

Study Guide for Midterm Examination

1 Exam Coverage

The midterm examination will cover the topics of the first six weeks of the course. These topics are presented in several different formats:

1. In-person class lectures.
2. Written **lecture notes**, **weeks 1–6**, available on the course web site.
3. Written **handouts**, available on the course web site. I especially recommend **handout 3** for reviewing number theory.
4. Textbook (Wenbo Mao), relevant sections from chapters 1–3, 5–8.
5. Other **resources** available in the library and on the web.

2 Review Outline

Below I give a list of topics, concepts, definitions, theorems, algorithms, and protocols that we have covered and I expect you to know. This list is not inclusive, as I'm sure I have missed some things.

1. Secret-message transmission problem.
 - (a) Model.
 - Alice.
 - Bob.
 - Eve (passive eavesdropper).
 - Mallory (active eavesdropper).
 - Plaintext.
 - Ciphertext.
 - Key.
 - Encryption function.
 - Decryption function.
 - (b) Attacks.
 - Known plaintext.
 - Chosen plaintext.
 - Known ciphertext.
 - Chosen ciphertext.
 - (c) Breaking system.
 - Finding key.

- Decrypting ciphertext.
 - Extracting partial information from ciphertext.
2. Information security in the real world.
3. Classical cryptography.
- (a) Cryptosystems.
- Caesar cipher.
 - One-time pad.
 - Simple XOR system.
 - Monoalphabetic cipher.
 - Playfair cipher.
 - Hill cipher.
 - Polyalphabetic cipher.
 - Transposition techniques.
 - Rotor machines.
 - Steganography.
- (b) Security.
- Kerckhoffs's assumption (that only key is secret).
 - Statistical inference.
 - Brute force attack.
 - Redundancy.
 - Entropy.
 - Information-theoretic security.
- (c) Stream cipher.
- Keystream generator.
 - Next-state generator.
- (d) Block cipher.
- Block size.
 - Padding.
 - Chaining modes.
 - Electronic Codebook Mode (ECB).
 - Cipher Block Chaining Mode (CBC).
 - Cipher-Feedback Mode (CFB).
 - Output Feedback Mode (OFB).
 - Propagating Cipher-Block Chaining Mode (PCBC).
 - Recoverability from lost/damaged ciphertext blocks.
4. Data Encryption Standard (DES).
- (a) Feistel network.
- (b) Block size.
- (c) Key size.

- (d) Subkey.
 - (e) S-box.
 - (f) Rounds.
 - (g) Decryption.
5. Message Authentication Codes (MACs).
- (a) Definition.
 - (b) Need for MACs; why encryption isn't enough.
 - (c) MACs from DES and other block ciphers.
6. Asymmetric cryptosystems.
- (a) Definition and requirements.
 - (b) Public key model.
 - (c) Need for resistance against chosen plaintext attack.
7. RSA.
- (a) Components.
 - Modulus.
 - Encryption key.
 - Decryption key.
 - Encryption function.
 - Decryption function.
 - (b) Algorithms needed.
 - Primality testing.
 - Finding modular inverse.
 - Fast modular exponentiation.
 - (c) Theoretical basis.
 - Prime number theorem.
 - Existence of modular inverse.
 - Proof that decryption function is inverse of encryption function.
 - (d) Computational efficiency.
 - (e) Security properties.
 - Factoring problem.
 - Computing $\phi(n)$ given factorization of n .
 - Factoring n given $\phi(n)$.
 - Factoring n given public and private keys.
 - (f) Hybrid system.
 - Use RSA for secure transmission of random session key.
 - Use symmetric cryptosystem for body of message.
8. Number theory.

- (a) Modular arithmetic.
 - Divides ($a|b$).
 - Division theorem: $a = bq + r, 0 \leq r < b$.
 - The remainder operator “ $a \bmod n$ ”
 - The congruence relation $a \equiv b \pmod{n}$
 - \mathbf{Z}_n .
 - Computing in \mathbf{Z}_n for large n .
 - Fast modular exponentiation.
 - (b) \mathbf{Z}_n^*
 - Relatively prime pairs of numbers.
 - Euler’s totient function $\phi(n)$
 - Euler’s theorem and Fermat’s little theorem.
 - Consequence: $x \equiv y \pmod{\phi(n)}$ implies $a^x \equiv a^y \pmod{n}$.
 - Greatest common divisor (gcd).
 - Euclidean gcd algorithm.
 - Diophantine equations and modular inverses.
 - Extended Euclidean algorithm.
 - (c) Chinese remainder theorem.
 - (d) Prime number theorem.
 - (e) Primitive roots.
 - Lucas test.
 - Discrete logarithm.
 - (f) Quadratic residues.
 - Square roots modulo a prime.
 - Square roots modulo a product of two distinct primes.
 - Euler criterion.
 - Finding square roots modulo prime p when $p \equiv 3 \pmod{4}$.
9. Cryptographic protocols based on number theory (besides RSA).
- (a) Diffie-Hellman key exchange.
 - (b) ElGamal key agreement.
 - (c) ElGamal public key cryptosystem.
 - (d) Goldwasser-Micali (QR) probabilistic cryptosystem.