Presentation Schedule

CSE 594: Modern Cryptography (Spring 2017)
Instructor: Omkant Pandey

April 18 (Tuesday)

- Modes of Encryption for Block Ciphers: FNU Gaurav
- Homomorphic Encryption: Venkata Kedarnath Pakala
- Attack Models for Encryption (CPA and CCA): Gustavo Poscidonio
- Proxy Re-Encryption: Sayan Bandyopadhyay

April 20 (Thursday)

- Searching on Encrypted Data: Swarnima Shrivastav
- Identity Based Encryption: Parkavi Sundaresan
- Attribute Based Encryption: Ravi Kumar Rajendran
- Functional Encryption: Arun Ramachandran

April 25 (Tuesday)

- Private Information Retrieval (PIR): Justin Maldonado
- Secret Sharing Schemes: Vaishali Chanana
- Ring Signatures and Group Signatures: Hemant Pandey
- Oblivious Transfer: Bharathkrishna Guruvayoor Murali

April 27 (Thursday)

- Side channel attacks (Timing attacks on RSA etc.): Him Kalyan Bordoloi
- Bitcoin / Crypto Currencies: Hyungjoon Ku
- Proof of Birthday Bound: Meghana Doppalapudi
- Differential Privacy: Subathra Vijayakumar

May 02 (Tuesday)

- Proofs of Storage/Retrievability: Venkata Jyothsna Donapati
- Program Obfuscation: Gangabarani Balakrishnan
- Multiparty Computation: Malini Mahalakshmi Venkatachari
- Introduction to PCP Theorem (without the proof): Aravind Warrier