ISSN: 2250-3676
Volume-4, Issue-2, 248-251

Anshu Sinha [1], Ravi Shekhar [2],. Alok Ranjan[3],Mohammed hasmat ali[4],shashi bhushan kumar[5]

[1] *Mr. Anshu Sinha, Asst.prof. Nit Patna*
[2] *Mr. Ravi Shekhar, Tech. Asst. Nit Patna*
[3]*Mr. Alok Ranjan, Asst. Prof. Nit Patna*
4Mr.Mohammed hasmat ali,Asst.prof.Nit Patna
5Mr.Shashi bhushan kumar,Asst.prof.Bit gaya

***Abstract*—Cryptography is the science of secret codes, it enables the confidential communication through an un-trusted medium .It helps to protect the message against unauthorized parties. This is a 128-bit Key dependent algorithm which has control over the 128-bit input data or plaintext. This work on the AES Encryption and Decryption Algorithm of 128 bits can be extended in the future**

***Keywords*— Cryptography, DES, TRIPLE DES (3 des), AES.**

I. INTRODUCTION

Serge Vaudenay, in his book "A classical introduction to cryptography", writes:

> *Cryptography is the science of information and communication security.*

Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use. Generally speaking, it uses an cryptographic system to transform a plaintext into a cipher text, using most of the time a key.

II. WORKING OF CRYPTOGRAPHY

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys.

The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

III. PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. New forms of cryptography came soon after the widespread development of computer communications.

In data and telecommunications, cryptography is necessary when communicating over any un-trusted medium, which includes just about *any* network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements including:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.

ISSN: 2250-3676
Volume-4, Issue-2, 248-251

IV. METHODS OF ENCRYPTION

Although there can be several pieces to an encryption method, the two main pieces are the algorithms and the keys. As stated earlier, algorithms are usually complex mathematical formulas that dictate the rules of how the plaintext will be turned into cipher text. A key is a string of random bits that will be inserted into the algorithm. For two entities to be able to communicate via encryption, they must use the same algorithm and, many times, the same key. In some encryption methods, the receiver and the sender use the same key and in other encryption methods, they must use different keys for encryption and decryption purposes.

V. SYMMETRIC ENCRYPTION

In a cryptosystem that uses symmetric cryptography, both parties will be using the same key for encryption and decryption, as shown in Figure 1.2. This provides dual functionality. As said, symmetric keys are also called secret keys because this type of encryption relies on each user to keep the key a secret and properly protected. If this key got into an intruder's hand, that intruder would have the ability to decrypt any intercepted message encrypted with this key.

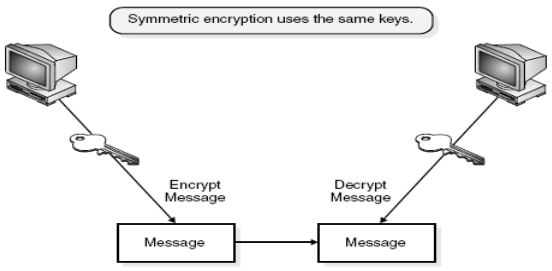

Figure 1.2 Using symmetric algorithms, the sender and receiver use the same key for encryption and decryption functions.

The security of the symmetric encryption method is completely dependent on how well users protect the key. If a key is compromised, then all messages encrypted with that key can be decrypted and read by an intruder.

If symmetric cryptosystems have so many problems and flaws, why use them at all? They are very fast and can be hard to break. Compared to asymmetric systems, symmetric algorithms scream in speed. They can encrypt and decrypt large amounts of data that would take an unacceptable amount of time if an asymmetric algorithm was used instead. It is also very difficult to uncover data that is encrypted with a symmetric algorithm if a large key size was used.

