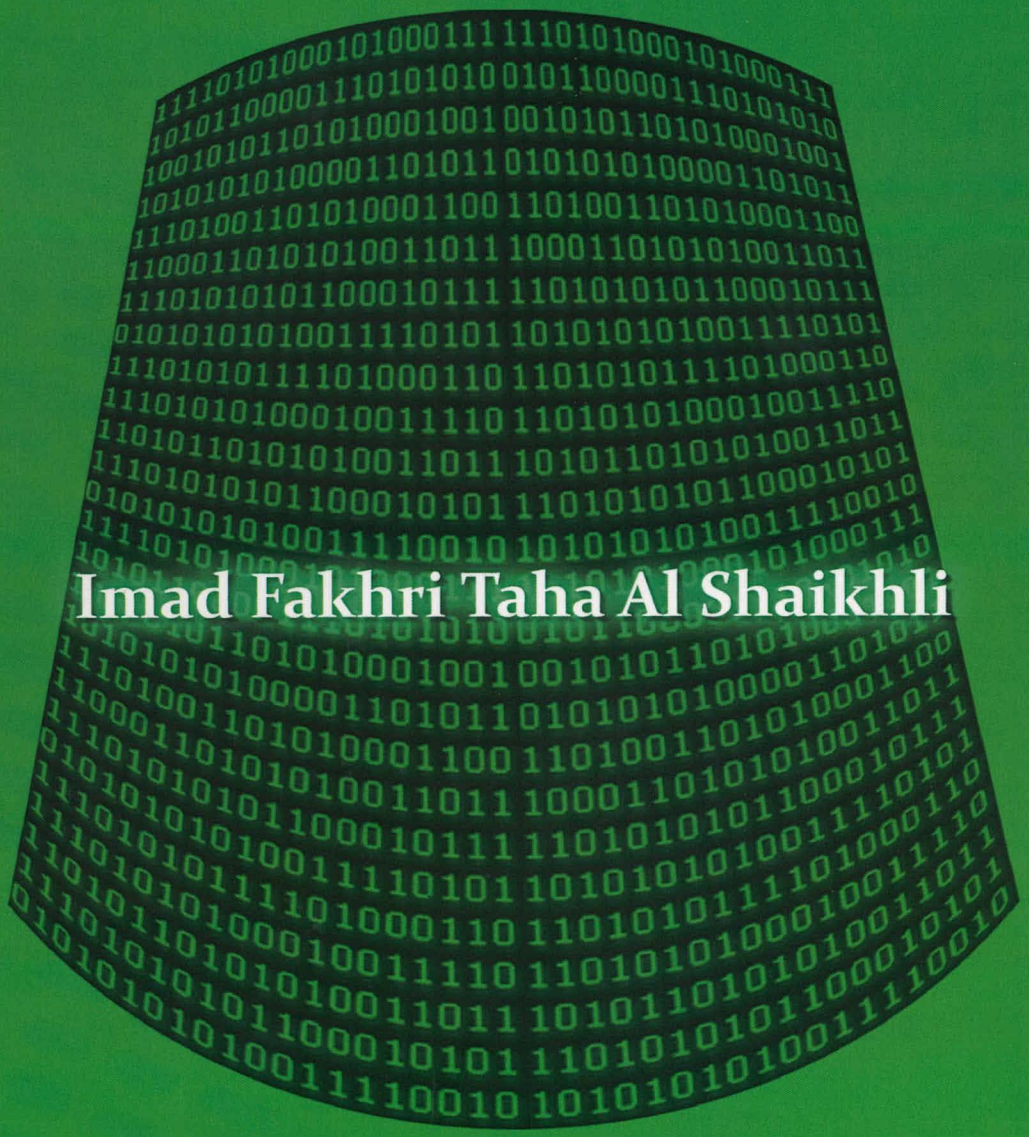
# Cryptography

## Past, Present and Future

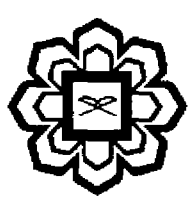


Imad Fakhri Taha Al Shaikhli

IIUM PRESS
INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

# Cryptography: Past, Present and Future

Imad Fakhri Taha Al Shaikhli



IIUM Press

Published by:

IIUM Press

International Islamic University Malaysia

First Edition, 2011



Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Imad Fakhri Taha Al-Shaikhli
Cryptography: Past, Present and Future
Imad Fakhri Taha Al-Shaikhli

ISBN: 978-967-418-091-1

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
**IIUM PRINTING SDN. BHD.**
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

# TABLE OF CONTENTS


Dedication I

Preface Vii

Acknowledgement Viii

**PART I Classical Cryptography** 1

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

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

**Chapter Three Polyalphabetic Subsitution Cipher** 17-23
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Nurhidayah Binti Abdulrashid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman

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

**PART II Modern Symmetric-Key Cryptography** 31

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

**Chapter Six Data Encryption Standard (DES)** 39-46
- Imad Fakhri Taha Al Shaikhli

- Sufyan Salim Mahmood Al Dabbagh
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

**Chapter Seven Advanced Encryption Standard(Rijndael)** 47-52
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

**Chapter Eight Trivium and Rabbit Stream Cipher** 53-61
- Imad Fakhri Taha Al Shaikhli,
- Sufyan Salim Mahmood Al Dabbagh
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

**PART III Hash Functions** 63

**Chapter Nine Introduction** 65-72
- Khanssaa Munthir Abdulmajed
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

**Chapter Ten Message Digest (MDX) Family** 73-80
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Khanssaa Munthir Abdulmajed
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

**Chapter Eleven SHA family hash function** 81-87
- Khanssaa Munthir Abdulmajed
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

**Chapter Twelve RIPEMD and Chameleon Hash Function** 89-96
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Khanssaa Munthir Abdulmajed
- Ahmad Faridi Abdul Matin

- Sibomana Hilali Hussein


**PARTIV Public Key & Digital Signature Schemes** 97

**Chapter Thirteen Rivest-Shamir-Adleman (RSA)** 99-105

- Iqram Mohammed Hayek
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Kusai Abu Hilal

**Chapter Fourteen Cryptanalysis of RSA** 107-112

- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Iqram Mohammed Hayek
- Kusai Abu Hilal

**Chapter Fifteen Digital Signature Algorithm** 113-115

- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Iqram Mohammed Hayek
- Kusai Abu Hilal

**Part V Zero-Knowledge Proof** 116

**Chapter Sixteen Background of Zero-Knowledge Proof** 117-120

- 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** 121-126

- 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** 127-132

- 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** 133-138
- Rusydi Hasan
- Imad Fakhri Taha Al Shaikhli
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juarah

**Part VI Secret Sharing** 139

**Chapter Twenty Introduction** 141-146
- Muhammad Israfil
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh

**Chapter Twenty One Shamir's Threshold Scheme** 147-150
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Muhammad Israfil

**Chapter Twenty Two Blakely's Secret Sharing Scheme** 151-155
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Muhammad Israfil

**Part VII Quantum Cryptography** 156

**Chapter Twenty Three Quantum Cryptography**
- Azeddine Messikh

# 14. Cryptanalysis of RSA


- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Iqram Mohammed Hayek
- Kusai Abu Hilal



**ABSTRACT**

In this article we will talk about the background of Rivest-Shamir-Adleman (RSA) cryptanalysis. Also we will introduce into small encryption exponent *e* for RSA, Small decryption exponent *d* for RSA. Also, we will describe common modulus attack and message concealing.


## BACKGROUND

While cryptography is the science concerned with the design of ciphers, cryptanalysis is the related study of breaking ciphers. Cryptography and cryptanalysis are somehow complimentary sciences: development in one is usually followed by further development in the other. Below we give a brief description of the main methods used to attack the RSA cryptosystem.

Two kinds of these attacks are usually distinguished.

- In an indifferent chosen-ciphertext attack, the adversary is provided with decryptions of any ciphertexts of its choice, but these ciphertexts must be chosen prior to receiving the (target) ciphertext c it actually wishes to decrypt.
- In an adaptive chosen-ciphertext attack, the adversary may use (or have access to)A's decryption machine (but not the private key itself) even after seeing the target ciphertext