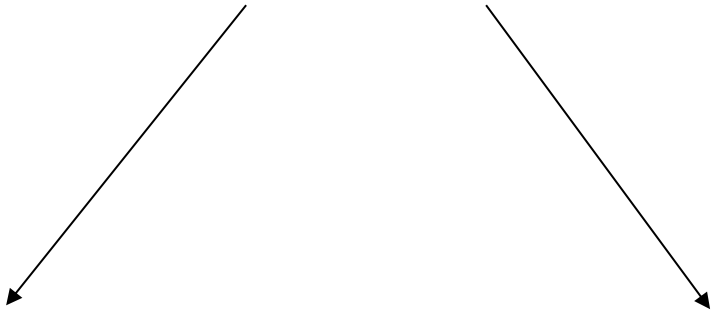
Follow-up Courses

ECE 646
Applied Cryptography



ECE 746
Advanced Applied Cryptography

ECE 747
Cryptographic Engineering

Applied Cryptography

Modular integer arithmetic

- Historical ciphers
- Classical encryption (DES, Triple DES, AES)
- Public key encryption (RSA, basics of ECC & PQC)
- Hash functions and MACs
- Digital signatures
- Public key certificates
- Cryptographic standards

Advanced Applied Cryptography

Operations in the Galois Fields $GF(2^n)$

- Details of AES and AES-GCM
- Stream ciphers
- Elliptic curve cryptosystems
- Post-Quantum Cryptography
- Secret sharing
- Zero-knowledge
- Random number generators
- Physical Unclonable Functions
- Attacks against implementations (timing, power, fault, cache attacks)
- Efficient and secure implementations of cryptography

Çetin Kaya Koç
Editor

Cryptographic Engineering

Springer

Selected Topics

- Random Number Generators
- Physical Unclonable Functions
- Differential Power Analysis, Electromagnetic Analysis
- Fault Analysis, Electromagnetic Fault Injection, Fault Tolerant Cryptography
- Cache Attacks
- Hardware Trojans
- Factoring, General Number Field Sieve
- Implementations of Cryptographic Functions on Constrained Devices / Embedded Systems
- Homomorphic Encryption
- Pairing Based Cryptosystems
- Post Quantum Cryptography

Related Courses

ECE 505
Hardware Security

ECE 508
Internet of Things

Related Courses

ECE 698: Independent Reading and Research

ECE 798: Research Project

ECE 799: Master's Thesis