

**ENCRYPTION USING FPGA**

**NOR ROBAINI BINTI IBRAHIM**

**UNIVERSITI MALAYSIA PAHANG**

“I hereby acknowledge that the scope and quality of this thesis is qualified for the award of the Bachelor Degree of Electrical Engineering (Hons.) (Electronics)”

Signature : \_\_\_\_\_

Name : NURUL HAZLINA BINTI NOORDIN

Date : 23 MEI 2008



UNIVERSITI MALAYSIA PAHANG

**BORANG PENGESAHAN STATUS TESIS♦**

JUDUL: ENCRYPTION USING FPGA

SESI PENGAJIAN: 2007/2008

Saya NOR ROBAINI BINTI IBRAHIM ( 850102-08-

mengaku membenarkan tesis (Sarjana Muda/~~Sarjana~~ /~~Doktor Falsafah~~)\* ini disimpan di Perpustakaan dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Malaysia Pahang (UMP).
2. Perpustakaan dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis 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)

\_\_\_\_\_  
(TANDATANGAN PENYELIA)

Alamat Tetap:

KG. KANDANG,  
KOTA SETIA, 36000 TELUK INTAN,  
PERAK

NURUL HAZLINA NOORDIN  
( Nama Penyelia )

Tarikh: 23 MEI 2008

Tarikh: : 23 MEI 2008

- CATATAN:
- \* Potong yang tidak berkenaan.
  - \*\* Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali tempoh tesis ini perlu dikelaskan sebagai atau TERHAD.
  - ♦ Tesis dimaksudkan sebagai tesis bagi Ijazah doktor Falsafah dan Sarjana secara Penyelidikan, atau disertasi bagi pengajian secara kerja kursus dan penyelidikan, atau Laporan Projek Sarjana Muda (PSM).

ENCRYPTION USING FPGA

NOR ROBAINI BINTI IBRAHIM

This thesis is submitted as partial fulfillment of the requirements for the award of the  
Bachelor of Electrical Engineering (Hons.) (Electronics)

Faculty of Electrical & Electronics Engineering  
Universiti Malaysia Pahang

MEI, 2008

“All the trademark and copyrights use herein are property of their respective owner. References of information from other sources are quoted accordingly; otherwise the information presented in this report is solely work of the author.”

Signature : \_\_\_\_\_

Author : NOR ROBAINI BINTI IBRAHIM

Date : 23 MEI 2008

**DEDICATION**

*To my beloved parents,*

*Hj Ibrahim Bin Mat Hassan and my late mother, Hjh. Asmaliah Binti  
Damanhuri for their full support, love, patience and encouragement during  
my degree's study.*

## ACKNOWLEDGEMENT

Assalamualaikum warahmatullahi wabarahkatu,

Thank you Allah for give me this opportunity to finish my undergraduate project. It is a very great pleasure for me to acknowledge the contribution of a large number of individuals that being supportive throughout this year. First of all, I would like to thank my supervisors, Puan Nurul Hazlina binti Noordin, for provide me precious helps, supports and motivation throughout the development of this project.

I would like to dedicate appreciation to my friends and course mates. Not to forget my beloved roommates who always lend me shoulders to cry on. We have gone through thick and thin together. All the courage and valuable memory you gave will never be forgotten. Thank you for always being by my side.

I also would like to acknowledge my parents and siblings. Thank you for your support and motivation. I am gratefully acknowledged the support, encouragement, and patience of my families. I am very happy to have family that always loves me and care about me. Without them, I will not be able to finish this project. Last but not least to all other peoples whose are not mention here. Your contributions are very much appreciated.

Thank you very much.



## **ABSTRACT**

Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a block cipher that can encrypt and decrypt digital information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits, this project implements the 128 bit standard on a Field Programming Gate Array (FPGA) using the VHDL, a hardware description language.

