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
# TABLE OF CONTENTS

Dedication  
Preface  
Acknowledgement  

## PART I Classical Cryptography

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

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

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

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

## 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  

### Chapter Six Data Encryption Standard (DES)
- Imad Fakhri Taha Al Shaikhli  

---

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedication</td>
<td>1</td>
</tr>
<tr>
<td>Preface</td>
<td>vii</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>viii</td>
</tr>
<tr>
<td>PART I Classical Cryptography</td>
<td>1</td>
</tr>
<tr>
<td>Chapter One Introduction</td>
<td>3-9</td>
</tr>
<tr>
<td>Chapter Two Monoalphabetic Substitution Cipher</td>
<td>11-16</td>
</tr>
<tr>
<td>Chapter Three Polyalphabetic Substitution Cipher</td>
<td>17-23</td>
</tr>
<tr>
<td>Chapter Four Machine-Based Cryptography</td>
<td>25-30</td>
</tr>
<tr>
<td>PART II Modern Symmetric-Key Cryptography</td>
<td>31</td>
</tr>
<tr>
<td>Chapter Five Block and Stream Cipher</td>
<td>33-38</td>
</tr>
<tr>
<td>Chapter Six Data Encryption Standard (DES)</td>
<td>39-46</td>
</tr>
</tbody>
</table>
Chapter Seven Advanced Encryption Standard (Rijndael)
- 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
- Imad Fakhri Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbagh
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

PART III Hash Functions

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

Chapter Eleven SHA family hash function
- Khanussa 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
- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Khanussa Munthir Abdulmajed
- Ahmad Faridi Abdul Matin
PARTIV Public Key & Digital Signature Schemes

Chapter Thirteen Rivest-Shamir-Adleman (RSA) 97
  - Iqram Mohammed Hayek 99-105
  - 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
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
16. 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

ABSTRACT

In this article we will talk about the background of zero-knowledge proof. Also we will introduce into motivation and historical notes.

BACKGROUND

This chapter connotes in details the concept of zero-knowledge proofs (ZKP), an interactive proof protocol in which a prover tries to convince a verifier of the existence of a proof but reveals nothing about it to the verifier. The motivation behind the creation of ZKP is the notion of proof which is also basis to people in general. Then, this part explains about interactive proof systems itself before further describes about ZKP and its variants that consists of perfect, statistical and computation zero-knowledge. Lastly, it introduces Feige-Fiat-Shamir identification scheme, the best known ZKP of identity that is lightweight and faster than public-key protocol such as RSA. It is hoped that this chapter can give a better understanding on topic of ZKP towards the reader. (Rosen, 2006)

Zero knowledge proofs were invented by Goldwasser, Micali and Rackoff in 82 (the paper appeared in FOCS 85). Zero-knowledge proofs (and interactive proofs in general, also introduced in that paper) turned out to be one of concepts in computer science, with applications