International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

TRIPLE AES ALGORITHM WITH GRAY CODE ENCRYPTED KEY USING VERILOG

D. SUMARANI, SHIVA KUMAR K.S

D SUMARANI, Dept.of ECE Engineering, BITM college, Karnataka, India. Email Id:sumarani073@gmail.com
Asst. Prof. SHIVA KUMAR K.S, Dept .of ECE Engineering, BITM college, Karnataka, India. Email Id: shivamcse72@gmail.com

---

Abstract - *This paper explains the advance approach for data security against first order differential electromagnetic and power analysis, using Advance Encryption Standard algorithm as base. In earlier algorithm where standard tables were referred to implement the substitution and inverse substitution box; combinational logic and GF fields is used which reduces the area, delay and scope for hacking. Key expansion method is used to generate keys for each round having Sub-bytes, Shift Rows, Mixed Column and Add Round Key as sub stages. As modification we have implemented decryption process for encrypted data. Key used here is the encrypted key to ensure high data security. This proposed algorithm is implemented using Verilog HDL and simulated by Modelsim 6.4c and synthesized by Xilinx tool. We have implemented a new Advanced Triple Encryption and Decryption blocks using gray code encrypted key. The result of this paper can be served for protecting the sensitive DATA in certain sectors like in Military/Defense applications..*

Key Words: Encryption, Decryption, Algorithm, Cipher Key, Cipher Text, Cryptography.

1. INTRODUCTION

Encryption and decryption widely known as cryptography plays an important role in DATA Security and transmission. Advanced Encryption algorithm has found importance in a variety of areas such as Defense, Smart cards, Web servers etc. because it is proven to offer high security of data because of features like no look up tables reference. Combinational Logics and composite arithmetic field operations are used which makes it unique from other cryptography works. This also results in reduction of area, delay and hacking probability. However, approach includes usage of Galois fields GF(2^8) which might increase the hardware complexity. We have the option of using Composite field arithmetic such that the field elements of GF(2^8) are mapped to some isomorphic composite fields in which field operations can be implemented by lower cost subfield operations. However, it is not feasible to use composite field arithmetic in all stages of AES as this also leads to complexity.

The Advanced Encryption and decryption algorithm uses the Plain data and a secret key called Cipher Key acting as input to Encryptor. The output of Encryptor is called Cipher Text which is fed to decryptor as input along with same key and the resultant output would be plain text. This algorithm works for fixed group of bits, usually 128 bits and it uses same length Cipher Key as shown in the following figure. The figure below shows the block diagram of basic encryption and decryption process.

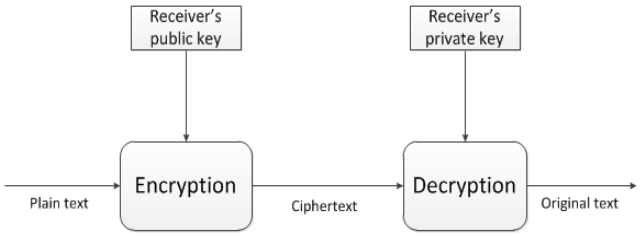


Figure 1: Basic Operation of Encryption and Decryption

2. ADVANCE ENCRYPTION AND DECRYPTION PROCESS

The main objective of this paper is to design Advanced Triple Encryption Algorithm to provide high data security by using advanced encryption standard algorithm with sub bytes, shift rows, mixed column and add round key approach. And also implement the Advanced Triple decryption. As an addition to enhance the data security, the key used for encryption and decryption is also encrypted using Gray code Encryption. Encryption and decryption is performed thrice with several sub stages involved as shown in the following figure 2. As mentioned, this encryption and decryption process is designed using Advanced Encryption Standard as base.

The Encryption process includes 3 AES steps, viz. Encryption followed by Decryption followed by Encryption. First we encrypt with Key1 and then decrypt with different key (i.e. Key2) and then we again encrypt with first key (Key1).

For Decryption, we follow similar process. We decrypt using Key1 followed by encryption using Key2 and the encryption using Key1.

