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      | 3-9 |
| - Imad Fakhri Taha Al Shaikhli |  
| - Rusydi Hasan                |  
| - Nurhidayah Binti Abdulrashid|  
| - Faizurimawaty Bt Padzilah  |  
| - Nabilah Bt Abd Rahman       |  
| Chapter Two Monoalphabetic Substitution Cipher | 11-16 |
| - Imad Fakhri Taha Al Shaikhli |  
| - Rusydi Hasan                |  
| - Nurhidayah Binti Abdulrashid|  
| - Faizurimawaty Bt Padzilah  |  
| - Nabilah Bt Abd Rahman       |  
| Chapter Three Polyalphabetic Substitution Cipher | 17-23 |
| - Imad Fakhri Taha Al Shaikhli |  
| - Rusydi Hasan                |  
| - Nurhidayah Binti Abdulrashid|  
| - Faizurimawaty Bt Padzilah  |  
| - Nabilah Bt Abd Rahman       |  
| Chapter Four Machine-Based Cryptography | 25-30 |
| - Rusydi Hasan                |  
| - Imad Fakhri Taha Al Shaikhli |  
| - Nurhidayah Binti Abdulrashid|  
| - Faizurimawaty Bt Padzilah  |  
| - Nabilah Bt Abd Rahman       |  

| PART II Modern Symmetric-Key Cryptography | 31 |
| Chapter Five Block and Stream Cipher | 33-38 |
| - 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) | 39-46 |
| - Imad Fakhri Taha Al Shaikhli    |  

Chapter Seven Advanced Encryption Standard (Rijndael)
- Suyan 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
- Suyan Salim Mahmood Al Dabbagh
- Muhammad Fadil Lubis
- Usman bin Mohd Azhar
- Nopan Ziro Ando

PART III Hash Functions

Chapter Nine Introduction
- Khansaa Muthir Abdulmajed
- Imad Fakhri Taha Al Shaikhli
- Suyan Salim Mahmood Al Dabbagh
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

Chapter Ten Message Digest (MDX) Family
- Imad Fakhri Taha Al Shaikhli
- Suyan Salim Mahmood Al Dabbagh
- Khansaa Muthir Abdulmajed
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

Chapter Eleven SHA family hash function
- Khansaa Muthir Abdulmajed
- Imad Fakhri Taha Al Shaikhli
- Suyan Salim Mahmood Al Dabbagh
- Ahmad Faridi Abdul Matin
- Sibomana Hilali Hussein

Chapter Twelve RIPEMD and Chameleon Hash Function
- Suyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Khansaa Muthir 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
- 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 Dabbag

Chapter Twenty One Shamir's Threshold Scheme 147-150
- Imad FakhrI Taha Al Shaikhli
- Sufyan Salim Mahmood Al Dabbag
- Muhammad Israfil

Chapter Twenty Two Blakely's Secret Sharing Scheme 151-155
- Sufyan Salim Mahmood Al Dabbag
- Imad FakhrI Taha Al Shaikhli
- Muhammad Israfil

Part VII Quantum Cryptography 156

Chapter Twenty Three Quantum Cryptography
- Azeddine Messikh
15. Digital Signature Algorithm

- Sufyan Salim Mahmood Al Dabbagh
- Imad Fakhri Taha Al Shaikhli
- Iqram Mohammed Hayek
- Kusai Abu Hilel

ABSTRACT

In this article we will talk about the background of digital signature algorithm. Also we will introduce into key generation and signing. Also, we will describe how to verifying with DSA and cryptanalysis of DSA.

BACKGROUND

Digital signature is actually a mathematical scheme to show if the digital message is authentic or not. We want to make sure that the message was created by a known sender, and wasn't modified while transferring. (Kleinjung, 2007)

The most widely used algorithm for digital signature is known as Digital Signature Algorithm (DSA), which is an United States Federal Government Standard for digital signatures. It was proposed in 1991 by NIST. DSA is actually a variant of ElGamal signature scheme, which was created by Egyptian cryptographer Taher Elgamal. He published his idea in 1985, in his paper named "A Public key Cryptosystem and a Signature Scheme Based on Discrete Logarithms" (Kleinjung, 2007)

Digital Signature Algorithm uses Secure Hash Algorithm (SHA-1). This algorithm has been revised in 1993 in response to public feedback concerning the security of the scheme (Stallings, 2005). Digital Signature Algorithm cannot be used for encryption or key exchange,