

BORANG PENGESAHAN STATUS TESIS

JUDUL: ENCHANCING EKO-TECH07 SYSTEM WITH SECURITY DATA
ELEMENT AND CONNECTION VIA HAND PHONE (EKO-
TECH07)

SESI PENGAJIAN: 2006/2007

Saya MUHAMMAD YAAKUB BIN RAMLI
(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 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)


(TANDATANGAN PENYELIA)

Alamat tetap: No. 9-91 (F) Selancar 06,

Pn. Siti Rahayu Selamat

Perwira Jaya, 85070 Segamat, Johor

Nama Penyelia

Tarikh: 5/11/2007

Tarikh: 5/11/2007

CATATAN: * Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)
* Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

**ENHANCING EKO-TECH07 SYSTEM WITH SECURITY DATA
ELEMENT AND CONNECTION VIA HAND PHONE
(EKO-TECH07)**

MUHAMMAD YAAKUB BIN RAMLI

This report is submitted in partial fulfillment of the requirements for the Bachelor of
Information and Communications Technology (Networking)

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

2007

DECLARATION

I hereby declare that this project report entitled
**ENHANCING EKO-TECH07 SYSTEM WITH SECURITY DATA ELEMENT
AND CONNECTION VIA HAND PHONE
(EKO-TECH07)**

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

STUDENT : _____ Date: _____
(MUHAMMAD YAAKUB RAMLI)

SUPERVISOR : _____ Date: _____
(PN. SITI RAHAYU SELAMAT)

DEDICATION

To my beloved parents...

Thanks for giving me a lot of your support,
both of you are my inspiration and encouragement will continue to guide me always.

ACKNOWLEDGEMENT

Assalamualaikum W.B.T

In the name of Allah the Almighty and most Merciful

I would like to praise upon Allah for letting me complete my PSM I project on time and with success. I would like to express my deep personal appreciation to the all individual who has contributed in order this Projek Sarjana Muda 1 (PSM1) whether directly or indirectly.

First of all, I would like to express my greatest gratitude to my supervisor, **Puan Siti Rahayu Selamat**, who had encouraged, directed, and guided me throughout the entire project with much penitence and very supportive. Her supervision had been the key factor for the success of the Projek Sarjana Muda 1 (PSM1). Special acknowledgement and appreciation to my parents, **Ramli Bin Awang** and **Siti Esah Binti Ahmad** and not forgetful to my adored family members for their moral support, full understanding and patience to be completion of this PSM1.

Finally, I wish to thank to my classmate and all friends for their cooperation, comments, advice contribution and support. The competition of this project would not have been successful without support, helps and encouragement from various people. Big thank to my friend, who assisted me throughout the project with their supportive attitude and engorgements.

ABSTRACT

This project is developed to enhance the capability of current system (EKO-TECH05) which was developed in year 2005 and will call as EKO-TECH07. This system is a tourism ticket management system for Malacca. This system is consisting of four main modules, which are registration module, administrator module, booking module and the search module. For each main module, it contains with sub modules i.e. examples information update, ticket booking and payment. EKO-TECH07 is upgraded with the security option for securing the data and running in web-based environment using network connection. Elliptic Curve Cryptography (ECC) is an encryption technique that used to encrypt the data before storing into the database. EKO-TECH07 can be accessed online or using hand phone. This project used prototype methodology to develop EKO-TECH07 because the enhancement is based on the weakness of the current system and the user requirements. The system analysis is done by analyzing the existing EKO-TECH05 system and the one that will be enhanced. As a conclusion, this system will be valuable and can be increase security characteristic for securing the data before stored in database. In this document more information about this project will be detailed.