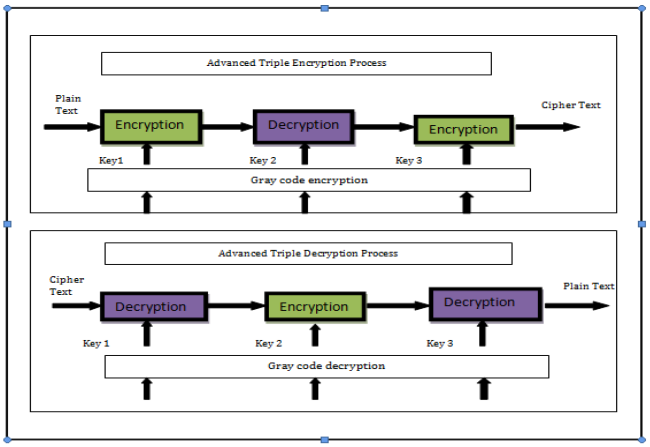


Figure 2: Block diagram of Advanced Triple Encryption and Decryption.

2.1 Encryption Process.

Encryption Process can be explained with the help of the following flow chart.

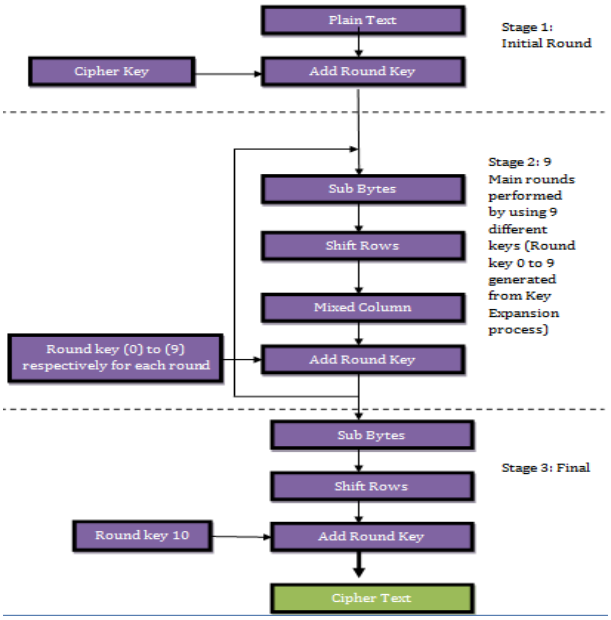


Figure 2.1 Flow chart of Encryption.

As shown in the above block diagram, we have 3 different stages involved in the Encryption process. We consider the input as 128 bits plain text and Cipher key of same length as plain text. Output will be encrypted text called Cipher text of length 128 bits.

Let us now discuss every process in detail.

Stage 1: Stage 1 is the initial stage, where in the plain text of length 128 bits as well as the gray code encrypted cipher key of length 128 bits are given as input to Add Round key. Add round key, simply performs the bitwise EXOR operation of the two inputs given

Stage 2: For Stage 2, the output of the Stage 1 will serve as input. Here in Stage 2, 9 rounds of main sub levels as shown in the Figure 2.1 are performed.

Stage3: Stage 3 is the final round in the encryption process. It is similar to stage 2 but there is no Mixed Column process as shown in the figure 2.1. It is done only once. In add round key process of stage 3, 10th round key is used. The output of stage 3 would be the Cipher Text which is nothing but the encrypted text.

2.2 Decryption Process.

For decryption, the input would be the encrypted data i.e. Cipher text of 128 bits. The process can be explained with help of a flow chart as shown in figure below:

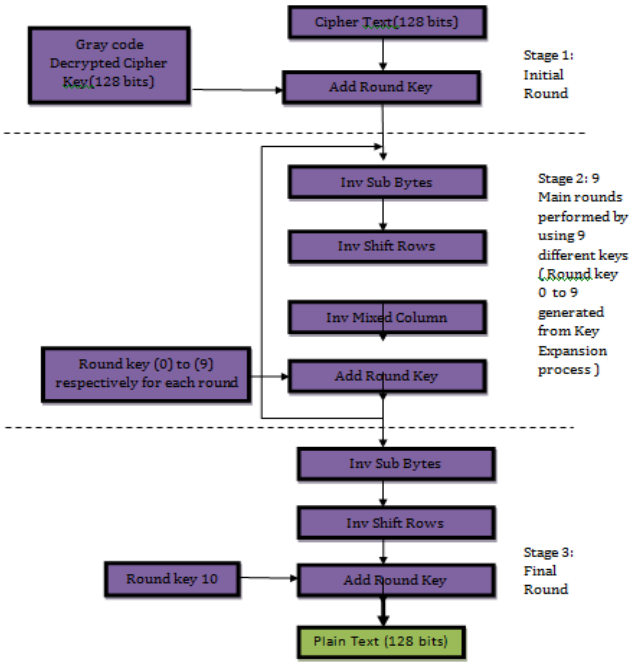


Figure 2.2 Flow chart of Decryption.

