Curriculum – mid sem exam

Dhiren Patel

Himanshu Patel

Midsem

- Question Paper – 30 marks
- Exam time – 90 minutes
- 3 Questions each of 10 marks
- Subjective as well as MCQ
- Options within questions
- Closed book, no open notes
- Calculators allowed

Dhiren Patel (2 questions)

- 1 Privacy (Bruce Schneier’s Blog) - Security (of Digital data/asset/account), Privacy concerns, Privacy by Design, (S.2992 and S.2710),
- 2. Security, CIA, McCumber’s cube, Attacks, Security primitives, ACL, RBAC, Critical Infrastructures and their protection,
- 3. Classical Cryptography – Perimeter Security (Confidentiality was the only objective), Transposition ciphers, Shift ciphers, Mono-alphabetic cipher, Polyalphabetic cipher, (Playfair, Hill, Vengere etc.)
- 4 Classical Crypto – One time pad, Vernam cipher, Rotor machines
- 5 Steganography – Hiding information, classical and modern steganography
- 6 Cryptanalysis and designing modern secure ciphers, Export Regulations (e.g. DES), One way Hash function, KPI – Security of Cipher (Block size, Key size, Core math functions)

Himanshu Patel (1 question)

- 1 Firewall (Network Security) – stateful and stateless, placement of firewall in network
- 2 IPSec – Transport and Tunnel mode, Security Association, IPSec anti-replay service, ESP