Principles of Information Security

Evaluation IV: reading and organization assignment

Abhigyan Ghosh
20171089

My Companion to Cryptography

1. Classical Cryptography
    1.1. Simple Cryptosystems
        1.1.1. The Shift Cipher
        1.1.2. The Substitution Cipher
        1.1.3. The Affine Cipher
        1.1.4. The Vignere Cipher
        1.1.5. The Hill Cipher
        1.1.6. The Permutation CIpher
        1.1.7. Stream CIphers
2. Origin of Modern Cryptography
    2.1. The Basic Principles of Modern Cryptography
        2.1.1. Principle 1 – Formulation of Exact Definitions
        2.1.2. Principle 2 – Reliance on Precise Assumptions
        2.1.3. Principle 3 – Rigorous Proofs of Security
    2.2. Shanon's Secrecy
        2.2.1. Encryption and Secrecy
        2.2.2. The Objectives of Cryptography
        2.2.3. Entropy
        2.2.4. Attacks
        2.2.5. Cryptographic Protocols
        2.2.6. Provable Security
3. Mathematical Concepts
    3.1. Basic Number Theory
        3.1.1. Integers
        3.1.2. Residues
        3.1.3. The Chinese Remainder Theorem
        3.1.4. Polynomials and Finite Fields
            3.1.4.1. The Ring of Polynomials
            3.1.4.2. Residue Class Rings
            3.1.4.3. Finite Fields
        3.1.5. Solving Quadratic Equations in Binary Fields
        3.1.6. Quadratic Residues
        3.1.7. The Group Z_n^*
        3.1.8. Elliptic Curves
            3.1.8.1. Plane Curves

4. Private-Key (Symmetric) Cryptography
    - 4.1. Private-Key Encryption and Pseudorandomness
        - 4.1.1. A Computational Approach to Cryptography
            - 4.1.1.1. The Basic Idea of Computational Security
            - 4.1.1.2. Efficient Algorithms and Negligible Success
            - 4.1.1.3. Proofs by Reduction
        - 4.1.2. A Definition of Computationally Secure Encryption
            - 4.1.2.1. A Definition of Security for Encryption
            - 4.1.2.2. Properties of the Definition
        - 4.1.3. Constructing Secure Encryption Schemes
            - 4.1.3.1. A Secure Fixed-Length Encryption Scheme
            - 4.1.3.2. Handling Variable-Length Messages
            - 4.1.3.3. Stream Ciphers and Multiple Encryptions
        - 4.1.4. Security under Chosen-Plaintext Attacks (CPA)
        - 4.1.5. Constructing CPA-Secure Encryption Schemes
            - 4.1.5.1. Pseudorandom Functions
            - 4.1.5.2. CPA-Secure Encryption Schemes from Pseudorandom Functions
            - 4.1.5.3. Pseudorandom Permutations and Block Ciphers
            - 4.1.5.4. Modes of Operation
        - 4.1.6. Security Against Chosen-Ciphertext Attacks (CCA)
    - 4.2. Message Authentication Codes and Collision-Resistant Hash Functions
        - 4.2.1. Secure Communication and Message Integrity
        - 4.2.2. Encryption and Message Authentication
        - 4.2.3. Message Authentication Codes – Definitions
        - 4.2.4. Constructing Secure Message Authentication Codes
        - 4.2.5. CBC-MAC
        - 4.2.6. Collision-Resistant Hash Functions
            - 4.2.6.1. Defining Collision Resistance
            - 4.2.6.2. Weaker Notions of Security for Hash Functions
            - 4.2.6.3. A Generic "Birthday" Attack
            - 4.2.6.4. The Merkle-Damgård Transform
            - 4.2.6.5. Collision-Resistant Hash Functions in Practice
        - 4.2.7. NMAC and HMAC
            - 4.2.7.1. Nested MAC (NMAC)
            - 4.2.7.2. HMAC
        - 4.2.8. Achieving Chosen-Ciphertext Secure Encryption
        - 4.2.9. Obtaining Privacy and Message Authentication

5. Public-Key (Asymmetric) Cryptography
    - 5.1. Private-Key Management and the Public-Key Revolution
        - 5.1.1. Limitations of Private-Key Cryptography
            - 5.1.1.1. The Key-Management Problem
            - 5.1.1.2. Key Distribution Centers
        - 5.1.2. The Public-Key Revolution
        - 5.1.3. Diffie-Hellman Key Exchange