The decryption process is very similar to encryption process. The input would be 128 bits encrypted cipher text and gray code decrypted cipher key. Every process followed during encryption is performed inversely during decryption as shown in the above block diagram

2.3 Key Expansion Process.

Key expansion process is used to expand 4 word i.e. 128 bits of cipher key into 44 words of key such that there will be 11 keys, 1st one would be the input cipher key, and the 10 keys for 9 main rounds and one for final round. Each round takes 4 words of key. Key expansion process shows how the input cipher key is arranged as 4×4 matrix and how it is expanded into 44 words

2.3 Gray Code Encoder.

To ensure high data security and as an enhancement, we have encrypted the Cipher key before the Encryption process from Binary to Gray Encoding method. And during decryption, we have decoded the key using Gray to Binary conversion.

4. SOFTWARE REQUIREMENT

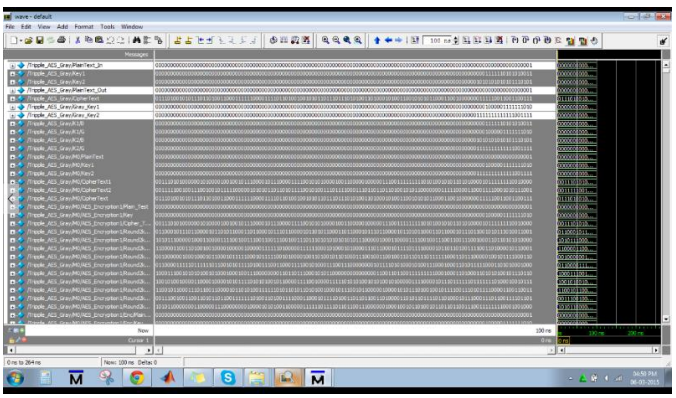
MODELSIM 6.4C:

Modelsim is a simulation tool for hardware design which provides behavioral simulation of a number of languages, i.e., Verilog, VHDL, and System C. Verilog HDL is an industry standard language used to create analog, digital, and mixed-signal circuits. HDLs are languages which are used to describe the functionality of a piece of hardware as opposed to the execution of sequential instructions like in a regular software application.

XILINX 9.1/13.2:

Xilinx Tools is a synthesize tools used for the design of digital circuits implemented using Field Programmable Gate Array (FPGA). Digital designs can be entered in various ways using the CAD tools, schematic entry tool, hardware description language (HDL) – Verilog or VHDL or a combination of both.

4. SIMULATION RESULT



3. CONCLUSION

An enhanced triple AES implementation with gray code encoding for key against the data hacking is presented. It is based on the Rijndael algorithm with its mathematical properties. The new design permits the construction of actual cores with efficient area and speed characteristics, while maintaining a very high protection level. We conducted relevant Triple AES Implementation with B2G Encoder and G2B Decoder Method.

REFERENCES

[1] K. Fu and J. Blum, "Controlling for cybersecurity risks of medical device software," Commun. ACM, vol. 56, no. 10, pp. 35–37, Oct. 2013.

[2] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," IEEE Pervasive Comput., vol. 7, no. 1, pp. 30–39, Jan./Mar.

[3] M. Rostami, W. Burleson, A. Jules, and F. Koushanfar, "Balancing security and utility in medical devices?" in Proc. 50th ACM/EDAC/IEEE Int. Conf. Design Autom., May/Jun. 2013, pp. 1–6.

[4] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," Proc. IEEE, vol. 102, no. 8, pp. 1174–1188, Aug. 2014

[5] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," IEEE Security Privacy, vol. 8, no. 1, pp. 81–85, Jan./Feb. 2010

[6] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker, "Challenges in access right assignment for secure home networks," in Proc. USENIX Conf. Hot Topics Secur., 2010, pp. 1–6.

[7] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," Computer, vol. 44, no. 9, pp. 51–58, Sep. 2011

BIOGRAPHIES

Name: D Sumarani
ECE Dept, BITM College, Ballari.
VTU, Belgaum
Karnataka, India