A MODEL FOR EVALUATION OF CRYPTOGRAPHY ALGORITHM ON UUM PORTAL

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

By
Norliana Binti Abdul Majid
June 2004

Copyright © Norliana Abdul Majid, 2004. All rights reserved

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)

NORLIANA ABDUL MAJID

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)

A MODEL FOR EVALUATION OF CRYPTOGRAPHY ALGORITHM ON UUM PORTAL

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): **MRS. HAMIRUL 'AINI HAMBALI**

Tandatangan
(Signature) :

Tarikh
(Date) : 4 July 2004

PERMISSION TO USE

In presenting this thesis in partial fulfilment of the requirement 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 purposes may be granted by my supervisor, in their absence, by the Dean of the Faculty of Information Technology. 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 material in this thesis, in whole or in part should be addressed to:

Dean of Faculty of Information Technology
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.

ABSTRAK

Kajian ini bertujuan untuk membangunkan dan menyediakan garispanduan untuk membina membangunkan model simulasi untuk menguji algoritma cryptografi dari segi kelajuan pengengkripan dan kelajuan pengdekripan di portal UUM. Pembangunan model simulasi ini melibatkan tujuh langkah iaitu definisi masalah, pembangunan model simulasi, pengujian dan pengesahan model, rekabentuk simulasi eksperimen, perlaksaan simulasi eksperimen, penaksiran keputusan dan implementasi keputusan. Pembanguna model simulasi ini melibatkan tiga tahap. Tahap pertama adalah pembinaan ID pengguna dan katakunci, tahap kedua melibatkan implementasi algorithma cryptografi kedalam tahap pertama dan tahap ketiga melibatkan implementasi parameter ujian iaitu kelajuan pengengkripan dan kelajuan pengdekripan.

Methodologi yang digunakan bermula dengan identifikasi masalah, identifikasi keperluan, analisis proses model dan merekabentuk model simulasi. Simulasi model dibangunkan dengan menggunakan Active Server Page, JavaScript dan SQL 7.0 sebagai pangkalan data. Kajian ini diakhiri dengan kesimpulan, yang menyatakan masalah dan limitasi yang dihadapi dalam melaksanakan kajian disamping mengutarakan beberapa cadangan untuk kajian akan datang.

ABSTRACT

The purposes of this project are to construct and provide guidelines to develop a simulation model to evaluate cryptography algorithm in terms of encryption speed and decryption speed on UUM portal. The development of the simulation model consists of seven steps. The steps are problem definition, construct the simulation model, test and validate the model, design the simulation experiments, conduct the simulation experiments, evaluate the result and implement the result. The development of the simulation model involves three level of development. Level one is the development of userID and password, level two involve the insertion of cryptography algorithm into the test bed and level three involve the insertion of the testing parameter speed coding.

The methodology used in this study begun with problem identification, requirement identification, analysed the model process and design the simulation model. The simulation model was developed using Active Server Page, JavaScript and SQL 7.0 as database. This project concludes by discussing problems and limitations that were encountered in completing this project, and offers a few recommendations for future development in this area.

ACKNOWLEDGMENT

With the name of Allah, his kindness and love with his blessing this study could be finished on time. This project could not be done without the help by all parties. Thank you to them who contribute to the successfulness of this project.

First of all I would like to thanks my parents that always give me love and support. To my project supervisor Mrs. Hamirul Aini Hambali, thank you for her kind tutelage, guidance, comments and suggestions through the development of this project. To Mr. Azmi Md Saman and Mr. Roshidi Din thank you for the comments and exhortation as the evaluators of this project.

Not forgettable to all my friends who together involve and struggle in making intersession project. The spirit and support together is appreciated and always be a memory. Finally to all people that involve directly and indirectly contribute to this project, thank you for the support and help, may Allah bless you all.

TABLE OF CONTENTS

CHAPTER THREE: RESEARCH METHODOLOGY

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

Security is one of the important criteria in web-based application. A lot of security techniques can be used to secure the important information. According to Wolfe (2000), the protection of information for business or private purpose in web-based application such as portal can be achieved through the careful selection and use of cryptographic tools. Schneier (1996) discuss a number of common cryptographic techniques that can be employed.

