

**FPGA BASED IMPLEMENTATION OF AES ENCRYPTION ALGORITHM  
USING XILINX SYSTEM GENERATOR**

**MUHAMMAD SUHAIMI BIN MINHAD**

**This report is submitted in partial of the requirement for the award of Bachelor of  
Electronic Engineering (Telecommunication) With Honours**

**Faculty of Electronic and Computer Engineering  
Universiti Teknikal Malaysia Melaka**

**JUNE 2016**

BORANG PENGESAHAN STATUS LAPORAN  
PROJEK SARJANA MUDA II

Tajuk Projek : FPGA BASED IMPLEMENTATION OF AES ENCRYPTION  
ALGORITHM USING XILINX SYSTEM GENERATOR

Sesi Pengajian :

1	5	/	1	6
---	---	---	---	---

Saya MUHAMMAD SUHAIMI BIN MINHAD  
(HURUF BESAR)

mengaku membenarkan Laporan Projek Sarjana Muda ini disimpan di Perpustakaan dengan syarat-syarat kegunaan seperti berikut:

1. Laporan adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan laporan ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. Sila tandakan ( ✓ ) :

SULIT\*

\*(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

TERHAD\*\*

\*\* (Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

TIDAK TERHAD

Disahkan oleh:


  
(TANDATANGAN PENULIS)

  
(COP DAN TANDATANGAN PENYELIA)

Tarikh: 17/06/16

17 Jun 2016  
PROF. DR. ZULKALNAIN BIN MOHD YUSSOF  
Profesor  
Fakulti Kejuruteraan Elektronik Dan Kejuruteraan Komput  
Universiti Teknikal Malaysia Melaka (UTeM)  
Hang Tuah Jaya  
76100 Durian Tunggal, Melaka

**"I hereby declare that the work in this project is my own except for summaries and quotations which have been duly acknowledge."**

**Signature** :  .....

**Author** : MUHAMMAD SUHAIMI BIN MINTAD .....

**Date** : 17/06/16 .....

“I acknowledge that I have read this report and in my opinion this report is sufficient in term of scope and quality for the award of Bachelor of Electronic Engineering (Industrial Electronics/ Computer Engineering/ Electronic Telecommunication/ Wireless Communication)\* with Honours.”

Signature



Supervisor's Name

PROF. DR. ZULKALNAIN BIN MOHD YUSSOF

*Profesor*

Fakulti Kejuruteraan Elektronik Dan Kejuruteraan Komputer

Universiti Teknikal Malaysia Melaka (UTeM), ...

Hang Tuah Jaya

75100 Durian Tunggal, Melaka

Date

17 JUN 2016

## DEDICATION

To my beloved family and friends...

## PENGHARGAAN

Alhamdulillah, syukur ke hadrat Ilahi kerana dengan izin dan restunya saya berjaya menyiapkan projek sarjana muda ini dengan sempurna.

Di kesempatan ini, saya ingin mengucapkan ribuan terima kasih kepada Prof. Dr. Zulkalnain Bin Mohd Yussof selaku penyelia projek tahun akhir saya di atas tunjuk ajar, bimbingan serta bantuan yang diberikan sepanjang tempoh penyiapan projek ini. Tanpa bantuan daripada beliau, nescaya saya tidak akan mampu menyiapkan projek sarjana muda ini dengan jayanya.

Saya juga merakamkan ribuan terima kasih kepada Mejar Mohd Yazid Bin Abd Rahman yang merupakan pelajar sekelas saya, di atas bantuan dan kerjasama yang diberikan dalam mengkaji kes ini. Dengan bantuan beliau, saya dapat memahami proses-proses enkripsi AES dalam masa yang singkat.

Akhir sekali, saya ingin mengambil kesempatan ini untuk mengucapkan terima kasih kepada sahabat-sahabat yang turut sama membantu sehingga tamatnya pengajian saya. Tanpa bantuan daripada semua pihak, saya tidak akan mampu menyiapkan projek sarjana muda saya dalam masa yang diperuntukkan.

