暨南大學
JINAN UNIVERSITY

Notes for the Final Exam

Time and Address

- **Closed-book Exam**
  - **Time:** 10:20am~12:10pm on (Friday) July 5th, 2024
  - **Address:** N233
- **Tutorial time (答疑时间)**
  - 10:30am-12:00pm on 06/26/2024 (Wednesday)
  - N416

Questions

- 1. Blank Filling 10%
- 2. Multiple Choice 20%
- 3. True-False 20%
- 4. Computations 15%
- 5. Algorithms 20%
- 6. Proofs 15%

Key Points of Review

- **Please review key points from:**
  - **Slides**
  - **Homeworks**
  - **Mid-term exercises**
  - **Textbook**

Ch2 The Classical Cryptography

1. **Famous ciphers in the history**
   - **Spartan Scytale cipher, Caesar Cipher, Enigma Machine, ...**
2. **The Substitution Cipher: The Shift/Affine/Vigenere/Hill Cipher**
   - **The size of key space**
   - **The Affine cipher over Z_{26} and Z_m**
   - **The monoalphabetic and polyalphabetic cryptosystem**
3. **The Permutation Cipher**
   - **The size of key space; The inverse of a permutation**
4. **The Stream Cipher**
   - **The Synchronous Stream Cipher over Binary Alphabets:**
     - **linear recurrence, degree, keystream, period, LFSR**
   - **Applications of Stream ciphers**

Ch2 The Classical Cryptography

5. **Cryptanalysis:**
   - **Kerckhoff's Principle**
   - **four different attack models**
   - **Attacks on the Affine Cipher, Stream Cipher,**
6. **Modular Arithmetic, Arithmetic Modulo m:**
   - **Zn & Zn***
   - **Euler Phi-Function**
   - **invertible elements**
   - **invertible matrix**

Ch3 – Shannon's Theory

1. **Perfect Secrecy:**
   - **Why introduce perfect secrecy?**
   - **Definition and proof**
2. **The One-time Pad Cryptosystem:**
   - **What? Characteristics?**
3. **The requirements of a unbreakable (unconditionally secure) system**
4. **Entropy: why introduce Entropy? Computations.**
5. **The Key Equivocation H(K|C): Meaning**
6. **Spurious Keys and Unicity Distance:**
   - **Definition**

Ch4 – Block Ciphers

1. **Iterated Block Cipher: basic idea**
2. **DES:**
   - **a) Description: rounds, plaintext/key/ciphertext length**
   - **b) the round function, S-box**
   - **c) Key schedule generation**
   - **d) Cryptanalysis**
3. **AES:**
   - **a) the high-level Description: rounds, plaintext/key/ciphertext length**
   - **b) four operations (SUBBYTES, SHIFTROWS, MIXCOLUMNS, ADDROUNDKEY) in each iteration**
   - **c) S-box:**
   - **d) Key schedule generation**
   - **e) Cryptanalysis**
4. **Modes of Operations for block ciphers:**
   - **a) Why introduce Modes?**
   - **b) ECB/CFB/CBC/OFB/CTR/CCM/GCM mode**

Ch5 – The Hash functions

1. **Security of Hash functions:**
   - **Preimage-resistant, Second Preimage-resistant, Collision-resistant**
2. **The Random Oracle Model and Las Vegas (randomized) algorithms**
   - **Las Vegas algorithm, Algorithms of finding Preimage, Second Preimage**
   - **Algorithms of finding Collision, Birthday problem and Birthday attack**
   - **Relationships of Collision, Second Preimage and Preimage Problems**
3. **Reduction method**
4. **Constructions of Iterated Hash Functions**
   - **Merkle-Damgard Construction: collision-resistant property, SHA-1**
   - **Sponge Construction: SHA-3**
   - **Discussions on the Security of SHA-like Hash functions: MD4, MD5, SHA-0, SHA-1, SHA-2**
5. **MAC:**
   - **a) HMAC, CBC-MAC, Authenticated Encryption**
   - **b) Security and attack: A known message attack, A chosen message attack, forgery**

Ch6 – The RSA cryptosystem

1. **PKC v.s. SKC**
2. **The RSA cryptosystem: Public key & private key, Encryption & decryption, an example of RSA**
3. **Implementing of RSA: Complexity**
4. **Euclidean-like Algorithms: to compute b^{-1} mod n**
5. **Applications of the Chinese Remainder Theorem**
6. **Security Discussions:**
   - **Factoring Integer n and related attacks**
   - **Provable security: Turing Reduction**
   - **Semantic security: definition**
   - **Security problem: $e(x_1x_2)=y_1y_2$**

Ch7 - The ElGamal cryptosystem

1. **The ElGamal cryptosystem:**
   - **Public key & private key, Encryption & decryption, (Randomized ideas), example**
2. **Discrete Logarithm Problem (DLP):**
3. **Algorithms for DLP: Shanks' algorithm**
4. **Security Discussions:**
   - **security: DLP is infeasible**
   - **different attack goals**
   - **Semantic security**
5. **ElGamal-like Cryptosystems over suitable (proper) groups:**
   - **The Elliptic Curve ElGamal Cryptosystem; ECDLP (What is ECDLP?)**
6. **Diffie-Hellman Problems and Security: CDH, DDH, DL**
   - **What are CDH, DDH?**
   - **Security level of DL, CDH, DDH**
   - **Applications of Turing Reduction**

Ch8 – The Signature Schemes

1. **The digital Signature**
   - **Public key & private key, Signing algorithm & Verification Algorithm**
2. **The RSA Signature**
3. **The ElGamal Signature**

Thank you!

Questions?