Cryptography as defined by most cryptographers is the art and science of keeping message secure. It is a process of changing readable and understandable information called plaintext into unreadable random data called ciphertext and then being able to translate the ciphertext back into plain text by the same process. Process of changing the plaintext into ciphertext is called encryption while process of translating the ciphertext into plaintext is called decryption (Wolfe, 2000).

The contents of the thesis is for internal user only

REFERENCES

Bassham, L. E., (2000). *Efficiency Testing ANSI Implementations of Round 2 Candidate Algorithms For The Advancrd Encryption Standard.*

Coopersmith, D., Gennaro, R., Halevi, S., Jutla, C., Matyas, S. M., Peyravian, M., Safford, D., and Zunic, N., (2000). *IBM Comments. Third AES Conference.*

Daemon, J., and Rijmaen, V., (2000). *Rijndael for AES. 3rd AES Conferemce.*

Dray, J., (1999). *Report on The NIST Java AES Candidate Algorithm Analysis.* Retrieve from http://csrc.nist.gov/encryption Standard Candidate Conference, pp.35-50

Dray, J., (2000). *Report on NIST Performance Analysis of The Final Round Java AES Candidates.* Retrieve from http://csrc.nist.gov/encryption Standard Candidate Conference

Foo, S., Leong, P. C., Hui, S. C., and Liu, S., (1999) Security Consideration in The Delivery of Web-based Application: A Case Study. *Information Management and Computer Security* 7(1),pp.40-49.

Gladdman, B., (1999). *Implementation Experience With AES Candidate Algorithms Second AES Conference*

Hazari, S., (2002). Challenges ofImplementing Public Key Infrastructure in Netcentric Enterprises. *Logistics Information Management,* 15(5/6), pp.385-392.

Irakleous, I., Furnel, S. M., Dowland, P. S., and Papadaki, M., (2002). An Experimental Comparison of Secret-based User Authentication Technologies. *Information Management and Computer Security,* 10(3), pp. 100-108.

Kamal, M. Z., and Amir, M. A. S., (2004). Password Retrieval Mechanism: An Evaluation on UUM Web Portal.

Nechvatal, J., Barker, E., Bassham, L., Burr, W., Foti, J., and Roback, E., (2000). *Report on The Development of Advanced Encryption Standard (AES).* Retrieved from http://www.nist.gov/aes/

Rivest, R. L., Robshaw, M. J. B., Sidney, R., and Yin Y. L., (1999). The RC6 Block Cipher. *NIST AES proposal.*

Saarinen, V., (2000). *Speed Versus Security.* Retrieve from http://www.tml.hut.fi/Studies/Tik-110300/2000/Newtech/speed_vs_sec_1.html.

Sadeh, T., and Walker, J., (2003). Library Portal: Toward The Semantic Web. *New Library World,* 104(1184/1185), pp. 11-19. retrieved from http://www.emeraldinsight.com/0307-4803.htm

Schneier, B., (1995). E-*mail Security: How to Keep Your ElectronicMessage Private.* New York: John Wiley & Sons Inc.

Schneier, B., and Whiting, D., (2000). *A Performance Comparison of The Five AES Finalist.*

Schneier, B., Kelsey, J., Whiting, D., Hall, C., and Ferguson, N., (1999). *The Twofish Encryption Algorithm: A 128-Bit Block Cipher.* New York: John Wiley & Sons Inc.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., and Ferguson, N., (2000). *Comments on Twofish as an AES Candidates.*

Splaine, S., (2002). *Testing Web Security: Assesing The Security of Key Sites and Applications.* Indianapolis, Indiana: Wiley Publishing Inc.

Sterbenz, A., and Lipp, P., (2000). *Performance of The AES Candidates Algorithm in Java.* Retrieve from http://csrc.nist.gov/encryption/aes.

Turban, E., and Aronsson, J. E., (1998). *Decision Support Systems and Intelligent Systems (International Edition).* Upper Saddler River, N.J: Prentice Hall.