## ABSTRAK

Algoritma AES digunakan secara meluas dalam sekuriti tentera dan juga e-perbankan. Projek ini membentangkan pemodelan 256 bit AES menggunakan Xilinx Sistem Generator dan pelaksanaannya pada FPGA. Pembangunan projek ini dibahagikan kepada dua fasa ; simulasi dan fasa pelaksanaan. Dalam fasa simulasi, kedua-dua enkripsi dan dekripsi dimodelkan menggunakan Xilinx Sistem Generator dengan merujuk kepada dokumen standard AES. Dalam fasa pelaksanaan, reka bentuk telah disintesis dan kemudian dilaksanakan pada FPGA . Keputusan yang diperolehi daripada pelaksanaan FPGA adalah serupa dengan simulasi.

## ABSTRACT

AES algorithm is widely used in military security and also e-banking. This project presents the 256 bit AES modelling of 256 using Xilinx System Generator and its implementation on FPGA. The development of the project is divided into two phases; simulation and implementation phase. In the simulation phase, both encryption and decryption were modelled using Xilinx System Generator by referring to the AES standard document. In the implementation phase, the design was synthesized and then implemented on FPGA. The results obtained from FPGA implementation was similar to simulation.



## TABLE OF CONTENT

<b>CHAPTER</b>	<b>CONTENT</b>	<b>PAGE</b>
	<b>PROJECT TITLE</b>	<b>i</b>
	<b>BORANG PENGESAHAN STATUS LAPORAN</b>	<b>ii</b>
	<b>STUDENT DECLARATION FORM</b>	<b>iii</b>
	<b>SUPERVISOR DECLARATION PAGE</b>	<b>iv</b>
	<b>DEDICATION</b>	<b>v</b>
	<b>ACKNOWLEDGEMENT</b>	<b>vi</b>
	<b>ABSTRAK</b>	<b>vii</b>
	<b>ABSTRACT</b>	<b>viii</b>
	<b>TABLE OF CONTENT</b>	<b>ix</b>
	<b>LIST OF FIGURE</b>	<b>xii</b>
 <b>CHAPTER 1: INTRODUCTION</b>		
	1.0 Overview	1
	1.1 Project Background	1
	1.2 Project Overview	2
	1.3 Objective of Project	3
	1.4 Scope of Project	3
	1.5 Thesis Outline	4
 <b>CHAPTER 2: LITERATURE REVIEW</b>		
	2.0 Overview	5
	2.1 Previous Projects	
	2.1.1 FPGA-Based Real-Time Implementation of AES Algorithm for Video Encryption	6

2.1.2	Simulation of Image Encryption using AES Algorithm	7
2.1.3	Advanced Encryption Standard	10
2.1.4	A Study of Encryption Algorithms AES, DES and RSA for Security	12
2.1.5	128-bit AES Decryption	16
2.2	Software and Theory	
2.2.1	MatLab (Simulink)	18
2.2.2	ISE Xilinx 14.4 (System Generator)	19
2.3	Hardware	
2.3.1	Field Programmable Gate Array (FPGA)	20
<b>CHAPTER 3 : METHODOLOGY</b>		
3.0	Overview	22
3.1	Introduction	22
3.2	Process of Project	23
3.3	AES Algorithm	26
<b>CHAPTER 4 : RESULT AND DISCUSSION</b>		
4.0	Overview	31
4.1	Simulation Result	31

