CS 4173/5173
COMPUTER SECURITY

Final Review

TIME AND LOCATIONS

- Time:
  - May 6, 2025, Tuesday
  - 4:30 PM – 6:30 PM

- Location:
  - Dale Hall 0103

BASIC CONCEPTS

- Final mainly covers materials after Midterm (Lecture11 ~ 23).
  - There will be no specific questions about symmetric key or hash function, but they may be combined with asymmetric cryptography

- Concepts of asymmetric cryptographic methods
  - Comparison between symmetric and asymmetric.
  - Why do we need to use asymmetric crypto to negotiate a session key?

- But you still need to know the basics of
  - Basic security concept, objectives.
  - Symmetric key
  - Hash functions

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
  - Factoring a large number
  - …
  - …
  - …

PUBLIC KEY CYPTO

- 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

AUTHENTICATION PROTOCOL

- Mutual authentication
- Some design guidelines.
- Common attacks.
  - Reflection attack
  - Man-in-the-middle
  - …
- Give an authentication protocol, analyze the security and vulnerabilities.

KDC AND PKI

- Needham Schroeder protocol
  - Steps shown in slides
  - details are not required (may only appear in Section I in Final)
- Kerberos
  - basic concepts
    - Belong to KDC or PKI?
  - details are not required (may only appear in Section I in Final)
- SSL/TLS
  - basic concepts
    - Basic steps shown in slides
  - details are not required (may only appear in Section I in Final)
- PKI
  - Certificates issued by PKI
    - Digital certificates vs digital signature
  - PKI models
  - details are not required (may only appear in Section I in Final)
- Advantages and disadvantages of KDC and PKI

OTHERS

- Homomorphic Encryption
  - Concepts
    - motivation and applications?
    - basic operations
    - Why do we need to add noise, and how to do the noise-deduction?
  - details are not required (may only appear in Section I in Final)
- Online Privacy and Tor
  - Concepts
    - What information could be disclosed when you visit a website?
    - What's Tor? what crypto Tor uses?
    - Why can Tor hide some information?
  - details are not required (may only appear in Section I in Final)
- Block Chain
  - Concepts
    - Basic architecture, centralized or distributed?
    - Proof of work
  - details are not required (may only appear in Section I in Final)

FINAL RULES

- Rules:
  - Please come 5-10 minutes earlier
  - Closed laptop/neighbor/cellphone/calculator
  - 100 pts, 3 sections.

- Cheat sheet:
  - TWO letter-sized (8.5 by 11 inches) cheat sheets, front and back.

FINAL: SECTION I

- Section I (40pts): Single Choice
  - 16 questions, 2.5 pts each

Examples:

_____ Which of the following is NOT computationally difficult?

[A] factoring a given large number [B] computing a primitive root of a large number

[C] verifying a large prime [D] computing the discrete logarithm of a large number

_____ Which is FALSE about Tor network

[A] No Tor node inside the Tor network can know your IP.

[B] Tor networking relies on encryption to ensure confidentiality.

[C] When you visit a website via tor, the website knows the visit is from Tor.

[D] The Tor browser is publicly available.

FINAL : SECTION II

- Section II (12pts): Calculation
  - 4 questions, 3 pts each

  Examples:
  - Compute 2^{-1} mod 3
  - Compute 23^{81} mod 55
  - Compute ø(100)
  - Compute GCD(333,121)

FINAL : SECTION III

- Section III (48pts): Answer Questions
  - 4-6 questions

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

  Examples:
  - Explain the reflection attacks against symmetric key based authentication, and explain potential countermeasures.
  - What is the man-in-the-middle attack?
  - There will be at least one question about analyzing the security of an authentication protocol design.