

BORANG PENGESAHAN STATUS TESIS

JUDUL: AES AND DES DATA ENCRYPTION SYSTEM

SESI PENGAJIAN: SESI 2009/2010

Saya CHEW CHU CHEE 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 penukaran antara institusi pengajian tinggi.
4. Sila tandakan(/)

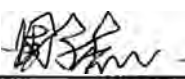
_____ SULIT (Mengandungi maklumat yang berdarjah

keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang

ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

_____ / _____ TIDAK TERHAD



(TANDATANGAN PENULIS)


Alamat Tetap: 39, Jalan Selera,

Taman Bukit Indah,

58200 Kuala Lumpur,

Malaysia

Tarikh: 25/6/2010



(TANDATANGAN PENYELIA)

En. Mohd Rizuan Bin Baharon

Tarikh: 25/6/2010

AES AND DES DATA ENCRYPTION SYSTEM

CHEW CHU CHEE

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


**FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA**


2010

DECLARATION

I hereby declare that this project entitled
AES AND DES DATA 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
(CHEW CHU CHEE)

SUPERVISOR :  Date: 25/6/2010
(EN MOHD RIZUAN BIN BAHARON)

DEDICATION

To my beloved parents...

ACKNOWLEDGEMENTS

I would like to show my gratitude and appreciation to my supervisor, Mr Mohd Rizuan for all his ideas and advices in guiding me throughout the project.

I would also like to thank my family members especially my parents. They have been giving me moral supports and all sorts of material supports throughout my years studying in this University.

Last but not least, I would like to say thank you to all my friends and course mates for their kindness in sharing knowledge and resources.

Thanks a lot.

ABSTRACT

Cryptography is an art where the message is transformed into other forms by using some algorithms. It is widely used in transferring data and message through network. The two algorithms used in this system are Advanced Encryption Standard (AES) and Data Encryption Standard (DES) which is the fundamental of the modern cryptography. The purpose of this project is to develop a system which can be served as a teaching tool for lecturers and students to use it when teaching or learning modern cryptography. Since the system is a teaching tool, it must be error free end user-friendly. This system was developed using Java programming language which is a type of object-oriented programming. The purpose of choosing Java because it can be run in multiplatform and it is easier to be improved in future. The methodology used is Object-Oriented Analysis and Design (OOAD) so that the system can be developed smoothly and fulfill all the scopes and objectives defined for this project.

ABSTRAK

Kriptografi merupakan suatu seni di mana maklumat akan diubah ke bentuk yang lain dengan menggunakan algoritma yang tertentu. Pada masa kini, kriptografi digunakan secara meluas untuk tujuan menghantar data atau mesej melalui rangkaian. Dua algoritma yang digunakan dalam projek ini ialah *Advanced Encryption Standard (AES)* dan *Data Encryption Standard (DES)*. *AES* dan *DES* merupakan asas kepada kriptografi moden. Tujuan sistem ini dibangunkan adalah untuk dijadikan alat bantu mengajar kepada pensyarah dan pelajar yang sedang mempelajari subjek kriptografi. Oleh itu, hasil pengiraan oleh sistem ini haruslah tepat dan benar. Oleh sebab system ini merupakan alat bantu mengajar, maka sistem ini mestilah bebas kesilapan (*error-free*) dan ramah pengguna. Sistem ini dibangunkan dengan menggunakan bahan pengaturcaraan Java yang berorientasi objek. Bahan pengaturcaraan Java dipilih kerana ia boleh diubahsuai dengan lebih senang pada masa hadapan. Metodologi yang digunakan dalam projek ini ialah *Object-Oriented Analysis and Design (OOAD)* supaya sistem ini dapat dibangunkan dengan lebih lancar dan memenuhi semua skop dan objektif projek ini.

TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	PROJECT TITLE	i
	ADMISSION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xiii
	LIST OF ATTACHMENTS	xv
CHAPTER I	INTRODUCTION	
	1.1 Project Background	1
	1.2 Problem Statement	2
	1.3 Objective	3
	1.4 Scope	3
	1.5 Project Significance	4
	1.6 Expected Output	4
	1.7 Conclusion	

CHAPTER II	LITERATURE REVIEW AND PROJECT METHODOLOGY	
2.1	Introduction	6
2.2	Literature Review	7
2.2.1	Domain	7
2.2.2	Keyword	7
2.2.3	Existing system	10
2.3	Proposed Solution	14
2.3.1	Project Methodology	14
2.4	Project Schedule and Milestones	18
2.5	Conclusion	18
CHAPTER III	ANALYSIS	
3.1	Introduction	19
3.2	Problem Analysis	20
3.3	Requirement analysis	22
3.3.1	Data Requirement	22
3.3.2	Functional Requirement	25
3.2.2.1	Algorithm of Data Encryption Standard (DES)	26
3.2.2.2	Algorithm of Advanced Encryption Standard (AES)	42
3.3.3	Non-functional requirement	54
3.3.4	Other requirement	55
3.4	Conclusion	56
CHAPTER IV	DESIGN	
4.1	Introduction	57
4.2	High-Level Design	57
4.2.1	System Architecture	58

4.2.2	User Interface Design	62
4.2.2.1	Navigation Design	62
4.2.2.2	Input Design	63
4.2.2.3	Output Design	64
4.3	Detailed Design	65
4.3.1	Software Design	66
4.4	Conclusion	66
CHAPTER V	IMPLEMENTATION	
5.1	Introduction	67
5.2	Software Development Environment Setup	68
5.3	Software Configuration Management	70
5.3.1	Configuration Environment Setup	70
5.3.2	Version Control Procedure	72
5.4	Implementation Status	73
5.5	Conclusion	75
CHAPTER VI	TESTING	
6.1	Introduction	76
6.2	Test Plan	76
6.2.1	Test Organization	76
6.2.2	Test Environment	77
6.2.3	Test Schedule	77
6.3	Test Strategy	78
6.3.1	Classes Of Tests	79
6.4	Test Design	80
6.4.1	Test Description	80
6.4.2	Test Data	81
6.5	Test Results And Analysis	83
6.5.1	Test Result For AES (128 bits)	83
6.5.2	Test Result For AES (192 bits)	87

6.5.3	Test Result For AES (256 bits)	89
6.5.4	Test Result For DES	91
6.6	Conclusion	93
CHAPTER VII PROJECT CONCLUSION		
7.1	Observation on Weaknesses and Strengths	94
7.2	Propositions for Improvement	95
7.3	Contribution	95
7.4	Conclusion	95
	REFERENCES	96
	BIBLIOGRAPHY	99
	APPENDICES	100

LIST OF TABLES

TABLE	TITLE	PAGE
3.1	Data Requirement For DES	22
3.2	Data Requirement For AES	24
3.3	Key Permutation	26
3.4	Initial Permutation	27
3.5	Expansion Permutation	30
3.6	Number Of Key Bits Shifted Per Round	31
3.7	Compression Permutation	32
3.8	S-Boxes	34
3.9	Result After Performing XOR Operation Between Expansion Permutation And Compression Permutation	37
3.10	Row For S-box	37
3.11	Column For S-box	38
3.12	Result After Performing S-box Substitution	38
3.13	P-box	39
3.14	Final Permutation	40
3.15	S-Box	44
3.16	RCon	52
3.17	Result For AddKeyround	54
3.18	Non-functional Requirement	54

3.19	Software Requirement	55
4.1	Table For Input Design	63
4.2	Table For Output Design	65
5.1	Working Directories	72
5.2	Version Of This System	72
6.1	Personal Computer Configuration	77
6.2	Test Schedule	78
6.3	List Of Tester	80
6.4	Test Data	81
6.5	Unit And Integration Testing Result	83

LIST OF FIGURES

DIAGRAM	TITLE	PAGE
2.1	Symmetric Encryption	8
2.2	Overall Structure Of AES Algorithm	9
2.3	AES In JCE	11
2.4	Styer's AES	12
2.5	Styer's DES	13
2.6	Fountain Model	15
3.1	Use Case Diagram For The Proposed System	25
3.2	A Round In DES	29
3.3	Overall Algorithm Of AES	42
4.1	Layered Architecture For AES And DES Data Encryption System	58
4.2	The AES And DES Data Encryption System Architecture	59
4.3	The High-level Class Diagram	60
4.4	The Sequence Diagram	61
4.5	Activity Diagram	62
5.1	The Software Development Environment Setup Architecture	68
5.2	Deployment Diagram	69
5.3	System Properties Windows	70
5.4	Environment Variables Windows	71
5.5	Edit System Variable Windows	71