**CHAPTER 5 : CONCLUSION AND RECOMMENDATION**

5.0 Overview	47
5.1 Conclusion	47
5.2 Recommendation	48
<b>REFERENCES</b>	<b>48</b>
<b>APPENDIX</b>	<b>49</b>

## LIST OF FIGURE

FIGURE	TITLE	PAGE
2.1	Full AES Key Storage Memory Address Encoding	7
2.2	Detailed Block Diagram of Encryption Part	9
2.3	AES-128 Block Example	11
2.4	AES Encryption and Decryption	15
3.1	Methodology Flowchart	23
3.2	FPGA architecture	26
3.3	Spartan-6 USB-FPGA Module	28
3.4	FPGA Design Flowchart	30
3.5	Overall AES Structure	33
3.6	Substitute Bytes Stage of The AES Algorithm	34
3.7	Shift Row Stage	35
3.8	Mix Column Stage	36
3.9	Add Round Key Stage	36
4.1	AES Encryption Block (Encryption)	38
4.2	AES Encryption (Round 1)	39
4.3	AES Encryption (Round 2 - Round 13)	39
4.4	AES Encryption (Round 14)	40
4.5	Substitute Byte Blockset	40
4.6	Shift Row Operation (Bit Basher)	41
4.7	Mix Column Subsystem	42
4.8	Mix Column Blockset	43
4.9	CipherText Obtained	44
4.10	AES Encryption Block (Decryption)	45
4.11	AES Decryption (Round 1)	45
4.12	AES Decryption (Round 2 - Round 13)	46

4.13	AES Decryption (Round 14)	46
4.14	Inverse Shift Row	47
4.15	Substitute Byte Blockset	48
4.16	Inverse MixColumn Subsystem	49
4.17	Inverse MixColumn Blockset (Subsystem)	50
4.18	Inverse Mix Column	50
4.19	Result Obtained	51
4.20	FPGA Implementation	51

## **CHAPTER 1**

### **INTRODUCTION**

#### **1.0 Overview**

This chapter will cover the introduction of the project where it involve of the project background, problem statement, objective of project, scope of project, thesis outline and summary of work.

#### **1.1 Project Background**

Multimedia data security is becoming an important concern due to the fact that multimedia applications affect many aspects of our life. To deal with the increasing use of multimedia in industrial process, security technologies are being developed. Multimedia encryption algorithms implemented in hardware have emerged as the most viable solution for improving the performance of Multimedia encryption systems. The introduction of reconfigurable devices and high level hardware programming languages has further accelerated the design of encryption technology in FPGA. In this

paper, we report on the implementation and hardware platform of a real time video encryption processing. The processing encrypts videos in real time using the AES Algorithm. We propose a computationally efficient architecture for AES. The system is optimized in terms of execution speed and hardware utilization.

## 1.2 Project Overview

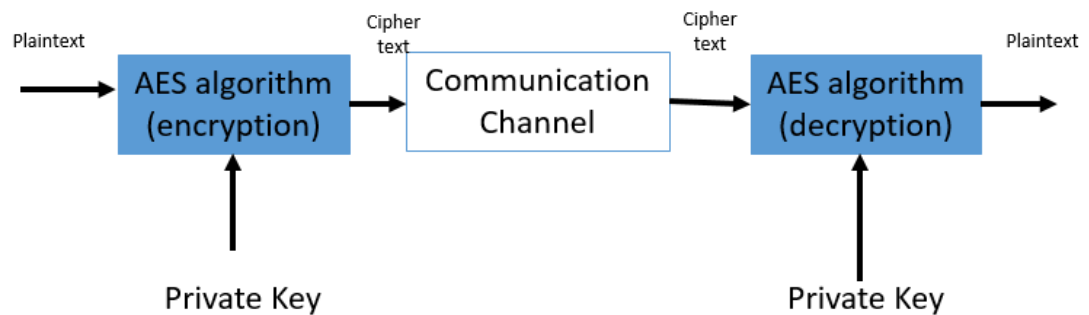
The project is related to the process of Encryption and Decryption of a plaintext using Advanced Encryption Standards (AES) algorithm, modelled in Xilinx System Generator.

- performing encryption and decryption of text.
- focus on AES algorithm to perform the cryptographic with 256-bit key expansion.

