

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. Shannon'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 \mathbb{Z}_n^*
- 3.1.8. Elliptic Curves
 - 3.1.8.1. Plane Curves

- 3.1.8.2. Normal Forms of Elliptic Curves
 - 3.1.8.3. Point Addition on Elliptic Curves
 - 3.1.8.4. Group Order and Group Structure of Elliptic Curves
- 3.2. Basic Probability Theory
 - 3.2.1. Finite Probability Spaces and Random Variables
 - 3.2.2. Birthday Paradox
 - 3.2.2.1. Collision bounds
 - 3.2.2.2. Simple Distinguisher
- 3.3. Basic Information Theory
 - 3.3.1. Huffman Encodings
- 3.4. Probabilistic Algorithms
 - 3.4.1. Coin Tossing Algorithms
 - 3.4.2. Monte Carlo and Las Vegas Algorithms
- 3.5. Discrete Logarithm
 - 3.5.1. Shank's Algorithm
 - 3.5.2. The Pollard Rho Discrete Logarithm Algorithm
 - 3.5.3. The Pohling-Hellman Algorithm
 - 3.5.4. The Index Calculus Method
- 3.6. Modular Squaring
 - 3.6.1. Square Roots Modulo n
 - 3.6.2. Factoring Algorithms
 - 3.6.2.1. The Pollard $p-1$ algorithm
 - 3.6.2.2. The Pollard Rho Algorithm
 - 3.6.2.3. Dixon's Random Squares Algorithm
- 3.7. Primality Testing
 - 3.7.1. Legendre and Jacobi Symbols
 - 3.7.2. The Solovay-Strassen Algorithm
 - 3.7.3. The Miller-Rabin Algorithm
- 3.8. Theoretical Constructions of Pseudorandom Objects
 - 3.8.1. One Way Functions
 - 3.8.1.1. Definitions
 - 3.8.1.2. Candidates
 - 3.8.1.3. Hard-Core Predicates
 - 3.8.2. Overview of Constructions
 - 3.8.3. Hard-Core Predicates from Every One-Way Function
 - 3.8.4. Constructions of Pseudorandom Generators
 - 3.8.4.1. Pseudorandom Generators with Minimal Expansion
 - 3.8.4.2. Increasing the Expansion Factor
 - 3.8.5. Constructions of Pseudorandom Functions
 - 3.8.6. Constructions of Pseudorandom Permutations
 - 3.8.7. Private-Key Cryptography – Necessary and Sufficient Assumptions
- 3.9. Computational Indistinguishability
 - 3.9.1. Pseudorandomness and Pseudorandom Generators
 - 3.9.2. Multiple Samples

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

5.2. Public-Key Encryption

5.2.1. Overview

5.2.2. Definitions

5.2.2.1. Security against Chosen-Plaintext Attacks

5.2.2.2. Security for Multiple Encryptions

5.2.3. Hybrid Encryption

5.2.4. RSA Encryption

5.2.4.1. “Textbook RSA” and its Insecurity

5.2.4.2. Attacks on RSA

5.2.4.3. Padded RSA

5.2.5. The El Gamal Encryption Scheme

5.2.6. Chosen-Ciphertext Attacks

5.2.7. Trapdoor Permutations and Public-Key Encryption

5.2.7.1. Trapdoor Permutations

5.2.7.2. Public-Key Encryption from Trapdoor Permutations

5.3. Additional Public-Key Encryption Schemes

5.3.1. The Goldwasser-Micali Encryption Scheme

5.3.1.1. Quadratic Residues Modulo a Prime

5.3.1.2. Quadratic Residues Modulo a Composite

5.3.1.3. The Quadratic Residuosity Assumption

5.3.1.4. The Goldwasser-Micali Encryption Scheme

5.3.2. The Rabin Encryption Scheme

5.3.2.1. Computing Modular Square Roots

5.3.2.2. A Trapdoor Permutation based on Factoring

5.3.2.3. The Rabin Encryption Scheme

5.3.3. The Paillier Encryption Scheme

5.3.3.1. The Structure of $\mathbb{Z}_{N^2}^*$

5.3.3.2. The Paillier Encryption Scheme

5.3.3.3. Homomorphic Encryption

5.4. Public-Key Cryptosystems in the Random Oracle Model

5.4.1. The Random Oracle Methodology

5.4.2. Public-Key Encryption in the Random Oracle Model

5.4.2.1. Security against Chosen-Plaintext Attacks

5.4.2.2. Security Against Chosen-Ciphertext Attacks

5.4.2.3. OAEP

5.4.3. RSA Signatures in the Random Oracle Model

6. Cryptographers

7. Applications of Modern Cryptography

7.1. Pseudorandom Objects in Practice: Block Ciphers

7.1.1. Substitution-Permutation Networks

7.1.2. Feistel Networks

7.1.3. DES – The Data Encryption Standard

7.1.3.1. The Design of DES

7.1.3.2. Attacks on Reduced-Round Variants of DES

- 7.1.3.3. The Security of DES
 - 7.1.4. Increasing the Key Size for Block Ciphers
 - 7.1.5. AES – The Advanced Encryption Standard
 - 7.1.6. Differential and Linear Cryptanalysis
 - 7.1.7. Stream Ciphers from Block Ciphers
- 7.2. Digital Signature Schemes
 - 7.2.1. Digital Signatures – An Overview
 - 7.2.2. Definitions
 - 7.2.3. RSA Signatures
 - 7.2.3.1. “Textbook RSA” and its Insecurity
 - 7.2.3.2. Hashed RSA
 - 7.2.4. The “Hash-and-Sign” Paradigm
 - 7.2.5. Lamport’s One-Time Signature Scheme
 - 7.2.6. * Signatures from Collision-Resistant Hashing
 - 7.2.6.1. “Chain-Based” Signatures
 - 7.2.6.2. “Tree-Based” Signatures
 - 7.2.7. Certificates and Public-Key Infrastructures