The following list outlines the strengths and weakness of symmetric key systems:

Strengths

- Much faster than asymmetric systems
- Hard to break if using a large key size

weaknesses

- Key distribution It requires a secure mechanism to deliver keys properly.
- Scalability Each pair of users needs a unique pair of keys, so the number of Keys grow exponentially.
- Limited security It can provide confidentiality, but not authenticity or non-repudiation.

The following are examples of symmetric key cryptography algorithms:

- Data Encryption Standard (DES)
- Triple DES (3DES)
- Advanced Encryption Standard (AES)

VI. METHOD AND DESIGN

DES uses a 64-bit key to encrypt 64-bit blocks of data through 16 rounds of permutations, xors , and table look-ups. The key is also shifted and permuted at each stage to increase security. DES is a symmetric algorithm, Which means that cipher text created using a particular key can be decrypted into plaintext using the same hardware and key. Figure 1.3 shows a data flow graph of how DES works.

ISSN: 2250-3676
Volume-4, Issue-2, 248-251

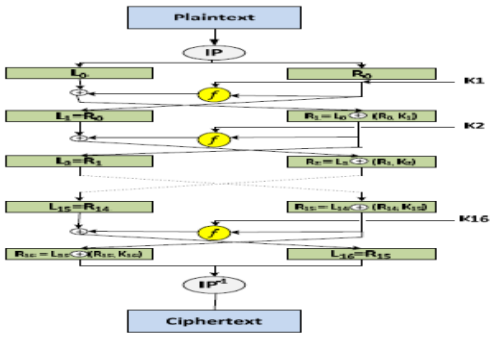

Figure 1.3 Des Data Flow Graph

The disadvantage of triple des system is time delay, which can be improve by AES

VII. ADVANTAGES OF AES:

- Through AES, input message of length 128 bits can be encrypted which is more than the DES and Triple DES.
- AES has the various secret key lengths such as 128 bits, 192 bits and 256 bits, whereas DES and Triple DES have fixed length of 64 bits.
- The cipher key is expanded into a larger key, which is later used for the actual operation.
- The Expanded Key shall ALWAYS be derived from the Cipher Key and never be specified directly.
- AES is very hard to attack or crack when compared to DES.
- AES will be faster when compared to the Triple DES.

VIII. APPLICATION

- This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in P. L. 100-235) requires cryptographic protection
- High speed ATM/Ethernet/Fiber-Channel switches
- Secure video teleconferencing
- Routers and Remote Access Servers
- In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.

IX. TOOLS REQUIREMENT

The AES Encryption and Decryption algorithm and the implementation has been discussed in the previous chapters. Now this chapter deals with the simulation and synthesis results of the implemented AES algorithm. Here Modelsim tool is used in order to simulate the design and checks the functionality of the design. Once the functional verification is done, the design is taken to the Xilinx tool for Synthesis process and the net list generation.

The Appropriate test cases have been identified in order to test this modeled AES Encryption and Decryption algorithm. Based on the identified values as the reference the plain text and the key of 128 bits is given as the input to the design and the obtained cipher text should match the reference result. This proves that the modeled design works properly as per the algorithm.

X. SIMULATION RESULTS

The test bench is developed in order to test the modeled design. This developed test bench will automatically force the inputs, which were taken from the reference, and will make the operations of algorithm to perform. The simulated result for the various cases has been discussed in this section.

This case deals with the both encryption and decryption for set of plain text and a key of 128 bits. The basic and common inputs for both encryption and decryption stage were clock (clk), chip enable (ce) and reset (rst). The reset signal is active high, that is, when the reset signal is set to high, the system will be in reset state

ISSN: 2250-3676
Volume-4, Issue-2, 248-251

and hence all the values will be '0'. Once the reset signal is set to low, the system will start its process.

. The two inputs named as "data_in" and "key_in" which takes the given plain text and the key.

Encryption

Here the first sets of inputs are taken from the reference as follows.