Xilinx System Generator is used in this project because it is easier to use for those who are not very familiar with Hardware Description Language (HDL) such as Verilog and VHDL. By using System Generator approach, it helps those people, also be able to model an AES algorithm.

The AES algorithm can be implemented using general purpose processor (using C) or Digital Hardware such as FPGA and ASIC. However, for real time encryption application, the AES should be implemented in Hardware. ASIC implementation can exploit massive parallelism in the AES algorithm and provide the highest performance in terms of speed and power but lacks the configurability. FPGA can take advantage of the AES parallelism and also offer flexibility and programmability. FPGAs are attractive because they can provide the speed, rapid prototyping and verification in hardware.

## Typical Data Encryption System



### 1.3 Objective of Project

Encryption is important to secure data from being accessed by unwanted personnel. The objectives of this project are being able to model an AES encryption algorithm using Xilinx System Generator and to implement them on FPGA.

### 1.4 Scope of Project

In this project, the main part is to model and implement the Advanced Encryption Standard AES-256 algorithm with Number of Round ( $N_r$ ) and apply it on FPGA board.



## 1.5 Thesis Outline

Chapter 1 is about the introduction of the project that consists of project background, problem statement, objectives, scope of project, and summary of work.

Chapter 2 is about the literature review that explains about the background study of the Advanced Encryption Standard and details about Field Programmable Gate Array and mostly about application and the technologies existed before FPGA technology. This literature review also explained about the parameter and technique involved in designing AES algorithm and also stages for each round of AES process.

Chapter 3 explained about the research methodologies that consist of steps of designing AES algorithm and also details about the specifications involved.

Chapter 4 mainly is for the result and analysis of AES algorithm after designing using Xilinx System Generator and Matlab Simulink.

Chapter 5 is about the conclusion, references future work and appendixes.

## CHAPTER 2

### LITERATURE REVIEW

#### 2.0 Overview

In this chapter will discuss the projects and paper work associated with this project. Related work was studied to produce the quality and reliability of the project. By analyzing the projects done before by other researchers, are likely to find out there are a few features about the projects done. They also recommend some future work that are a few features about the projects done. They also recommend some future work that can be undertaken to improve the project. In addition, there are a few ideas that are used to implement this project from other projects similar. An extended literature review process from beginning to end of the project. By review the previous work, the right of action for the project reliable and marketable. In addition, there are a few findings from the internet and books used in this project. Along analysis at the beginning of the project, special features specified in this project and the components used in this project is determined. In addition it is functional and well understood concept.

## 2.1 Previous Projects

### 2.1.1 Title : FPGA-Based Real-Time Implementation of AES Algorithm for Video Encryption by Sonia Kotel, Medien Zeghid, Adel Baganne, Toufik Saidani, Yousef Ibrahim Daradkeh, and Tourki Rached. [1]

Multimedia data security is becoming an important concern due to the fact that multimedia applications affect many aspects of our life. To deal with the increasing use of multimedia in industrial process, security technologies are being developed. Multimedia encryption algorithms implemented in hardware have emerged as the most viable solution for improving the performance of Multimedia encryption systems. The introduction of reconfigurable devices and high level hardware programming languages has further accelerated the design of encryption technology in FPGA. In this paper, we report on the implementation and hardware platform of a real time video encryption processing. The processing encrypts videos in real time using the AES algorithm. We propose a computationally efficient architecture for AES.

The system is optimized in terms of execution speed and hardware utilization. The design as know AES encryption processor is developed in Xilinx System Generator and integrated as a dedicated hardware peripheral to the Microblaze 32 bit soft RISC processor with the EDK embedded system and implemented targeting a Spartan3A DSP 3400 device (XC3SD3400A-4FGG676C). The video encryption processing has been verified successfully. The input comes from a live video acquired from a CMOS camera and the encrypted video is displayed on a DVI display screen.



