# Syllabus

**Week 1:** Introduction: Principals of cryptography; Classical algorithms; Attacks on cryptographic systems.

**Week 2:** Stream ciphers and pseudo-random generators. One-time pads. Some information theoretical results on cryptography.

**Week 3:** Private key cryptography: Data Encryption Standard (DES), Function, performance, implementation, security. Overview on other modern block ciphers, including AES. Key length and long-term security.

**Week 4:** Private key cryptography: Operation modes of block ciphers. Multiple encryption. Key whitening.

**Week 5:** Introduction to public-key cryptography. One-way functions. Some number theory: Euclid's algorithm, Euler's Phi function.

**Week 6:** Public key cryptography: RSA, Function, performance, implementation, security. Recent results on successful attacks on RSA.

**Week 7:** Midterm exam.

**Week 8:** Public key cryptography: The generalized discrete logarithm problem. Diffie-Hellman key exchange protocol.

**Week 9:** Elliptic curve systems, function and security. ElGamal encryption schemes.

**Week 10:** Digital Signatures: The ElGamal and the RSA signature scheme. Message Authentication Codes (MACs).

**Week 11:** Hash functions: Principals; Important algorithms; Birthday attack. Protocols: Security Services.

**Week 12:** Protocols: Key distribution and key agreement; Private-key vs. public-key approaches.

**Week 13:** Certificates. Identification schemes: Challenge-and-response protocols.

**Week 14:** Final exam.

### Important dates

*First day of class:* Wednesday, September 6

*Project proposals due:* Wednesday, October 11

*Midterm exam:* Wednesday, October 18

*Project report due:* Wednesday, December 6

*Final exam:* Wednesday, December 13