Cryptography (CS04)

Sanoj S Vijendra
22B0916
Mentor: Sharvari Medhe

Objectives:

Week1: First two videos from youtube. Chapter1 and ch2: stream ciphers.

Week2: Next three videos from youtube. Ch3: The Data Encryption Standard (DES) and Alternatives (from book).

Week 3: Next four videos. Ch4: The Advanced Encryption Standard (AES) (from book).

Week 4: Next two videos. Ch5: More About Block Ciphers (from book).

Mid-Term Report Submission

Week 5: Next three videos. Ch6: Introduction to Public-Key Cryptography(from book).

Week 6: Next four videos. Ch7: The RSA Cryptosystem (from book).

Week 7: Next four videos. Ch8: Public-Key Cryptosystems Based on the Discrete Logarithm Problem (from book).

Week 8: Last two videos. Ch9: Elliptic Curve Cryptosystems and Ch10: Digital Signatures (from book).

Remaining chapters: If time permits I will cover Post Quantum Cryptography also.

End-Term Report Submission

References:

1) Book : **Understanding Cryptography**
2) **Youtube playlist:**
   https://youtube.com/@introductiontocryptography4223?si=vd2IFozBeYB-xEc2