Week	Dates	Syllabus (IAM 502) 2021-2
1	March 07-11	Linear Feedback Shift Registers: Generating Functions, Minimal Polynomial and Families of Recurring Sequences, Characterizations and Properties of Linear Recurring Sequences.
2	March 14-18	Linear Feedback Shift Registers: Generating Functions, Minimal Polynomial and Families of Recurring Sequences, Characterizations and Properties of Linear Recurring Sequences.
3	March 21-25	Stream Ciphers and Pseudo Random Numbers. Pseudo random sequences, Linear Congruential Generators, Cryptographic Generators, Design of Stream Cipher, One Time Pad
4	March 28- April 01	Stream ciphers using LFSRs, additive generators.
5	April 07-08	Stream ciphers using LFSRs, additive generators.
6	April 11-15	Non-linear Filtering Functions
7	April 18-22	Non-linear Combiners
8	April 25-29	Gifford, Algorithm M, PKZIP. Other Stream Ciphers and Real Random Sequence Generators: RC4, SEAL, WAKE
9	May 05-06	Gifford, Algorithm M, PKZIP. Other Stream Ciphers and Real Random Sequence Generators: RC4, SEAL, WAKE
10	May 09-13	Non-linear Feedback Shift Registers
11	May 16-20	Cascading Multiple Stream Ciphers
12	May 23-27	Generating Multiple Key Streams from a Single Pseudo-Random-Sequence Generator
13	May 30-June 03	Generating Multiple Key Streams from a Single Pseudo-Random-Sequence Generator
14	June 06-10	Randomness Tests
15	June 13-17	Catch up