ABSTRAK

Projek ini adalah merupakan satu projek yang mana meningkatkan keupayaan daripada projek yang sebelumnya. EKO-TECH05 adalah sebuah sistem pengurusan tiket pelancongan bagi negeri Melaka. EKO-TECH05 adalah satu sistem yang dibangunkan dalam tahun 2005 dan dalam projek ini, sistem akan di panggil EKO-TECH07. Di dalam sistem ini terdapat beberapa modul yang tertentu. Antara modul yang terdapat dalam sistem ini ialah modul pendaftaran, modul admin, modul tempahan, dan modul carian. Di dalam setiap modul terdapat beberapa lagi sub-sub modul seperti kemas kini maklumat, tempahan tiket dan pembayaran. Projek ini dijalankan adalah untuk menaik taraf daripada sistem yang sebelumnya. Modul dan elemen yang dipertingkatkan adalah elemen keselamatan bagi keselamatan data dan elemen *network* iaitu menghubungkan dengan *network based* teknologi. Dalam elemen keselamatan data, projek ini adalah menggunakan pendekatan teknik *encryption*. Manakala bagi *network based* teknologi pula, projek ini menggunakan pendekatan *online* sistem dan menghubungkan sistem dengan telefon bimbit. Metodologi pembangunan sistem ialah metodologi prototaip. Ini kerana metodologi yang membenarkan pengguna mencuba prototaip sistem sebelum menggunakan sistem yang sebenar. Pembangunan sistem ini menggunakan teknik SDLC dengan pembangunan dilakukan fasa demi fasa. Analisa sistem telah dilakukan dengan menganalisis sistem sedia ada dan menganalisis modul yang hendak dipertingkatkan. Secara kesimpulannya sistem ini dapat meningkat nilai pada sistem ini di samping dapat meningkatkan ciri-ciri keselamatan bagi data. Di dalam dokumen ini menerangkan projek ini dengan secara terperinci.

TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLE	xi
	LIST OF FIGURES	xiii
	LIST OF ABBREVIATIONS	xv
	LIST OF APPENDIX	xvi
CHAPTER I	INTRODUCTION	
	1.1 Introduction	1
	1.2 Project Background	1
	1.3 Problem statement	3
	1.4 Objective	4
	1.5 Scope	5
	1.6 Project significance	5
	1.7 Expected Output	6

1.8	Conclusion	6
CHAPTER II	LITERATURE REVIEW AND PROJECT METHODOLOGY	
2.1	Introduction	7
2.2	Fact and Findings	8
	2.2.1 Encryption Concept	8
	2.2.2 RSA Encryption Algorithm	9
	2.2.2.1 How Does Work?	
	2.2.3 Data Encryption Standard (DES) Encryption Algorithm	12
	2.2.3.1 How Does Work?	12
	2.2.3.2 Security in DES Algorithm	15
	2.2.3.3 Advantage and Disadvantage of DES Encryption Algorithm	15
	2.2.4 Elliptic Curve Cryptography Algorithm	16
	2.2.4.1 How Does Work?	17
2.3	Project Methodology	21
	2.3.1 Planning	24
	2.3.2 Analysis	24
	2.3.3 Design	25
	2.3.4 Implementation	25
2.4	Project Requirements	25
	2.4.1 Software Requirements	25
	2.4.2 Hardware Requirements	26
	2.4.3 Other Requirements	27
2.5	Project Schedule and Milestones	27
	2.5.1 Project Schedule	28
2.6	Conclusion	29

CHAPTER III	ANALYSIS	
3.1	Introduction	30
3.2	Problem Analysis	31
3.2.1	Existing System Problem Analysis	31
3.2.1.1	Module in Current System	32
3.2.2	New System Problem Analysis	34
3.2.2.1	Implement the Encryption Technique	38
3.3	Requirement Analysis	42
3.3.1	Data Requirement	42
3.3.2	Functional Requirement	45
3.3.2.1	Context Diagram	45
3.3.2.2	Data Flow Diagram Level 0	46
3.3.2.3	Data Flow Diagram Level 1	47
3.3.2.4	Data Flow Diagram Level 2	48
3.3.3	Other Requirement	49
3.3.3.1	Software Requirement	49
3.3.3.2	Hardware Requirement	51
3.3.3.3	Network Requirement	51
3.4	Conclusion	52
CHAPTER IV	DESIGN	
4.1	Introduction	53
4.2	High-Level Design	54
4.2.1	Raw input/data	54
4.2.2	System Architecture	57
4.2.3	User Interface Design	58
4.2.3.1	Navigation Design	63

