UNIVERSITI TEKNIKAL MALAYSIA MELAKA

IMPLEMENTATION OF RSA ENCRYPTION AND DECRYPTION ON FPGA

This report is submitted in accordance with the requirement of the Universiti Teknikal Malaysia Melaka (UTeM) for the Bachelor of Computer Engineering Technology (Computer Systems) with Honours

by

CHEN JIAN SING

B071310469

921211-14-5063

FACULTY OF ENGINEERING TECHNOLOGY

2016

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN PROJEK SARJANA MUDA

TAJUK: **Implementation of RSA Encryption and Decryption on FPGA**

SESI PENGAJIAN: **2016/17 Semester 1**

Saya **CHEN JIAN SING**

Mengaku membenarkan Laporan PSM ini disimpan di Perpustakaan UniversitiTeknikal Malaysia Melaka (UTeM) dengan syarat-syarat kegunaan seperti berikut:

1. Laporan PSM adalah hak milik Universiti Teknikal Malaysia Melaka dan penulis.
2. Perpustakaan Universiti Teknikal Malaysia Melaka dibenarkan membuat salinan untuk tujuan pengajian sahaja dengan izin penulis.
3. Perpustakaan dibenarkan membuat salinan laporan PSM ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (✓)

□ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia sebagaimana yang termaktub dalam AKTA RAHSIA RASMI 1972)

□ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

□ TIDAK TERHAD

Disahkan oleh:

____________________ ____________________

Alamat Tetap:

Block 8-7-18 Taman Miharja
Jalan Loke Yew
55200 K.L.

Cop Rasmi:

Tarikh: ____________________

Tarikh: ____________________

** Jika Laporan PSM ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan PSM ini perlu dikelaskan sebagai SULIT atau TERHAD.

Rujukan Kami (Our Ref) :
Rujukan Tuan (Your Ref) :

28 DISEMBER 2016

Pustakawan
PerpustakaanUTeM
Universiti Teknikal Malaysia Melaka
Hang Tuah Jaya,
76100 Durian Tunggal,
Melaka.

Tuan/Puan,

PENGKELASAN LAPORAN PSM SEBAGAI SULIT/TERHAD LAPORAN PROJEK SARJANA MUDA TEKNOLOGI KEJURUTERAAN (SISTEM KOMPUTER): CHEN JIAN SING

Sukacita dimaklumkan bahawa Laporan PSM yang tersebut di atas bertajuk***"Implementation of RSA Encryption and Decryption on FPGA"*** mohon dikelaskan sebagai *SULIT / TERHAD untuk tempoh LIMA(5) tahun dari tarikh surat ini.

2. Hal ini adalah kerana IANYA MERUPAKAN PROJEK YANG DITAJA OLEH SYARIKAT LUAR DAN HASIL KAJIANNYA ADALAH SULIT.

Sekian dimaklumkan. Terimakasih.

Yang benar,

____

* Potong yang tidak berkenaan

NOTA: BORANG INI HANYA DIISI JIKA DIKLASIFIKASIKAN SEBAGAI SULIT DAN TERHAD. JIKA LAPORAN DIKELASKAN SEBAGAI **TIDAK TERHAD**, MAKA BORANG INI **TIDAK PERLU DISERTAKAN** DALAM LAPORAN PSM

DECLARATION

I hereby, declared this report entitled “Implementation of RSA encryption and decryption on FPGA” is the results of my own research except as cited in references.

Signature : ………………………………………….

Author’s Name : …………………………………………

Date : …………………………………………

APPROVAL

This report is submitted to the Faculty of Engineering Technology of UTeM as a partial fulfillment of the requirements for the degree of Bachelor Degree of Computer Engineering Technology (Computer Systems) with Honours. The member of the supervisory is as follow:

………………………………

(Project Supervisor)

ABSTRACT

RSA (Rivest, Shamir, and Adleman) cryptosystem is the most secure algorithm that can be used to protect information during the communication between system and system. Without this RSA cryptosystem, every hardware tendency to be hacked is very high which the information can be easily taken by third party. Based on NIST after 31 December, 2013 has recommended that RSA-1024 certificate be eliminated and replace with RSA-2048, or stronger keys. From industry experts also, 1024-bit of RSA is now often used by cybercriminal and a high risk compromised by cybercriminal. This is because due to the short length 1024 bit in had been used. Hence, in this project, will try to develop and implement this RSA algorithm in FPGA using Verilog language. While puTTy act as user interface to check the result which encryption the plain text will become cipher text and decryption the cipher text will become plain text again. At the end of this project will analysis and compare with the previous project in processing speed, allocation space in FPGA and circuit using in the FPGA.