6.1	Input Page For AES (128 bits) – Testing 1	84
6.2	Output Page For AES (128 bits) – Testing 1	84
6.3	Input Page For AES (128 bits) – Testing 2	85
6.4	Output Page For AES (128 bits) – Testing 2	85
6.5	Input Page For AES (128 bits) – Testing 3	86
6.6	Output Page For AES (128 bits) – Testing 3	86
6.7	Input Page For AES (192 bits) – Testing 1	87
6.8	Output Page For AES (192 bits) – Testing 1	87
6.9	Input Page For AES (192 bits) – Testing 2	88
6.10	Output Page For AES (192 bits) – Testing 2	88
6.11	Input Page For AES (256 bits) – Testing 1	89
6.12	Output Page For AES (256 bits) – Testing 1	89
6.13	Input Page For AES (256 bits) – Testing 2	90
6.14	Output Page For AES (256 bits) – Testing 2	90
6.15	Input Page For DES – Testing 1	91
6.16	Output Page For DES – Testing 1	91
6.17	Input Page For DES – Testing 2	92
6.18	Output Page For DES – Testing 2	92

LIST OF ATTACHMENTS

ATTACHMENT	TITLE	PAGE
A	GANTT CHART	101
	UML NOTIFICATION	
B.1	UML Notification For Converter Class	102
B.2	UML Notification For StringToArrayList Class	102
B.3	UML Notification For ValidateHex Class	102
B.4	UML Notification For Encryption Class	104
B.5	UML Notification For InputGUI Class	105
B.6	UML Notification For StateMatrix Class	106
B.7	UML Notification For SBox Class	106
B.8	UML Notification For AddRoundKey Class	107
B.9	UML Notification For ShiftRows Class	107
B.10	UML Notification For MixColumns Class	107
B.11	UML Notification For SubBytes Class	107
B.12	UML Notification For ArrangeInputMatrix Class	108
B.13	UML Notification For ProcessMessage Class	108
B.14	UML Notification For GetSubKey Class	109
B.15	UML Notification For OutputGUI Class	110

C	ALGORITHM OF CLASSES ACCORDING TO THEIR PACKAGE	111
	C.1 Algorithm For Classes Of Input Package	111
	C.2 Algorithm For Classes In AES Package	136
	C.3 Algorithm For Classes In DES Package	149
	C.4 Algorithm For Classes Of Output Package	162
D	UNIT TEST CASE	171
	D.1 Unit Test Cases For Input Module (AES 128 bits)	171
	D.2 Unit Test Cases For Input Module (AES 192 bits)	177
	D.3 Unit Test Cases For Input Module (AES 256 bits)	183
	D.4 Unit Test Cases For Input Module (DES)	189
	D.5 Unit Test Cases For Output Module	194
E	INTEGRATION TEST CASE	195
	E.1 Integration Test Case For Input Module	195
	E.2 Integration Test Case For Output Module	196
	FEEDBACK FORM FOR SYSTEM TESTING	197
G	USER MANUAL	198
	G.1 Main Page	198
	G.2 MessageBox Display When The Key Or Message Are Left Blank	199
	G.3 MessageBox Display When The Key Or Message Are Less Than The Default Size Defined By The Algorithms	199
	G.4 MessageBox Display If The Message Or Key Contain Non Hexadecimal	199

	Characters If The Input Form Chosen Is Hexadecimal	
	G.5 Output Page	200
H	PROJECT PROPOSAL FORM	201
I	LOG BOOK	207

CHAPTER I

INTRODUCTION

1.1 Project Background

Data Encryption Standard (DES) was introduced in 1977 and it is used widely due to the rapid development in hardware with memory and the use of computer networks until today (Eskicioglu and Litwin, 2001). It is used to encrypt data to store in personal computer or to send over internet for security purpose. Owing to the fast path development in Science and Technology, there are many machines or hardware created to break the DES code which is in 56-bits in several minutes. As a result, Advanced Encryption Standard (AES) started to develop in year 2000 with more possibilities of key and more time needed to break the code (Yenuguvanilanka and Elkeelany, 2008).

