JABATAN HAL EHWAL AKADEMIK
(Department of Academic Affairs)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

HASNIRA BINTI MD. LAZIM

calon untuk Ijazah
(candidate for the degree of) **MSc. (IT)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/ her project paper of the following title)

THE IMPLEMENTATION OF SECURING PLAINTEXT FILE USING CRYPTOGRAPHY METHOD IN A WEB-BASED ENVIRONMENT

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the filed is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **MR. AZMI MD. SAMAN**

Tandatangan
(Signature) :

AZMI BIN MD SAMAN
Pensyarah
Fakulti Teknologi Maklumat
Universiti Utara Malaysia

Tarikh
(Date) : 26/6/2004.

THE IMPLEMENTATION OF SECURING PLAINTEXT FILE USING CRYPTOGRAPHY METHOD IN WEB BASED ENVIRONMENT

A thesis submitted to the Graduate School in parlial
Fulfilment of the requirement for the degree
Master of Science (Information Technology)
Universiti Utara Malaysia

By
Hasnira binti Md Lazim
June 2004

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Graduate School
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.

ABSTRAK

Matlamat penyelidikan ini adalah untuk mencari sistem cryptography yang bersesuaian untuk *encrypt* dan *decrypt* fail .doc, mengimplimentasi kaedah cryptography itu pada aplikasi mudah menyerupai aplikasi email dan merekabentuk dan menjalankan satu set penilaian untuk memastikan keselamatan *'plaintext file'* di dalam persekitaran berasaskan web. Metodologi dan prosedur pengujian yang digunakan semasa penilaian ke atas sistem cryptography yang di implementasikan pada system aplikasi email adalah berdasarkan kepada model simulasi. Hasil daripada pengujian menggunakan set penilaian yang dibentuk, didapati ia dapat menunjukkan pencapaian sistem cryptography. ClipSecure dipilihkan menjadi sistem cryptography yang paling sesuai didalam skop projek ini kerana ia ada sembilan pilihan algoritma, ditambah dengan *hardcore mode* dan punya sokongan untuk kedua-dua jenis *encryption* iaitu message dan fail.

ABSTRACT

The objective of this research is primarily to find the best fit cryptography system that can encrypt and decrypt the extension file .doc, implement it in a simple application which works similar to email and construct and run a set of evaluation to securing plaintext file in a web based environment. The methodology and testing procedure which are used during this evaluation is based on a simulation model. Result from the evaluation set constructed is found able to show the performance of the cryptography system. ClipSecure is rated to be the best fitted features of cryptography system in this project scope for it has choices of nine algorithms, plus a hardcore mode and support for both message and file encryption.

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful,
I would like to thank:

My supervisor, Encik Azmi b Md Saman, for his help and advice in conducting this study, also to Encik Roshidi Din for his guidance and explanation of cryptography methods.

My meticulous proof reader and also my beloved husband, Shahrizan Hayazi b Minai for checking my English and re-reading the thesis, and also for his enthusiastic support, tireless effort and constant patience when dealing with my queries and general ramblings,

My father, Md Lazim b Md Dam, mother, Rapiah bt Abu, and my brothers and sister, whose constant love and support give me confidence in all aspect of life,

My other friends and colleagues, who have help me along the way.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Web security is a complex topic, encompassing computer system security, network security, authentication services, message validation, personal privacy issues, and cryptography (W3C, 2004). The continuous explosive growth of the World Wide Web's applicative usage has brought with it a need to securely protect sensitive communications sent over the Internet.

Businesses that accept transactions via the Web can gain a competitive edge by reaching a worldwide audience, at very low cost. But the Web poses a unique set of security issues, which businesses must address at the outset to minimize risk. Customers will submit information via the Web only if they are confident that their personal information, such as credit card numbers, financial data, or medical history, is secure.

Most encrypted transactions use a combination of private keys, public keys, symmetric keys, hash functions, and digital certificates to achieve authentication (both of the user and the Web server), confidentiality, data integrity, and non repudiation by either party. The general problem of securing file proposed in this thesis is the cryptographic protection of message and file generated by the usage of the electronic mail.

REFERENCES

Benjamin, Lail. (2002).Broadband Network & Device Security. *Brandon A Nordin.* 18 - 21

Bradley, J. (2000). *The SSLP Reference Implementation Project.* Retrieve 28 April 2004 from http://www.cs.bris.ac.uk/~bradley/publish/SSLP/contents.html

Danesh, A., Mehrassa, A. & Lau, F. (2002). *Safe and Secure – Your Home Network and Protect Your Privacy Online.* Indiana:Sams Publishing

ELSIE FOH.(2002). *DBS to ensure safety, hacker incident not taken lightly.* Retrieve 24 March 2004 from http://www.sensecurity.org/dbs.htm

Kangas, E. (2003). *The Case For Secure Email.* Retrieve 24 March 2004 from http://www.luxsci.com/extranet/articles/email-security.html#1

Karagiannis, K. (2002). *Securing Your E-Mail.* Retrieve 24 March 2004 from http://www.pcmag.com/category2/0,1738,671308,00.asp

Lawnham, D. (2001). Student expelled for Email Fraud. *Australian IT.* Retrieve 10 March 2004 from http://australianit.news.com.au

Miller, G. (2002). *Information Hiding: Past, Present, Future.* Retrieve 24 March 2004 from http://www.eco.utexas.edu/faculty/Norman/BUS.FOR/course.mat/SSim/

Netscape.com. (2004). *Netscape's Tech Briefs.* Retrieve 8 April 2004 from http://home.netscape.com/security/techbriefs/index.html

Noorulsadiqin Azbiya. (2003). *Utilizing Snort in the Analysis of Intrusion Detection System.* Universiti Utara Malaysia.

Rabaiotti, J. (2003). *Implementing an RSA Crypptography System for Windows.* . Retrieve 28 March 2004 from http://www.cs.cf.ac.uk/user/Antonia.J.Jones/Freeware/Encryption/JRabaiottiReport.pdf

Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C. Second Edition.* USA:John Wiley & Sons Inc

Schneier, B. (1995). *E-Mail Security – How to keep Your Electronic Message Private.* USA:John Wiley & Sons Inc

Setco.org. (2004). *SET Secure Electronic Transaction LLC.* Retrieve 8 April 2004 from http://www.setco.org/setmark/

Singh, S (1999) *The Code Book.* USA:Fourth Estate

SoftAlley Inc. (2003). *Cryptographic Technologies –A Comparison.* Retrieve 28 March 2004 from http://www.softalley.com/products/gargoyle/3.11/eSecure.html

Splaine, S. (2002). *Testing Web Security Assessing the Security of Web Sites and Application.* Indiana: John Wiley & Sons Inc

Stein, L.D. (1998). *Web Security: A Step by Step Reference Guide.* Massachussetts:Addison-Wesley.

Tuban, E. & Aronson, J. E. (2001). *Decision Support Systems and Intelligent Systems.* New Jersey:Prentice Hall.

VeriSign.com. (2004). *VeriSign, Inc.* Retrieve 8 April 2004 from http://www.verisign.com/

Whitman, M.E. & Mattord, H.J. (2003). *Principles of Information Security.* Massachusetts:Thomson Course Technologies