# Introduction and Overview Ch. 1

## Encryption

## History

## The Expanding Scope of Cryptography

## The Layers of Cryptography

# Review of Probability and Classical Ciphers A.3, Ch. 1

## Review of Probability

## Probability Spaces

## Random Variables

## Expectation of a random variable

## Markov’s Inequality

## Chernoff Bound

## Conditioning

# Private Key Encryption: Classical Ciphers

# Perfect Secrecy Ch. 2

## Perfect Indistinguishability

### Perfect Secrecy (Shannon Secrecy)

### Perfect Adversarial Indistinguishability

### Statistical Security

# Review of Algorithms and Complexity A.2, B.0, B.1

## Algorithms

## Polynomial Time

### Problems believed not to be in P

### Asymptotic vs. Concrete Complexity

## Randomized Algorithms

### Definition

### Primality Testing

# Computational Security 3.0-3.2

## Computational Indistinguishability

## Concrete Formalization

### Indistinguishable Encryptions (Concrete)

## Asymptotic Formalization

### Indistinguishable Encryptions (Asymptotic)

## Examples of Insecure Schemes

### Shift Cipher

### Biased One-Time Pad

## Semantic Security

## Partial Semantic Security

## Partial Semantic Security -> Indistinguishable Encryptions

# Stream Ciphers 3.3-3.4

## Motivation

## Looking Random

## Linear Congruential Generator

## Pseudo Random Generator Definition

### Efficiency

### Expansion

### Pseudo Randomness

## Efficiently Testable Statistical Properties of Truly Random Sequences are satisfied by Pseudorandom Sequences

## If G is a PRG then (Gen, Enc, Dec) has indistinguishable encryptions