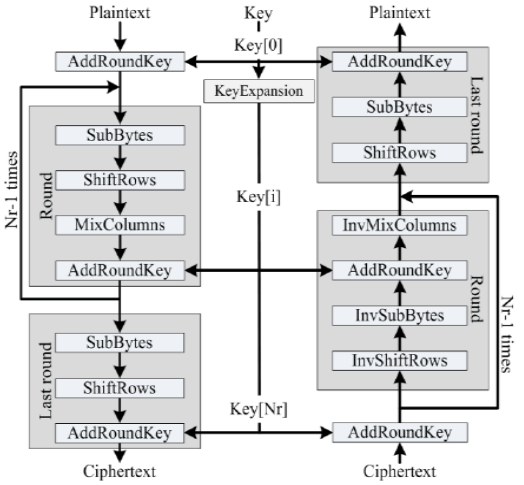


Figure-4: Block diagram

VI.RESULT&ANALYSIS

11010111001010101001101111011110001000100010010011111101011111101111011101000100111001101111111110010110110011111000111110011011

128'h 1f4 enc input

128'h d72a9bde2224fd7ef744e6ff96cf8f9b.... enc output

128'h d72a9bde2224fd7ef744e6ff96cf8f9b...dec input

"128'h 1f4 dec output

rst,sel= 1st 10,2nd 00, 3rd 11;

