

# Cryptography

## Past, Present and Future

Imad Fakhri Taha Al Shaikhli

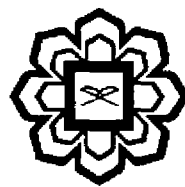


IIUM PRESS

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

# **Cryptography: Past, Present and Future**

**Imad Fakhri Taha Al Shaikhli**



IIUM Press

Published by:

IUM Press

International Islamic University Malaysia

First Edition, 2011

©IUM Press, IUM

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without any prior written permission of the publisher.

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 :

**IUM 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
<b>PART I Classical Cryptography</b>	<b>1</b>
<b>Chapter One Introduction</b>	<b>3-9</b>
- Imad Fakhri Taha Al Shaikhli	
- Rusydi Hasan	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
<b>Chapter Two Monoalphabetic Substitution Cipher</b>	<b>11-16</b>
- Imad Fakhri Taha Al Shaikhli	
- Rusydi Hasan	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
<b>Chapter Three Polyalphabetic Substitution Cipher</b>	<b>17-23</b>
- Imad Fakhri Taha Al Shaikhli	
- Rusydi Hasan	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
<b>Chapter Four Machine-Based Cryptography</b>	<b>25-30</b>
- Rusydi Hasan	
- Imad Fakhri Taha Al Shaikhli	
- Nurhidayah Binti Abdulrashid	
- Faizurimawaty Bt Padzilah	
- Nabilah Bt Abd Rahman	
<b>PART II Modern Symmetric-Key Cryptography</b>	<b>31</b>
<b>Chapter Five Block and Stream Cipher</b>	<b>33-38</b>
- Sufyan Salim Mahmood Al Dabbagh	
- Imad Fakhri Taha Al Shaikhli	
- Muhammad Fadil Lubis	
- Usman bin Mohd Azhar	
- Nopan Ziro Ando	
<b>Chapter Six Data Encryption Standard (DES)</b>	<b>39-46</b>
- Imad Fakhri Taha Al Shaikhli	

- Sufyan Salim Mahmood Al Dabbagh	
- Muhammad Fadil Lubis	
- Usman bin Mohd Azhar	
- Nopan Ziro Ando	
<b>Chapter Seven Advanced Encryption Standard(Rijndael)</b>	<b>47-52</b>
- Sufyan Salim Mahmood Al Dabbagh	
- Imad Fakhri Taha Al Shaikhli	
- Muhammad Fadil Lubis	
- Usman bin Mohd Azhar	
- Nopan Ziro Ando	
<b>Chapter Eight Trivium and Rabbit Stream Cipher</b>	<b>53-61</b>
- Imad Fakhri Taha Al Shaikhli,	
- Sufyan Salim Mahmood Al Dabbagh	
- Muhammad Fadil Lubis	
- Usman bin Mohd Azhar	
- Nopan Ziro Ando	
<b>PART III Hash Functions</b>	<b>63</b>
<b>Chapter Nine Introduction</b>	<b>65-72</b>
- Khanssaa Munthir Abdulmajed	
- Imad Fakhri Taha Al Shaikhli	
- Sufyan Salim Mahmood Al Dabbagh	
- Ahmad Faridi Abdul Matin	
- Sibomana Hilali Hussein	
<b>Chapter Ten Message Digest (MDX) Family</b>	<b>73-80</b>
- Imad Fakhri Taha Al Shaikhli	
- Sufyan Salim Mahmood Al Dabbagh	
- Khanssaa Munthir Abdulmajed	
- Ahmad Faridi Abdul Matin	
- Sibomana Hilali Hussein	
<b>Chapter Eleven SHA family hash function</b>	<b>81-87</b>
- Khanssaa Munthir Abdulmajed	
- Imad Fakhri Taha Al Shaikhli	
- Sufyan Salim Mahmood Al Dabbagh	
- Ahmad Faridi Abdul Matin	
- Sibomana Hilali Hussein	
<b>Chapter Twelve RIPEMD and Chameleon Hash Function</b>	<b>89-96</b>
- Sufyan Salim Mahmood Al Dabbagh	
- Imad Fakhri Taha Al Shaikhli	
- Khanssaa Munthir Abdulmajed	
- Ahmad Faridi Abdul Matin	

