CS 454/654 Reliability and Security of Computing Systems

Mid Term 2 Study Guide

---

1. Finite Fields and Galois Fields (GF)

- Definitions: Understand the concepts of Groups, Rings, and Fields, focusing on their properties.
- Galois Field (GF): Know how Galois Fields work, specifically GF(p) where p is prime.
- Polynomial Arithmetic: Practice performing multiplication in Galois Fields. Review examples from the AES arithmetic in the slides.
- Practice: For a field like GF(7), generate the closure under multiplication and understand how to check for properties such as associativity and distributivity.

2. Symmetric Key Encryption and AES

- AES (Advanced Encryption Standard): Understand how AES operates at a high level, focusing on its key components without diving into unnecessary detail.
- AES Stages: Familiarize yourself with the four main stages of each AES round:
    - **Substitute Bytes**
    - **ShiftRows**
    - **MixColumns**
    - **AddRoundKey**
- Confusion and Diffusion: Learn how AES achieves confusion (scrambling the relationship between ciphertext and key) and diffusion (spreading the influence of individual plaintext bits across the ciphertext).
- Avalanche Effect: Study the importance of the avalanche effect in encryption and why small changes in input lead to large changes in output, enhancing encryption security.

3. DES, Triple DES, and Attacks

- Triple DES Encryption: Understand how Triple DES works. Practice drawing the diagram and explaining the encryption process.
- Meet-in-the-Middle Attack: Review how this attack can be used against Double DES.
- Block Cipher Modes: Study the five main block cipher modes of operation and their characteristics:
    - ECB (Electronic Codebook)
    - CBC (Cipher Block Chaining)
    - CFB (Cipher Feedback)
    - OFB (Output Feedback)
    - CTR (Counter Mode)
- Application Scenarios: Practice explaining which block cipher mode is best suited for specific scenarios, such as:
    - Satellite Communication: Use modes that handle data loss well, like CBC or OFB.

    - High-Speed E-commerce Transactions: Use CTR for efficient, parallel encryption.
    - Standalone Encryption Key Transmission: Use ECB or CBC with padding for secure single-block encryption.

4. Cryptographic Hash Functions

- Definition and Purpose: Understand cryptographic hash functions and their role in ensuring data integrity and security.
- Comparison to Symmetric Ciphers: Differentiate hash functions from symmetric encryption, focusing on use cases and properties.
- Digital Signatures: Review how hash functions verify digital signatures by generating unique hashes of messages, ensuring integrity and authenticity.

5. RSA Encryption, Diffie-Hellman, and Public-Key Cryptography

- RSA Algorithm: Understand the RSA encryption and decryption process, including:
    - Generating Keys: Calculating the modulus, totient, encryption exponent, and decryption exponent.
    - Encryption and Decryption: Familiarize yourself with RSA steps for securing data.
- Public-Key Cryptography: Study the differences between symmetric encryption (shared key) and public-key encryption (different public and private keys).
- Diffie-Hellman Key Exchange: Learn the Diffie-Hellman process for securely exchanging keys over an insecure channel. Practice the diagram and steps involved.

6. Key Applications of Cryptographic Algorithms

- Public-Key Cryptosystems: Review applications of public-key cryptosystems, such as ensuring confidentiality, authenticating users, and verifying digital signatures.
- Brute-Force Attacks: Understand brute-force attack principles and countermeasures used in hash functions and public-key cryptosystems.

Practice Problems

- Galois Fields:
    - Define groups and the properties they must satisfy.
    - Given a field like GF(7), generate the closure under multiplication.
- Symmetric Encryption and AES:
    - Explain the avalanche effect and its significance in symmetric encryption.
    - List the operations within one AES round and discuss their roles.
- RSA Encryption:
    - Given two prime numbers, walk through RSA encryption and decryption steps. Calculate the modulus, totient, public key, private key, and perform decryption on a ciphertext.
- Hash Functions:
    - Compare cryptographic hash functions to symmetric cipher algorithms.
    - Explain how hash functions support digital signatures.

- Triple DES and Block Ciphers:
    - Draw the Triple DES encryption diagram.
    - Justify the optimal block cipher mode for different encryption scenarios (e.g., satellite communication, high-speed transactions, secure key transmission).

Key Focus Areas

- Polynomial Arithmetic in Finite Fields: Mastery of polynomial operations is essential, particularly as used in AES and finite fields.
- Symmetric vs. Asymmetric Encryption: Understand the fundamental differences, strengths, and use cases of symmetric (e.g., AES) and asymmetric encryption (e.g., RSA).
- Cryptographic Hash Function Properties: Ensure clarity on collision resistance and preimage resistance and how they secure data in applications like digital signatures.
- RSA Steps: Practice RSA encryption and decryption thoroughly.
- Block Cipher Modes: Understand each mode's function and its best application for secure communications.

Good luck with your preparation!