Advance Cryptography

Review of number theory, group, ring and finite fields, quadratic residues, Legendre symbol, Jacobi symbol, Probability, Probability, Discrete random variable, Continuous random variable, Markov's inequality, Chebyshev's inequality, normal distribution, the geometric and binomial distributions.

Formal Notions of Attacks: Attacks under Message Indistinguishability: Chosen Plaintext Attack(IND-CPA), Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2), Attacks under Message Non-malleability: NM-CPA and NM-CCA2, Inter-relations among the attack model.

Public key cryptography, RSA cryptosystem, probabilistic encryption, homomorphic encryption, Elliptic curve cryptosystems, Cryptographic hash functions.

Digital signatures and the notion of existential unforgability under chosen message attacks. Elgamal digital signature scheme. Schnorr signature scheme. Zero Knowledge Proofs and Protocols,

Bitcoin, Blockchain technology, Incentives and proof of work. Bitcoin Mining, Mining pools, Mining incentives and strategies, Bitcoin Pooled Mining Reward Systems.

References

1. W. Mao, Modern Cryptography: Theory & Practice, Pearson Education, 2004.
2. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies, 2016.
3. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, An Introduction to Mathematical Cryptography: Springer publication .
4. Koblitz, N. Course on Number Theory and Cryptography, Springer Verlag, 1986 4.
5. Menezes, A, et.al. Handbook of Applied Cryptography, CRC Press, 1996.
6. Thomas Koshy, Elementary Number Theory with applications, Elsevier India, 2005.

CS845

Guide: Dr. Kunwar Singh
40611006 (CSE)
Mr. Lohith J. J