A SECURE MESSAGE HANDLER USING MICROSOFT CRYPTOAPI

CHESSDA UTTRAPHAN A/L EH KAN

This thesis is submitted as a fulfillment of the
requirements for the award of the degree of Master in
Electrical Engineering

Faculty of Engineering
Kolej Universiti Teknologi Tun Hussein Onn

NOVEMBER, 2003

To my family who love me, especially to my parents for education
they gave me, their support and understanding

ACKNOWLEDGEMENT

I would like to thank my supervisor, Associate Professor Dr. Zainal Alam Bin Haron for his guide and his encouragement during this master project. I'm also would like to thanks Associate Professor Dr. Mohd Nor Bin Mohd Than and Mr. Awtar Singh A/L Karnail Singh for the advice they gave in completing this project.

ABSTRACT

In this project, a message handler with security features is developed using Microsoft CryptoAPI. The source code is written in Visual Basic to take advantage of the extensive graphical features of the language. A Visual Basic module called clsCryptoAPI was developed to make calls to the advapi32.dll where the functions for the CryptoAPI reside. This module comprises seven routines, which are; a ByteToArray routine, ConvertByteToHex routine, ConvertStringFromHex routine, ConvertStringtoHex routine, CreateHash routine, CryptEncrypt routine, and CryptDecrypt routine. These routines were compiled together to form the *Dynamic Link Library (DLL)* file. This dll file serves as a reference for any Visual Basic application which needs to call the CryptoAPI function. A simple application is also developed to illustrate how to use this module to develop the user applications. This application demonstrates how to hash, encrypt and decrypt the string and various types of files using several cryptography algorithms provided by the CryptoAPI function. This project also shows how to use a cryptography technique in network systems.

ABSTRAK

Dalam projek ini, program *message handler* dengan ciri-ciri keselamatan dibangunkan dengan menggunakan Microsoft CryptoAPI. Kod sumber ditulis dalam bahasa Visual Basic. Dalam projek ini, modul yang dinamakan clsCryptoAPI dibangunkan untuk memanggil fungsi CryptoAPI yang terletak di dalam advapi32.dll. Modul ini mengandungi beberapa rutin seperti; rutin ByteToArray, rutin ConvertByteToHex, rutin ConvertStringFromHex, rutin ConvertStringtoHex, rutin CreateHash, rutin CryptEncrypt, dan rutin CryptDecrypt. Rutin-rutin ini digabungkan bersama untuk meghasilkan fail *Dynamic Link Library (DLL)*. Fail dll ini digunakan sebagai rujukan kepada mana-mana aplikasi Visual Basic yang perlu memanggil fungsi CryptoAPI. Aplikasi ringkas juga dibangunkan untuk menunjukkan bagaimana untuk menggunakan modul ini dalam applikasi pengguna. Applikasi ini menunjukkan bagaimana untuk melakukan *hash*, *encrypt* dan *decrypt* string dan juga bagaimana untuk membuat *encryption*/*decryption* pelbagai format fail dengan menggunakan beberapa algorithma cryptography. Projek ini juga menunjukkan bagaimana untuk menggunakan teknik cryptography dalam sistem rangkaian.

CONTENTS

GLOSSARY OF TABLES

GLOSSARY OF FIGURES

GLOSSARY OF ABBREVIATIONS

3DES	-	Triple DES
API	-	Application Program Interface
COM	-	Component Object Model
CSP	-	Cryptographic Service Provider
DES	-	Data Encryption Standard
IDEA	-	International Data Encryption Algorithm
MD2	-	Message Digest 2
MD4	-	Message Digest 3
MD5	-	Message Digest 5
SHA	-	Secure Hash Algorithm
RSA	-	Rivest-Shamir-Adelman
RC2	-	Rivest Cipher 4
RC2	-	Rivest Cipher 2
VB	-	Visual Basic
WCCO	-	Wiley CryptoAPI COM Object

CHAPTER I

INTRODUCTION

1.1 Project Background

The purpose of this project is to study the essentials of cryptography and to learn how to write the cryptographic code by calling the API function from Microsoft® Windows operating system.

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Data communications channels are often insecure, subjecting messages transmitted over the channels to passive and active threats. With a passive threat, an intruder intercepts messages to view the data. This intrusion is also known as eavesdropping. With an active threat, the intruder modifies the intercepted messages [7]. An effective tool for protecting messages against the active and passive threats inherent in data communications is cryptography.

1.2 Motivation

In the age of e-commerce, there are various concerns of online privacy and security. The most popular technique to protect the data is cryptography. Microsoft includes a suite of cryptographic routines with some of the strongest ciphers in the world. This cipher comes with Microsoft Window Operating Systems. It is called the CryptoAPI. This API function is designed to be called from C and very hard to use because the documentation is uneven. Because of programming in Visual Basic is more simple and easy to developed Windows applications than C. Therefore, It is needs to develop a COM wrapper that can replace CryptoAPI's arcane and inscrutable interface with something far simpler.

