UNIVERSITI PUTRA MALAYSIA

IMPLEMENTATION AND EVALUATION OF LARGE RSA ENCRYPTION AND DECRYPTION KEYS FOR INTERNET SECURITY

SEDDEQ H. BELGASSEM.

IMPLEMENTATION AND EVALUATION OF LARGE RSA ENCRYPTION AND DECRYPTION KEYS FOR INTERNET SECURITY

By

SEDDEQ H. BELGASSEM

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

June 2004

Dedicated To my Beloved Family,

my Parents, my Brothers,

and my Sisters

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

IMPLEMENTATION AND EVALUATION OF LARGE RSA ENCRYPTION AND DECRYPTION KEYS FOR INTERNET SECURITY

By

SEDDEQ H.BELGASSEM

June 2004

Chairman: Associate Professor Abd Rahman Ramli, PhD

Faculty: Engineering

The Internet is a powerful tool in today's ever-growing society. Computer Information and Internet security has recently become a popular subject due to the explosive growth of the Internet and the migration of commerce practices to the electronic medium. We use the Internet for many things, such as research, banking, and commercial sales. In each of this business, their needs to be save haven for which security is not compromised while companies run its business online. Thus the authenticity and privacy of the information transmitted and the data received on networked computers is of utmost importance. The deployment of network security procedures requires the implementation of Cryptographic algorithms. To facilitate this security issue, it is best to define a problem and advice a solution. The problem is computer crime via hackers, crackers, and thieves. The solution is to apply a security system upon the online system. The Science of cryptography provides one means to combat these attacks. These include encryption, decryption, authentication, and digital signature. Performance has always been the most critical characteristic of a cryptographic algorithm, which determines its effectiveness.

In this research the most popular and used algorithm, which is RSA, is implemented with a new modification in order to reduce the calculation time of the algorithm. A large encryption and decryption key sizes ranging from 1024 bit to 3072 bit have been generated and used in order to provide a high level of security. The computation results show that the key generation process using the modified algorithm is around three times faster than the old implementation. Both old and new implementationss are used to encrypt and decrypt different sizes and types of files using different generated key sizes. The results show that the most time lagging comes from image files, followed by PDF files, and then text files Moreover the encryption and decryption process using the modified system is around twice faster than the old system.

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

IMPLEMENTASI DAN PENILAIAN BESAR RSA KUNCI ENKRIPSI DAN DIKRIPSI UNTUK SEKURITI INTERNET

Oleh

SEDDEQ ELHASHMI. B. GHRARE

June 2004

Pengerusi: Profesor Madya Abd Rahman Ramli, Ph.D

Faculti: Kejuruteraan

Internet merupakan suatu alat yang amat berguna di dalam masyarakat yang semakin berkembang kini. Maklumat komputer dan sistem keselamatan Internet akhir-akhir ini menjadi subjek yang popular kerana perkembangan pantas Internet dan migrasi dalam amalan perdagangan kepada media elektronik. Kita meggunakan Internet untuk pelbagai perkara seperti kajian, perbankan dan jualan dagangan. Dalam setiap urusan ini, mereka perlu berasa selamat di mana keselamtan bukan satu kompromi sedang syarikat menjalankan urusan mereka atas talian. Demikian ketulinan dan rahsia maklumat yang dihantar dan data yang diterima di dalam rangkaian komputer amat besar kepentingannya. Prosedur pembahagian rangkaian keselamatan memerlukan perlaksanaan algoritma kriptografi. Untuk memudahkan isu keselamatan ini, adalah

lebih baik menentukan masalah dan memberi penyelesaian. Masalahnya adalah jenayah komputer melalui penggodam, penceroboh dan pencuri. Penyelesaiannya adalah dengan menggunakan sistem keselamatan di atas sistem talian. Sains kriptografi menyediakan suatu perjuangan menentang serangan. Ini termasuk *Penyulitan*, *nyahsulitan*, pengesahan dan tandatangan digital. Perlaksanaan merupakan ciri-ciri yang paling kritikal bagi algoritma kriptografi, di mana menentukan kesannya.

Di dalam kajian ini, algoritma yang popular dan selalu digunakan seperti RSA telah diimplimentasikan. Ia diperbaharui untuk mengurangkan masa kiraan algotitma . Kunci encrripsi dan dekripsi yang besar yang bersaiz antara 1024 bit hingga 3072 bit telah digunakan bertujuan untuk menyediakan sekuriti yang bertaraf tinggi.

