

CS 549: Cryptography and Network Security

Objectives

- We cover in this course principles and practice of cryptography and network security:
 - Classical systems, symmetric block ciphers (DES, AES, other contemporary symmetric ciphers), linear and differential crypt-analysis, perfect secrecy, public-key cryptography (RSA, discrete logarithms), algorithms for factoring and discrete logarithms, cryptographic protocols, hash functions, authentication, key management, key exchange, signature schemes, email and web security, viruses, firewalls, digital rights management, and other topics.

Prerequisites

- CS 430.

Syllabus

Particular topics to be covered include (but are not limited to):

- Introduction
- Conventional Encryption
 - Classical Techniques
 - Modern Techniques
 - Algorithms
 - Confidentiality Using Conventional Encryption
- Public-Key Encryption and Hash Functions
 - Public-Key Cryptography
 - Introduction to Number Theory
 - Message Authentication and Hash Functions
 - Hash and Mac Algorithms
 - Digital Signatures and Authentication Protocols
- Network Security Practice and System Security (by presentations)
 - Authentication Applications
 - Electronic Mail Security
 - IP Security
 - Web Security
 - Intruders, Viruses, and Worms
 - Firewalls

Edited March 2006 ([html](#), [css](#) checks)