1.3 Significance of the Project

The COM wrapper for CryptoAPI was developed due to the difficulty of calling the CryptoAPI function directly from Visual Basic. The significance of the project is that the COM wrapper to be interfaces with CryptoAPI, in long term it is expected to be useful for the development of cryptographic programming skill based on Visual Basic, which is identified to be relevant to computer and communication security problem solving.

1.4 Objective

The objectives of this project are:

1. To study the essential of conventional and modern cryptosystem.

2. To study the function of Microsoft® CryptoAPI and how to call it from Visual Basic.

3. To write a set of cryptographic code for data encryption and decryption. This code can be integrated into application software such as Microsoft Word or E-Mail application.

1.5 Scope of Work

The scope of the project had been defined as follows:

1. This project will only focus on study of available cryptographic algorithm but not to develop a new algorithm.

2. Familiarizing with Visual Basic language, CryptoAPI function and cryptographic coding technique.

3. Implementing the cryptosystem in application software and test the performance.

1.6 Schedule

This project is scheduled for two semesters, which span for eight months. The specifications and requirements were derived in the first semester while coding for cryptosystem, synthesis, compilation, implementation and testing were done in the second semester.

1.7 Report Outline

This thesis had been written in six chapters. Chapter 1 reviews the background of the project. Chapter 2 concentrates on literature review, particularly on the fundamental of cryptography, Cryptography algorithm, CryptoAPI and Visual Basic code used in this project. Chapter 3 is mainly on the research methodologies being employed during the running of this project, tools used and the design consideration taken. In chapter 4 the implementation of the cryptosystem is described. Chapter 5 describes on the experiments conducted, results obtained and discussion while chapter 6 is the concluding remark

The detail of the DES and RSA algorithm are given in Appendix A. Appendix B shows flowchart for each routine. Appendix C exhibits Visual Basic codes for all routines.

CHAPTER II

LITERATURE REVIEW

2.1 Overview

This chapter reviews some related topics that include the fundamental of cryptography, cryptographic algorithm, several issues on cryptography, Visual Basic programming and architecture of Microsoft CryptoAPI. Similar previous work is also reviewed in this chapter.

2.2 Cryptography and Cryptanalysis

Cryptography is the science of mapping readable text, called plaintext, into an unreadable format, called ciphertext, and vice versa. The mapping process is a sequence of mathematical computations. The computations affect the appearance of the data, without changing its meaning. It is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [1].

To protect a message, an originator transforms a plaintext message into ciphertext. This process is called encryption or encipherment. The ciphertext is transmitted over the data communications channel. If the message is intercepted, the intruder only has access to the unintelligible ciphertext. Upon receipt, the message

recipient transforms the ciphertext into its original plaintext format. This process is called decryption or decipherment. The encryption and decryption concepts are illustrated in figure 2.1.

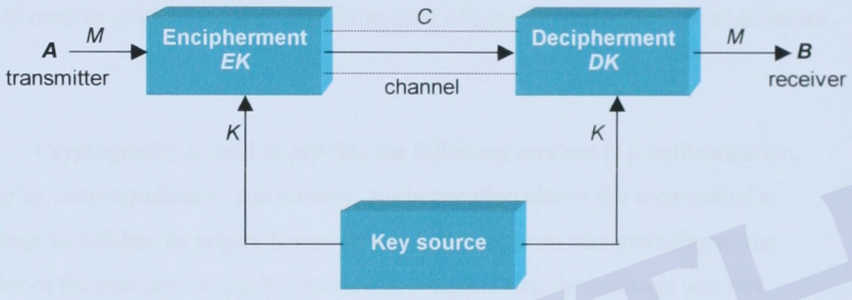

Figure 2.1a: Cipher system

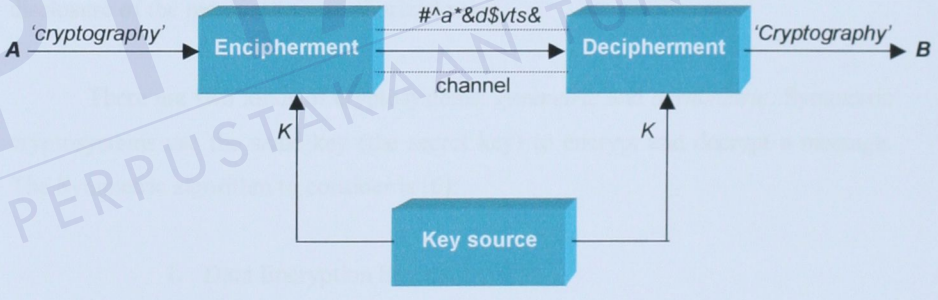

Figure 2.1b: Example of encipherment and decipherment

The mathematical operations used to map between plaintext and ciphertext are identified by cryptographic algorithms. Cryptographic algorithms require the text to be mapped, and, at a minimum, require some value which controls the mapping process. This value is called a key. Given the same text and the same algorithm, different keys produce different mappings.

