BORANG PENGESAHAN STATUS TESIS*

JUDUL: Data Transmission Secrecy Via AES System (AES)

SESI PENGAJIAN: 2008/2009

Saya Rebecca Lourdes

(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: ____________________

____

____

Tarikh: ____________________

(TANDATANGAN PENYELIA)

MOHAMAD RADZI BIN MOTSID
Pensyarah
Fakulti Teknologi Maklumat dan Komuni
Universiti Teknikal Malaysia Melaka (UT

Nama Penyelia

Tarikh: 12/7/09

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

DATA TRANSMISSION SECRECY VIA AES SYSTEM (DTS)

REBECCA A/P LOURDES

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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2009

DECLARATION

I hereby declare that this project report entitled

DATA TRANSMISSION SECRECY VIA AES SYSTEM (DTS)

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

STUDENT :________________________________ DATE: _____________

(REBECCA D/O LOURDES)

SUPERVISOR:________________________________ DATE: 10/7/09.

(MR. MOHAMMAD RADZI BIN MOTSIDI)

DEDICATION

To my beloved parents, Lourdes Pius Francis and Rajeswary David for their seems less expressions and love and fully support….

To my supervisor, Mr. Mohammad Radzi bin Motsidi, for making it all worthwhile…

ACKNOWLEDGEMENTS

I as a project developer for this software system would like to convey my gratitude to almighty God in giving me strength and courage in completing my PSM. The credit also goes to my beloved parent Lourdes Pius Francis and Rajeswary David, my fiancée Vicknes Ratha Krishnan, my siblings, Theresa Lourdes, Boy and Bethoven and my friends Clva hansneary Clvakumaran, Chitradevi Egamulum, Sharmini Mohan, Geetha Nagendran. Kasthuri Sivarajoo and Krystle Arakasamy, for giving me moral support and guided me in some problems during developing phases.

I also would like to thank my supervisor Mr. Mohammad Radzi bin Motsidi and for giving full support and encouragement for me to develop this project successfully. My thanks also go to Mrs. Marliza Ramli, my panel whom commented on my weaknesses and made me repair my mistakes.

Last but not least, special thanks for Mr. Mohd Sanusi bin Azmi whom also guided me in my needy times and solved most of my curiosity.

ABSTRACT

This paper presents a system on the framework of a computational system with LAN architecture which applies client server application. This system will be able to generate cryptography keys and exchange them between client and server in secure way. So by using cryptography technique, user will be able to transfer their username and password entered in E-Faculty webpage to database securely. This system uses Java as programming language. The targeted user for this system is UTeM staffs.

ABSTRAK

Sistem ini mengunakan aplikasi “client server” di mana pertukaran data berlaku d anatara “client server”. Untuk system, prototype yang dipilih ialah E-Faculty dimana penghantaran “username” dan “password” dihantar dari laman web ke database untuk tujuan validasi.Oleh yang itu, teknik “cryptography” digunak untuk menghantar maklumat dengan selamat.Sistem ini adalah sistem untuk pertukaran kunci “cryptography” untuk menghantar maklumat sulit di dalam sesuatu rangkaian.

TABLE OF CONTENTS

CHAPTER	SUBJECT		PAGE
	ACKNOWLEDGEMENTS		iii
	ABSTRACT		iv
	ABSTRAK		v
	TABLE OF CONTENTS		vi
	LIST OF TABLES		x
	LIST OF FIGURES		xii
	LIST OF ATTACHMENTS		xiv
CHAPTER I	INTRODUCTION		1
	1.1	Project Background	1
	1.2	Problem Statements	2
	1.3	Objective	3
	1.4	Scope	4
	1.5	Project Significance	6
	1.6	Expected Output	7
	1.7	Conclusion	7
CHAPTER II	LITERATURE REVIEW AND PROJECT METHODOLOGY		8
	2.1	Introduction	8

