ECE 471/571: Fundamentals of Information and Network Security

Midterm Exam Preparation Guide

Exam date: Mar. 20, 2024
(Open on 3/20 at 12am, close at midnight 11:59pm,
Submit your worksheet in D2L, Midterm Exam folder)
Time Duration: 2 hours (enforced)

1. The exam will be open book, open note, in the form of a timed quiz on D2L. The time limit is 120-minutes. There will be about 5 or 6 problems that you need to answer/solve. Each problem may contain multiple sub-problems. Example types of the questions are: T/F, multiple choices, short answers, and numerical calculation. The former two types do not require detailed explanations of your answer. For the latter two types, the answers are expected to include some analysis and calculation (you need to show the intermediate steps, and a calculator is allowed (non-programmable)). Submit your final answers in the online quiz, and write down your explanation/analysis to support your answer in a separate worksheet and upload it right after the exam to D2L final exam folder.

2. Graduate students (ECE571) and undergraduate students (ECE471) will receive different sets of exam questions (more than 50% of the questions will be different). Generally speaking, graduate students can expect relatively more in-depth questions (such as those involving more modular arithmetic and probability calculations). However, the amount of calculations will not be much in the exam.

3. Generally speaking, anything that has been covered in the lectures before Mar. 17th, 2023 might be tested in the exam. Reviewing the lecture notes (power-points) on Piazza, in-class exercises on Tophat (or D2L quizzes), the homework assignments & project would all be helpful.

4. Have a deep understanding of the principles and concepts, and how to apply them in scenarios relevant to information and network security is more important than just knowing the details. More specifically, the following topics are considered fundamentals in this course. You are expected to know them by heart.

   - Introduction to Information and Network Security:
     - Understand the basic goals of information and network security, such as confidentiality, integrity, authentication, non-repudiation, availability, etc.
     - What are the common threat/adversary models: passive and active attacks, identify the security attacks in terms of the violations of the security services.

    - Common terminology: concept of secure communication over an insecure channel
    - Basic modular arithmetic, such as modular addition, multiplication, exponentiation, Euclid’s algorithm, etc.

- Classical Encryption Techniques:
    - Early ciphers: Shift, Affine, Substitution, Vigenere, Hill, Permutation ciphers. Understand block and stream ciphers.
    - Cryptanalysis: understand the principles of the four cryptanalysis approaches (ciphertext-only, known-plaintext, chosen-plaintext, chosen-ciphertext), and be able to apply them to break simple ciphers.
    - Three types of Cryptography: Secret key, Public key, Hash functions. What security goals and they are able to achieve, respectively?

- Measures of Security and Ideal Cryptosystems:
    - Perfect secrecy: definitions, and how to test whether a cryptosystem is perfectly secure.
    - One-time-pad: construction, XOR operation, and why it is perfectly secure, pros and cons.

- Symmetric Key Cryptography:
    - Product cryptosystems: what is idempotent cryptosystem and its impact on security of a cipher.
    - Notions of symmetric key cryptography, and computational security
    - Substitution-permutation networks: general structure and why do we need it.
    - DES
        - The Feistel structure, and general idea of Mangler function: S-Boxes and permutation, the key length of DES and its relationship with the security level;
        - How to make more secure DES? – Triple DES, meet-in-the-middle attack, and how is Triple DES designed, why?
    - AES
        - Understand the high-level structure and why it is secure, and comparison with DES
    - Understand why a block cipher is secure: what are the desired properties must the DES/AES algorithm satisfy? (e.g., the non-linear property, strict avalanche, bit independence) Why?
    - Five modes of encryption (how to encrypt large messages), their pros and cons
    - Pseudorandom number/sequence generation and stream ciphers
        - What are the criteria to evaluate the security of PRNG or PRSG?
        - Common ways of generating pseudorandom numbers and their security

- Hashes and Message Digest:
    - The desired properties of cryptographic hash functions: one-way property (preimage resistance), second preimage resistance, collision resistance, and randomness, why are they needed.

- The complexity of breaking each property, the Birthday paradox and related probability calculations
- The length requirement for a message digest (how many bits are considered sufficient?)
- General iterated construction of message digests

- Message authentication codes: understand the security requirements of MACs, how to construct secure keyed hash function (e.g., HMAC, CBC-MAC, etc).
- Applications of hash functions: e.g., integrity check, authentication, commitment protocols, encryption, etc. How to securely combine hash with encryption to achieve both confidentiality and authentication/integrity protection.

- Public Key Cryptography
    - The basic concepts of public key cryptography, including public key encryption and signatures, what security properties they can achieve.
    - The RSA cryptosystem: know how public/private keys are generated; how to use public/private keys to encrypt/decrypt messages; the vulnerabilities of textbook RSA and remedies
    - Digital signature schemes: different levels of security requirements, and three attack models; RSA signatures: construction, possible attacks, hash and then sign.
    - Applications of public key encryption and digital signatures – basic applications, and how to securely combine signature with encryption to achieve both confidentiality and authentication/integrity protection.