ABSTRAK

Kripto (Rivest, Shamir, and Adleman) sistem *bagi RSA adalah algoritma yang paling selamat yang boleh digunakan untuk melindungi maklumat semasa berkomunikasi antara sistem dan sistem. Tanpa kriptografi RSA ini, setiap kecenderungan perkakasan untuk digodam adalah sangat tinggi yang mana maklumat boleh diambil oleh pihak ketiga dengan mudah. Berdasarkan NIST selepas 31 Disember 2013 telah disyorkan bahawa sijil RSA-1024 dihapuskan dan menggantikan dengan RSA-2048, atau kekunci yang lagi kuat. Daripada pakar-pakar industri juga, 1024-bit RSA kini sering digunakan oleh cybercriminal dan risiko yang tinggi dikompromi oleh cybercriminal. Ini adalah kerana disebabkan oleh pendek kekunci iaitu 1024 bit dalam telah digunakan. Oleh itu, dalam projek ini, akan cuba untuk membangunkan dan melaksanakan algoritma RSA ini dalam FPGA menggunakan bahasa Verilog. Walaupun PuTTy bertindak sebagai antara muka pengguna untuk menyemak keputusan yang penyulitan teks biasa akan menjadi teks cipher dan penyahsulitan teks cipher akan menjadi teks biasa lagi. Pada akhir projek ini akan analisis dan perbandingan dengan projek sebelumnya dalam kelajuan pemprosesan, ruang peruntukan dalam FPGA dan litar menggunakan dalam FPGA.*

DEDICATION

To my beloved parents who taught me that the best kind of knowledge to have is learned for its own sake. It is also dedicated to my supervisor who taught me that even the largest task can be accomplished if it is done one step at a time.

ACKNOWLEDGMENT

I would like to thank Sir Aiman Zakwan bin Jidin. He has been the ideal thesis supervisor. His sage advice, insightful criticisms, and patient encouragement aided the writing of this thesis in innumerable ways.

Thank you.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

CHAPTER 2: LITERATURE REVIEW

CHAPTER 3: METHODOLOGY

CHAPTER 4: RESULT AND DISCUSSION

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS, SYMBOLS AND NOMENCLATURE

ASIC	Application Specific Integrated Circuit
FPGA	Field-Programmable Gate Array
GCD	Greatest Common Divisor
IP	Intellectual Property
ISE	Integrated Synthesis Environment
NIST	National Institute Of Standards and Technology
PLD	Programmable Logic device
RSA	Rivest, Shamir, Adelman (an algorithm)
VHDL	Very High Speed Integrated Circuit Hardware Description Language

Chapter 1

INTRODUCTION

1.0 Background

This project is about the encryption and decryption data. There are many type of data which can categories as file data, password data (window account lock), and password internet data. This project is more focus on password's internet data. In this technology world, any password can be cracked easily if do not implement a new system on it. If the password was cracked, all the confidential document maybe taken by attacker and do activity criminal.

This project are very interesting to learn because it consists many code and few hardware to function it well. If this project success, not only the help technology world brighter and it also help protect the privacy.

This project will involve Altera Quartus design with using Verilog HDL language as the coding implementation part for the FPGA system. While PuTTy act as a user interface to let the user decide the encrypt data and the decrypt data. This project is predict that, when user enter a data with a public key (prime number), the encrypt data was show. Then, cipher text was created by using the formula. By using the decryption key, the cipher test can be decrypt become plain text back.

1.1 Problem Statement

Cryptography was frequently used without aware of it. This was because human only know the software using to do their project but cryptograph was not. For example, unlock the phone, log-in email, log-in Facebook, and Wi-Fi password. All this password will encrypt first before it send to the medium (like internet). In the Internet, Internet do not recognize the person that log in, they only recognize the username and password input by user, if is correct, it let it access. Hence, this encryption is more and more frequent use by human to prevent the password hack and secure the privacy. Whether there have many encryption can be found in the internet, if this encryption is keep outdated, one day will be break by attackers. Thus, this encryption should keep up to date or implement a more secure encryption to protect the information being from stole. In the cryptography has a lot of complex calculation to find the encryption key and decryption key. By using the FPGA which have a parallel execution to find the encryption key and decryption key, faster and efficient compare to programmable logic Device

1.2 Objective

The objectives of the project are:

- To develop an effective hardware RSA of encryption and decryption on FPGA.
- To study the Extended Euclidean algorithm to find decryption key.
- To analyze functionality and performance of the hardware.