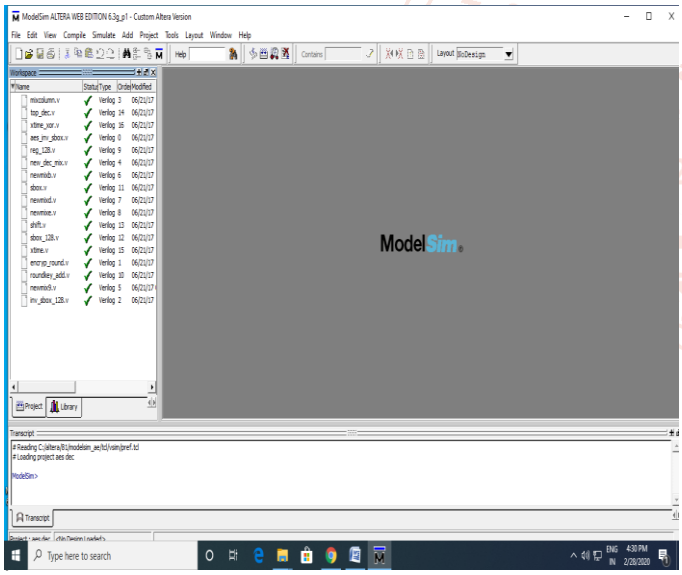


Figure-5:compile code

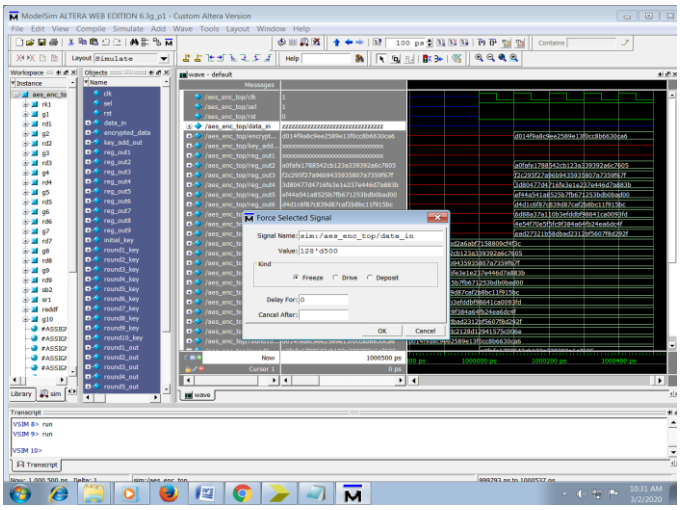


Figure-6: AES Encryption Input:128'd500

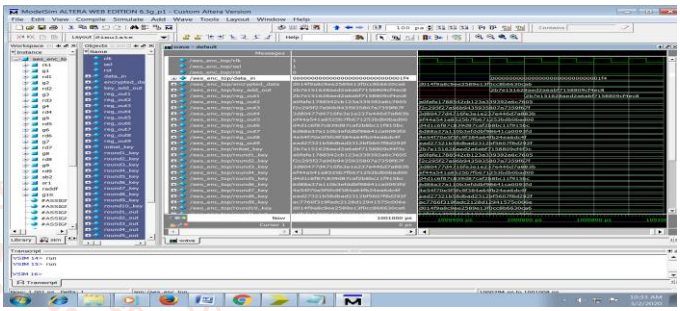


Figure-7: AES Encryption Input:128'd500 converted to hexadecimal equal to 000000000000000000000000000001F4

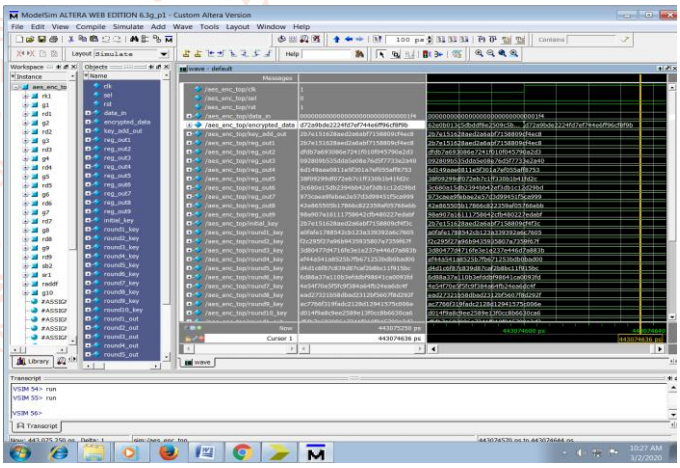


Figure-8: AES Encryption output: d72a9bde2224fd7ef744e6ff96cf8f9b

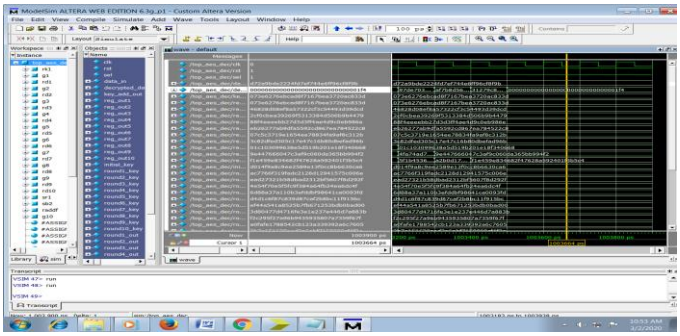
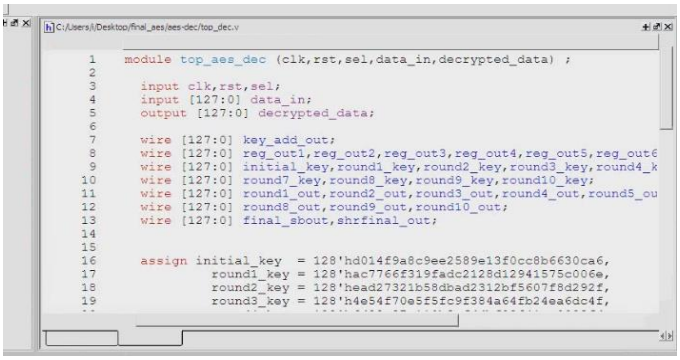


