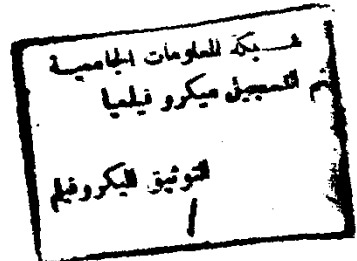


**AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE**



A THESIS
Submitted to the Department of Mathematics
(Computer Science)

On



INFORMATION SECURITY

*In Partial Fulfilments for Degree of
Master Science*

By
Aboul-Ella Otifey

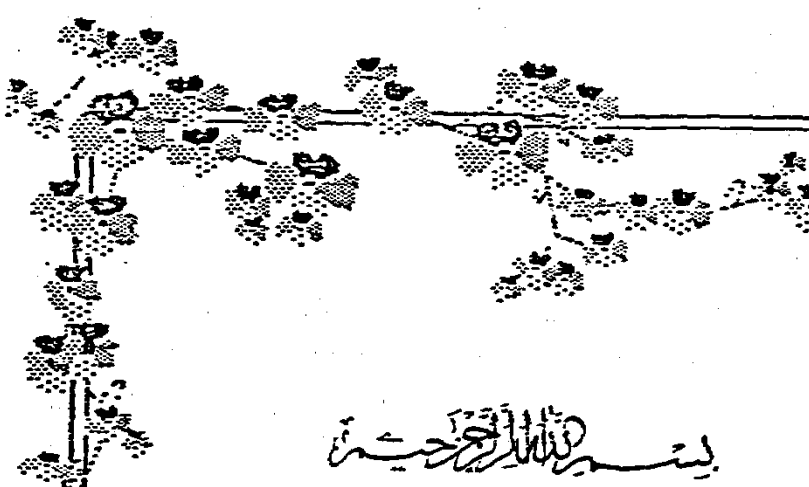
49007

Supervised By

Dr. Mahmoud K.A. Khairat
Late Prof. Dr. B.B. Baghos
Dr. Samh Samy Dauod

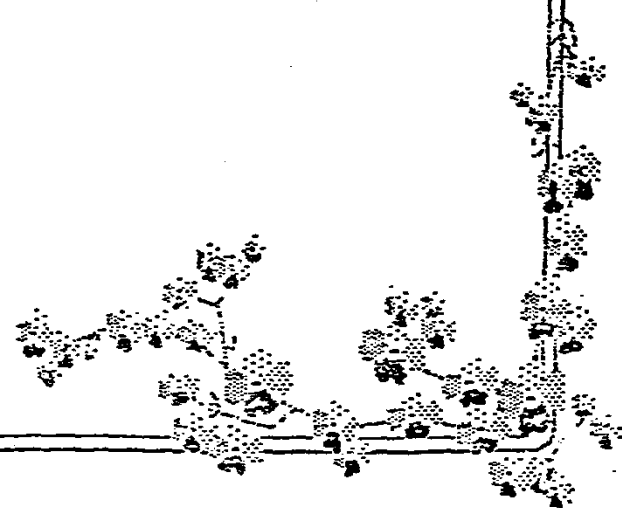
Cairo, 1993





بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ
”مَخْلَقَ السَّمَوَاتِ وَالْأَرْضِ أَكْبَرُ مِنْ خَلْقِ
النَّاسِ وَلَكِنَّ أَكْثَرَ النَّاسِ لَا يَعْلَمُونَ“

سورة غافر - الآية ٥٧





ACKNOWLEDGEMENT

ACKNOWLEDGEMENT

I would like to express my deep gratitude to Dr. Mahmoud K. A. Khairat, Associate Prof., Mathematics Department, Faculty of Science, Ain Shams University, for suggesting the problem, valuable guidance through his supervision of this work and for the following up every aspect of the thesis.

I much indebted to late Prof. Dr. B. B. Baghos, Artificial Satellites Department, National Research Institute of Astronomy and Geophysics, Helwan, Cairo, Egypt, for his continuous guidance

I much indebted to Dr. Samh. Samy Danod Associate Prof., Mathematics Department, Faculty of Science, Ain Shams University for his helpful spirit.

