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

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>Introduction</td>
<td>1-3</td>
</tr>
<tr>
<td></td>
<td>Imad Fakhri Taha Al Shaikhli</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rusydi Hasan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nurhidayah Binti Abdul rashid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Faizurimawaty Bt Padzilah</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nabilah Bt Abd Rahman</td>
<td></td>
</tr>
<tr>
<td>Two</td>
<td>Monoalphabetic Substitution Cipher</td>
<td>11-16</td>
</tr>
<tr>
<td></td>
<td>Imad Fakhri Taha Al Shaikhli</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rusydi Hasan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nurhidayah Binti Abdul rashid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Faizurimawaty Bt Padzilah</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nabilah Bt Abd Rahman</td>
<td></td>
</tr>
<tr>
<td>Three</td>
<td>Polyalphabetic Substitution Cipher</td>
<td>17-23</td>
</tr>
<tr>
<td></td>
<td>Imad Fakhri Taha Al Shaikhli</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rusydi Hasan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nurhidayah Binti Abdul rashid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Faizurimawaty Bt Padzilah</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nabilah Bt Abd Rahman</td>
<td></td>
</tr>
<tr>
<td>Four</td>
<td>Machine-Based Cryptography</td>
<td>25-30</td>
</tr>
<tr>
<td></td>
<td>Rusydi Hasan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Imad Fakhri Taha Al Shaikhli</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nurhidayah Binti Abdul rashid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Faizurimawaty Bt Padzilah</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nabilah Bt Abd Rahman</td>
<td></td>
</tr>
</tbody>
</table>

## PART II Modern Symmetric-Key Cryptography

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Five</td>
<td>Block and Stream Cipher</td>
<td>33-38</td>
</tr>
<tr>
<td></td>
<td>Sufyan Salim Mahmood Al Dabbagh</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Imad Fakhri Taha Al Shaikhli</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Muhammad Fadil Lubis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Usman bin Mohd Azhar</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Nopan Ziro Ando</td>
<td></td>
</tr>
<tr>
<td>Six</td>
<td>Data Encryption Standard (DES)</td>
<td>39-46</td>
</tr>
<tr>
<td></td>
<td>Imad Fakhri Taha Al Shaikhli</td>
<td></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
- Khanssa Muthir 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
- Khanssa Muthir Abdulmajed
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

Chapter Eleven SHA family hash function
- Khanssa Muthir 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
- Khanssa Muthir Abdulmajed
- Ahmad Faridi Abdul Matin
PART IV 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
Chapter Nineteen Feige-Fiatt-Shamir Identification Scheme
- Rasydi Hasn
- 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
6. Data Encryption Standard (DES)

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

ABSTRACT

In this article we will talk about the background of Data Encryption Standard (DES), description of DES and how we will encrypt the plaintext and decrypt the cipher text using that cipher. Also we will introduce into mode of operation of DES and the cryptanalysis of DES.

DESCRIPTION OF DES

Data Encryption Standard DES is a Feistel-type Substitution-Permutation Network (SPN) cipher, specified in FIPS PUB 46. The result of a 1970s effort to produce a U.S encryption standard. DES is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. There are 72,000,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. The key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. A 16 cycle Feistel system is used, with an overall 56-bit key permuted into 16 48-bit subkeys, one for each cycle. To decrypt, the identical algorithm is used, but the order of