- Sibomana Hilali Hussein

<b>PARTIV Public Key &amp; Digital Signature Schemes</b>	<b>97</b>
<b>Chapter Thirteen Rivest-Shamir-Adleman (RSA)</b>	<b>99-105</b>
<ul style="list-style-type: none"> <li>- Iqram Mohammed Hayek</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Kusai Abu Hilal</li> </ul>	
<b>Chapter Fourteen Cryptanalysis of RSA</b>	<b>107-112</b>
<ul style="list-style-type: none"> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Iqram Mohammed Hayek</li> <li>- Kusai Abu Hilal</li> </ul>	
<b>Chapter Fifteen Digital Signature Algorithm</b>	<b>113-115</b>
<ul style="list-style-type: none"> <li>- Sufyan Salim Mahmood Al Dabbagh</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Iqram Mohammed Hayek</li> <li>- Kusai Abu Hilal</li> </ul>	
<b>Part V Zero-Knowledge Proof</b>	<b>116</b>
<b>Chapter Sixteen Background of Zero-Knowledge Proof</b>	<b>117-120</b>
<ul style="list-style-type: none"> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Rusydi Hasan</li> <li>- Siti Khairunnisa Mohd Bakri</li> <li>- Nur Dalilah Bt More Yusoff</li> <li>- Nur Khairunnisa Bt Juara</li> </ul>	
<b>Chapter Seventeen Interactive Proof Systems</b>	<b>121-126</b>
<ul style="list-style-type: none"> <li>- Rusydi Hasan</li> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Siti Khairunnisa Mohd Bakri</li> <li>- Nur Dalilah Bt More Yusoff</li> <li>- Nur Khairunnisa Bt Juara</li> </ul>	
<b>Chapter Eighteen Zero-Knowledge Proof</b>	<b>127-132</b>
<ul style="list-style-type: none"> <li>- Imad Fakhri Taha Al Shaikhli</li> <li>- Rusydi Hasan</li> </ul>	

- Siti Khairunnisa Mohd Bakri	
- Nur Dalilah Bt More Yusoff	
- Nur Khairunnisa Bt Juara	
<b>Chapter Nineteen Feige-Fiat-Shamir Identification Scheme</b>	<b>133-138</b>
- Rusydi Hasan	
- Imad Fakhri Taha Al Shaikhli	
- Siti Khairunnisa Mohd Bakri	
- Nur Dalilah Bt More Yusoff	
- Nur Khairunnisa Bt Juara	
<b>Part VI Secret Sharing</b>	<b>139</b>
<b>Chapter Twenty Introduction</b>	<b>141-146</b>
- Muhammad Israfil	
- Imad Fakhri Taha Al Shaikhli	
- Sufyan Salim Mahmood Al Dabbagh	
<b>Chapter Twenty One Shamir's Threshold Scheme</b>	<b>147-150</b>
- Imad Fakhri Taha Al Shaikhli	
- Sufyan Salim Mahmood Al Dabbagh	
- Muhammad Israfil	
<b>Chapter Twenty Two Blakely's Secret Sharing Scheme</b>	<b>151-155</b>
- Sufyan Salim Mahmood Al Dabbagh	
- Imad Fakhri Taha Al Shaikhli	
- Muhammad Israfil	
<b>Part VII Quantum Cryptography</b>	<b>156</b>
<b>Chapter Twenty Three Quantum Cryptography</b>	
- Azeddine Messikh	

## 18. Zero-Knowledge-Proof

- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Siti Khairunnisa Mohd Bakri
- Nur Dalilah Bt More Yusoff
- Nur Khairunnisa Bt Juara

### ABSTRACT

In this article we will talk about the background of variant of zero-knowledge proof.

Also we will introduce into perfect and statistical of zero-knowledge proof. Moreover, we will describe the Computational of zero-knowledge proof.

### BACKGROUND

Zero-Knowledge proofs are interactive proofs system  $(P, V)$  that yield nothing (to the verifier) beyond the fact that the assertion is indeed valid. Whenever  $x \in L$ , the verifier is able to generate on its own the conversations it could have had with the prover during an interactive proof of  $x \in L$ . The verifier learns nothing as the result of a conversation with the prover that it could not have learned on its own by generating the conversation itself other than the fact that  $x \in L$ . Zero-Knowledge proofs exhibit an extreme contrast between being convinced of the validity of the message and learning anything in addition (while receiving such convincing proof). A fundamental result regarding the zero-knowledge proof systems is their existence, under reasonable complexity assumptions, for any set in NP and it is presented for the Graph 3-Colorability. Suppose the prover wish to convince the verifier that a certain input graph is three-colorable, without revealing to the verifier the coloring that the prover knows. The prover can do so in a sequence of  $|E|^2$  stages, each of which goes as follows. (Micciancio, 2003)