Figure-9: AES Decryption Input :128'h d72a9bde2224fd7ef744e6ff96cf8f9b The output is : 000000000000000000000000000001F4



```
module top_aes_dec (clk,rst,sel,data_in,decrypted_data) ;

  input clk,rst,sel;
  input [127:0] data_in;
  output [127:0] decrypted_data;

  wire [127:0] key_add_out;
  wire [127:0] reg_out1,reg_out2,reg_out3,reg_out4,reg_out5,reg_out6
  wire [127:0] initial_key,round1_key,round2_key,round3_key,round4_k
  wire [127:0] round7_key,round8_key,round9_key,round10_key;
  wire [127:0] round1_out,round2_out,round3_out,round4_out,round5_ou
  wire [127:0] round8_out,round9_out,round10_out;
  wire [127:0] final_sbout,shrfinal_out;


  assign initial_key  = 128'hd014f9a8c9ee2589e13f0cc8b6630ca6,
         round1_key = 128'hac7766f319fadc2128d12941575c006e,
         round2_key = 128'head27321b58dbad2312bf5607f8d292f,
         round3_key = 128'h4e54f70e5f5fc9f384a64fb24ea6dc4f,
```

Figure-10: AES DECERPATION CODE

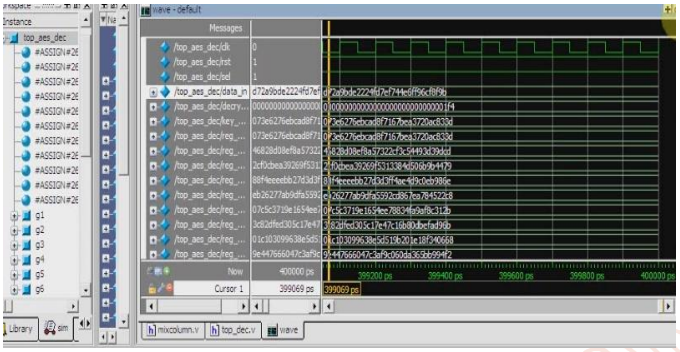


Figure-11: AECS_DEC

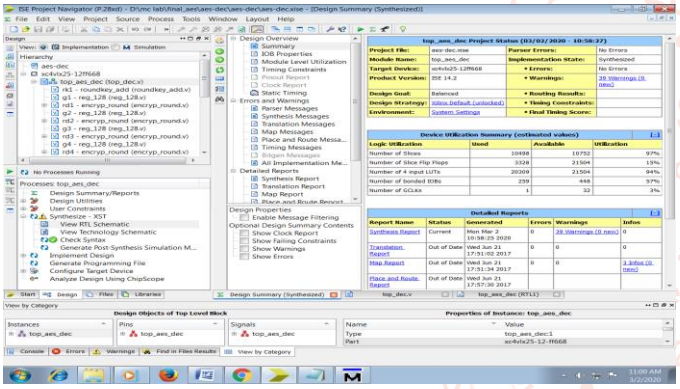


Figure-12: AES Decryption Design summary (draw table for design summary)

The final structural overview of the project is shown in the image above. This design brief was completed assuming the use of an FPGA. IOB testing is very expensive but is often overlooked by reducing information and yield parameters. B. When accepting information and keys as information one after another and displaying image messages individually to translate the content. This can cause the IOB to drop to very low levels. The remaining basic principles prevent usage from becoming very low. This way you can realize your project on his FPGA board mentioned above. ”

VII. APPLICATONS

1) Can be used for smart card security, remote sensor framework, remote work framework.
2) AES has high computational efficiency and can be used in high-speed applications such as broadband connections.
3) AES is ideal for closed spaces where encryption or decryption is implemented. RAM and ROM requirements are very low.
4) Web servers that need to manage various cipher suites.
5) Insightful applications requiring security with current encryption to the system

VIII.CONCLUSION

“We have presented the potential of an improved AES-DES solution as a system that supports the current AES architecture. With these estimates, remote exchanges, electronic payment exchanges, credit cards, video It creates a generally more secure and attack-resistant encryption method that can be used in various areas such as disk systems. This article describes the use of 128 AES devices in equipment. The numbers were connected using Xilinx and Modelsim,” and the results were “verified using standard test vectors.” Estimation is performed by Verilog. Implementing AES integration on equipment actually improves throughput efficiency, regardless of whether zone integrity and speed switching are compromised in each case due to equipment usage. The improved AES-DES considers strategies to enhance current AES plans. This model provides better nonlinearity than simple AES and converges with DES, resulting in better resolution and "less likely" logarithmic traps in the model.

