Companion to Information Security

Zubair Abid (20171076)

April 2020

Contents

1 Introduction **6**
- 1.1 What is Information Security about? . . . 6
- 1.2 The Language of Cryptography . . . 6
- 1.3 Modern Cryptography . . . 6
- 1.4 General goals of Information Security . . . 6

2 The Origins of Modern Cryptography **6**
- 2.1 The Caesar Cipher . . . 6
- 2.2 Shift Ciphers . . . 6
- 2.3 Monoalphabetic Substitution Cipher . . . 6
- 2.4 Polyalphabetic Substitution Cipher . . . 6
- 2.5 Brute force over the key space . . . 6
- 2.6 Frequency Analysis . . . 6
- 2.7 Frequency Attacks . . . 6
- 2.8 Kerckhoff's Principle . . . 6
- 2.9 Requirements for an unbreakable cipher . . . 6
- 2.10 Shannon's Perfect Secrecy . . . 6
- 2.11 One time pad . . . 6

3 Mathematical Background **6**
- 3.1 Prime numbers . . . 6
- 3.2 Primality Testing . . . 6
- 3.3 Factoring Algorithms . . . 6
- 3.4 Modular Arithmetic . . . 6
- 3.5 Groups . . . 6
- 3.6 Cyclic Groups . . . 6
- 3.7 Elliptic Curve Groups . . . 6
- 3.8 Rings . . . 6
- 3.9 Fields . . . 6
- 3.10 Finite Fields . . . 6
- 3.11 Fermat's Little Theorem . . . 6
- 3.12 Turing Machines . . . 6
- 3.13 Oracles . . . 6

4 Cryptographic Concepts **6**
4.1 Adversary . . . 6
4.2 Birthday Attack . . . 6
4.3 Bit-commitment . . . 6
4.4 CBCMAC . . . 6
4.5 CCA Security . . . 6
4.6 Channel . . . 6
4.7 Chosen Ciphertext Attack (CCA) . . . 6
4.8 Chosen Plaintext Attack (CPA) . . . 6
4.9 Cipher . . . 6
4.10 Cipher Block Chaining (CBC) . . . 6
4.11 Ciphertext-only security . . . 6
4.12 Collision Resistance . . . 6
4.13 CPA Security . . . 6
4.14 Decisional Diffie-Helman (DDH) Assumption . . . 6
4.15 Decryption . . . 6
4.16 Diffie-Helman Key Exchange . . . 6
4.17 Digital Signature . . . 6
4.18 Discrete Logarithm Problem . . . 6
4.19 Encryption Schemes . . . 6
4.20 Entropy . . . 6
4.21 Expectation . . . 6
4.22 Feistel Structures . . . 6
4.23 General Access Structure . . . 6
4.24 Hard-core predicate . . . 6
4.25 Hash and Sign paradigm . . . 6
4.26 Hash Functions . . . 6
4.27 Heuristic Security . . . 6
4.28 Interactive Digital Signature . . . 6
4.29 Interactive Proofs . . . 6
4.30 Least and most significant bit . . . 6
4.31 Message Authentication Codes (MAC) . . . 6
4.32 Modes of Operation of Encryption . . . 6
4.33 Negligible Functions . . . 6
4.34 Nonce . . . 6
4.35 Oblivious Transfer . . . 6
4.36 One-way Functions . . . 6
4.37 Oracle Function . . . 6
4.38 Output Feedback Mode (OFB) . . . 6
4.39 Perfect Secrecy . . . 6
4.40 PKCS v1.5 . . . 6
4.41 Probabilistic Encryption . . . 6
4.42 Probabilistic Polynomial Turing Machine (PPTM) . . . 6
4.43 Provably secure RSA: RSA-OAEP . . . 6
4.44 Private Key . . . 6
4.45 Pseudo-random generators . . . 6

4.46 Pseudo-random functions 6
4.47 Pseudo-random permutations 6
4.48 Public Key 6
4.49 Public Key Cryptography 6
4.50 Random Oracle Model 6
4.51 Randomized Counter Mode (RCM) 6
4.52 RSA 6
4.53 Secret Sharing 6
4.54 Secure Channel Capacity 6
4.55 Secure Two-Channel Communication 6
4.56 Symmetric Key Cryptography 6
4.57 Trapdoor one-way Functions 6
4.58 Trusted Third Party 6
4.59 Zero Knowledge Proofs (ZKP) 6

