

Universiti Teknologi MARA

**A Study on One Way Hashing
Function and its Application for
FTMSK Webmail**

Noor Hasimah Ibrahim Teo

Thesis submitted in fulfillment of the requirements for
**Bachelor of Science (Hons) Information
Technology**
**Faculty of Information Technology And
Quantitative Science**

November 2005

DECLARATION

I certify that this thesis and the research to which it refers are the product of my own work and that any ideas or quotation from the work of other people, published or otherwise are fully acknowledged in accordance with the standard referring practices of the discipline

NOVEMBER 21, 2005



NOOR HASIMAH IBRAHIM TEO

2003327385

ABSTRACT

Password is a normal way for 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 are many chances of password to be sniffed or hack by intruders. FTMSK webmail is using password as an authentication method. The problem was, their lecturer is not allowed to send examination question through email. This means that they do not trust the security of webmail. There are several techniques use to transform plaintext password to other form of password. One of it is call one-way hashing function. One-way hashing function consists of several algorithms. However MD5 is the most common hashing function currently in use. The research are aim to determine security of using one way hashing function at client side for FTMSK webmail login system and design framework for one way hashing function. A prototype is developed using MD5 algorithm and based on prototype approach, since it study on existing system. Tests are run for both FTMSK webmail and prototypes to determine whether the plain text password can be retrieved. Furthermore framework for one way hashing function is designed. Password need to be store in database on server in the form of hashing value. Secure password during transmission can be obtained by running protection on the client side of client server architecture.

TABLE CONTENTS

CONTENT	PAGE
Acknowledgement	iii
Abstract	iv
List of Tables	ix
List of Figures	x - xi
CHAPTER ONE: INTRODUCTION	
1.0 Background of the Problem	1 - 2
1.1 Problem Statement	2
1.2 Aim	3
1.3 Objective	3
1.4 Scope	3
1.5 Significant of Research	3
CHAPTER TWO: LITERATURE REVIEW	
2.0 Introduction	4
2.1 The Important of Good Password	5
2.2 Possible Password Attack	5 - 6
2.3 UNIX Password Security	7
2.4 Encryption versus Hashing	7 - 11
2.5 One-Way Hashing Function	12 - 13
2.6 Algorithms in One-Way Hashing Function	13 - 21
2.7 Encryption Techniques	21 - 22
2.8 Application of One-Way Hashing Functions	22 - 26
2.9 Secure Socket Layer	26 - 27
2.10 Client Side Implementation	27 - 28

2.11	Conclusion	28
------	------------	----

CHAPTER THREE: METHODOLOGY

3.0	Introduction	29
3.1	Research Methodology	30
3.1.1	Problem Assessment	31
3.1.2	Research Planning	31
3.1.3	Data Collection	31 – 32
3.1.4	Data Analysis	32 – 33
3.1.5	Research Design	33 – 39
3.1.6	Construct Prototype	39 – 40
3.1.7	Prototype Testing	40
3.1.8	Outcome Analysis	40
3.1.9	Research Documentation	40

CHAPTER FOUR: CONSTRUCTION OF PROTOTYPE

4.0	Introduction	41 – 42
4.1	Construction of Webmail Registration System Prototype	42
4.1.1	Creating a Web Page	42 – 43
4.1.2	Creating Database	44
4.1.3	Establishing Connection and System Guidance	45 – 48
4.2	Construction of Webmail Login System Prototype	48 – 49
4.2.1	Creating Web Page	49 – 50
4.2.2	Establishing Connection and System Guidance	50 – 53

CHAPTER FIVE: RESULTS AND ANALYSIS

5.0	Introduction	54
-----	--------------	----