COMP7120/8120 Cryptography and Data Security

Review
Basic Concepts

- Concepts of security, objectives, cryptography and attacks
- Concepts of symmetric and asymmetric cryptographic methods
- Concepts of hash functions
- Denial-of-service attacks: concepts, attack and defense
Symmetric Crypto

• Block ciphers
  - Avalanche effects
  - Feistel cipher: architecture and computation

• DES
  - Parameters
  - Architecture
  - Double-DES and attacks
  - Triple-DES

• AES
  - Parameters
Modes of Operations

• ECB
  - Architecture, pros/cons

• CBC
  - Architecture, pros/cons

• CFB
  - Architecture, pros/cons

• CTR
  - Architecture, pros/cons

• You should be able to choose one based on the application requirements.
Hash Functions

• Basic properties

• Common hash functions and parameters
  - MD5, SHA1, SHA256

• Applications of hash functions
  - Message authentication: HMAC vs CBC-MAC
  - Message integrity check
  - Password with salt
  - Commitment protocols
  - ...

www.memphis.edu
Basic Number Theory

• Computations
  - Totient function and properties
  - multiplicative inverses
  - mod operations
  - GCD

• Extended Euclid’s algorithm

• Fermat’s and Euler’s theorems

• Difficult things in number theory
Public Key Crypto

- RSA
  - All details
  - Public key and private key generation
  - Encryption and decryption; signature and verification
- RSA-based key negotiation
  - All details
- Diffie-Hellman key negotiation
  - All details
- DSS is NOT required.
Authentication Protocol

• Mutual authentication
• Some design guidelines.
• Common attacks.

• Give an authentication protocol, analyze the security and vulnerabilities.
KDC and PKI

• Needham Schroeder protocol
  - Steps
    - details are not required

• Kerberos
  - basic concept
    - details are not required

• PKI
  - Certificates issued by PKI
    - PKI models

• Advantages and disadvantages of KDC and PKI
Midterm Rules

• In-class exam:
  - Please come 5-10 minutes earlier
  - Closed laptop/neighbor/cellphone
  - 100 pts, 3 sections.

• Cheat sheet:
  - One letter-size (8.5 by 11 inches) cheat sheet, front and back.
Midterm: Section I

- Section I (45pts): Single Choice
  - 15 questions, 3 pts each
  - Sample:

Which of the following design is to achieve confidentiality
[A] use salt when hashing a password
[B] send a message as fast as possible
[C] choose ECB as mode of operation
[D] publish a private key
Midterm: Section II

- Section II (20pts): Calculation
  - 5 questions, 4 pts each
  - Samples:

  Compute $2^{-1} \mod 3$
  Compute $\varphi(100)$
Midterm: Section III

• Section III (35pts): Answer Questions
  - 4 questions

You will be asked to design a security scheme, or analyze a given design (e.g., an authentication protocol or an encryption scheme)