Revision

Sushmita Ruj

Topics

- Classical Ciphers
- Security notions
- Symmetric Key encryption:
  - one-time pad,
  - Stream Ciphers, RC4,
  - PRG,
  - Block ciphers,
  - Modes of encryption

Topics

- Semantic Security
- Message Integrity: MAC, unforgeabilty
- Hash functions: properties. Constructions
- Merkle Trees
- Number Theory: Modular arithmetic, Euclidean and extended Euclidean algo, Groups, Square-Multiply, Fermat’s little theorem, Chinese remainder theorem Groups, factoring problem,

Topics

- Public key Encryption
- Trapdoor Functions, Trapdoor permutation
- RSA
- Discrete Log assumption
- Diffie-Hellman key exchange
- El Gamal Encryption
-

Topics

- Digital Signatures, unforgeabilty
- PKI
- Blcockhains
- ZKP:
- Identification schemes:
- Fiat Shamir Transformation
- BLS signatures
- Cloud Auditing
- PQC: Hash-based signatures
- Secret Sharing

All the best!