1.3 Work scope

This project of main task is the operation of 2048-bit RSA encryption and decryption woks. But the ASCII code have to study first, because this convert the character of the data into binary or value to do the encryption conversion later.

For FGPA part, Altera Quartus is a design platform to implement the hardware description language. While Verilog HDL language is used to construct the behaviors of the product. This is because Verilog HDL language are more commercialize in the market use. Besides that this language can also use in other hardware also not only for FPGA.

For the user interface, PuTTy is one of the choice to let the user communicate with the FPGA hardware. RS 232 which act like a transmission between PC and FPGA.

All above must do research and study, and try to understand all the working process and the coding process also. Moreover, the process time will be taken to measure for data encrypt and decrypt, to know the different on long and short data input. After the project successful implemented, it will be tested and analysis on the different term of conditions.

1.4 Outline

In the chapter 2 will discuss more on the hardware and the software used on. For chapter 3 will discuss on the methodology mean the step work success to implement for this project. Chapter 4 is about the result get from the chapter 3 and written in the word form. If the project fail to get the result, will discuss why this will happen.

Chapter 2

LITERATURE REVIEW

2.0 Introduction

In this chapter separate into 2 main part which will discuss later. First was cryptography and how it works. Second was about the hardware part that study the previous project to get the information about this project. Lastly, discuss about the software part. Software was implement into many different way to go.

2.1 Cryptography

Cryptography is the word come from Greek, *kryptós* which mean hidden, secret. In general cryptograph means constructing and analyzing protocols to prevent third parties or public from reading private message. This message include data confidentiality, data integrity, authentication are modern cryptograph. Modern cryptography exists between disciplines of mathematics, computer science and electrical engineering. In modern cryptography, there are 2 types of encryption and decryption which is symmetric-key cryptography and asymmetrical-key cryptography.

2.1.1 Symmetric-key cryptography

Symmetric-key cryptography stands for the encryption method which both sender and receiver share the same key. In this way their keys are same, both sender and receiver may know how to decrypt the cipher text later.

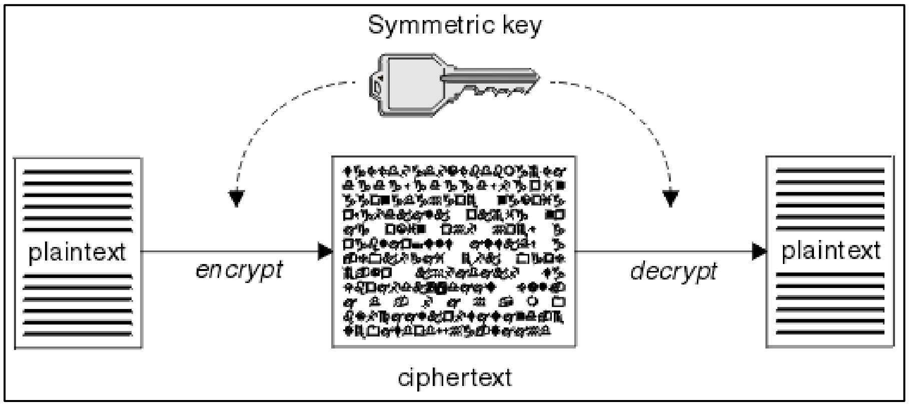

Figure 2.1: Symmetric-key cryptography

(Source:https://www.ibm.com/support/knowledgecenter/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009800_.htm)

Figure 2.1 show the process for a symmetric-key cryptography. The plain text which the readable text or information that need receiver to know it. While cipher text which is an unknown text, with this cipher text, no one can read though it what it the meaning of the text, except decrypt it into plain text. The plaintext was using a key to encrypt into cipher text, then this both key and cipher text were transmit into medium and sent to receiver. The receiver use the key that sent from sender to decrypt the cipher text into plain text. If a ruler draw a line on the cipher text. It can see that what on the left are reflected to the right and this was called as symmetrical. The most common symmetric-key cryptography was Data Encryption Standard (DES), and Advanced Encryption Standard (AES). (Swapna, 2014) The disadvantage for symmetric cryptography is both sender and received were known the encryption key and decryption key.

