CS 475:Lecture Summary

3rd February 2004

Reading: Chapters 3 (omitting sections 3.5 and 3.6) and 4 (omitting section 4.1) from the textbook

Review: Last week, we studied DES and used a simplified version to show an example of encryption.

This Week's Topics:

- Block Cipher Modes:
  1. ECB (Electronic Code Book)
  2. CBC (Cipher Block Chaining)
  3. CFB (Cipher FeedBack)
  4. OFB (Output FeedBack)
  5. CTR (Counter)
- Arithmetic in simple finite fields
  1. Modulo arithmetic; Extended Euclidean algorithm for GCD
  2. The finite field GF(2) and polynomials over GF(2)
  3. GF(2^8) and modular polynomial arithmetic (modulo the polynomial $(x^8 + x^4 + x^3 + x + 1)$; used in AES)
- AES (Advanced Encryption Standard): will use Problem 5.4 as example.
  1. Overall structure
  2. Stages: substitution, row shifting, column mixing (arithmetic over GF(2^8)), and key addition.
  3. AES Decryption.