2.2 Literature Review 9

2.2.1 Domain 9

2.2.2 Keyword 10

2.2.3 Previous Research 14

2.2.3.1 Methodologies 14

2.2.3.2 Comparison of Methodologies 16

2.2.3.3 Techniques 17

2.2.3.4 Software Requirements 18

2.2.3.5 Hardware Requirements 18

2.2.3.6 Network Requirements 18

2.3 Proposed Solution 19

2.3.1 Project Methodology 19

2.3.1.1 Evaluation and Maintenance Phase 22

2.4 Project Schedule and Milestones 23

2.5 Conclusion 24

CHAPTER III ANALYSIS 25

3.1 Introduction 25

3.2 Problem Analysis 26

3.2.1 Current Scenario 30

3.3 Requirement Analysis 33

3.3.1 Data Requirement 33

3.3.2 Functional Requirement 34

3.3.2.1 Server 38

3.3.2.2 Client 42

3.3.3 Non-functional Requirement 44

3.3.4 Other Requirements 44

3.4 Conclusion 47

CHAPTER IV DESIGN 48

4.1 Introduction 48

4.2 High- Level Design 49

4.2.1 System Architecture 49

4.2.2 User Interface Design 51

4.2.2.1 Navigation Design 53

4.2.2.2 Input Design 56

4.2.2.3 Output Design 56

4.2.3 Database Design 58

4.2.3.1 Conceptual and Logistic Database Design 59

4.3 Detailed Design 62

4.3.1 Software Design 62

4.3.1.1 Data Store 71

4.3.2 Physical Database Design 73

4.3.2.1 Data Definition Language (DDL) 73

4.3.2.2Data Manipulation Language (DML)73

4.4 Conclusion 74

CHAPTER V IMPLEMENTATION 75

5.1 Introduction 75

5.2 Software Development Environment Setup 76

5.3 Software Configuration Management 78

5.3.1 Configuration Environment Setup 78

5.3.2 Setup and Configuration Step 79

5.3.3 Version Control Procedures 80

5.4 Implementation 81

5.5 Conclusion 83

CHAPTER V TESTING 84

6.1 Introduction 84

6.2 Test Plan 85

6.2.1 Test Organization 85

6.2.2 Test Environment 87

6.2.3 Test Schedule 87

6.3 Test Strategy 88

6.3.1 Classes Of Test 89

6.4 Test Design 92

6.4.1 Test Description 92

6.4.2 Test Data 96

6.5 Test Results And Analysis 97

6.6 Conclusion 102

CHAPTER V PROJECT CONCLUSION 103

7.1 Observation on Weaknesses and Strength 103

7.1.1 Strengths 104

7.1.2 Weaknesses 104

7.2Propositions for Improvement 105

7.3 Contribution 105

7.3.1 User Manual 106

7.4 Conclusion 106

REFERENCES 108

APPENDIXES 109

LIST OF TABLES

TABLE	TITLE	PAGE
2.1	Comparison between Existing Systems	16
2.2	Project Milestone	23
3.1	Data Requirement for Table Login	33
3.2	Data Requirement for Table AES	33
3.3	Data Requirement for Table RSA	34
3.4	Specification of computer device	47
4.1	Data Dictionary of DTS System	61
5.1	Implementation Status	81
6.0	Categories of user	86
6.1	Test Facilities Component	87
6.2	Test Schedule	88
6.3	Test Cases for Login Module	93
6.4	Test Cases for generating RSA keys Module	93
6.5	Test Cases for generating AES keys Module	94
6.6	Test Cases for Transferring Files Module	94
6.7	Test Cases for Read from file and write into file Module	94
6.8	Test Cases for Encryption and Decryption using RSA algorithm Module	95
6.9	Test Cases for Encryption and Decryption using AES algorithm Module	95

6.10 Test Data for Username and Password in Login Module 96
6.11 Test Case Result for Login Module 97
6.12 Test Case Result for generating RSA keys Module 98
6.13 Test Case Result for generating AES keys Module 98
6.14 Test Case Result for Transferring Files Module 99
6.15 Test Case Result for Read from file and write into file Module 100
6.16 Test Case Result for Encryption and Decryption using RSA algorithm Module 100
6.17 Test Case Result for Encryption and Decryption using AES algorithm Module 101

