Cryptography: Past, Present and Future

Imad Fakhri Taha Al Shaikhli

IIUM Press
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Dedication</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>vii</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>viii</td>
</tr>
<tr>
<td><strong>PART I Classical Cryptography</strong></td>
<td>1</td>
</tr>
<tr>
<td>Chapter One Introduction</td>
<td>3-9</td>
</tr>
<tr>
<td>- Imad Fakhri Taha Al Shaikhli</td>
<td>11-16</td>
</tr>
<tr>
<td>- Rusydi Hasan</td>
<td></td>
</tr>
<tr>
<td>- Nurhidayah Binti Abdulrashid</td>
<td></td>
</tr>
<tr>
<td>- Faizurimawaty Bt Padzilah</td>
<td></td>
</tr>
<tr>
<td>- Nabilah Bt Abd Rahman</td>
<td></td>
</tr>
<tr>
<td>Chapter Two Monoalphabetic Substitution Cipher</td>
<td>11-16</td>
</tr>
<tr>
<td>- Imad Fakhri Taha Al Shaikhli</td>
<td></td>
</tr>
<tr>
<td>- Rusydi Hasan</td>
<td></td>
</tr>
<tr>
<td>- Nurhidayah Binti Abdulrashid</td>
<td></td>
</tr>
<tr>
<td>- Faizurimawaty Bt Padzilah</td>
<td></td>
</tr>
<tr>
<td>- Nabilah Bt Abd Rahman</td>
<td></td>
</tr>
<tr>
<td>Chapter Three Polyalphabetic Substitution Cipher</td>
<td>17-23</td>
</tr>
<tr>
<td>- Imad Fakhri Taha Al Shaikhli</td>
<td></td>
</tr>
<tr>
<td>- Rusydi Hasan</td>
<td></td>
</tr>
<tr>
<td>- Nurhidayah Binti Abdulrashid</td>
<td></td>
</tr>
<tr>
<td>- Faizurimawaty Bt Padzilah</td>
<td></td>
</tr>
<tr>
<td>- Nabilah Bt Abd Rahman</td>
<td></td>
</tr>
<tr>
<td>Chapter Four Machine-Based Cryptography</td>
<td>25-30</td>
</tr>
<tr>
<td>- Rusydi Hasan</td>
<td></td>
</tr>
<tr>
<td>- Imad Fakhri Taha Al Shaikhli</td>
<td></td>
</tr>
<tr>
<td>- Nurhidayah Binti Abdulrashid</td>
<td></td>
</tr>
<tr>
<td>- Faizurimawaty Bt Padzilah</td>
<td></td>
</tr>
<tr>
<td>- Nabilah Bt Abd Rahman</td>
<td></td>
</tr>
<tr>
<td><strong>PART II Modern Symmetric-Key Cryptography</strong></td>
<td>31</td>
</tr>
<tr>
<td>Chapter Five Block and Stream Cipher</td>
<td>33-38</td>
</tr>
<tr>
<td>- Sufyan Salim Mahmood Al Dabbagh</td>
<td></td>
</tr>
<tr>
<td>- Imad Fakhri Taha Al Shaikhli</td>
<td></td>
</tr>
<tr>
<td>- Muhammad Fadil Lubis</td>
<td></td>
</tr>
<tr>
<td>- Usman bin Mohd Azhar</td>
<td></td>
</tr>
<tr>
<td>- Nopan Ziro Ando</td>
<td></td>
</tr>
<tr>
<td>Chapter Six Data Encryption Standard (DES)</td>
<td>39-46</td>
</tr>
<tr>
<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
- Khunssaa 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
- Khunssaa Munthir Abdulmajed
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

Chapter Eleven SHA family hash function
- Khunssaa 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
- Khunssaa Munthir Abdulmajed
- Ahmad Faridi Abdul Matin
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 133-138
- Rasydi 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
3. Polyalphabetic Substitution Cipher

- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Nurhidayah Binti Abdulrahid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman

ABSTRACT

In this article we will talk about the history of polyalphabetic substitution cipher and how the people were encrypt the plaintext and decrypt the cipher text using that cipher. Also we will introduce into Vigenere Cipher and Autokey Cipher.

BACKGROUND

A polyalphabetic substitution cipher is any cipher based on substitution. It is used to harden the monoalphabetic substitution where it uses more than one alphabet and does switching between the alphabets systematically (Cornell, 2004). With this method, frequency analysis will no longer work the same way as the previous method. The Alberti cipher by Leon Battista Alberti around 1467 was believed to be the first polyalphabetic cipher. Alberti used a mixed alphabet to encrypt a message, but whenever he wanted to he would switch to a different alphabet, indicating that he had done so by including an uppercase letter or a number in the cryptogram. For this encipherment Alberti used a decoder device, his cipher disk, which implemented a polyalphabetic substitution with mixed alphabets. Although Alberti is usually considered the father of polyalphabetic cipher, it has been claimed that polyalphabetic ciphers