HYBRID ENCRYPTION FOR DIGITAL SIGNATURE

NAVINDRAN A/L SUBRAMANIAM

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS*

JUDUL : HYBRID ENCRYPTION FOR DIGITAL SIGNATURE

SESI PENGAJIAN : 2013 / 2014

Saya NAVINDRAN A/L SUBRAMANIAM

mengaku membenarkan tesis Projek Sarjana Muda 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)	(TANDATANGAN PENYELIA)
Alamat tetap: No 30 Jalan 2/14,	Dr. Zul Azri Muhamad Noh
	Nama Penyelia
Taman Bukit Rawang Jaya,,	
48000, Rawang, Selangor.	
Tarikh _____	Tarikh: _____

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

HYBRID ENCRYPTION FOR DIGITAL SIGNATURE

NAVINDRAN A/L SUBRAMANIAM

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
2014

DECLARATION

I hereby declare that this project report entitled

HYBRID ENCRYPTION FOR DIGITAL SIGNATURE

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

STUDENT :_____ Date :_____

(NAVINDRAN A/L SUBRAMANIAM)

SUPERVISOR :_____Date :_____

(DR ZUL AZRI MUHAMA NOH)

DEDICATION

A special feeling of gratitude to my beloved parents, siblings, friends who have encouraged, guided and inspired me throughout my journey of education. I also dedicate this dissertation to my supervisor who have supported me throughout the process. I will always appreciate all they have done. All of you have been my best supporters.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank to my supervisor of this project, Dr. Zul Azri Muhamad Noh for the valuable guidance and advice. He inspired me greatly to work in this project. His willingness to motivate me contributed tremendously to my project. I also would like to thank his for showing me some example that related to the topic of my project.

Grateful appreciation is also extended to the lecturers of Faculty of Information & Communication Technology University Technical Malaysia, Melaka for their support and providing me with a good environment and facilities to complete this project. Understanding and cooperation given by them are countless and valuable for me.

Finally, an honorable mention goes to my families and friends for their understandings and supports on me in completing this project. Without helps of the particular that mentioned above, I would face many difficulties while doing this project. Last but not least, thank you once again and may god bless all of us and thank you, for always being there for me. This is only a beginning of my journey.

ABSTRACT

The Hybrid Encryption For Digital Signature is developed to be used by users who use the Digital Signature as to authenticate the electronic document. Digital signature is used to authenticate the electronic document. However, it does not guarantee confidentiality. The Hybrid Encryption For Digital Signature is developed to provide confidentiality to the electronic document. The advantage of using this system is that, it provides an extra layer of security to the electronic document, by encrypting it before sending via email. The receiver on the other hand, decrypts the document, and is able to read the file. Furthermore, the system is developed using the combination of RSA and AES algorithm, making in more secure. Hackers will find it very hard to decrypt the document and it will take years to be cracked. In a nutshell, the Hybrid Encryption For Digital Signature helps users to protect their valuable documentation and data from hackers.

ABSTRAK

Hybrid Encryption for Digital Signature dibangunkan untuk digunakan oleh pengguna yang menggunakan Digital Signature untuk mengesahkan dokumen elektronik seperti e-mel. Digital Signature digunakan untuk mengesahkan dokumen elektronik. Walau bagaimanapun, ini tidak menjamin kesulitan dokumen tersebut. Hybrid Encryption for Digital Signature dibangunkan untuk menyediakan sulitan dokumen elektronik tersebut. Kelebihan menggunakan sistem ini ialah, ini menyediakan lapisan tambahan keselamatan kepada dokumen elektronik dengan menyulitkan sebelum menghantar melalui e-mel. Penerima pula sisi, decrypts dokumen itu, dan mampu untuk membaca fail. Selain daripada itu, sistem ini dibangunkan dengan menggunakan gabungan RSA dan algoritma AES, menjadikannya lebih selamat. Penggodam akan merasa sangat sukar untuk menggodam dokumen itu dan ia akan mengambil masa untuk memecahkannya. Secara ringkas, Hybrid Encryption for Digital Signature membantu pengguna untuk melindungi dokumen dan data berharga mereka daripada penggodam.

TABLE OF CONTENTS

Chapter 2

Chapter 3

Chapter 5

Chapter 6

Chapter 7

LIST OF TABLE

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Project Background

Internet, as we know it does bring us with a lot of advantages to human in many ways. It's a network that have few millions of network such as private network, public network or a specialized government network that either linked with wireless technology or cable technology such as fiber optic. The internet has become a middle-man to communicate between users. The amount of data that we can transfer throughout the internet is enormous and that does include wherever the person is, they can send or receive multiple data across the internet service. The internet provide a large range of data information and service such as Hypertext Transfer Protocol (HTTP) and a protected one Hypertext Transfer Protocol Secured (HTTPS) to become one part of medium to send and receive an email and in sum of foregoing, it has created a lot of security drawbacks.

