A STUDY ON ONE WAY HASHING FUNCTION AND ITS APPLICATION TO FTMSK WEBMAIL

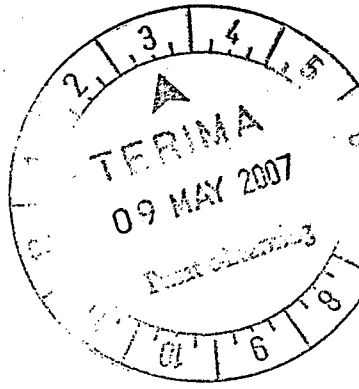
INSTITUT PENYELIDIKAN, PEMBANGUNAN DAN PENGKOMERSILAN
UNIVERSITI TEKNOLOGI MARA
40450 SHAH ALAM, SELANGOR
MALAYSIA

BY :

MOHD ROSLI MOHD DAUD
PRASANNA RAMAKRISHNAN
ISMASSABAH BINTI ISMAIL
NURMAISARA ZA'BA
MOHD HAIAR HASRUL IONO
SUZANA BAHARUDDIN
SYAMSUL ARIFFIN YAHAYA
AZLAN ABDUL AZIZ

DECEMBER 2007

UNIVERSITI TEKNOLOGI MARA
Institut Penyelidikan, Pembangunan dan Pengkomersilan (IRDC)
Institute of Research, Development and Commercialisation (IRDC)
(Sebelum ini dikenali sebagai Biro Penyelidikan dan Perundingan)
40450 Shah Alam, Malaysia
Website : http://www.irdc.uitm.edu.my



Tarikh : 8 Mei 2007
Surat Kami : 600-IRDC/ST.5/3/1237

Encik Md Rosli Md Daud
Ketua Projek
Fakulti Teknologi Maklumat & Sains Kuantitatif
Universiti Teknologi MARA (UiTM)
40450 SHAH ALAM

Tuan/puan,

DAFTAR PROJEK PENYELIDIKAN
TAJUK PROJEK : A STUDY ON ONE WAY HASHING FUNCTION AND ITS APPLICATION FOR FTMSK WEBMAIL

Dengan segala hormatnya perkara di atas adalah dirujuk.

Sukacita dimaklumkan bahawa pihak IRDC meluluskan permohonan tuan/puan dan ahli-ahli projek seperti berikut untuk mendaftarkan projek penyelidikan tuan/puan bertajuk seperti di atas yang sedang dijalankan dengan menggunakan **pembiayaan sendiri.**

Ahli projek : 1. En. Syamsul Ariffin Yahaya
2. En. Mohd Nor Hajar Hasrol Jono
3. En. Prasanna Ramakrisnan
4. Pn. Nurmaisara Za'ba
5. Pn. Suzana Baharuddin
6. Pn. Ismassabah Binti Ismail
7. En. Azlan Abdul Aziz

Oleh itu, pihak kami berharap agar tuan/puan dapat menghantar dua (2) naskah laporan akhir mengikut format yang telah ditetapkan setelah menamatkan projek penyelidikan tersebut.

Sekian, harap maklum. Terima kasih.

Yang benar,

PROF. DR. AZNI ZAIN AHMED
Penolong Naib Canselor (Penyelidikan)

s.k : 1. Dekan
Fakulti Teknologi Maklumat & Sains Kuantitatif

2. Prof. Madya Dr. Mohd Hanafiah Abidin
Ketua Penyelidikan (Sains & Teknologi)
IRDC, UiTM Shah Alam

HMIa

Tarikh : 5 December 2007
No. Fail Projek : 600-IRDC/ST.5/3/1237

Mohd Rosli Mohd Daud
Fakulti Teknologi Maklumat dan Sains Kuantitatif
Universiti Teknologi MARA
40450 Shah Alam

Penolong Naib Canselor (Penyelidikan)
Institut Penyelidikan, Pembangunan dan Pengkomersilan (IRDC)
UiTM, Shah Alam

Ybhg. Prof.,

LAPORAN AKHIR PENYELIDIKAN "A STUDY ON ONE WAY HASHING FUNCTION AND ITS APPLICATION FOR FTMSK WEBMAIL"

Merujuk kepada perkara di atas, bersama-sama ini disertakan 3 (tiga) naskah Laporan Akhir Penyelidikan bertajuk "A STUDY ON ONE WAY HASHING FUNCTION AND ITS APPLICATION FOR FTMSK WEBMAIL" oleh kumpulan Penyelidik dari Fakulti Tekologi Maklumat dan Sains Kuantitatif untuk makluman pihak tuan/puan.

Sekian, terima kasih.

Yang benar,

MOHD ROSLI MOHD DAUD
Ketua
Projek Penyelidikan

TABLE OF CONTENTS

CHAPTER 1: PROBLEM DESCRIPTION 1

1.1 Background of the Problem 1

1.2 Problem Statement 2

1.3 Aim 2

1.4 Objective 3

1.5 Scope 3

1.6 Significance of Research 3

CHAPTER 2 : LITERATURE REVIEW 4

2.1 Introduction 4

2.2 The Importance of Good Passwords 5

2.3 Possible Password Attack 6

2.4 UNIX Password Attack 7

2.5 Encryption versus Hashing 8

2.6 One Way Hashing Functions 12

2.7 Algorithms in One-Way Hashing Function 13

2.8 Encryption Techniques 18

2.9 Application of One Way Hashing Functions 19

2.10 Secure Socket Layer (SSL) 23

2.11 Client Side Implementation 24

2.12 Conclusion 25

ABSTRACT

Password is a normal way to securing data from intruders. The widespread use of password is in email account. The advances of technology have reduced the function of password in security, where there is a chances to be sniff or hack by intruders. This situation was shown in FTMSK staff webmail which using password (in plaintext) as security purpose but staffs are not allowed to send exam question or other important document through email. The reason given is for security purpose. There are several techniques use to transform plaintext password to other form of password which is call encryption. Encryption need to be done on the client side on client server architecture to obtain secure password during transmission. One type of encryption is 'one-way hashing function' which consists of several algorithms such as Message Digests (MD), Secure Hash Algorithm (SHA) and RIPEMD etc. MD5 and SHA1 are the most common hashing function currently in use. Both are produce at the same year (1994) and come from the same extension, which is MD4. The research are aim to study on Message Digests version 5 (MD5) and Secure Hash Algorithm version 1 (SHA1) with the use for password in email account. Prototypes are developed for both MD5 and SHA1 in one way hashing function using evolutionary approach. It tests for the processing time and length of hashing value.