ICS423: Data Security and Cryptography I

Synopsis

History of secret communication and confidential data storage. Elements of cryptography and cryptanalysis. Classical ciphers. Symmetric key cryptography. Public key cryptography.

Lectures

1. Basic ideas of data security
   (a) Flow security refresher
   (b) History of secret communication
   (c) Steganography
   (d) Cryptography and cryptanalysis
2. Classical ciphers
   (a) Substitution
   (b) Transposition
   (c) Cryptanalysis
3. Information theory of secret communication
   (a) Probability and information
   (b) Perfect secrecy
   (c) Redundancy and unicity distance
4. Symmetric key cryptography
   (a) Confusion and diffusion
   (b) Feistel networks
   (c) Block ciphers
   (d) Stream ciphers
5. Public key cryptography
   (a) One-way and trapdoor functions
   (b) Classic public key primitives
   (c) Semantic and adaptive security