CONTENTS

CONTENTS

SUMMARY	iii
PREFACE.....	iv
Chapter I : Foundation of Cryptology	
1.1 Cryptography.....	1
1.2 Cryptanalytic Attack.....	4
1.3 Block Cipher Design.....	5
1.4 One Way Function.....	10
1.5 Cipher Techniques.....	12
1.5.1 Transposition Ciphers.....	12
1.5.2 Substitution Ciphers.....	13
1.5.3 Product Ciphers.....	19
1.5.3.1 The Data Encryption Standard.....	19
1.5.3.2 Avalanche and Complementarity Properties.....	22
1.5.3.3 Known DES Design Criteria.....	23
Chapter II : Public Key System	
2.1 Computing Inverses.....	29
2.1.1 The Chinese Remainder Theorem.....	36
2.2 Exponentiation Ciphers.....	38
2.2.1 Pohlig-Hellman Algorithm	40
2.2.2 RSA-Technique.....	41
2.2.3 Security of the RSA - Algorithm.....	42
2.2.4 Primarily Tests.....	43
2.2.5 Cryptanalysis of RSA system.....	44
2.3 Knapsack Techniques.....	45
2.3.1 Simple Knapsack Algorithm.....	46
2.3.2 Trapdoor knapsack Algorithm.....	47
2.3.3 Trapdoor knapsack Public Key Algorithm.....	49
2.3.4 Complexity of Knapsack Problem.....	49
2.4 Applications.....	50
2.4.1 Authentication Techniques.....	50
2.4.1.1 Authentication in Communication System.....	50
2.4.1.2 Authentication of Password.....	51
2.4.2.1 Encrypted Password Table.....	52

CONTENTS

2.4.2.2 Test Pattern Approach.....	54
2.4.2.3 A New Password System.....	56
2.4.2 Digital Signature Techniques.....	60
2.4.2.1 Digital Signature with Symmetric Encryption.....	60
2.4.2.1 Digital Signature with Public Key System.....	62
Chapter III : Access Control Mechanisms	
3.1 An Abstract Model Based on Access Control Matrix.....	65
3.1.1 Protection State Transition.....	66
3.2 Implementation of the Access Matrix.....	73
3.2.1 Access Control List	73
3.2.2 Capability List	74
3.2.3 Key-Lock Method	75
3.2.3.1 Single Key - Lock System	76
3.2.3.2 A Review of Hwang's and Chang's Access Control Scheme	77
3.3 Key Lock Mechanism Based on Lagrange Interpolating Polynomial	81
3.3.1 Changing an Access Rights	85
3.3.2 Insertion or Deletion of a User	86
3.3.3 Insertion or Deletion of a File	86
3.3.4 The Complexity Time	87
3.3.5 Comparisons.....	88
Chapter IV : IMPLEMENTATION	
4.1 Substitution Implementation.....	91
4.2 Permutation Implementation.....	94
4.3 Data Encryption Standard Implementation.....	97
4.4 Crypto Program.....	109
Glossary of Terms.....	117
REFERENCES	125
ARABIC SUMMARY	

SUMMARY

The work in this thesis consists of four chapters and glossary of terms :

Chapter-I : (*Foundations of Cryptology*) We introduce the fundamental concepts of cryptology. This is followed by a brief description of the two basic functions, one way function and trapdoor one way function. Detailed description of the symmetric encryption techniques, such as substitution , transposition and product techniques.

Chapter-II : (*Public Key System*) Here we describe the basic principles of public key systems, computing inverses and exponentational ciphers. A detailed description of the Rivest, Shamir and Adelman (RSA) technique and its practical implementation is given. We introduce the Merkle-Hellman Knapsack technique. Detailed explanation of the Merkle-Hellman Knapsack, including the encryption technique and complexity of its algorithm is given. Finally, two applications using cryptographic techniques, one is *Authentication* and the other is *Digital Signatures* are discussed. In addition, a new approach for authentication of password is considered.

Chapter-III : (*Access Control Mechanism*) Here we describe the basic mechanisms that control access by subjects (e.g., users) to objects (e.g, files). Moreover, we describe the " *Graham and Denning* " and " *Harrison, Ruzzo and Ullman* " models. Various approaches to the implementation of mechanisms for preventing illegal access of subjects to objects are discussed, such as the *Accessor List*, *Capability List* and *Key-Lock Matching*. Moreover, we review HWANG's, and CHANG's access control schemes. Finally, a new protection system based upon " *Lagrange Interpolation Formula* " that implement a single key lock system is considered.

Chapter-IV : (*Implementation*) This chapter contains the source code of software that implements some encryption / decryption algorithms for the three basic techniques (*Substitution ciphers* , *Permutation ciphers* and *product ciphers*). The source code of these programs written in C Language, and is implemented on *IBM Personal Computers under MS - DOS*.

PREFACE

PREFACE

Data security is one of the major research issues of the day. Vast amounts of data are stored in large computer data base and transmitted between computers and terminal devices linked together in complex communications networks. Without appropriate safeguards, these data are sensitive to interception (e.g. Via wiretaps) during transmission, or they may be physically removed or copied while in storage. Data are also sensitive to unauthorized deletion, modification, or addition during transmission or storage. The only known practical method for protecting data transmitted through communication networks is by the applications of *cryptography*.

The goal of this thesis is to study the cryptographic algorithms to enforce protection in communication channels and to protect the stored data from unauthorized users.

