SHA ENCRYPTION SYSTEM

TAN SU NING

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS

JUDUL: SHA Encryption System

SESI PENGAJIAN: 2009/2010

Saya TAN SU NING

(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi 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	

(TANDATANGAN PENULIS)
Alamat tetap: No. 226, Lot 87, Sample Park, Phase 3, Jln Tun Hussein Onn, 97000 Bintulu, Sarawak.
Tarikh: 25/06/2010

(TANDATANGAN PENYELIA)
En. Mohd Rizuan Bin Baharon
Nama Penyelia

Tarikh: 25/06/2010

SHA ENCRYPTION SYSTEM

TAN SU NING

This report is submitted in partial fulfillment of the requirement for the Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2010

DECLARATION

I hereby declare that this project report entitled

SHA ENCRYPTION SYSTEM

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : ______________________ Date: 25/6/2010

(TAN SU NING)

SUPERVISOR : ______________________ Date: 25/6/2010

(MOHD RIZUAN BIN BAHARON)

DEDICATION

To my beloved family.

ACKNOWLEDGEMENT

First of all, I am heartily thankful to my supervisor, Mr Mohd Rizuan for his encouragement, guidance and support from initial to the final level of the project.

I would like to express my deepest appreciation to my family members especially my parents as well. They have been giving me both moral supports and material supports.

Besides, I would like to say thank you to all my friends and course mates for their kindness in sharing knowledge and resources. Thanks to Mr. Chew Chu Chee for his patient and brilliantly helping me overcome many programming obstacles in implementing this project.

Last but not least, I offer my regards and blessings to all of those who supported me in any respect during the completion of the project.

ABSTRACT

In the world of information technology, cryptography is a must for hiding the real meaning of information from unauthorized users. Secure Hash Standards are commonly used in generating digital signature. SHA-1 and SHA-256 are algorithms specified in Secure Hash Standard. SHA-1and SHA-256 are used to encrypt variable length of input message to fixed length of message digest. The main objective of this project is to develop a system as a learning tool for lecturers and students of Network Security. The system will perform SHA-1 and SHA-256 encryption and display the encryption process transparently. This project is developed by using Object-Oriented Analysis and Design (OOAD) methodology. Java programming language is chose to develop this system as it is a type of object-oriented programming language.

ABSTRAK

Dalam dunia teknologi maklumat, kriptografi merupakan suatu kemestian untuk menyembunyikan erti maklumat yang sebenar daripada pengguna yang tidak sah. *Secure Hash Standard* biasa digunakan untuk menghasilkan tandatangan digital. SHA-1 dan SHA-256 merupakam algoritma yang telah ditentukan dalam *Secure Hash Standard.* SHA-1dan SHA-256 digunakan untuk menyembunyikan erti sebenar mesej yang berlainan panjang ke *message digest* yang sama kepanjangannya. Tujuan utama projek ini adalah untuk membangunkan satu sistem untuk membantu pangajaran dan pembelajaran bagi pensyarah dan pelajar dalam mata pelajaran Keselamatan Rangkaian. Sistem ini akan melakukan SHA-1 dan SHA-256 dan memaparkan proses penyulitan secara telus. Projek ini dibangunkan dengan menggunakan kaedah *Object-Oriented Analysis and Design* (OOAD). Bahasa pengaturcaraan Java telah dipilih untuk membangunkan sistem ini kerana ia merupakan sejenis bahasa pengaturcaraan yang berorientasikan objek.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	-	Advanced Encryption Standard
API	-	Application Programming Interface
ASCII	-	American Standard Code for Information Interchange
ATM	-	Automatic Teller Machines
DES	-	Data Encryption Standard
DSA	-	Digital Signature Algorithm
ERD	-	Entity Relationship Diagram
FIPS	-	Federal Information Processing Standards
JCA	-	Java Cryptography Architecture
JCE	-	Java Cryptography Extension
JDK	-	Java Development Kit
JRE	-	Java Runtime Environment
JVM	-	Java Virtual Machine
MAC	-	Message Authentication Code
NSA	-	National Security Agency
OOA	-	Object-Oriented Analysis
OOAD	-	Object-Oriented Analysis and Design
OOD	-	Object-Oriented Design
OS	-	Operating System
PHP	-	Pre-Hypertext Processor
SDK	-	Software Development Kit
SHA	-	Secure Hash Algorithm
U.S	-	United States

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.1 Project Background

Computer security issues had been raised since few decades ago. Computer security ensures the computer is being protected from any harms. Principles that need to be achieved in order to invent a secure environment for computers are confidentiality, integrity and availability. One of the methods to fulfill these principles is encryption. Several encryption methods normally used are Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA and Secure Hash Algorithm (SHA). This project is focusing on SHA encryption only.

Secure Hash Algorithm (SHA) hash functions are a set of hash functions used to perform encryption which specially designed by National Security Agency (NSA) and published as United States (U.S) Federal Information Processing Standards (FIPS). Different structures of SHA algorithms produce different size of message digest. There are four (4) standard SHA which are SHA-1, SHA-256, SHA-384 and SHA-512. The processes of SHA-1 and SHA-256 are the main focus of this project.

All the algorithms are iterative, one-way hash functions that use to encrypt a message and produce a condensed representation of the message called a message digest. The message digest is used during generation of a signature for the message. These algorithms will determine the message's integrity. This is because any changes make on the input message will probably encrypted into different message digest. Thus, it is useful in generating and verifying the digital signatures and message authentication codes.