Daripada keputusan komputasi, didapati bahawa proses penjanaan kunci dengan menggunakan implementasi yang diperbaharui adalah tiga kali lebih laju daripada implementasi yang lama. Kedua-dua implementasi yang lama dan baru digunakan untuk menenkrip dan mendekrip file yang pelbayai saiz dan jenis yang menggunakan saiz penjanaan kunci yang berbeza. Keputusan menunjukkan bahawa kebanyakan masa lngah adalah daripada file imge, diikuti dengan file PDF dan file text. Selain daripada itu, enkripsi dan dekripsi proses yang menggunakan sistem yang diperbaharui adalah dua kali lebih laju daripada sistem yang lama.

ACKNOWLEDGMENTS

I would like to thank ALLAH (S.W.T) for giving me this opportunity to continue my study and giving me the patience and perseverance to successfully complete my M.Sc thesis.

I am very thankful to my supervisor Associate Professor Dr. Abd Rahman Ramli for his helpful guidance and suggestions. I also appreciate all cooperation from the committee members Mrs. Azizah Ibrahim and Mr. Sayed Abd Rahman .

My gratitude goes to the Faculty of Engineering, the staff of School of Postgraduate Studies, and the staff of the Library for providing a studying and research environment.

Finally, I also owe much to my family, my special appreciation and gratitude goes to my parents for being a source of encouragement and always ask ALLAH to help me. Last but not least, I would like to acknowledge all my brothers, and sisters for their love, constant support and encouragement in all my endeavors.

Thanks to every person support me to produce my humble research work.

SEDDEQ H. BELGASSEM

TABLE OF CONTENTS

Page

DEDICATION ii
ABSTRACT iii
ABSTRAK v
ACKNOWLEDGMENTS vii
APPROVAL viii
DECLARATION x
LIST OF TABLES xiv
LIST OF FIGURES xvi
LIST OF ABBREVIATIONS xviii

1 INTRODUCTION

1.1 Overview 1
1.2 Internet Security 2
1.3 Statement of Problem 5
1.4 Research Objectives 7
1.5 Motivation 8
1.6 Research Contribution 10
1.7 Thesis Organization 11

2 LITERATURE REVIEW AND BACKGROUND

2.1 Previous Work 13
2.2 The Terminology of Cryptology 18
2.2.1 The Cryptographic System 18
2.2.2 Cipher System 19
2.2.2.1 Substitution Cipher System 20
2.2.2.2 Transposition Cipher Systems 24
2.3 Information Security and The Aspects of Cryptology 25
2.3.1 Aspects of Cryptology 26
2.3.1.1 Random Number Generators 27
2.3.1.2 One Way Functions 27
2.4 Symmetric Key Cryptography 28
2.4.1 The International Data Encryption Algorithm 29
2.4.1.1 Description of the IDEA System 30
2.4.2 Blowfish Algorithm 33
2.4.2.1 Description of the Blowfish Algorithm 34
2.4.3 RC5 Algorithm 37
2.4.3.1 Description of RC5 Algorithm 37
2.5 Asymmetric Key Cryptography 40

2.5.1 The Rivest-Shamir Aldeman (RSA) Algorithm 42
2.5.1.1 Requirements of the RSA Algorithm 43
2.5.1.2 Number Theory 44
2.5.2 The Diffie-Hellman Key Agreement (DHKA) Algorithm 45
2.5.2.1 Description of the DHKA Algorithm 45
2.5.3 The Raike Public-Key (RPK) Cryptosystem 46
2.6 Comparison Between Cryptographic Algorithms 47
2.6.1 Format of The Input 48
2.6.2 Memory Size 49
2.6.3 Input Type and Size 52
2.6.4 Cracking Capability 52
2.6.5 Weaknesses 54
2.6.6 Type of Operations 55
2.7 Summery 56

3 METHODOLOGY

3.1 Introduction 57
3.2 Description of Implementation 59
3.2.1 Key Generation Module 60
3.2.2 Data Encryption Module 61
3.2.3 Data Decryption Module 61
3.3 System Description 61
3.4 Summery 69

4 RESULTS AND DISCUSSION

4.1 Introduction 70
4.2 Key Generation Computation 71
4.2.1 Key Generation using The Proposed Algorithm 71
4.3 Encryption and Decryption Computations 74
4.3.1 Encryption and Decryption of 20 KB File Size 75
4.3.2 Encryption and Decryption of 35KB File Size 77
4.3.3 Encryption and Decryption of 1 MB File Size 79
4.4 Summery 80