LIST OF FIGURES

DIAGRAM	TITLE	PAGE
2.0	History of cryptography	11
2.1	Example of confidentiality violation	13
2.2	SE-6600R Serial Data Encrypter	15
2.3	Object-Oriented Development Life Cycle	20
3.0	E-Faculty Webpage	27
3.1	Packet captured through Wireshark	28
3.2	Use Case Diagram of Password Based Authentication	31
3.3	Sequence diagram of Password based Authentication	32
3.4	Use Case Diagram of Generating and Exchanging Cryptographic keys	35
3.5	Use Case Diagram of User's Login	36
3.6	Sequence Diagram of new E-Faculty after DTS implementation	37
3.7	Flow chart of Generating Public and Private Key	39
3.8	Flow Chart to send PublicKey.key	40
3.9	Flow Chart of Receiving and Decrypting an Encrypted Secret Key	41
3.10	Flow Chart of Generating Secret Key	42
3.11	Flow Chart of Receiving Public Key and Encrypting the Secret Key	43
4.0	The Architecture of DTS system	51
4.1	User Interface	51
4.2	Alert Message of Successful Login	52
4.3	Alert Message of Unsuccessful Login	53
4.4	Navigation flow of Visible DTS system	54

4.5 Navigation Flow of Behind of DTS system 55
4.6 Login interface 57
4.7 Interface when User key in data 57
4.8 Alert Message of Successful Login 58
4.9 Alert Message of Unsuccessful Login 58
4.10 ERD model for DTS system 59
4.11 Third Normal Form for Table Login 62
5.1 Architecture of DTS 76
5.2 Detailed Architecture of DTS 77

LIST OF ATTACHMENTS

ATTACHMENT	TITLE	PAGE
A	Log Book	109
B	Proposal	110
C	Gantt Chart	118
D	User Manual	125

CHAPTER I

INTRODUCTION

1.1 Project Background

Year 2009 entertain us in the warmest way as we have just step into its entrance path. 52 years we have been independently building up an extreme growth in the technology where it really helps to build thegood name of our country among bunches of competing country all over the world. Yet, it has to be sad climax if we could scratch out the growth of forgery cases. Forgery is touching its ultimatum level where it is found in many department and aspects andstealing the secret of a confidential data has been one of it. There is no more perfect reliance for a server to ensure the data sent is only viewed by the respected party he intended. This gala has to be snub but is there a perfect way to do it? On protecting the data, there is a perfect method to do which is merely known as encryption.

Although moral values and good working etiquettes are taught to all human beings especially in a field that concerns in securing and respects others private data, not many implements that. During data communications in one or more network, data hacking and stealing is very common and growing bigger as the intruders are hunger for money and fame. So, network security is becoming vital especially for firms and companies that concerns data security during data transmission. Therefore, when transmitting a data from one network to another or from one computer to another, security plays a major role. Hence, this project uses cryptography method when transmitting a data from a client to server in order to save the data from trespassers.

Encryption is the process of using cryptography. Cryptography uses mathematical algorithms to translate data into a clear unreadable format that can only be efficiently deciphered with a specific cryptographic key or inverse algorithm process. Hence, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people.**Decryption** is the process of converting encrypted data back into its original form as it can be understood.

This project will apply cryptography technique into unsecure E-Faculty website that have been used for meeting room and lab booking in Faculty of Infrastructure and Communication Technology (FTMK), University of Technical Malaysia Melaka (UTeM).

1.2 Problem Statement

E-Faculty is a web application for laboratory and meeting room booking in the FTMK, UTeM. The application has been used for several years. The major problem of this application is the process of booking is unsecured where the username and password are transferred from client to server inplain text. This username and password is readable by whoever that are connected in the same network. So, the E-Faculty needs a application that can secure the transmission of username and password.

1.3 Objectives

The objectives of this proposed system are;

- **To apply cryptography technique in prototype applications.**

  Generate keys to be used in prototype applications is to do the encryption and decryption process since it is using the AES standard. There are 3 keys generated in this system, Shared Key or Seaet Key which is generated by using AES algorithm, Public Key and Private Key which are generated using RSA algorithm. Shared key generated in client group whereas public and private key generated in server.

- **To integrate key generator into prototype of dient server application.**

  The AES key is generated in client while the RSA key is generated in server. The AES key generated is based on 128bits key whereas the RSA key is generated based on 1024-bits key.

- **Apply secure key exchange**

  The Shared Key genemted using AES standard that will be used for communication between client and server. The Shared key will be transmitted using Public Key encryption generated using RSA standard. AES using the asymmetric encryption therefore only one key the Shared Key ca be used for both the encryption and decryption. Therefore key exchange is important because only server can generate the key to encrypt and decrypt which is the public key and private key.

- **To apply a prototype of secure client server application.**

  The generated shared key is encrypted by the public key generated by the server and it is transfer through the LAN cable but unable to read by others. The encrypted shared key is then received by the server and it is decrypted to view the original data by theprivate key generate by server.