2.1.2 Asymmetric-key cryptography

Asymmetric-key cryptography is a cryptography system that using 2 kinds of different keys- a key pair to do the encryption and decryption. Public Key was made freely available to anyone. Private Key was kept as secret or only know by the owner. Both sender and receiver know the secret key, then can encrypt and decrypt all message that use the secret key.

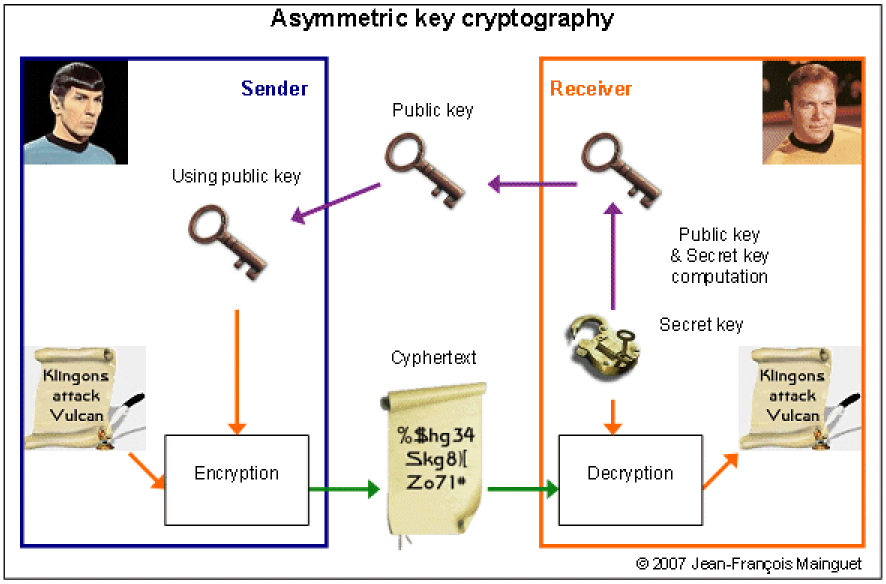

Figure 2.2: Asymmetric-key cryptography (Source: http://biometrics.mainguet.org/basics/cryptography.htm)

In this asymmetric-key cryptography, any people can encrypt a message using a public key of the receiver, but for this cryptography message only can decrypted by receiver received the private key from sender. This situation is to prevent the plain text falling into wrong hands over the internet or a large network. Besides the algorithm using to encrypt and decrypt should match with each other, else during the decryption it will not become plain text again or wired text. Hence, user no need to worry about their cipher text when the public keys passing over the internet. A big issue that for asymmetric encryption was a slower process than symmetric cryptography but it more secure than symmetric cryptography. (Swapna, 2014)

2.1.2.1 RSA

RSA is one of the type of asymmetric cryptography. RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute. RSA named by the 3 inventor first character name. This RSA was frequently use in this 20 century. This is because RSA was the most secure cryptography and RSA algorithm have a special calculation call modulus. During the encryption process the plain text have to power with the encrypt number then modulus with an N value (multiple with 2 coprime number) to become cipher text. When during the decryption process this cipher text have to decrypt with a decrypt number with an N value to get back the plain text (multiple with 2 coprime number). It look easy, but the problem is to pick encrypt and decrypt value have to using the RSA algorithm with meet some of the criteria with it. Below show an easy simple and the critera process example:

Encryption(5,14)

Plain text = B which represent 2 in number

2^5(mod 14) = 32 (mod14) = 4 (mod 14)

Cipher text = 4 which represent as D

Decryption(11,14)

Cipher text = D which represent 4 in number

4^{11}(mod 14) = 4194304 (mod 14) = 2 (mod 14)

Plain text = 2 which represent B =>get back the correct plain text

Above show the encryption using encryption(e,N)= encryption(5,14) which to encrypt the plain txt using the formula above. So, how to determine the e? During the decryption(d,N)= decryption(11,14) to decrypt the cipher text using the formula above to get back the d. So how to determine the d?