4.2.3.2	Input Design	64
4.2.3.3	Output Design	67
4.2.4	Database Design	68
4.2.4.1	Entity Relationship Design	68
4.2.4.2	Data Dictionary	69
4.3	Conceptual and Logical Database Design	71
4.3.1	Detail Design	71
4.4	Conclusion	78

CHAPTER V IMPLEMENTATION

5.1	Introduction	74
5.2	Software Development Environment setup	75
5.2.1	Environment Setup	76
5.3	Software Configuration Management	77
5.3.1	Configuration environment setup	78
5.3.1.1	Dynamic Environment	78
5.3.1.2	Static Environment	78
5.3.2	Version Control Procedure	79
5.4	Implementation Status	80
5.5	Implementation ECC Algorithm	81
5.5.1	Encryption Data	81
5.5.1.2	Encryption	81
5.5.2	Decrypt Data	83
5.5.2.1	Decryption	84
5.5.2.2	Conversion of the Encryption String to the Decryption Key	84
5.6	Implementation in the module	85
5.6.1	User Registration Module	85
5.6.2	Log-in Module	88

5.6.3	Ticket Reservation Module	90
5.6.4	Payment Reservation Module	92
5.6.5	Admin Log-in Module	94
5.7	Conclusion	96

CHAPTER VI TESTING

6.1	Introduction	97
6.2	Test Plan	98
6.2.1	Test Organization	98
6.2.2	Test Environment	99
6.2.2.1	Overview	99
6.2.2.2	Hardware	99
6.2.2.3	Software	100
6.2.3	Test Schedule	100
6.3	Test Strategy	101
6.3.1	Classes of tests.	102
6.4	Test Design	105
6.4.1	Test Description	105
6.4.2	Test Data	111
6.5	Test Results and Analysis	113
6.5.1	Test Result for User Registration Module	113
6.5.2	Test Result for Login Module	115
6.5.3	Test Result for User Change Password Module	117
6.5.4	Test Result for Admin Log-in Module	118
6.5.5	Test Result for Ticket Reservation Module	120
6.5.6	Test Result for Payment Reservation Module	121
6.5.7	Test Result for Forum Module	124

6.5.8	Test Result for Pool Module	126
6.6	Conclusion	128
CHAPTER VII	PROJECT CONCLUSION	
7.1	Observation on Weakness and Strengths	129
7.1.1	System Strengths	130
7.1.2	System Weakness	130
7.2	Propositions for Improvements	131
7.3	Conclusion	131
	REFERANCE	132
	APPENDIX A	133
	APPENDIX B	134

LIST OF TABLES

TABLE	TITLE	PAGE
2.1	NIST Recommended Key Sizes	19
2.2	Relative Computation Costs DES and ECC	20
2.3	Activity and Project Deliverables for PSM I	28
3.1	Elliptic Curve Cryptography Algorithm Key Sizes	40
3.2	Details information for tourist (Table Name: Tourist Information)	42
3.3	Details Information for the Reservation (Table Name: Reservation Information)	43
3.4	Details Information for the Admin (Table Name: Admin Information)	43
3.5	Detail Information for the Credit Card (Table Name: Card Credit Information)	43
3.6	Details Information for the Destination/Location (Table Name: Destination Information)	44
4.1	Basic User Registration	54
4.2	User Login Information	55
4.3	Log-in System	55
4.4	Ticket Reservation	56