Input = 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34

Cipher Key = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

The above inputs were represented in the hexadecimal format which contains 16 bytes, that is, 128 bits. So when the proper inputs were given as the input to the system, "din_valid" and "k_en" signals will go high. These signals represents that the valid data and the proper key is given to the system. Hence the output of the encryption process, that is, the cipher text for the given set of inputs is obtained as follows.

Cipher Text = 39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32

Decryption

The above cipher text, that is, encrypted data will be given as the input to the decryption stage and the same key should be provided.

Input = 39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32

Cipher Key = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c

Here the "din_valid" signal will goes high only after the encryption process. Hence the decryption process will be carried out and the final output, that is, the same plain text which is given as the input to the encryption stage will be achieved.

Final Output = 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34

Thus the simulation result which is shown in the figure 4.1 gives the clear view on the AES operation which was explained above.

Hence the figure 5.1 & 5.2 shows the internal operation of the AES Encryption process and the figure 5.3 & 5.4 shows that the internal operations carried out in the AES Decryption process. The output values of the each stage which were fed as input to the next process.

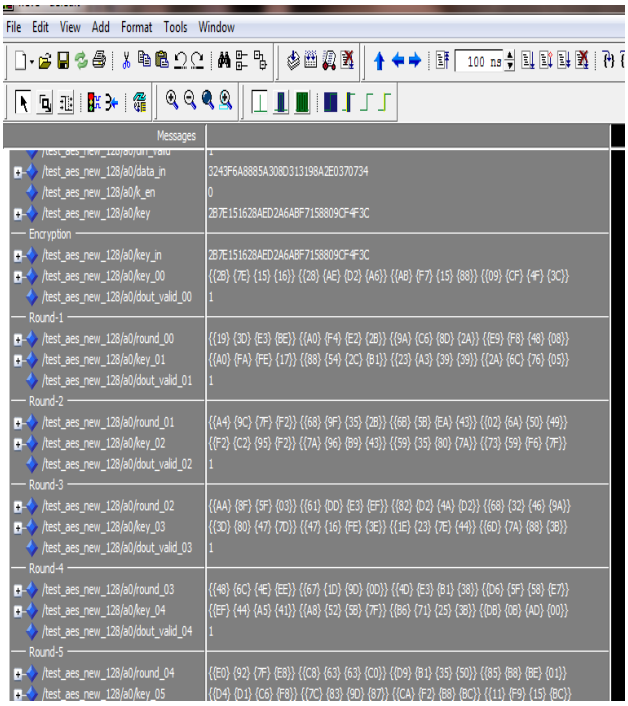

FIGURE 5.1 ENCRYPTED OUTPUT FROM ROUND 1 TO ROUND 5

ISSN: 2250-3676
Volume-4, Issue-2, 248-251

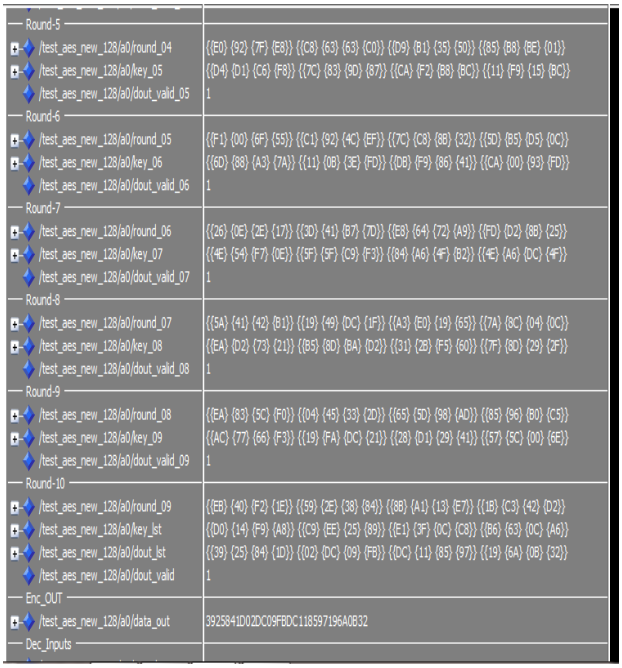

FIGURE 5.2 ENCRYPTED OUTPUT FROM ROUND 6 TO ROUND 10

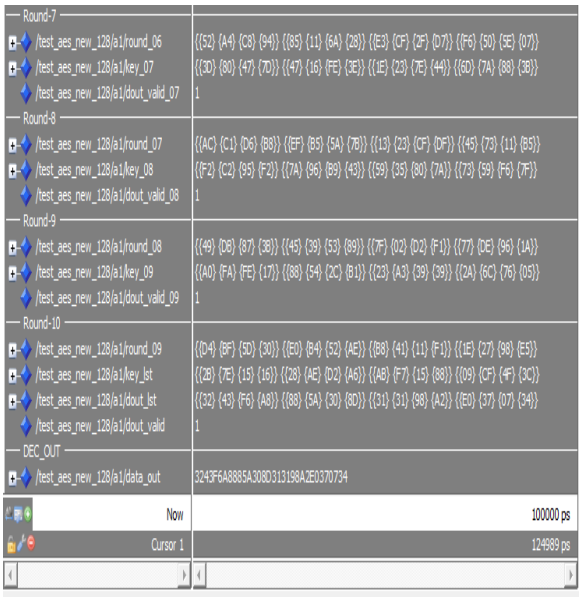

FIGURE 5.4 DECRYPTED OUTPUT FROM ROUND 7 TO 10

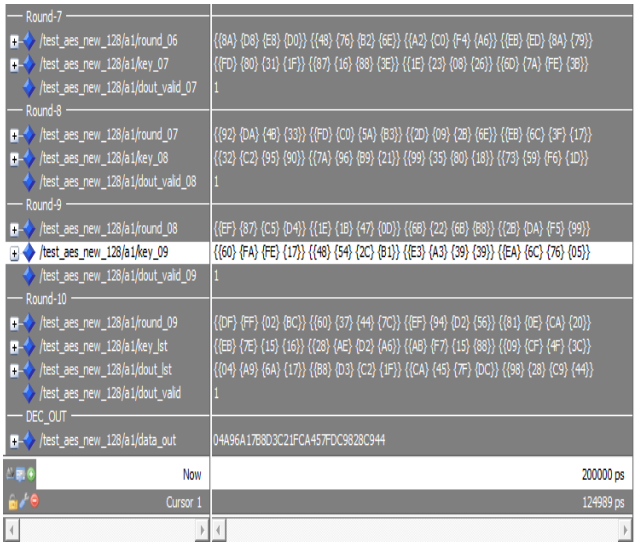

FIGURE 5.5 DECRYPTED OUTPUT WHEN ENCRYPTION & DIFFERENT KEY ARE DIFFERENT

From fig 5.5 it can be seen that when we give decrypted key which is different from encrypted key then data output is "04 A9 6A 17 88 D3 C2 1F CA 45 7F DC 98 28 C9 44" which is different from data input

Thus the simulation result of the AES algorithm for both encryption and decryption has bee discussed above in different cases.

XI. SYNTHESIS REPORT

Delay	Power
24.716 ns	81 mw

Table 5.1 synthesis report of AES

The device power & delay utilization summery is shown above in which their give the details of how much power & delay AES takes for its synthesis

Timing Summary:

Minimum period: 24.716ns (Maximum Frequency: 40.459 MHz)

In timing summery, details regarding time period and frequency is shown are approximate while synthesize. After place and routing is over, we get the exact timing summery. Hence the maximum operating frequency of this

ISSN: 2250-3676
Volume-4, Issue-2, 248-251

synthesized design is given as 40.459 MHz and the minimum period as 24.716ns..