This system can be used for many purposes such as a teaching tool for subjects related to data encryption, comparison tool for the encryption in network field and so on. Currently, there are quite number of existing systems for data encryption. However, many of them only support for either one of the algorithms. Besides that, they only show the final result after the data encrypted. The additional function for this system is it supports both DES and AES algorithm. Instead of only showing the ciphertext, this system is able to display the results obtained in every single rounds.

1.2 Problem statement

AES and DES algorithm are very important to the students who are studying Computer Science especially for those who are majoring in Networking. To learn and understand these algorithms is not easy if there are no simulation tools to help them. Maybe they can understand the concept of these two algorithms, but when it comes to practical part where they are asked to do exercises, they might face problem in finding the correct and accurate answer. To err is human, the answer could be wrong if they are careless when doing calculation. So it would be better if they have a tool where they can compare their answer.

There are dozens of simulation tools we could find through internet but most of them only show the final result. So if the answer was wrong, it is very hard to trace back where they have done wrongly. Besides that, it is hard to find a tool which can support both of the algorithms and most of the system can only run online or we need to purchase before we can use it. To avoid plagiarism issues, most of the online tools or applications have set some default keys instead of letting the user to key in their own key to perform AES or DES; this could be one of the limitations of online system. To be different from others, this system is developed using Java Programming Language which is able to work offline or normally known as standalone software. Moreover, it can be run in many other platforms as the computers in lab might be installed with other operating system such as Linux, Sun Solaris, Fedora and so on. Lastly, user can choose their own preferred key to perform the algorithms.

1.3 Objective

The objectives to develop this system are:

- To develop an error-free and user-friendly system to perform the AES and DES algorithm.
- To develop a system that can be used to display the results in every rounds of the process for both algorithms.
- To develop a system which can be used as teaching tool or comparison for the results obtained.

1.4 Scope

The scopes of this project are:

- Covered the encryption part only for both of the algorithms.
- Targeted to students, lectures and networking engineer (responsible for data encryption part only).
- Developed a standalone type data encryption system that contains two methods which are DES and AES.

1.5 Project Significance

This system is developed for students or lecturers who are learning or teaching subjects related to data encryption. This is because this system can show the results obtained in every round for DES and AES, so they can be more confirmed to their answer. Besides that, they are able to trace back their mistakes easily.

1.6 Expected Output

The system will have interfaces that:

- Allow the user to choose the type of encryption algorithm they want to use.
- Allow user to enter the message (plaintext) and key.
- Display the results in every single round.

1.7 Conclusion

In conclusion, this is a system to encrypt message using either DES algorithm or AES algorithm. It is expected to display the results of every rounds of the process during encryption. The purpose of developing this system is to hope that it is able to serve as teaching or comparison tool. Developing this system is the next activity after this, the programming language chosen to develop this system is Java. Besides that,

literature review and project methodology will be discussed in the following chapters based on the articles and journals found. The next chapter is about the literature review and project methodology which will be discussing about the previous research and the methodology used to develop this system.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

In this chapter, the two main topics on literature review and proposed solution are being discussed. First of all, in the topic of literature review, there are three parts or subtopics which will describe mainly about the issues and topics related to Data Encryption Standard (DES) and Advanced Encryption Standard (AES). The first part is about the domain of this project and the second part is describing some of the keywords related to the project. The last part is about the previous researches done by other researchers. All of them are based on some journals or findings which could be found on websites or reference books. Thus, during doing literature review, it could be an opportunity to read and study deeply about what is data encryption all about.

The second main topic for this chapter is proposed solution. After studying the findings, it is time to analyse them and propose the solutions for this project. Hence, this topic comprises of several subtopics to describe about the methodology being used and the project schedule or milestones. Thus, when doing this chapter, it involves a lot in applying the knowledge for the related subjects such as Software Development, Software Engineering, Project Management and etc.