CSCI 454/554 Computer and Network Security

Midterm Preview

Topics covered by Midterm

- Topic 1. Basic Concepts
- Topic 2. Basic Cryptography
- Topic 3. Secret Key Cryptography
- Topic 4. Hash Functions
- Topic 5. Basic Number Theory and Public Key Cryptography

Open book in-class exam

Topic 1. Basic Concepts (1)

- Be able to give examples of contributing factors to network security problems.
- Be able to explain the following concepts:
    - Three (CIA) security objectives: confidentiality, integrity, availability
    - Security policies, security mechanisms, security assurance
    - Three general types of security mechanisms: prevention, detection, and tolerance
    - Threat, vulnerability, risk
    - Threat model, attack model

Topic 1. Basic Concepts (2)

- Be able to give example interpretations of the three security objectives in specific context
- Be able to give examples and their explanations of security services (encryption, authentication, integrity, non-repudiation, access control, intrusion detection, etc.)
- Be able to explain what is security by obscurity and why it is bad

Topic 2. Basic Cryptography (1)

- Be able to draw a diagram to explain what are plaintext, ciphertext, encryption, decryption, and key.
- Be able to explain the four kinds of cryptanalysis techniques: ciphertext only analysis, known plaintext analysis, chosen plaintext analysis, and chosen ciphertext analysis.
- Be able to explain what are unconditional security, computational security, and one-time pad.
- Be able to explain the following types of cryptography and difference between them:
  - Secret key cryptography
  - Public key cryptography
  - Hash functions

Topic 2. Basic Cryptography (2)

- Be able to explain what are block cipher and stream cipher.
- Be able to give four examples for the application of secret key cryptography.
- Be able to give four examples for the application of public key cryptography.
- Be able to give four examples for the application of hash functions.

Topic 3. Secret Key Cryptography (1)

- Be able to draw a figure to explain and illustrate Feistel cipher.
- Be able to explain why consecutive permutations (or consecutive substitutions) do not enhance the security of encryption.
- Be able to explain what are confusion and diffusion and how they are generally achieved in Feistel ciphers.
- Be able to describe the basic facts of DES and AES, including block size, key size, general structure, number of rounds, and brief history.
- Be able to explain and use the DES subkey generation algorithm, the DES per-round expansion algorithm, and S-Boxes.

Topic 3. Secret Key Cryptography (2)

- Be able to explain the AES state, S-Box, inverse S-Box, MixColumn and inverse MixColumn function, and sub-key generation.
- Be able to explain what are avalanche effect, DES weak keys and semi-weak keys.
- Be able to explain and draw figures to illustrate the following block cipher modes of operations:
  - ECB
  - CBC
  - OFB
  - CFB
  - CTR

Topic 3. Secret Key Cryptography (3)

- Be able to describe the chaining dependency, error propagation, and error recovery properties for the above block cipher modes of operations
- .Be able to explain the meet-in-the-middle attacks against double DES.
- Be able to explain and draw a figure to illustrate triple DES, triple DES in CBC mode with CBC on inside and outside.
- Be able to explain and draw figures to illustrate how block cipher can achieve (1) message authentication only, (2) both message authentication and encryption with authentication tied to plaintext, and (3) both message authentication and encryption with authentication tied to ciphertext.
- Be able to explain the Data Authentication Algorithm achieved with DES in CBC mode.

Topic 4. Hash Functions (1)

- Be able to explain what is a hash function and the properties of hash functions, including one-way property, weak collision free property, and strong collision free property.
- Be able to explain the birthday paradox problem, birthday attacks, why the size of hash function must be at least 128 bits.
- Be able to describe the following applications of hash functions
  - File authentication
  - User authentication (assuming two users share a secret key)
  - Commitment using hash functions
  - Message encryption
  - Digital signature

Topic 4. Hash Functions (2)

- Be able to explain how to build hash using block cipher through block chaining techniques, its weakness due to meet-in-the-middle attacks, and how the meet-in-the-middle attack can be launched.
- Be able to describe the MD5 hash function, including the hash image size, the padding procedure, the block size, the processing of each message block, and the security concerns of MD5.
- Be able to describe the SHA-1 hash function, including the hash image size, the padding procedure, the block size, the processing of each message block, and the security concerns of SHA-1.
- Be able to describe the HMAC message authentication algorithm.
- Be able to describe the extension attack against the hash-based authentication algorithm using H(k|M|padding).

Topic 5. Basic Number Theory PKC (1)

- Be able to explain the concept of greatest common divisor (GCD) and use Euclid algorithm to calculate GCD manually.
- Be able to apply extended Euclid algorithm manually.
- Be able to perform modular arithmetics.
- Be able to explain what is multiplicative inverses and use extended Euclid algorithm to calculate multiplicative inverse.
- Be able to explain Fermat's theorem and Euler's theorem, and use them to speed up modular exponentiation.

Topic 5. Basic Number Theory PKC (2)

- Be able to explain the Totient function and calculate the Totient function for given integers.
- Be able to explain the order of an integer modular n.
- Be able to explain what are a primitive root and discrete logarithms, and manually calculate discrete logarithms for small integers.
- Be able to describe key generation, encryption, decryption, signature generation, and signature verification operations in RSA algorithm. Be able to manually perform these operations for small numbers.
- Be able to describe the probable-message attack against RSA and how PKCS #1 defeats this attack.
- Be able to describe the timing attack against RSA and how blinding defeats this attack.

Topic 5. Basic Number Theory PKC (3)

- Be able to describe key generation and key exchange for Diffie-Hellman (D-H) protocol. Be able to manually perform these operations for small numbers.
- Be able to explain what is man-in-the-middle attack against D-H protocol and how to prevent it.
- Be able to describe D-H protocol in phone book mode.
- Be able to describe how D-H protocol is used for encryption.
- Be able to explain key generation, signature generation, and signature verification in DSA algorithm. Be able to manually perform these operations for small numbers.