|  |  |  |  |
| --- | --- | --- | --- |
| S. no | Topics | No. of lecture Required | CO |
| 1 | Basic Cryptographic Techniques, | 1 | CO1 |
| 2 | Computational Complexity | 1 | CO1 |
| 3 | Finite Fields, Number Theory | 1 | CO1 |
| 4 | DES | 1 | CO1 |
| 5 | AES | 1 | CO1 |
| 6 | Public Key Cryptosystems | 1 | CO1 |
| 7 | Traffic Confidentiality, Cryptanalysis | 1 | CO1 |
| 8 | Intractable (Hard) Problems | 1 | CO1 |
| 9 | Hash Functions | 1 | CO1 |
| 10 | OSI Security Architecture Privacy of Data. | 2 | CO1 |
| 11 | Linear Cryptanalysis, Elliptic Curve Architecture and Cryptography, , | 1 | CO2 |
| 12 | Differential Cryptanalysis, | 1 | CO2 |
| 13 | DES, Triple DES | 1 | CO2 |
| 14 | Message Authentication and Digital Signatures | 1 | CO2 |
| 15 | Attacks on Protocols | 1 | CO2 |
| 16 | Elliptic Curve Architecture and Cryptography | 1 | CO2 |
| 17 | Public Key Cryptography and RSA, | 1 | CO2 |
| 18 | Key Management, Authentication requirements | 1 | CO2 |
| 19 | Evaluation criteria for AES, Digital forensics including digital evidence handling: Media forensics | 2 | CO2 |
| 20 | Cyber forensics, Software forensics, Mobile forensics. | 1 | CO2 |
| 21 | