

CO 487/687 Applied Cryptography

Instructor: Alfred Menezes

This course is an introduction to applied cryptography aimed primarily at undergraduate students.

Topics:

- * Symmetric-key encryption: Classical ciphers, one-time pad, stream ciphers (RC4), Feistel networks, DES, AES, modes of operation.
- * Hash functions and data integrity: Hash functions (SHA-1, SHA-2), parallel collision search, message authentication codes (CBC-MAC, HMAC).
- * Authenticated encryption: Encrypt-then-MAC, AES-GCM.
- * Public-key encryption: RSA, elliptic curves.
- * Signature schemes: RSA, ECDSA, quantum-safe signature schemes.
- * Key establishment: Elliptic curve Diffie-Hellman key agreement.
- * Key management: Certification authorities, public-key infrastructures.
- * Deployed cryptography: IEEE~802.11 WEP, IEEE~802.11 WPA2, Secure Sockets Layer (SSL/TLS), Google's Key Management Service, cryptocurrencies (Bitcoin), Fast IDentity Online (FIDO), privacy-enhancing technologies (Tor, OTR).

Suggested reading: None (the course is self-contained).

Prerequisites: None.