5 CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion 81
5.2 Future work 82

BIBLIOGRAPHY 84
APPENDIX 88
BIODATA OF THE AUTHOR 94

LIST OF TABLES

Table		Page
1.1	New ways and Old Ways of Doing Things	8
2.1	Homophone list for the letters of message	22
2.2	Encryption Pseudocode for IDEA system	31
2.3	Decryption Pseudocode for IDEA system	33
2.4	Algorithm to compute the subkeys for IDEA Decryption	33
2.5	Blowfish Algorithm for encryption and decryption	36
2.6	Algorithm to compute P and S subkeys for Blowfish Algorithm	36
2.7	Algorithm to compute the subkeys for the RC5 Algorithm	39
2.8	Comparison Criteria	47
2.9	Format of the Input	49
2.10	Memory requirements	51
2.11	Cryptanalysis issues	53
2.12	Mathematical operations used in cryptography	56
4.1	Key generations Time	73
4.2	The 20 KB file Encryption and Decryption time using 1024-bit Key size	75
4.3	The 20 KB file Encryption and Decryption time using 2048-bit Key size	76

4.4 The 20 KB file Encryption and Decryption time using 3.072-bit Key size 76

4.5 The 350 KB file Encryption and Decryption time using 1024-bit Key size 77

4.6 The 350 KB file Encryption and Decryption time using 2048-bit Key size 78

4.7 The 350 KB file Encryption and Decryption time using 3.072-bit Key size 78

4.8 The 1 MB file Encryption and Decryption time using 1024-bit Key size 79

4.9 The 1 MB file Encryption and Decryption time using 2048-bit Key size 79

4.10 The 1 MB file Encryption and Decryption time using 3.072-bit Key size 80

LIST OF FIGURES

Figure **Page**

2.1 Encryption and Decryption Method 19

2.2 Simple substitution cipher 20

2.3 Homophonic substitution cipher 21

2.4 Polyalphabetic substitutions 23

2.5 Encryption Mapping of polyalphabetic substitution cipher 23

2.6 The Rail Fence Transposition cipher 25

2.7 Encryption and Decryption with one secrete key 28

2.8 Flowchart for the IDEA system. 30

2.9 Flowchart of the Blowfish algorithm. 35

2.10 Flowchart for RC5 Algorithm 38

2.11 Encryption and Decryption with two different keys 41

3.1 The implemented system module 59

3.2 The Implemented Algorithm execution 62

3.3 Prime Number Generation Pseducode 62

3.4 Key Generation Pseducode 63

3.5 Key generation Flow chart 64

3.6 Encryption Procedure Flow chart 66

3.7 Decryption Procedure Flow chart 67

4.1 Old Method of Key Generation 71

4.2 The Modified Method of Key Generation 72

4.3 Key generation time 73

LIST OF ABBRIVIATIONS

ASCII	American Standard Code for Information Interchange
API	Application Programming Interface
ARPA	Advanced Research Project Agency.
ATM	Asynchronous Transfer Mode
CPU	Central Processing Unit
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DHKA	Diffie-Hellman Key Agreement Algorithm
ECC	Elliptic Curve Cryptosystem
E-Mail	Electronic Mail
GF	Galois Field
IDEA	International Data Encryption Algorithm
IFP	Integer Factorization Problem
IMP	Interface Message Processor.
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISP	Internet Service Provider
LAN	Local Area Network
MD5	Message Digest 5
NFS	Number Field Sieve

NP	Non Deterministic Polynomial
PGP	Pretty Good Privacy
PKC	Public Key Cryptography
SKC	Secrete (Symmetric) Key Cryptography
RC5	Rivest Cipher Number 5
RPK	Raike Public-Key Algorithm
RSA	Rivest, Shamir and Adleman
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network

CHAPTER 1

INTRODUCTION

On the Internet, information passes from one computer to another through numerous systems before it reaches its destination. Normally, the users of these intermediary systems don't monitor the Internet traffic routed through them, but someone who's determined can intercept and eavesdrop on your private conversations or credit card exchanges. Worse still, they might replace your information with their own and send it back on its way. 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.

1.1 Overview

In section 1.2 a discussion of Internet security issues is introduced. A problem associated with computer crime on the Internet will be discussed with a solution. This solution deals with the countermeasures that can be applied to computer crime and primarily deals with cryptology. Then, in section 1.3 the statement of problem will be presented which is associated with the security provided by the algorithm using small keys. The research objectives of the research are summarized in section 1.4. The motivation and contribution of this work are explained in section 1.5, and section 1.6 respectively. Finally, in section 1.7 thesis organization is presented.