IX.FUTURE SCOPE

This proposed computation can be made many times more surprisingly secure by extending the number of accents in the cryptographic computation to adapt it to the required security level. You can also "apply" a retrograde process that reduces the number of accents to reduce security.

"Moved Encryption Standard (AES) is the most secure symmetric encryption method with expanded overall authentication. AES is a profitable Methods such as Sub Bytes (S-Box) ensure higher security and faster encryption/decryption. Subbyte and key schedule. Extensive research has been done on S-Box/Inv movement. S-Box and Mix Columns/Inv. Mix columns in submitted ASICs and FPGAs to animate AES calculations and reduce circuit area. "reduced."

REFFERNCES

[1] Behrouz A. Forouzan, Cryptography and Network security, TMH

[2] M.B Vishnu, S.K. Tiong, Zaini M, Koh S P, “Security Enhancement of Digital Motion Image Transmission using Hybrid AES-DES

[3] algorithm," 14th Asia-Pacific Conference on Communications, APCC 2008, pp 1-5,2008

[4] Maire McLoone, John V. McCanny, "High Performance Single Chip FPGA Rijndael Algorithm Implementations," Proceedings of the Third International Workshop on Cryptographic Hardware & Embedded Systems , Springer-Verlag London UK, ISBN:3-54

[5] Sanchez-Avila, C.; Sanchez-Reillol R, "The Rijndael block cipher: A comparison with DES," 35th IEEE International Carnahan conference on Security Technology, pp229-234, 2001

[6] McLoone, M. McCanny, J.V, "A high performance FPGA implementation of DES ," IEEE Workshop on Signal Processing Systems, SiPS 2000,pp 374-383,2000

[7] Standaert, F.-X, Rouvroy G, Quisquater, J.- J," FPGA Implementations of the DES and Triple-DES Masked Against Power Analysis Attacks," International conference on Field Programmable Logic and Applications, FPL '06. pp 1-4, 2006

[8] Saeid Taherkhani, Enver EveOrhanGemikonaklir, "Implementation of Non- Pipelined and PipelinedData Encryption Standard (DES) Using Xilinx Virtex -6 FPGA Technology," 10thComputer & Information Technology(CIT 2010), pp 1257-1262, 2010

[9] Design of VLSI system by Dr Danial J. Miynek

[10] William Stallings, Cryptography and Network Security: Principles and Practice, 2nd ed., Prentice-Hall, Inc. 2000.

[11] http://www.xilinx.com

[12] M.Pitchaiah, Philemon Deniel, Praveen 2012 "Implementation of Advanced Encryption Algorithm" International Journal of Scientific & Engineering Research ISSN 2229-5518.

[13] Behrouz A. Forouzan, "Cryptography and Network Security" TMH.

[14] Gireesh Kumar P, P. Mahesh Kumar 2013 "Implementation of AES Algorithm Using Verilig " International Journal of Embedded systems ISSN 2249-6556.

[15] Data Encryption Standard (DES) ,Federal Information Processing Standards Publication (FIPS PUB 46-3)Reaffirmed

[16] William Stallings "Cryptography and network Security" Principles and practise Fourth Edition

[17] S,Lara , Accelerating algorithms in hardware, date visited:(10/06/2008)http://www.embedded.com /show/Article.jhtml?articleID=175 00157

[18] NIST, Advanced Encryption Standard (AES), (FIP PUB 197) http://csrc.nist.gov/publications

[19] Wikipedia: www.wikipedia.org.