

Summary of Topics Covered

CMSC/Math 456

Instructor: Daniel Gottesman

Fall 2023

This is a list of the major topics we covered in class that are eligible for questions on the final. This should not be considered a completely comprehensive list, as some of these topics involved considerable discussion and had sub-topics of their own. In addition, there were some additional smaller comments that I didn't feel merited an entry in this list that could still be relevant for a final exam question. However, you can expect that the bulk of the questions on the final will be relevant to the topics drawn from this list.

There will be a slight emphasis on material not covered in the two midterms, but there will also be many questions on topics previously covered by the midterms.

- Classical cryptography
 - Substitution cipher
 - Shift cipher
 - Vigenère cipher
 - Frequency analysis
 - One-time pad
 - Probability and conditional probability
 - Kerckhoff's principle
- Modern private-key encryption
 - Definition of private-key encryption
 - Perfect secrecy
 - Threat models
 - Computational assumptions
 - Pseudorandom generators
 - Pseudo one-time pad
 - EAV security
 - Reductions
 - Stream ciphers
 - RC4
 - Chosen plaintext attacks
 - Birthday paradox
 - Pseudorandom functions
 - Block ciphers; ECB, CBC, and CTR modes
 - Feistel networks

- Substitution-permutation networks
- Avalanche effect
- DES
- AES
- Side-channel attacks
- Modular arithmetic and group theory
 - Modular division
 - Euclid’s algorithm
 - Modular exponentiation, repeated squaring
 - Order
 - Definition of group
 - Subgroups
 - Lagrange’s Theorem
 - Cyclic groups
 - Euler totient function, Euler-Fermat theorem
 - Chinese remainder theorem
- Key exchange
 - Diffie-Hellman
 - Definition of key exchange
 - Security of key exchange
 - Pohlig-Hellman algorithm
 - Finding prime numbers
 - Hardness of discrete log
 - Man in the middle
- Public key encryption
 - El Gamal encryption
 - Definition of public-key encryption
 - Security of public-key encryption
 - RSA encryption
 - Hardness of factoring
 - KEM/DEM
- Authentication
 - MACs
 - Security of MACs
 - MACs based on pseudorandom functions
 - CBC-MAC
 - Hash functions

- * Collision resistance
- * Merkle-Damgård construction
- * Overview of standard hash functions
- * Birthday attacks on hash functions
- * Hash functions as random oracles
- * Hash functions for key derivation
- * Other applications of hash functions
- * Merkle trees
- * Bit commitment
- Hash-and-MAC
- Attack on padding oracle
- Chosen ciphertext attacks
- Unforgeability and authenticated encryption
- Strongly secure MACs
- RSA-OAEP
- CCA security of KEMs
- Digital signatures
- Transferability and non-repudiation
- Security of digital signatures
- RSA signatures
- Identification schemes
- DSA
- Web of trust
- Certificate authorities
- TLS
- Forward secrecy
- Other protocols (qualitative only)
 - Quantum algorithms for cryptography
 - Quantum key distribution
 - Lattices
 - Learning with errors problem and encryption
 - Secret sharing
 - Multiparty computation
 - Zero-knowledge proofs