4.5	Credit Card Payment Ticket Reservation	56
4.6	Registration Module Form	64
4.7	Log-in System Module Form	65
4.8	Ticket Reservation Module Form	65
4.9	Credit Card Payment Module Form	66
4.10	Output Design	67
4.11	TOURIST Table Description	69
4.12	TICKET_RESRERVATION Table Description	70
4.13	VERIFY_RESRERVATION Table Description	70
4.14	ADMIN Table Description	70
4.15	CREDIT_CARD Table Description	71
4.16	DESTINATION Table Description	71
4.17	Description of Data Flow Diagram: Registration Module	73
4.18	Description of Data Flow Diagram: Log-in Module	75
4.19	Description of Data Flow Diagram: Payment Module	77
5.1	Database EKO-TECH07	76
5.2	Computer Requirement	76
5.3	Internet Browser Requirement	76
5.4	EKO-TECH Version	79
5.5	Implementation Status of Modules	80
6.1	Test Schedule	100
6.2	Test Description	105
6.3	EKO-TECH07 Interface unit testing	108
6.6	User Acceptance Unit Testing	111
6.7	EKO-TECH07 Test Data	112
6.8	Module 1 Test Case Result	113
6.9	Module 2 Test Case Result	115
6.10	Module 3 Test Case Result	117
6.11	Module 4 Test Case Result	118
6.12	Module 5 Test Case Result	120
6.13	Module 6 Test Case Result	121
6.14	Module 6 Test Case Result	124
6.15	Module 6 Test Case Result	126

LIST OF FIGURES

FIGURE	TITLE	PAGE
2.1	Structure Design of DES	13
2.2	DES Round Function	14
2.3	Evolutionary Prototyping	23
3. 1	Basic Flow the Current System EKO-TECH05	31
3.2	Flow the Existing EKO-TECH05: Registration Module	32
3.3	Example Data in the Database is Not Secure	33
3.4	Flow Data in Registration Module with Elliptic Curve Cryptography Algorithm	35
3.5	Flow Data Log-in Module with Elliptic Curve Cryptography Algorithm	36
3.6	Example Encryption Data for Securing the Data	37
3.7	Context Diagram	45
3.8	Data Flow Diagram Level 0	46
3.9	Data Flow Diagram Level 1 (Reservation)	47
3.10	Flow Data (Payment Process) Elliptic Curve Cryptography Algorithm	48
4.1	Client Server Architecture	57
4.2	Detail System Architecture	58
4.3	Registration Module Interface	59
4.4	Login Module Interface	60

4.5	Ticket Reservation Module Interface	61
4.6	Credit Card Payment Module Interface	62
4.7	EKO-TECH07 Navigation Design	63
4.8	Entity Relationship Diagram (ERD)	68
4.9	Data Flow Diagram: Registration Module	72
4.10	Data Flow Diagram: Log-in Module	74
4.11	Data Flow Diagram: Payment Module	76
5.1	Software Development Environment Setup for EKO-TECH07	75
5.2	Flow Description for Encryption Data	81
5.3	Encryption Data Process	82
5.4	Flow Description for Decrypt Data	83
5.5	Decrypt Data Process	84
5.6	User Registration Module	85
5.7	User Registration Module (Log-in Information)	85
5.8	User Registration Module (Registration Conformation)	87
5.9	User Registration Module (Saved in Database)	87
5.10	Log-in Module	88
5.11	Log-in Module (Member Page)	89
5.12	Log-in Module (Log-in Error)	89
5.13	Ticket Reservation Module	90
5.14	Ticket Reservation Module (Saved in Database)	91
5.15	Payment Reservation Module	92
5.16	Payment Reservation Module (Payment Conformation)	93
5.17	Payment Reservation Module (Saved in Database)	93
5.18	Admin Log-in Module	94
5.19	Admin Log-in Module (Admin Page)	95
5.20	Admin Log-in Module (Log-in Error)	95
6.1	User Registration Module	108
6.2	User Log-in Module	108
6.3	Ticket Reservation Module	109
6.4	Payment Reservation Module	109
6.5	Admin Log-in Module	109

6.6	Forum Module	110
6.6	Send Forum	110
6.7	Pool Module	110
6.8	Duplicate Username	114
6.9	Database	114
6.10	Validation Function	114
6.11	Validation Function	114
6.12	Login Error	116
6.13	Login Form	116
6.14	Change Password Form	117
6.15	Validation Function	117
6.16	Admin Log-in Form	119
6.17	Log-in Error	119
6.18	Ticket Reservation Form	120
6.19	Validation Function	120
6.20	Payment Reservation Form	122
6.21	Database	122
6.22	Validation Function	122
6.23	Ticket Print	122
6.24	Forum Module	124
6.25	Forum Main Page	124
6.25	Send Forum	125
6.26	Pool Function	127
6.27	Pool Result	127

