MODIFIED DATA ENCRYPTION STANDARD ALGORITHM FOR TEXT-BASED APPLICATIONS

By

ASEM IB. MOHAMED KHMAG

Thesis Submitted to the School Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master Science

April 2006

DEDICATION

TO

MY BELOVED FAMILY

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in partial fulfilment of the requirements for the degree of Master of Science

MODIFIED DATA ENCRYPTION STANDARD ALGORITHM FOR TEXT-BASED APPLICATIONS

By

ASEM IB. MOHAMED KHMAG

April 2006

Chairman: Associate Professor Abd Rahman Ramli, PhD

Faculty : Engineering

Today security is the important thing that we need to transfer data from location to another safely. As there is strong security, there is great hacker and spies at the other side. Therefore, many models and systems are looking for an ideal method to provide a secure environment for better optimization of the electronic connected-world. Cryptography accepts the challenge and plays the main role of the modern secure communication world. The purpose of this thesis is to introduce and demonstrate a new algorithm for Internet and e-mail security.

The proposed algorithm was developed based on the combination of symmetric and asymmetric algorithm whereas the length of the key and digital signature was considered. In this manner, the length of the key would not affect the time execution of this algorithm and digital signature in the end of message would increase the authentication between the sender and the recipient.

The main steps in this algorithm started with reading the plain text "original message" from the user. The second step is to apply the hash method on this message by using shuffle mechanism. Now the message is ready to do the encryption process that is dividing the text message to 128 8-bit for each four sub keys, so if the text message less than 128 8-bit then use another sub key. The last step is to send the message to another side (the recipient).

To retrieve the original message the recipient must apply the inverse of all the previous stages i.e. rehashing and decryption. In this study comparison between the proposed algorithm and RSA algorithm (asymmetric algorithm) was examined and successful results were obtained. Because of its short time execution and higher authentication, using this algorithm will ensure the security for internet applications.

.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi sebahagian keperluan untuk ijazah Master Sains

PENGUBAHSUAIAN ALGORITMA PIAWAI PENYULITAN DATA UNTUK PENGGUNAAN TEKS ASAS

Oleh

ASEM IB. MOHAMED KHMAG

April 2006

Pengerusi: Profesor Madya Abd Rahman Ramli, PhD

Fakulti : Kejuruteraan

Pada hari ini, keselamatan adalah perkara penting yang kita perlukan untuk memindah data dari satu tempat ke tempat lain dengan selamat. Dengan adanya keselamatan yang kuat, terdapat juga penggodam dan perosak yang menanti. Oleh itu, banyak model dan sistem cuba untuk mencari kaedah yang ideal untuk menyediakan persekitaran yang selamat untuk lebih mengoptimumkan dunia rangkaian elektronik. Tujuan kajian ini adalah untuk memperkenalkan dan mendemonstrasi algoritma baru untuk keselamatan Internet dan e-mel.

Algoritma tersebut dibangunkan berdasarkan kepada gabungan algoritma simetrik dan tidak simetrik dimana panjang kekunci dan tandatangan digital diambil kira. Dengan cara ini, panjang kekunci tidak memberi kesan kepada masa pelaksanaan algoritma ini dan tandatangan digital pada penghujung mesej akan meningkatkan pengesahan antara pengirim dan penerima.

Langkah utama dalam algoritma ini bermula dengan membaca “mesej asal” teks biasa daripada pengguna. Langkah kedua ada menerapkan kaedah hash pada mesej ini dengan menggunakan mekanisma “shuffle”. Sekarang mesej tersebut sedia untuk dilakukan proses penyulitan enkripsi dengan membahagikan mesej teks kepada 128 8-bit untuk setiap 4 sub kekunci, supaya jika mesej kurang daripada 128 8-bit maka sub kekunci lain digunakan. Langkah terakhir adalah menghantar mesej kepada penerima.

Untuk mendapatkan mesej asal, penerima perlu melaksanakan songsangan kepada semua peringkat terdahulu, contohnya mengulang cincang nyahsulitan. Dalam kajian ini perbandingan antara algoritma dicadangkan dan algoritma RSA (algoritma tidak simetrik) diperiksa dan keputusan yang baik berjaya diperolehi. Oleh kerana masa pelaksanaan yang singkat dan tahap pengesahan yang tinggi, penggunaan algoritma ini akan memastikan keselamatan aplikasi Internet.

ACKNOWLEDGMENTS

First, all praise be to Almighty ALLAH SWT. The only creator, sustainer and efficient assembler of the world, for giving me the strength, ability and patience to complete this work.

I would like to acknowledge and thank my supervisor Assoc. Prof. Dr. Abd Rahman Ramli.and En Shaiful for accepting me as one of his postgraduate students. I would also like to thank him for his cheery nature, assistance, guidance and mentorship throughout the years. This dissertation would have never been completed without his help. He has provided me with all facilities needed to complete this work. Also I would like to thank my members of supervisory committee, Dr. Elsadig Ahmed Mohamed Babiker. and En Shaiful Jahari Hashim for their assistance, constructive suggestions, and guidance for execution of the research project.

Special thank goes to Dr. Ahmed Ekhmaj, a person whose sacrifice, encouragement and unlimited financial support have made this work successful. None of this would have been possible without his support. I would like to take this opportunity to thank my friends for their friendship. We all have had memorable moments. I am especially grateful to my mother, a person whose courage, fortitude and patience I have always admired. Last but not least, I would like to gratefully express to my brothers and sisters for their unwavering support, best wishes and encouragement through both good and bad times.

I certify that an Examination Committee has met on 14th April 2006 to conduct the final examination of Asem Ib. Mohamed Khmag on his Master of Science thesis entitled "Modified Data Encryption Standard Algorithm for Text-Based Applications" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommended that the candidate be awarded the relevant degree. Member of the Examination Committee are as follows:

Mohd Adzir Mahdi, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Mohamad Hamiruce Marhaban, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Khairi Bin Yusuf, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Abdul Hanan Bin Abdullah, PhD
Professor
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia
(External Examiner)

HASANAH MOHD. GHAZALI, PhD
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date :

This thesis submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the Supervisory Committee are as follows:

Abd Rahman Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Shaiful Jahari Hashim
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

AINI IDERIS, PhD
Professor/Dean
School of Graduate
Studies
Universiti Putra
Malaysia

Date:

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

ASEM IB MOHAMED KHAMG

Date:

TABLE OF CONTENTS