1.4 Scope

- **Prototype**

  The prototype that is chosen for Data Transmission Secrecy via AES System (DTS) is E-Faculty system which is used for lab and meeting room booking. The system requires username and password from the autborized user. Then the username and password is sent through the LAN network to the database server. When it reaches the database server, the username and password will be validated. After the validation, the user can use the system to book the lab or meetig room. When they booked the lab or meeting room, any of the authorized party such as Registrar or officer can grant their request.

- **Technique**

  Technique that is used in DTS system is cryptography technique. All the username and password is transferred through the LAN network. So, before the data are transmitted, the username and password are encrypted and sent to server. After reaching server, the username and password will be decrypted back. By this the connection will be secure from hands of hackers

- **Platform**

  The platform that is used to apply for cryptography is by using Java as the programming language. Java source code will be used to encrypt and decrypt the data that is transmitted through the connection. As Java Standard Edition provide the platform specifically for security features, it will be easier to generate keys, encrypt and decrypt the data according to certain standards.

- **Standard**

  Standard that is chosen to work the system's cryptography are two standards and they are Advanced EncryptionStandard (AES) and RSA algorithm. An algorithm called Rijndael was developed by Joan Daemon and Vincent Rijmen is accepted to be used for AES cryptography. AES is based on 128-bit blocks with 128-bit keys. AES uses symmetric key to encrypt and also decrypt. The another standard that is applied in this system is RSA algorithm which uses 1024 bits and applies asymmetric keys for encryption and decryption. The asymmetric keys are known as Public key and Private key.

- **Process**

  Overall process involves both Server and Client to generate keys. Server will generate asymmetric keys; Public and Private Key whereas, client will generate Secret key. First, the server will send Public key to client. Client will use the Public key to encrypt the secret key. Then, the encypted secret key will be sent to server which it will be decrypted back again into original secret key using Private Key.

  When any authorized user sign in to the elab booking system, the user's username and password will be sent through the connection. So before the username and passwords are sent through the connection, the data will be encrypted using secret key in client. After that, it will be transmitted through the connection and when it reaches server, the server will decrypt back the data using secret key that was decrypted in server previously. Finally the user will be authenticated and allowed to use the system freely.

- **User**

  The type of authenticated user in DTS system is FTMK lecturers and other staff like technicians who have the authority tobook the lab. Students are not allowed use this system as this system only for those who can book lab.

1.5 Project Significance

The significance of this project towards the society is their personal particulars are no longer on threat. Threat, in this context means, their password cannot not be seen and used by others. This simply means, it is purely secure and confidential.

The approach of using Advanced Encryption Standard (AES) compare to Data Encryption Standard (DES), is much more better and significance because the use of 56-bit key and 64-bit blocks is no longer consider safe against attacks based on exhaustive key search. The latest standard of AES is based on 128-bit blocks with 128-bit keys.

1.6 Expected Output

As what has been planned and deoided on planning phase, the system would be Java base application and be more user friendly with GUI design. The system should be able to encrypt data before sending and will be used to authenticate user by decrypting it in the server side. Both this encryption and decryption process comes out with a symmetric key and asymmetric concept combination where a Public Key, Private Key and Shared Key will be produced. The Public and Private Key will be generated in server side while the Shared Key will be generatd in client side.

1.7 Conclusion

The cryptography method used in the EFaculty lab booking system, expected to be useful to the user to encrypt and decrypt the users' password with the symmetric and asymmetric key concept combination. Data Transmission Serecy via AES System (DTS) will produce the secure environment for the users to enter their password peacefully as it will not be hacked by any intruder.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

In developing any new project, the initial step that a programmer should take, is doing researches and study so that he or she can identify information, ideas and methods that relevant to his or her project. By this theoretical base for research, one can determine the nature of his or her project. According to Sharmini d/o Mohan (2007), *Software System for Mould Manufacturing purposes with Mobile Technology*, to develop a new project, the research are very important because all the information from the research about the project is used as a guideline to develop a new project and execute it successfully.

This chapter discusses and studies on Literature Review and Methodology about the E-Faculty user's encrypted username and password transmission across the wired medium from one node to another in one network.For this project, the research will be done by reference to books, articles, online journals about the existing systems that are