In chapter (I) , we describe an overview of the recent cryptographic achievements and techniques. Moreover, we give a brief description to be the Data Encryption Standard (DES) - algorithm . This chapter, also presents some possible known DES design criteria to aid in cryptanalysis of the DES or to aid in designing new and extended DES style schemes.

Although historically its original driving force, the establishment of secure communication over insecure channels is not the only purpose of cryptography. Indeed, modern cryptography (*both secret- and public - key*) has innumerable other applications.

In chapter (II), we shall discuss two of these applications in detail; one is *authentication* and the other is *digital signature*.

A protocol for authentication of password is an important link in the whole computer security issue. In the log - on process , the user supplies a unique IDentification ID_i " Typically publicly known " followed by a secret Password PW_i " Typically selected to be known only to the user ". Based on internally stored information " *Password table* " , the system checks to see

PREFACE

if the (ID_i, PW_i) pair is valid. The security of the system then entirely depends on the secrecy of the "password table" and the strength of the individual passwords.

The most straightforward approach is to store the *password table* directly in the computer system. Yet this is *dangerous* because, with current computer and operating system design, it is almost impossible to prevent the disclosure of a stored "Password table".

Some approaches were developed to overcome this problem. Evans, Kantrowitz and Weiss (Eva74) used a one way function to encrypt secret password and Lennon, Matyas and Meyer (Len81) proposed a test pattern approach as the basis of password validation.

In section (2.4.2.3), we will propose a new approach for authentication of password, that requires only simple computation while user's are free completely to choose their own identities and password. In our system, the password table does not need to be protected and the system does not keep a list of password.

Time sharing computer systems have permitted large numbers of users to share common data bases. Because of this users have begun to be concerned with rising importance of information security. It is generally agreed that some kind of information protection measure is required to prevent disclosures to unauthorized persons. An access control mechanism grants a user in a system the access right to access information resources (*programs, files, utility routines, etc.*) in the system. For instance, users may be able to access files via *Read, Write, Execute or Append* access rights, but different users will be given different access rights to individual files (Jam85). Various approaches to the implementation of mechanisms for preventing illegal access of subjects to objects; include, *the accessor list, capability list and key lock matching*.

Wu and Hwang proposed a single key lock system based on the Galois Field $GF(P)$, where P is the smallest prime number that is larger than all access rights a_{ij} of the access control matrix.

PREFACE

Later, Chang's proposed a key lock access control scheme based on *Chinese Remainder Theorem and Extended Euclid's Algorithm*.

In section (3. 3) We propose a new access control mechanism based on " *Lagrange Interpolation Formula* " that implement a single key lock system. In our method, every legal user is given a digital key and every secured resource is given a digital lock. Through a simple operation, the access rights that the i^{th} accessor possesses on the j^{th} resource can immediately be determined. Using our method, the representations of keys and locks are shorter and simpler. Moreover, faster operations and easier constructions of keys and locks are also achieved. Compared to Hwang's and Chang's methods, the access rights of a user to a file is revealed by applying straightforward division operations on the user's keys. In addition, our system is suitable for changing a privilege value, insertion or deletion of a user, and insertion or deletion of a file with a small change in the key and lock values.

CHAPTER I

FOUNDATION OF CRYPTOLOGY

FOUNDATION OF CRYPTOLOGY

For thousands of years, *cryptography* has been the art of providing secure communication over insecure channels, and *cryptanalysis* has been the dual art of breaking into such communications. Historically, *cryptology* (the combined art of cryptography and crypt analysis) has been almost exclusively in the hands of the military and diplomats. With the advent of the computer revolution, and more importantly of a society in which vast amounts of personal, financial, commercial and technological information are stored in computer data base and transferred over computer networks, the necessity for civilian cryptography has become overwhelming.

In this chapter, we introduce the basic concepts of cryptology and we give an overview of the classical cryptographic algorithms. In section (1.2) we describe the several cryptanalytic attacks to find the key that was used to encrypt a ciphertext for *conventional and public key algorithms*. Section (1.3), we describe the block cipher design property in order to understand the Data Encryption Standard algorithm (DES) which we shall described later. Section (1.4) we give a brief description of the two basic functions, *one - way - function and trapdoor one way function*. A description of the classical cipher algorithms are given in section (1.5).

1.1 Cryptography

Cryptography is the only known practical method for protecting data transmitted through communications networks that use land lines, communications satellites, and microwave facilities, etc.

Cryptography is defined as the method and process of transforming intelligible text into an unintelligible text. The transformation process from intelligible text to unintelligible text is known as enciphering or encryption. The reversal of the process from unintelligible text to original text is known as deciphering or decryption. The original intelligible text is known as **plaintext** or cleartext. The transformed unintelligible form is known as **ciphertext**.