CYBR 5310 Design of Cryptographic Algorithms and Protocols
Midterm study guide

Introduction:
Kerckhoffs' Principle
Thread/attack models
Perfectly secret
One-time pad
Limitations of perfectly secrecy
Shannon's theorem

Block cipher:
Substitution-permutation networks
Feistel Network
DES
- Construction, such as round function, sub-key, expansion, s-boxes, permutation
- 3DES

Avalanche effect
AES
- 4 stages

Secret-Key Encryption:
Historical Ciphers
- Substitution

Encryption Modes
- Padding for block cipher
- Initial Vector

Authenticated Encryption

One-Way Hash Functions:
Properties
- One-way
- Collision resistant
  - Collision Attacks

MD
SHA
Merkle–Damgard construction
Applications of One-Way Hash Functions
Message Authentication Code (MAC)
- Length Extension Attack

Lab practices