Figure 2.1 Full AES Key Storage Memory Address Encoding

For our proposed architecture, a memory elements configured as RAM are used to store the RoundKeys (Figure 2.1). Three RAM's with 2-bit input address and 128 bit output are used. The three RAM's as know IPRam1, IPRam2 and IPRam3 blocks are automatically generated by the Xilinx tool. The first AES Round uses the encryption key from the IPRAM1. Then, each turn uses its own key. This arrangement allows simple decoding logic to select the appropriate key for the both AES Round.

### 2.1.2 Title : Simulation of Image Encryption using AES Algorithm by P.Karthigaikumar and Soumiya Rasheed.[2]

With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Because of widely using images in industrial process, it is important to protect the confidential image data from unauthorized access. This paper presents the design of a 128 bit encoder using AES Rijndael Algorithm for image encryption. The AES algorithm defined by the National Institute of Standard and Technology(NIST) of United States has been widely accepted. Optimized and Synthesizable VHDL code is developed for the implementation of 128- bit data encryption and process. Xilinx ISE9.2i software is used for synthesis. Timing simulation is performed to verify the functionality of the designed circuit.

Transmission of sensitive data over the communication channel have emphasized the need for fast and secure digital communication networks to achieve the requirements for secrecy, integrity and non-reproduction of exchanged information. Cryptography provides a method for securing and authenticating the transmission of information over insecure channels. It enables us to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it. The urgency for secure exchange of digital data resulted in large quantities of different encryption algorithms which are evaluated on the basis of throughput speed of operation and area requirements. There are mainly two types of cryptographic algorithms: symmetric and asymmetric algorithms. Symmetric systems such as Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES) uses an identical key for the sender and receiver; both to encrypt the message text and decrypt the cipher text. Asymmetric systems such as Rivest-Shamir-Adelman (RSA) & Elliptic Curve Cryptosystem (ECC) uses different keys for encryption and decryption. Symmetric cryptosystems is more suitable to encrypt large amount of data with high speed.

To replace the old Data Encryption Standard, in September 12 of 1997, the National Institute of Standard and Technology (NIST) required proposals to what was called Advanced Encryption Standard (AES). Many algorithms were presented originally with researches from 12 different nations. On October 2nd 2000, NIST has announced the Rijndael Algorithm is the best in security, performance, efficiency, implement ability & flexibility. The Rijndael algorithm was developed by Joan Daemen of Proton World International and Vincent Rijmen of Katholieke University at Leuven. AES encryption is an efficient scheme for both hardware and software implementation. As compare to software implementation, hardware implementation provides greater physical security and higher speed. Hardware implementation is useful in wireless security like military communication and mobile telephony where there is a greater emphasis on the speed of communication. Most of the work has been presented on hardware implementation of AES using FPGA.