In the modern world, transmission of data between two or more parties are becoming essential in their daily life. Whether it's for private and personal messages or for business resolutions, data and information need to be transferred between them. Information data and few attachment sometimes can be transferred using Electronic mail (Email) where in this period of time age, everyone is using email from big profile company, enterprises , lawyers and to a normal shop lots where they use email to communicate with their vendors, customer and colleague co-worker. Information such as receipt, financial statement, reports, case-statement, invoices and transaction files are attached to email will be transferred across the internet. Complication throughout this services is that it will create few drawbacks. First of all, communication/interaction between two users are not confidential through the internet where there are quite number of software developer develop to sniff packet to obtain information such as system password or a document password or for monitoring purpose. These software or tools are used to capture used by hackers on a network to obtain confidential data and attachment, hence making this tool breaking the confidentiality, integrity, and authentication are exposed. In multilevel business trade, information that is being transferred should be classified and need to be protected and keep it out from being captured or reached out from the hackers that might be hired from the competitor side or disgruntled public people. If one of the data or attachments leaked out, the outcome of it might be nasty in view of financial lost, contact lost, or system failure without knowing why. Therefore, it is important to secure the classified file or attachments from hackers or anyone that is trying to obtain the information.

Digital signature is used to verify the receiver that the sender are sending the file to the receiver, not someone who try to impersonate and modify the data. A digital certificate that is valid will give the receiver a trust that the message is sent by the sender which is authenticated by the sender. This service always being used in financial transaction to avoid data tampering or forgery in the information of the file. The message will electrically send and receive to verify the signature by the digital signature. It does provide verification and reliability but it does not give data privacy used for the

message (Forouzan, 2008). Both sender and receiver won't notice that the message is intercepted and hacker can read and modify the content and yet hackers also can eavesdropping to listen and obtain the information of the message. This is dangerous because originally the message was verified by the user using the digital signature and the content that has been modify will give the idea to the receiver that the sender send this message which can be a ruckus. Content confidentiality still remain questioned. Hence, a cryptography should be applied to digital signature so that the content or the information of the message is encrypted and to ensure confidentiality of the content.

By proposing this project, the system will able to give confidentiality of the information for the receiver. The system should be giving security over the internet protected by the digital signature.

1.2 Problem Statement

Quite numbers of drawbacks are found in current system. In normal situation, digital signature does not provide any data confidentiality. User are incapable of sending or receiving a message without knowing that the content of the data is being captured and the information are being stolen. In addition, the hacker can easily detect data using software that are specialized in sniffing to monitor the network. Since most of the user face a problem to encrypt a data because to do so it might take time, hence a cryptography system can be applied to protect the message using cryptography.

1.3 Objective

The objectives of this system are:

1. To design a system that can encrypt and decrypt documents.
2. To develop a system that can do hybrid encryption
3. To provide data confidentiality in digital signature

1.4 Scope

Scopes of the system are the skills how the information will be installed by the developer where this project will allow user to encrypt and decrypt an information using a passcode generated by the sender themselves. The main purpose is to protect the file that is sent and received using the digital signature.

It must be able to encrypt and decrypt all kind of files that have a software that can be associates with to open the file.

The role is to:

1. Encrypt and decrypt all types of file and information
2. Provide confidentiality; by using Rivest-Shamir-Adleman (RSA) and Advance Encryption Standard (AES), this function will be enabled.

1.5 Project Significance

The advantages of this system is that it provide data confidentiality against hackers which it will bring benefit to both sender and receiver that sending and receiving classified information. The sender want the file that they verified to reach safely to the destination. The other hand, receiver wants a data or attachment that not being altered by irresponsible personnel that. It's a win-win situation for both sender and receiver.

1.6 Expected Output

The expected output of this system is, the sender will send a classified information or attachments throughout the email using the cryptosystem where the system will encapsulate the file with 3 layers of security where the first layer will be the AES encryption, next the encrypted file of AES will be forwarded to be encrypt with RSA encryption and finally it will be attached with Secure Hash Algorithm (SHA-2)

passcode where the sender have to keyed in the 16 codes where the receiver will enter the same passcode that the sender keyed in. This system will be a benefit for both user if hacker tried to hack, it will take time for them to reverse the algorithm encrypted to obtain the data.

1.7 Conclusion

At the finishing point of this project, this system will eventually help user to protect their information from being reached out by unintended user. This project can be used in home or office where the user only needed their laptop or pc which the software is being installed. This project does help in adapting the process of how cryptography works to protect information from hackers. In next chapter, the content will be discussed is literature review about project and information collected from facts or articles.