Cryptography
Past, Present and Future

Imad Fakhri Taha Al Shaikhli

IIUM PRESS
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA
# TABLE OF CONTENTS

Dedication 1
Preface Vii
Acknowledgement Viii

## PART I Classical Cryptography

### Chapter One Introduction
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Nurhidayah Binti Abdul rashid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman 3-9

### Chapter Two Monoalphabetic Substitution Cipher
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Nurhidayah Binti Abdul rashid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman 11-16

### Chapter Three Polyalphabetic Substitution Cipher
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Nurhidayah Binti Abdul rashid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman 17-23

### Chapter Four Machine-Based Cryptography
- Rusydi Hasan
- Imad Fakhri Taha Al Shaikhli
- Nurhidayah Binti Abdul rashid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman 25-30

## PART II Modern Symmetric-Key Cryptography

### Chapter Five Block and Stream Cipher
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando 33-38

### Chapter Six Data Encryption Standard (DES)
- Imad Fakhri Taha Al Shaikhli 39-46
PARTIV Public Key & Digital Signature Schemes

Chapter Thirteen Rivest-Shamir-Adleman (RSA)
- Iqram Mohammed Hayek
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Kusai Abu Hilal

Chapter Fourteen Cryptanalysis of RSA
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Iqram Mohammed Hayek
- Kusai Abu Hilal

Chapter Fifteen Digital Signature Algorithm
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Iqram Mohammed Hayek
- Kusai Abu Hilal

Part V Zero-Knowledge Proof

Chapter Sixteen Background of Zero-Knowledge Proof
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juarah

Chapter Seventeen Interactive Proof Systems
- Rusydi Hasan
- Imad Fakhri Taha Al Shaikhli
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juarah

Chapter Eighteen Zero-Knowledge Proof
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juarah

Chapter Nineteen Feige-Fiat-Shamir Identification Scheme  
- Rusydi Hasan
- Imad Fakhri Taha Al Shaikhli
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juarah

Part VI Secret Sharing  

Chapter Twenty Introduction  
- Muhammad Israfil
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh

Chapter Twenty One Shamir’s Threshold Scheme  
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Muhammad Israfil

Chapter Twenty Two Blakely’s Secret Sharing Scheme  
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Israfil

Part VII Quantum Cryptography

Chapter Twenty Three Quantum Cryptography  
- Azeddine Messikh
10. Message Digest (MDx) Family

- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Khansaa Munther Abdulmajed
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

ABSTRACT

In this article we will talk about the description of Message Digest (MDx) Family. Also we will introduce into Message Digest 2 (MD2), Message Digest 4 and 5 (MD4 and MD5). Moreover, we will describe the Security of the MDx family hash function.

DESCRIPTION

According to the IETF’s memorandum in regards to MD2, MD4 and MD5, all of these algorithms take as input a message of arbitrary length and produce as output a 128-bit (16 bytes) message digest of the input. These algorithms were intended for digital signature applications where a message needs to be compressed securely before being signed with a private key under the public key cryptography such as the RSA. Despite their apparent similarities they are different in many ways. (Kaliski, 1992; Rivest, 1992)

Essentially, MD2, MD4 and MD5 all use the same mechanism. The message is divided into blocks of certain size (depending on which message digest is in use). Each block will then be processed with a compression function (see Figure 10.1). (Robshaw, 1996)