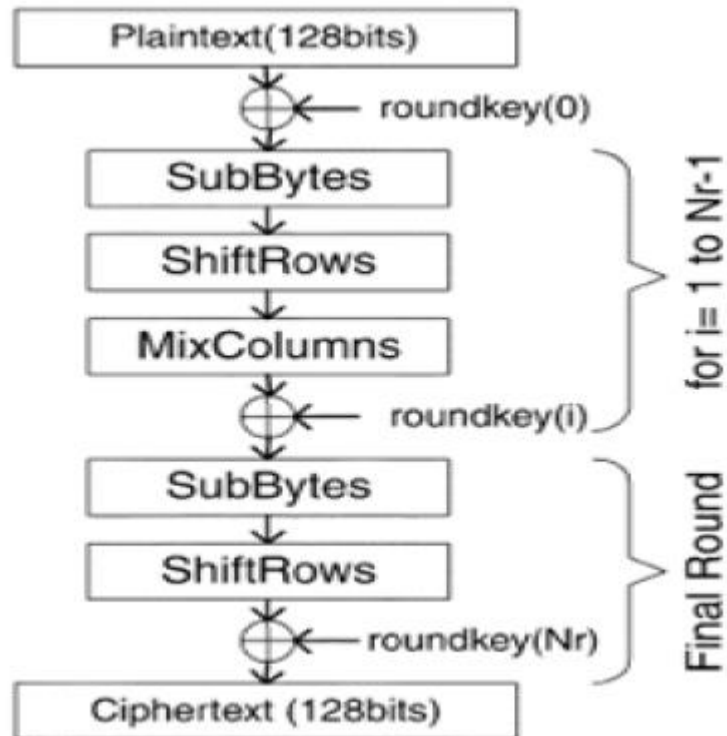


Figure 2.2 Detailed Block diagram of encryption part

In the encryption of the AES algorithm(Figure 2.2), each round except the final round consists of four transformations:

- i. SubBytes: Operates in each byte of the State independently. Each byte is substituted by corresponding byte in the S-box.
- ii. ShiftRow: Cyclically shifts the rows of the State over different offsets.
- iii. MixColumn: In this operation the column of the State are considered as polynomials over  $GF(2^8)$  and are multiplied with a fixed polynomial. The MixColumn component does not operate in the last round of the algorithm.
- iv. AddRoundKey: Involves bit-wise XOR operation.

### 2.1.3 Title : Advanced Encryption Standard by Douglas Selent.[3]

Advanced Encryption Standard (AES) is the current standard for secret key encryption. AES was created by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, replacing the old Data Encryption Standard (DES). The Federal Information Processing Standard 197 used a standardized version of the algorithm called Rijndael for the Advanced Encryption Standard. The algorithm uses a combination of Exclusive-OR operations (XOR), octet substitution with an S-box, row and column rotations, and a MixColumn. It was successful because it was easy to implement and could run in a reasonable amount of time on a regular computer.

On January 2, 1997 the National Institute of Standards and Technology (NIST) held a contest for a new encryption standard. The previous standard, DES, was no longer adequate for security. It had been the standard since November 23, 1976. Computing power had increased a lot since then and the algorithm was no longer considered safe. In 1998 DES was cracked in less than three days by a specially made computer called the DES cracker. The DES cracker was created by the Electronic Frontier Foundation for less than \$ 250,000 and won the RSA DES Challenge II-2. Current alternatives to a new encryption standard were Triple DES (3DES) and International Data Encryption Algorithm (IDEA). The problem was IDEA and 3DES were too slow and IDEA was not free to implement due to patents. NIST wanted a free and easy to implement algorithm that would provide good security.

Additionally they wanted the algorithm to be efficient and flexible. After holding the contest for three years, NIST chose an algorithm created by two Belgian computer scientists, Vincent Rijmen and Joan Daemen. They named their algorithm Rijndael after themselves. Supposedly Rijndael can only be pronounced correctly by people who can speak Dutch and the closest English approximation is “Rhine Dahl”. On November 26, 2001 the Federal Information Processing Standards Publication 197 announced a standardized form of the Rijndael algorithm as the new standard for

encryption. This standard was called Advanced Encryption Standard and is currently still the standard for encryption.

		Block			
		0	1	2	3
0	T			a	s
1	h		i		t
2	i		s	t	.
3	s			e	.

**Figure 2.3 AES-128 block example**

Each character is stored in a cell of the block. The blank cells shown in the diagram are not really blank as they represent the spaces in the text. Depending on how the algorithm is implemented the characters may be stored as integer values, hexadecimal values, or even binary strings. All three ways represent the same data. Most diagrams show the hexadecimal values, however integer and string manipulation is much easier to do when actually programming AES. Figure 1 shows the values as characters for demonstration purposes to show how the text is stored into the block. The plain text is stored into blocks column by column and block by block until all the data is stored.

In the example used above there were exactly 16 characters used for simplicity. In order to use the Rijndael algorithm the data must be a multiple of the block size, since all blocks need to be complete. When the data is not a multiple of the block size some form of padding must be used. Padding is when extra bits are added to the original data. One forms of padding includes adding the same bytes until the desired size is reached. Another option is padding with all zeros and having the last byte represent the number of zeros.