Cryptographic algorithms need not be kept secret. The success of cryptography is attributed to the difficulty of inverting an algorithm [2]. In other words, the number of mappings from which plaintext can be transformed into ciphertext is so great, that it is impractical to find the correct mapping without the key. For example, the DES (Data Encryption Standard) uses a 56-bit key. A user with the correct key can easily decrypt a message, whereas a user without the key would need to attempt random keys from a set of over 72 quadrillion possible values [3].

Cryptography is used to provide the following services [1]: authentication, integrity, non-repudiation, and secrecy. Authentication allows the recipient of a message to validate its origin. It prevents an imposter from masquerading as the sender of the message. Integrity assures the recipient that the message was not modified en route. Note that the integrity service allows the recipient to detect message modification, but not to prevent it. There are two types of non-repudiation service. Non-repudiation with proof of origin provides the recipient assurance of the identity of the sender. Non-repudiation with proof of delivery provides the sender assurance of message delivery. Secrecy, also known as confidentiality, prevents disclosure of the message to unauthorized users.

There are two kinds of cryptosystems: *symmetric* and *asymmetric*. Symmetric cryptosystems use the same key (the secret key) to encrypt and decrypt a message. The Symmetric algorithm to consider is [6]:

1. Data Encryption Standard (DES)
2. Triple DES
3. International Data Encryption Algorithm (IDEA)
4. Rivest Cipher #4 (RC4)

The asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Asymmetric cryptosystems are also called *public key* cryptosystems and the algorithm to consider is [6]:

1. Diffie-Hellman
2. Rivest, Shamir, and Adelman (RSA)

Cryptanalysis is the area within cryptology which is concerned with techniques for deciphering encrypted data without prior knowledge of which key has been used. This is more commonly known as 'hacking'. Successful cryptanalysis requires at least a fundamental insight into cryptographic algorithm and methods.

2.3 The Data Encryption Standard (DES)

The data encryption standard (DES) [NBS77] is the system developed for the U.S. government for use by the general public. It has been officially accepted as a cryptographic standard both in the United States and abroad. Many hardware and software systems have been designed using the DES. The DES algorithm is a careful and complex combination of two of the fundamental building block of encryption; Substitution and Permutation (transportation).

The algorithm derives its strength from repeated application of these two techniques, one on the top of the other, for a total of 16 cycles. Plaintext is encrypted as a block of 64 bits. Although the key is 16 bits long, in effect the key can be any 56 bits number. The user can change the key at will any time security of the old key may be uncertain.

The algorithm is derived from two concepts of Shannon's theory of information secrecy, which publish in 1949 ([SHA49]). Shannon identified two techniques to conceal information that is confusion and diffusion. Confusion is the technique to change the information so that the output bits have no obvious relationship to the input bits. Diffusion attempts to spread the effect of the plaintext bit to other bits in the ciphertext.

REFERENCES

[1] A. Menezes, P. van Oorschot, and S. Vanstone. (2001). *Handbook of Applied Cryptography*. CRC Press.

[2] Bondi, R. (2000). *Cryptography for Visual Basic®: A Programmer's Guide to the Microsoft® CryptoAPI*. New York: John Wiley & Sons, Inc.

[3] C. P. Pfleeger. (1997). *Security in Computing*. Prentice Hall PTR.

[4] F. Dachselt and W. Schwarz, *Chaos and Cryptography*. IEEE trans. Circuits and Systems, vol. 48, No. 12, pp 1498 – 1509, Dec 2001.

[5] P. W. Wong and M. Nasir, *Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification*. IEEE trans. Image Processing, vol. 10, No. 10, pp 1593 – 1601, Oct 2001.

[6] G. Shafi, *New Directions in Cryptography: Twenty Some Years Later*. Proceeding IEEE, 1997.

[7] S. Burnett and S. Paine. (2001). *RSA Security's Official Guide to Cryptography*. RSA Press, McGraw – Hill

[8] Smith, R. E. (1997). *Internet Cryptography*. Massachusetts: Addison Wesley Longman, Inc.

[9] V. Subbarao and E. Rassi, Data Encryption Performance and Evaluation Schemes. Proceeding IEEE, 2002.

[10] W. Stallings. (1995). *Cryptography and Network Security: Principles and Practice*. Prentice Hall International Inc.

[11] G. R. Blakley. (2000). *Twenty Years of Cryptography in the Open Literature.* Texas A&M University.

[12] F. Piper. *Encryption.* European Conference on Security and Detection, 28 – 30 April 1997. Conference Publication No. 437, IEE, 1997

[13] T. C. Wan. *Integrating Public Key Cryptography Into the Simple Network Management Protocol (snmp) Framework.* Proceeding IEEE, 2002.

[14] E. A. Azeem, R. Seireg and S. I. Shaheen. *Cryptographic Security Evolution of MD4 Hash Function.* Proceeding of the Thirteenth Radio Science Conference, March 19-21 1996, Cairo, Egypt

[15] J.M. Dukovic and D.T. Joyce. *An Evolution of Object-Based Programming with Visual Basic.* Proceeding IEEE, 1995.

[16] Deitel H.M., Deitel P.J. and Neito T.R. (1999). *Visual Basic 6: How to Program.* Prentice Hall.