## **ABSTRAK**

Piawaian Penyulitan Maju (AES), satu Federal Information Processing Standard (FIPS), adalah diluluskan di mana kriptografik algoritma yang boleh digunakan untuk melindungi data elektronik. Algoritma AES adalah satu sifar blok yang boleh encrypt dan decrypt maklumat digital. Algoritma AES adalah berupaya menggunakan cryptographic kunci-kunci 128, 192, dan 256 bits, di mana projek ini menggunakan 128 bit mata piawaian pada Field Programming Gate Array (FPGA) menggunakan VHDL, satu perkakasan bahasa penggambaran.

## TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	<b>TITLE OF PAGE</b>	<b>i</b>
	<b>DECLARATION</b>	<b>ii</b>
	<b>DEDICATION</b>	<b>iii</b>
	<b>ACKNOWLEDGMENT</b>	<b>iv</b>
	<b>ABSTRACT</b>	<b>v</b>
	<b>ABSTRAK</b>	<b>vi</b>
	<b>TABLE OF CONTENT</b>	<b>vii</b>
	<b>LIST OF FIGURES</b>	<b>x</b>
	<b>LIST OF TABLES</b>	<b>xi</b>
	<b>LIST OF ABBREVIATIONS</b>	<b>xii</b>
<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
	1.1 Overview	1
	1.2 Objectives	1
	1.3 Problem statement	2
	1.4 Scope of project	2
<b>2</b>	<b>LITERATURE REVIEW</b>	<b>3</b>
	2.1 Encryption	3
	2.1.1 Symmetric cryptography (Private-key cryptography)	4

2.1.1.1	Data Encryption Standard (DES)	5
2.1.1.2	Advanced Encryption Standard (AES)	5
2.1.1.3	Twofish	6
2.1.2	Asymmetric cryptography (Private-key cryptography)	7
2.1.2.1	Pretty Good Privacy (PGP)	8
2.2	Field Programming Gate Array (FPGA)	9
2.2.1	Verilog Hardware Description Language (VHDL)	9
<b>3</b>	<b>METHODOLOGY</b>	<b>11</b>
3.1	Methodology Flow Chart	11
3.1.1	SubBytes	12
3.1.2	ShiftRows	13
3.1.3	MixColumns	13
3.1.4	AddRoundKey	15
3.2	Software implementation	15
3.3	Project development	16
3.3.1	Initial stage	16
3.3.2	First stage	16
3.3.3	The systems	17
3.3.4	Systems operation	19
<b>4</b>	<b>RESULT AND DISCUSSION</b>	<b>23</b>
4.1	Introduction	23
4.2	Result analysis	24
4.2.1	prgmctrl.vhd	24
4.2.2	ps2_keyboard.vhd	26
4.2.3	key_ram.vhd	28
4.2.4	sbox_rom.vhd	29
4.2.5	lcd_top.vhd	30
4.2.6	aescore.vhd	31
4.3	Costing and commercialization	32

<b>5</b>	<b>CONCLUSION</b>	<b>33</b>
5.1	Conclusion	33
5.2	Recommendation	34
	<b>REFERENCES</b>	<b>35</b>
	<b>APPENDIX</b>	
	APPENDIX A	36

## LIST OF FIGURES

<b>FIGURE NO</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	Encrypting and decrypting with the same key	4
2.2	Encrypting and then decrypting with public-private key	4
2.3	AES algorithm process	6
3.1	AES flow chart of encrypting data	11
3.2	SubBytes applies the S-Box to each byte of the state	12
3.3	S-Box: substitution values for the byte xy (in hexadecimal format)	12
3.4	ShiftRows cyclically shifts the last three rows in the state	13
3.5	MixColumns operates on the state column-by-column	14
3.6	XORs each column of the state with a word from the key schedule	15
3.7	VHDL sub-systems block diagram	17
3.8	MixColumn constant array	21
3.9	Inverse MixColumns constant array	21
3.10	MixColumns ()Inverse	21
3.11	MixColumns ()	22
4.1	Sub-system pgrmctrl.vhd	24
4.2	Simulation waveform of pgrmctrl.vhd	25
4.3	Sub-system ps2_keyboard.vhd	26
4.4	Simulation waveform of ps2_keyboard.vhd	27
4.5	Sub-system key_ram.vhd	28
4.6	Simulation waveform of key_ram.vhd	28
4.7	Sub-systems sbox_rom.vhd	29
4.8	Simulation waveform of sbox_rom.vhd	29
4.9	Sub-system lcd_top.vhd	30
4.10	Simulation waveform of lcd_top.vhd	30
4.11	Simulation waveform of aescore.vhd	31