1.2 Internet Security

The Internet has been a major part of many people's lives in the past decade. Today Internet has its privileges and its shortcomings. The dawn of the Internet started in the 1960s with the Department of Defense (DoD) turning to the periodically defense agency called (Defense), Advanced Research Project Agency (ARPA). Around the same time, the DoD wanted a command and control network that would survive a nuclear war. The idea of circuit-switched lines as considered too vulnerable, so packet switching was suggested. It went under investigation in some universities. This later involved the development of software for the subnets, which included Interface Message Processors (IMP). The subnets and hosts of the nodes of the network were collectively called ARPANET. By 1972, the invention of the TCP/IP (Transmission Control Protocol/Internet Protocol) model and protocols expanded the growth of ARANET.

By 1983, ARPANET was divided into two networks, one for defense purposes and the other for civil purposes. The defense network was called MILNET (MILitary NETwork) and the civil network remained as ARPANET, which lasted until 1990, when it was dismantled because it had been taken over by newer networks for which it was spawned by.

The ARPANET was the first network that started a chain of other networks. In the 1980s, the large collection of networks became viewed as an Internet (short for interconnected network), This view later became known as the Internet. By 1990, the Internet was at 3,000 networks and 200,000 computers, with the one-millionth host attached two years later. All of this growth was accomplished by having existing networks connecting to the Internet. This growth double every two years, as calculated by [Pax94], and continues to grow even today.

The Internet stays together by the TCP/IP reference model and protocol stack, which provides universal services comparable to telephone service. The Internet (machine perspective) implies running a TCP/IP protocol stack, processing an IP (Internet Protocol) address, and being able to send IP packets to all other machines (hosts) on the Internet. An alternative way of being on the Internet is for a host to connect to an ISP's (Internet Service Provider's) router via a dial-up from the host's modem. Thus, a temporary IP address is assigned and being able to send IP packets to the other Internet hosts is capable.

After 1990, the Internet started to grow to the point that companies started to get into the idea of establishing online business. This is why we have YAHOO and AMAZON.COM today. One major issue regarding the Internet is security. This issue spawned research ideas to develop security protocols for the Internet to protect against confidentiality threats, data integrity, and privacy concerns.

Threats have many interpretations. These interpretations could include unauthorized release of information, unauthorized removable or modification of information, or unauthorized denial to access information when permitted. Computer security is the area of security that protects against unauthorized threats, just like the three examples mentioned. To apply computer security a policy must be set up that includes a set of rules and regulations that policies information access.

There are many ways to police information access. One way is to have a stand-alone computer and have only two "trustworthy" people possess all passwords. This the way it was done before the down of computer networking. In this approach, the information is safeguarded against users who do not possess the appropriate passwords. The approach on how the password system is accomplished is due to one-way hash functions. One-way hash functions are functions in such a matter that the user provides a password and is encrypted by the system in such a way that it is computationally infeasible to decrypt the file holding the password. Mathematically, a one-way hash function, it is easy to compute in one direction and hard to compute in the other direction. In other words it is easy to compute $f(x)$ given x, and hard to compute x given $f(x)$. So a one way function is used to encrypt secret information efficiently.

Another way to police information is to permit everyone to access the system, but with certain levels of security access. The process of using one-way functions mentioned earlier is also used here, but all users enter a username and password to access the system. This approach could also be applied to other systems connected to a network. All the user has to do is know the location and name of the other systems and attach it to itself to gain access. Although, some systems may require the user to provide a second username and password pair in order to gain access to it. Unfortunately, this kind of access is not flawless. It lacks randomness, it has issues related to multiple hosts, and it has the potential for eavesdropping.

1.3 Statement of Problem

There are many ways computer crime can occur. For example, viruses, Trojan horses, hackers, and crackers are described as areas related to computer crime techniques (Kabay 1996). This problem is primarily affected by business that possesses networked computer systems and also affected the Internet as well. Cryptography accepts the challenge and plays the main role of the modern secure communication world. Modern cryptographic systems are used to guarantee that no one but the intended recipient can decipher the contents of the message or the information. Its basis on specific algorithms, which deal with the encryption and decryption operations. Encryption mechanism converts the plaintext to cipher text; meanwhile the decryption mechanism converts this cipher text back to its original form (Plaintext). Different sets of public and private key cryptographic algorithms have been invented to be used for information security on the internet. Each algorithm has its effectiveness, weaknesses and other characteristics. Looking for secure information comes with implementing those cryptographic algorithms. In other words the problem is the computer and Internet crime, in which the hackers always attack the resources and cause many troubles to the governments and