Cryptography: Past, Present and Future

Imad Fakhri Taha Al Shaikhli

IIUM Press
TABLE OF CONTENTS

Dedication I
Preface Vii
Acknowledgement Viili

PART I Classical Cryptography 1

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

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

Chapter Three Polyalphabetic Substitution Cipher 17-23
- Imad Fakhri Taha Al Shaikhli
- Rusydi Hasan
- Nurhidayah Binti Abdul rashid
- Faizurimawaty Bt Padzilah
- Nabilah Bt Abd Rahman

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

PART II Modern Symmetric-Key Cryptography 31

Chapter Five Block and Stream Cipher 33-38
- Sufyan Salim Mahmoud 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
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
- Khansaa Munthur 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
- Khansaa Munthur Abdulmajed
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

Chapter Eleven SHA family hash function
- Khansaa Munthur 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
- Khansaa Munthur Abdulmajed
- Ahmad Faridi Abdul Matin
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Authors</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thirteen</td>
<td>Rivest-Shamir-Adleman (RSA)</td>
<td>Iqram Mohammed Hayek, Imad Fakhri Taha Al Shaikhli, Sufyan Salim Mahmood Al Dabbagh, Kusai Abu Hilal</td>
<td>99-105</td>
</tr>
<tr>
<td>Fourteen</td>
<td>Cryptanalysis of RSA</td>
<td>Imad Fakhri Taha Al Shaikhli, Sufyan Salim Mahmood Al Dabbagh, Iqram Mohammed Hayek, Kusai Abu Hilal</td>
<td>107-112</td>
</tr>
<tr>
<td>Fifteen</td>
<td>Digital Signature Algorithm</td>
<td>Sufyan Salim Mahmood Al Dabbagh, Imad Fakhri Taha Al Shaikhli, Iqram Mohammed Hayek, Kusai Abu Hilal</td>
<td>113-115</td>
</tr>
<tr>
<td>Part V</td>
<td>Zero-Knowledge Proof</td>
<td></td>
<td>116</td>
</tr>
<tr>
<td>Sixteen</td>
<td>Background of Zero-Knowledge Proof</td>
<td>Imad Fakhri Taha Al Shaikhli, Rusydi Hasan, Siti Khairunnisa Mohd Bakri, Nur Dalilah Bt More Yusoff, Nur Khairunnisa Bt Juarah</td>
<td>117-120</td>
</tr>
<tr>
<td>Seventeen</td>
<td>Interactive Proof Systems</td>
<td>Rusydi Hasan, Imad Fakhri Taha Al Shaikhli, Siti Khairunnisa Mohd Bakri, Nur Dalilah Bt More Yusoff, Nur Khairunnisa Bt Juarah</td>
<td>121-126</td>
</tr>
<tr>
<td>Eighteen</td>
<td>Zero-Knowledge Proof</td>
<td>Imad Fakhri Taha Al Shaikhli, Rusydi Hasan</td>
<td>127-132</td>
</tr>
</tbody>
</table>
- 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
12. RIPEMD and Chameleon Hash Function

- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Khansaa Munthir Abdulmajeed
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

ABSTRACT

In this article we will talk about the description of RIPEMD and Chameleon Hash Function. Also we will introduce into RIPEMD, RIPEMD-160 and their security. Also, we will talk about the Chameleon digital signatures property, Process of Chameleon hash function and the security of Chameleon hash function.

BACKGROUND OF RIPEMD

RIPEMD (Race Integrity Primitives Evaluation) hash value algorithm that was based on the implementation of MD4. Due to its weakness, improved versions were designed Preneel (1997). The most popular of which is RIPEMD-160. Other versions were developed, notably: RIPEMD-128, RIPEMD-256, RIPEMD-512. RIPEMD is considered as the first algorithm to efficiently use the 32-bit processors that were in use at that time.

One unique technique that the RIPEMD uses is that it uses two parallel versions of MD4 in its compression function. The two versions of MD4 used in the compression function only differ in round constants used by each MD4 version. At the ending the compression function, the words of right and left halves of the MD4 are added.