**LIST OF TABLES**

<b>TABLE NO.</b>	<b>TITLE.</b>	<b>PAGE</b>
3.1	Opcode table	20
3.2	Status word table	20
4.1	Sample data from <i>http://cegt201.bradley.edu</i>	26
4.2	Sample data from <i>http://cegt201.bradley.edu</i>	28
4.3	Sample data from <i>http://cegt201.bradley.edu</i>	29

## LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
Affine	A transformation consisting of multiplication by a matrix followed by Transformation the addition of a vector.
Array	An enumerated collection of identical entities (e.g., an array of bytes).
Bit	A binary digit having a value of 0 or 1.
Block	Sequence of binary bits that comprise the input and output. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes.
Byte	A group of eight bits that is treated either as a single entity or as an array of 8 individual bits.
Cipher	Series of transformations that converts plaintext to ciphertext using the Cipher Key.
Cipher Key	Secret, cryptographic key that is used by the Key Expansion routine to generate a set of Round Keys; can be pictured as a rectangular array of bytes, having four rows and n columns.
Ciphertext	Data output from the Cipher or input to the Inverse Cipher.
Inverse Cipher	Series of transformations that converts ciphertext to plaintext using the Cipher Key.
Key Expansion	Routine used to generate a series of Round Keys from the Cipher Key.
Plaintext	Data input to the Cipher or output from the Inverse Cipher.
Rijndael	Cryptographic algorithm specified in this Advanced Encryption Standard (AES).



Round Key	Round keys are values derived from the Cipher Key using the Key Expansion routine; they are applied to the State in the Cipher and Inverse Cipher.
State Intermediate	Cipher result that can be pictured as a rectangle array of bytes, having four rows and m columns.
S-box	Non-linear substitution table used in several byte substitution transformations and in the Key Expansion routine to perform a one-for-one substitution of a byte value.
Word	A group of 32 bits that is treated either as a single entity or as an array of 4 bytes.
Word	A group of 32 bits that is treated either as a single entity or as an array of 4 bytes.

# CHAPTER 1

## INTRODUCTION

### 1.1 Overview

AES is an algorithm for performing encryption (and the reverse, decryption) which is a series of well-defined steps that can be followed as a procedure. The original information is known as plaintext, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format that can read by a human or computer without the proper mechanism to decrypt it; it should be resemble random gibberish to those not intended to read it. The encryption procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt or decrypt. In the past, cryptography helped ensure secrecy in important communications, such as those of government covert operations, military leaders and diplomats. Cryptography has come to be in widespread use by many civilians who cannot have extraordinary needs for secrecy, although typically it is transparently built into the infrastructure for computing and telecommunications [1].

### 1.2 Objectives

This project is more towards on implement encryption technology with using FPGA as a device for encrypting data.

The objectives of this project are:

- i. To study the encryption technology that widely use in communication as a guidance for secrecy.
- ii. To implement Advanced Encryption Standard (AES) with using digital concept.

### 1.3 Problem Statement

There are four algorithms in AES which is subbytes transformation, shiftrows transformation, mixcolumns transformation and addroundkey transformation. Each of these algorithms has mathematical equation and it can be proved with using digital concept.

- i. Subbytes transformation

$$b_i' = b_i \text{ XOR } b_{(i+4) \bmod 8} \text{ XOR } b_{(i+5) \bmod 8} \text{ XOR } b_{(i+6) \bmod 8} \text{ XOR } b_{(i+7) \bmod 8} \quad (1.1)$$

- ii. Shiftrows transformation

$$s'_{r,c} = s_{r,(c+\text{shift}(r,Nb)) \bmod Nb} \quad \text{for } 0 < r < 4 \text{ and } 0$$