LIST OF ABBREVIATIONS

UTeM	Universiti Teknikal Kebangsaan Malaysia
EKO-TECH	Sistem Pengurusan Tiket Pelancongan Negeri Melaka
RSA	RSA Encryption Algorithm
DES	Data Encryption Standards
ECC	Elliptic Curve Cryptography Algorithm
SDLC	Software Development Life Cycle
DFD	Data Flow Diagram
IFP	Integer factorization problem
DLP	Discrete logarithm problem
DSA	Digital Signature Algorithm
ECDLP	Elliptic curve discrete logarithm problem
AES	Advance Encryption Standard
NIST	National Institute of Standards and Technology
PHP	Hypertext Preprocessor
PK	Primary Key
FK	Foreign Key

LIST OF APPENDIX

ATTACHMENT	TITLE	PAGE
APPENDIX A	EKO-TECH07 Gantt Chart	133
APPENDIX B	User Manual EKO-TECH	134

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter explain briefly all the processes in existing EKO-TECH05 system. The developer must recognize the problem of the current system by doing some study. Then the developer can state the objectives of the system which are solution of the system scope like user, modules and functions of this system which explain categories of user and modules that will be identified. Generally, the developer must identify the project significance to the end users and the area of study and the expected output as conclusion.

1.2 Project Background

Computer networking is one of the major fields in the world of Information Technology (IT). Not only that it provides connectivity to wired network, it also

connects users all over the world wirelessly with all the latest technology evolving. Among the devices used to connect between networks are routers, switches and hubs.

In this project, an enhancement system will be developed known as web based technology security system and view with latest connection. EKO-TECH05 is one project for the tourism at Malacca, when EKO-TECH05 is a *Sistem Pengurusan Tiket Pelancongan Negeri Melaka* project. EKO-TECH05 has a ticket reservation module for tourism, beside than this reservation payment is using credit card.

EKO-TECH05 is not providing the security element for securing their data. Because on this EKO-TECH05 created it's just developing a one web based basic project requirement. During analysis done on the EKO-TECH05, system like *Pengurusan Tiket Pelancongan Negeri Melaka* it found that the security is mostly important. For example in the transaction module and login module, the data is important to be secure.

In this project, EKO-TECH05 will be enhanced or upgraded with the data information security and network based technology and EKO-TECH05 will be called EKO-TECH07. This improvement is an encryption data for the secret and confidential data to make sure the data storing in the data base is perfectly safe. For network based technology in this system is a user can online access using the internet connection. Beside that, user also can access with their hand phone with 3G/WAP/GPRS technology. In this case EKO-TECH07 is easier to access every where every time.

1.3 Problem statement

Today, all business activities have using the computer; mostly system in Malaysia has using the computer system. It so many aspect to repair-it in the online system or web based technology beside the normal characteristic for the web based. With the current method, in the EKO-TECH05 system now, two problems arise:

- 1. EKO-TECH05 now is not secure because secret data like password and credit card pin number is not encrypted.**

Basically in the web based system, the data like password, the secret information, has been store in the system database can be viewed or known for the system admin. The system admin also a human being and cannot be 100% to hold the secret information. The secret information like be an account number, pin number, and also username and password to login the system.

- 2. EKO-TECH05 now is running standalone system.**

Beside that, online technology is widespread in Malaysia. Today the latest connection is using internet and wireless connection, i.e. using their hand phone like 3G, WAP, and GPRS. Therefore, this system need for upgrading into network environment, user friendly and easy to access anywhere anytime.

1.4 Objective

The objectives of this project are:

- i. To enhance EKO-TECH05 system and come out as an EKO-TECH07. EKO-TECH07 will be enhanced with the security data option and using the network based technology, like internet connection and wireless connection.
- ii. To integrate the EKO-TECH07 into network based technology. In this project, EKO-TECH07 has a running in the network environment. i.e. internet connection and wireless connection.
- iii. To implement the encryption algorithm for securing data in the database. In this project EKO-TECH07 is provide the security option for securing the data with the encryption technique.