5 Theorems and Schemes **6**
5.1 Defining Schemes for Cryptography 6
5.2 Shannon's theory of Perfect Secrecy 6
5.3 One-time pads are perfectly secret 6
5.4 Every perfectly secret scheme is isomorphic to the one-time pad . 6
5.5 Perfectly secret schemes need —m— sized key 6
5.6 Relaxations to Perfect Secrecy 6
5.7 Existence of one-way functions implies P!=NP 6
5.8 Ciphertext-only security exists iff one way functions exist 6
5.9 Arbitrary expansion pseudo-random generators exist iff one way functions exist 6
5.10 Using the Discrete Logarithm Problem as a one way function . . 6
5.11 MSB of DLP is a hardcore predicate 6
5.12 No deterministic scheme is CPA-secure 6
5.13 Pseudo-random functions exist iff Pseufo-random generators exist 6
5.14 CPA-secure encryption schemes can be built from OWFs 6
5.15 Data Encryption Standard (DES) 6
5.16 Advanced Encryption Standard (AES) 6
5.17 Merkle-Damgard transform 6
5.18 Designing a MAC from Pseudo-random functions 6
5.19 Using MAC to build a CCA-secure scheme 6
5.20 Collision-resistant hash functions 6
5.21 Designing hash functions from DLP 6
5.22 Diffie-Helman Key Exchange 6
5.23 El-Gamal Public Key Cryptography 6
5.24 RSA Public Key Cryptography 6
5.25 Textbook RSA is not CPA-secure 6
5.26 Constructing a digital signature from RSA 6
5.27 Constructing a bit-commitment scheme from one-way permutations 6
5.28 Oblivious transfer problem 6
5.29 Bit-commitment scheme using oblivious transfer 6

5.30 Bit-commitment is NP-Complete 6
5.31 Building an interactive digital signature based on DLP 6
5.32 Building a digital signature based on DLP 6
5.33 Shamir's Secret Sharing scheme 6
5.34 Decentralised ledgers using OWFs 6

6 Notable Cryptographers **6**
6.1 Al-Khalil ibn Ahmad al-Farahidi 6
6.2 Augustus the Younger 6
6.3 Ibn 'Adlan 6
6.4 Francesco I Gonzaga 6
6.5 Ibn al-Durayhim 6
6.6 Ahmad al-Qalqashandi 6
6.7 Ibn Wahshiyya 6
6.8 Giovanni Battista della Porta 6
6.9 Étienne Bazeries 6
6.10 Friedrich Kasiski 6
6.11 Charles Babbage 6
6.12 Auguste Kerckhoffs 6
6.13 Elizebeth Smith Friedman 6
6.14 Jack Good 6
6.15 Nigel de Grey 6
6.16 Alan Turing 6
6.17 William Thomas Tutte 6
6.18 Gottfried Köthe 6
6.19 Helmut Grunsky 6
6.20 Oswald Teichmüller 6
6.21 Claude Shannon 6
6.22 Ross Anderson 6
6.23 Paulo S. L. M. Barreto 6
6.24 George Blakley 6
6.25 Don Coppersmith 6
6.26 Joan Daemen 6
6.27 Horst Feistel 6
6.28 Ralph Merkle 6
6.29 Bart Preneel 6
6.30 Vincent Rijmen 6
6.31 Ronald L. Rivest 6
6.32 Adi Shamir 6
6.33 Leonard Adleman 6
6.34 Whitfield Diffie 6
6.35 Martin Hellman 6
6.36 Clifford Cocks 6
6.37 Taher Elgamal 6
6.38 Shafi Goldwasser 6
6.39 Alfred Menezes 6

6.40 Victor Miller . . . 6
6.41 David Naccache . . . 6
6.42 Pascal Paillier . . . 6
6.43 Michael O. Rabin . . . 6
6.44 Moti Yung . . . 6
6.45 Niels Ferguson . . . 6
6.46 Mitsuru Matsui . . . 6
6.47 David Wagner . . . 6
6.48 Alex Biryukov . . . 6
6.49 Gilles Brassard . . . 6
6.50 Oded Goldreich . . . 6
6.51 Oded Regev . . . 6
6.52 Phillip Rogaway . . . 6
6.53 Srinathan Kannan . . . 6
6.54 Amit Deshpande . . . 6
6.55 Satya Lokam . . . 6
6.56 Manoj M. Prabhakaran . . . 6

7 The influence of Cryptography **6**
7.1 Secure end-to-end communication on the internet . . . 6
7.1.1 Banking Activities . . . 6
7.1.2 Military Use . . . 6
7.1.3 Secure corporate communication . . . 6
7.2 Application on Data Integrity . . . 6
7.3 Blockchains . . . 6
7.4 Cryptocurrencies . . . 6
7.5 Techniques from cryptography are used in other fields . . . 6

8 Final Perspectives **6**
8.1 Cryptography is Fascinating, Fantastic, and Fundamental . . . 6
8.2 Cryptographic thinking . . . 6
8.3 Research Areas in Cryptography . . . 6
8.4 A crisis in Crpytography . . . 6