XII. COMPARISON OF AES WITH TRIPLE DES

	Advance encryption system	Triple data encryption system
Delay	24.716 ns	29.543 ns
Data length	128 bit	64 bit (max)

Table 5.2 comparison of AES with TDES

XIII. CONCLUSION

This is a 128-bit Key dependent algorithm which has control over the 128-bit input data or plaintext. The original message is taken to 10 round operations which produces the cipher text. This resultant encrypted data is fed as the input to the decryption and 10 rounds operations are carried out and then the same plain text is achieved. Given the same input key and data (plaintext or cipher text) any implementation that produces the same output (cipher text or plaintext) as the algorithm specified in this standard is an acceptable implementation of the AES.

The simulation results have been verified for the different appropriate test cases. Finally the developed model is taken to the Xilinx tool and done the implementation. From the result we can conclude that AES takes 24.716 ns while triple des takes 29.543 ns. So AES is faster than triple data encryption system. AES can be used with 128 bit data & 128 bit bit key as compared to triple des which is used with 64 bit data & 128 bit key so AES provide more security as compared to triple des

XIV. FUTURE SCOPE

. This work on the AES Encryption and Decryption Algorithm of 128 bits can be extended in the future in the following ways:

As this algorithm supports the key length of 192 bits and 256 bits, the work can be extended by increasing the key length which increases both the security level to high and also making the difficulties in hacking level.

Also this work can be extended by developing a switch. This switch will be used to switch the system of key lengths to either of 128 bits, 192 bits and 256 bits for handling all the three key lengths.

XV. REFERENCES

[1] Irma B. Fernandez, M. S. E. E. Wunnava V. Subbarao, 1994 "Encryption based Security for ISDN Communication Technique & Application" IEEE transactions, pp.70-73,.

[2] Hessian Guendouz & Samir Bouaziz, 1994. "Rapid prototype of a Fast Data Encryption Standard with Integrity Processing for Cryptographic Applications" IEEE, pp.VI-434-437,

[3] Bruce Schneier and Mudge, 1999. "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)", CQRE '99, Springer-Verlag, pp. 192-203,

[4] Federal Information Processing Standards,2001"Specification for advanced encryption standard" Publication 197, pp.1-47.

[5] Guido Bertoni; Aril Bircan; Luca Breveglieri; 2003 Pasqualina Fragneto; Marco Macchetti. Vittorio Zaccaria; "Performances of the Advanced Encryption Standard in embedded Systems with Cache Memory" IEEE transactions,.

[6] Chih-Hsu Yen and Bing-Fei Wu, June 2006 "Simple Error Detection Methods for Hardware Implementation of Advanced Encryption Standard", IEEE transactions on computers, vol.55, no. 6, pp.720-731,

[7] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin, 2008 "Effect of Security Increment to Symmetric Data Encryption through AES Methodology", IEEE Ninth ACIS International

ISSN: 2250-3676
Volume-4, Issue-2, 248-251

Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp 291-294,.

[8]Ahmad H. Omari, Basil M. Al-Kasasbeh, Abeer A. Omari Dynamic Cryptography Algorithm for Real-Time Applications DCA-RTAPROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON APPLIED MATHEMATICS, SIMULATION, MODELLING (ASM'09)

[9]Xinmiao Zhang, Student Member, IEEE, and Keshab K. Parhi, Fellow, IEEE SEPTEMBER 2004,High-Speed VLSI Architectures for the AES Algorithm IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 12, NO. 9,

[10]Alexandra Camacho, Isaac Sanchez, Eugene B. John and Ram Krishnan

Department of Electrical and Computer Engineering The University of Texas at San Antonio Design and Low Power VLSI Implementation of Triple -DES Algorithm

[11] Ashwini M. Deshpande, Mangesh S. Deshpande, Devendra N. Kayatanavar, June 2009"FPGA Implementation of AES Encryption & Decryption", International conference on control automation, communication and energy conservation, pp.1-6,4th-6th