Each algorithm can be described in two (2) stages which are preprocessing and hash computation. Preprocessing involves message padding, message parsing into *m*-bit blocks and setting initialization values for hash computation. The hash computation will generate a message schedule from the padded message and uses the schedule, along with the functions, constants, and word operations to generate a series of hash values. The final hash values generated will be used to determine the message digest.

1.2 Problem Statements

The existing SHA encryption systems require users to key in the message they want to encrypt and the systems will show the message digest to the users. These systems do not show on how the SHA is working. People like lecturers, students of Network Security and those who want to know how SHA work are facing difficulties in teaching and understanding the SHA concept. The existing systems cannot help in solving their problem. Therefore, a new system that shows on how SHA algorithms run need to be implement in order to overcome and solve this problem.

1.3 Objectives

Objectives that will be achieved at the end of this project are:

- To develop a system that will perform SHA-1 and SHA-256 algorithms transparently.
- To develop a system that is useful as a learning tool and result comparison tool for lecturers and students of Network Security.

1.4 Scope

The scope for this project is to develop a standalone system that runs SHA algorithms. The targeted users for the system are lecturers, students and those who involve in network security field. This system will encrypt the input message to the message digest where the process of encryption will be transparent to all users.

1.5 Project Significance

The system will benefit those who want to understand on how SHA algorithms work. The users will key in the message they want to encrypt and choose which SHA algorithms (SHA-1 or SHA-256) to encrypt the message. The system will show the process of message padding, message parsing, setting initialization values and hash computation to users before the system end the encryption by showing the message digest.

1.6 Expected Output

The final result/product of this project is a standalone SHA encryption system that helps public to understand how SHA algorithms work.

1.7 Conclusion

In conclusion, a system that performs SHA-1 or SHA-256 will produce at the end of the project. It is expected that the results of every process performed by the algorithms will be transparent to users. The system is specially design as a teaching tool or comparison tool. The next chapter will discuss about literature review and project methodology.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

This chapter is mainly about literature review on Secure Hash Algorithms (SHA) encryption and methodology that going to be used in SHA Encryption System of this project. This chapter has brief explanations about the domain, keywords and previous research about this project. From the literature review, a solution is proposed to complete this project. A project schedule and milestones are also being produced to ensure that the project will complete within the time given and fulfill the project requirements.

Literature review can be defined as discussing about published information in a particular subject area, and sometimes information in a particular subject area within a certain time period. It can be just a simple summary of the sources. The resources of literature review can be journal articles, books, conference, government or corporate reports, newspapers, theses, Internet and magazines. In this project, Internet and books are the main resources to complete this chapter. Some journal articles are found too. Information found from the books and findings had been analyzed and summarized into this chapter.

Project methodology plays a very important role in this project because it is a framework or structure that is used to structure, plan, and control the process of developing a system. There are few methodologies can be used to develop a system.

Some examples of methodologies can be used are prototyping, spiral, waterfall, rapid allocation development, and object-oriented analysis and design (OOAD). In this chapter, explanation of the most suitable methodology for this project will be described.

2.2 Literature Review

2.2.1 Domain

SHA Encryption System that will be developed in this project is related to ICT in Defense and ICT in Education and Training. This system will do encryption of message using SHA-1 or SHA-256. As this system will show the processes (preprocessing and hash computation) in detail, it can be used as a teaching tool in the field of ICT in Education and Training.

2.2.2 Keyword

- **Information Security**

  The definition of information security is the measures and controls of information and the system and hardware that store data from theft or unintended users, corruption, or natural disaster. According to Mike Horton and Clinton Mugge (2003), information security is a fluid process that is always in motion and never ending. Ideally, it should be dealt with in a manner in which adequate processes and procedures are governing the right assets. [5]

  Three principal goals of information security are confidentiality, integrity and availability. Confidentiality is defined as ensuring the data is only accessible by the authorized person(s) only. The confidentiality of data is often protected by segmentation and strict access control measures to prevent unauthorized access. Integrity is defined as ensuring the data is accurate and unchangeable. Integrity is critical when data is used for performing transactions, statistical analysis, or mathematical computations. Availability is defined as ensuring the data or system is accessible at the point in time it is needed. Availability can be critical when data or applications must be accessed in real time.

- **Cryptography**

The availability of cryptography is a must for governmental, medical, industrial and financial operations, both domestic and internationally. Strong cryptography can be a best defense against potential domestic and foreign "cyber terrorism". Cryptography is the art and science of hiding the real meaning of information from unauthorized or unintended recipients. According to Dieter Gollmann(2005), in the traditional definition, cryptography is the science of secret writing but modern cryptography is very much a mathematical discipline. Cryptography is a translation mechanism which can enhance computer security, but it is not a substitute for computer security.[3]

- **Encryption**

Encryption can be defined as a cryptography method or a algorithmic scheme that is used to convert messages or any important data to humanly unreadable except by someone who knows how to decrypt it. The receiver of the encrypted messages must use a "key" to decrypt the message to the original messages. The "key" is an algorithm that undoes the work of the encryption algorithm. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key. It helps in protect the confidentiality of data. Encryption was largely been used by militaries and governments to facilitate secret communications before Interne is being introduced to the public. But, nowadays, public are aware of encryption as they are using some Internet services such as online marketing, online banking, cash deposit and withdrawal through Automatic Teller Machines (ATM) and etc.