**Name: - Kunal Uppal** **Subject Name: -CIS**

**Branch/Semester: - 7th Sem SecA** **Subject Code:-CSE-419N**

| Sr. No. | Lecture | Topics To Be Covered | Planned on | Covered On | Remarks |
|---|---|---|---|---|---|
| 1 | L 1 | **Unit I: Basics of Cryptography**: Introduction to Computer Security | 18.7.19 | | |
| 2 | L 2 | Principles of Computer Security | 19. 7.19 | | |
| 3 | L 3 | Introduction to cryptography | 22. 7.19 | | |
| 4 | L 4 | Security threats:Virus | 23. 7.19 | | |
| 5 | L 5 | Security threats:Trojen Horse, Worm | 25. 7.19 | | |
| 6 | L 6 | Security attacks:Active and Passive | 26. 7.19 | | |
| 7 | L 7 | Types of security attacks | 29.7.19 | | |
| 8 | L 8 | **Content Beyond Syllabus: Antivirus** | 30.7.19 | | |
| 9 | L 9 | Types of cryptography | 1.8.19 | | |
| 10 | L 10 | Classical cryptography and their cryptanalysis:Substitution techniques | 2.8.19 | | |
| 11 | L 11 | Classical cryptography and their cryptanalysis:Substitution techniques | 5.8.19 | | |
| 12 | L 12 | Classical cryptography and their cryptanalysis:Transposition techniques | 6.8.19 | | |
| 13 | L 13 | Perfect secrecy | 8.8.19 | | |
| 14 | L 14 | Shannon's theorem | 9.8.19 | | |
| 15 | L 15 | Stream ciphers | 12.8.19 | | |
| 16 | L 16 | **Unit II: Authentication Mechanism and Security Algorithms:**Access control mechanism | 13.8.19 | | |
| 17 | L 17 | Discretionary v/s mandatory access control | 16.8.19 | | |

| | | | | | |
|---|---|---|---|---|---|
| 18 | L 18 | Pseudorandom permutations | 19.8.19 | | |
| 19 | L 19 | Practical block ciphers (3-DES, AES) | 20.8.19 | | |
| 20 | L 20 | **Content Beyond Syllabus:IDEA** | 22.8.19 | | |
| 21 | L 21 | RSA Algorithm | 23.8.19 | | |
| 22 | L 22 | RSA:Modes of operation | 27.8.19 | | |
| 23 | L 23 | Message Authentication Codes(MAC):Functions | 29.8.19 | | |
| 24 | L 24 | MACs:HMAC,CMAC | 30.8.19 | | |
| 25 | L 25 | Hash functions-Introduction | 2.9.19 | | |
| 26 | L26 | Hash functions-Tiger Hash | 3.9.19 | | |
| 27 | L 27 | Gear hash | 5.9.19 | | |
| 28 | L 28 | Pseudorandom generators | 6.9.19 | | |
| 29 | L 29 | Public key infrastructure | 9.9.19 | | |
| 30 | L 30 | **Unit III: Key Exchange Protocols:**CCA-secure encryption | 10.9.19 | | |
| 31 | L 31 | Diffie-Hellman key exchange | 12.9.19 | | |
| 32 | L 32 | Public key crypto systems (El Gamal, Paillier) | 13.9.19 | | |
| 33 | L 33 | Public key crypto systems (Rabin, Goldwasser) | 16.9.19 | | |
| 34 | L34 | Key exchange protocols | 19.9.19 | | |
| 35 | L 35 | PGP:Pretty Good Privacy | 26.9.19 | | |
| 36 | L 36 | Kerberos | 27.9.19 | | |
| 37 | L 37 | **Content Beyond Syllabus-KDC Protocols** | 30.9.19 | | |
| 38 | L 38 | IPSEC/VPN | 1.10.19 | | |
| 39 | L 39 | IPSEC/VPN | 4.10.19 | | |
| 40 | L 40 | SSL | 7.10.19 | | |

| | | | | | |
|---|---|---|---|---|---|
| 41 | L 41 | S/MIME:Certificate | 8.10.19 | | |
| 42 | L 42 | S/MIME:Message Processing | 10.10.19 | | |
| 43 | L 43 | PKCSv1.5 | 11.10.19 | | |
| 44 | L 44 | PKCSv1.5 | 14.10.19 | | |
| 45 | L 45 | **Unit IV: Digitized Security:** Digital signatures:Introduction | 15.10.19 | | |
| 46 | L 46 | Digital signatures:Message Digest | 17.10.19 | | |
| 47 | L 47 | Digital signatures:MD5 | 18.10.19 | | |
| 48 | L 48 | Secure hash algorithm(SHA) | 24.10.19 | | |
| 49 | L 49 | SHA1 | 25.10.19 | | |
| 50 | L 50 | Rabin finger print | 31.10.19 | | |
| 51 | L 51 | Digital certificates:Introduction | 04.11.19 | | |
| 52 | L 52 | Digital certificates:Concept,Creation | 05.11.19 | | |
| 53 | L 53 | Digital signature standards:DSS | 07.11.19 | | |
| 54 | L 54 | Firewall | 08.11.19 | | |
| 55 | L 55 | Intrusion detection systems | 11.11.19 | | |
| 56 | L 56 | Byzantine agreement | 14.11.19 | | |
| 57 | L 57 | Secure multiparty computation | 15.11.19 | | |
| 58 | L 58 | Secure multiparty computation | 18.11.19 | | |
| 59 | L 59 | Interactive proof systems | 19.11.19 | | |
| 60 | L 60 | Revision | 20.11.19 | | |