

ON PROBLEMS OF AUTHENTICATION AND DIGITAL SIGNATURE IN CRYPTOGRAPH

THESIS
SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS
OF THE AWARD
OF THE (M. Sc.) DEGREE

رسالة

519.7
D. A

PRESENTED BY

6293

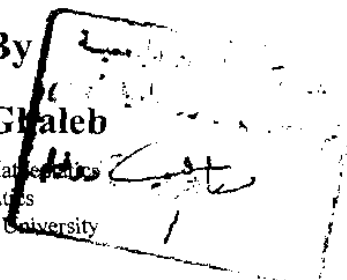
DOWLAT ABED ELAZZEZ MOHAMED ZAKI



Supervised By

Dr. Fayed F. M. Ghaleb

Associate Professor of Pure Mathematics
Department of Mathematics
Faculty of Science, Ain Shams University



SUBMITTED TO

Department of Mathematics
Faculty of Science
Ain Shams University

CAIRO, EGYPT

1997



ACKNOWLEDGMENT

*First of all, gratitude and thanks to **ALLAH** who always helps and guides me.*

*I wish to express my deepest thanks and deep appreciation to my supervisor **D. Fayed Fayek Mohamed Galeb**, Department of Mathematics, Faculty of Science, Ain Shams University, for suggesting the problem dealt with in this thesis, his helpful guidance, fruitful discussions and kind encouragement during my course of study.*

*Also, I would like to express my deep gratitude to **Dr. Mohamed Hamed El Zahar**, Department of Mathematics, Faculty of Science, Ain Shams University, for his constructive help.*

CONTENTS

CONTENTS

	Page
SUMMARY.	i
ABSTRACT.	iv
CHAPTER 1: INTRODUCTION TO CRYPTOLOGY AND DATA SECURITY.	
Introduction.	1
1.1. Cryptology.	2
1.1.1. Cryptography.	4
1.1.2. Cryptanalysis.	6
1.1.2.1. Ciphertext-Only Attack.	7
1.1.2.2. Known-Plaintext Attack.	8
1.1.2.3. Chosen-Plaintext Attack.	8
1.1.2.4. Chosen-Ciphertext Attack.	9
1.2. Threats to Data.	9
1.3. Cryptographic System (Cryptosystem).	12
1.3.1. Private-Key Cryptosystem.	13
1.3.1.1. Advantages of Private-Key Cryptosystems.	14
1.3.1.2. Problems of Conventional Cryptosystems and their solutions.	14
1.3.2. Public-Key Cryptosystem.	15
1.3.2.1. Secrecy for Public-Key System.	16
1.3.2.2. Authenticity for Public-Key Cryptosystem.	17
1.3.2.3. Secrecy and Authenticity for Public-Key Cryptosystem.	18
1.3.2.4. Advantages of Public-Key Cryptosystem.	19
1.4. Protocol.	20
1.4.1. Types of Protocol.	21
1.4.1.1. Arbitrated and Adjudicated Protocols.	21
1.4.1.1.1. Advantages and Disadvantages of Arbitrated and Adjudicated Protocols.	22
1.4.1.2. Self-Enforcing Protocol.	22
1.4.2. Attacks Against Protocol.	23

	Page
CHAPTER II: AUTHENTICATION.	
Introduction.	26
2.1. User Authentication Problem and its Solution.	26
2.1.1. Continuous Protocol.	27
2.1.1.1. Simple Continuous and Password Protocols.	27
2.2. Message Authentication Problem.	28
2.2.1. Elementary Authentication Protocols	29
2.2.1.1. Elementary Protocol "Based on Private-key Cryptosystem".	29
2.2.1.2. Elementary Protocol "Based on Public-Key Cryptosystem".	30
2.2.2. Shamir's Fast Authentication Protocol.	31
2.2.3. Ong-Schnorr-Shamir Authentication Protocol.	34
2.2.4. El Gamal's Authentication Protocol.	35
2.2.5. Subliminal Channel.	37
2.2.5.1. Elementary Subliminal Channel.	37
2.2.5.2. Ong-Schnorr-Shamir Subliminal Channel.	39
2.2.5.3. El Gamal Subliminal Channel.	40
2.2.5.4. Seberry-Jones Subliminal Channel.	41
CHAPTER III: DIGITAL SIGNATURE.	
Introduction.	42
3.1. Digital Signature.	42
3.2. Digital Signature Protocol.	43
3.2.1. Types of Digital Signature Protocol.	43
3.2.1.1. Digital Signature Protocol without Arbiter.	43
3.2.1.1.1. Diffie-Lamport Signature Protocol.	43
3.2.1.1.2. Rabin Signature Protocol.	50
3.2.1.1.3. Matyas-Meyer Signature Protocol.	54
3.2.1.1.4. General RSA Signature Protocol.	58
3.2.1.1.5. Lamport Signature Protocol.	59

	Page
3.2.1.1.6. Fail-Stop Signature Protocol.	60
3.2.1.2. Digital Signature Protocols with Arbiter.	61
3.2.1.2.1. Elementary Protocol with Arbiter "Based on Symmetric Cryptosystem".	61
3.2.1.2.2. Elementary Protocol with Arbiter "Based on Asymmetric Cryptosystem".	63
 CHAPTER IV: NEW DIGITAL SIGNATURE PROTOCOLS.	
Introduction.	62
4.1. DES Cipher.	62
4.1.1. Permutation Box.	63
4.1.2. Exclusive-OR Operation.	64
4.1.3. S-Box.	64
4.1.4. DES Encryption Algorithm.	65
4.1.5. DES Decryption Algorithm.	71
4.1.6. Key Scheduler.	71
4.2. RSA Cipher.	73
4.3. DES Signature Protocol.	75
4.3.1. Signature Protocol for Key.	75
4.3.2. Signature Protocol for Message.	76
4.4. RSA Signature Protocol.	78
 Appendix A: IMPLEMENTATION OF DES DIGITAL SIGNATURE PROTOCOL.	 80
 Appendix B: IMPLEMENTATION OF RSA DIGITAL SIGNATURE PROTOCOL.	 105
 REFERENCES.	 117
 ARABIC SUMMARY.	

✓

ABSTRACT

ABSTRACT

Name : *Dowlat Abed El Azzez Mohammed.*

Subject: On Problems of Authentication and Digital Signature in Cryptograph.

Place : Mathematics Department, Faculty of Science,
Ain Shams University.

Key Words: Encryption, Decryption, Plaintext, Ciphertext, Key, Cryptology, Cryptography, Cryptanalysis, Cryptanalyst, Data Security, Cryptosystem, Protocol, Authentication, Digital signature, Compression.

The main purpose of this thesis is to study the authentication and digital signature protocols. Most authentication and digital signature protocols are based on cryptosystem. So we start by discussing cryptosystem. We then discuss the authentication and digital signature problems and protocols. We also introduce two digital signature protocols.

This thesis consists of four chapters and two appendices. In Chapter I, an introduction for cryptology (cryptography and cryptanalysis) is given. This chapter also includes a study of cryptosystem and its types. In Chapter II, we discuss the authentication problems (user and message), and their solutions. In Chapter III, we study digital signature and illustrate its protocols. Finally, in Chapter IV, we introduce two digital signature protocols which are based on DES and RSA ciphers. The implementations of these protocols, in the C language, are given in the two appendices.

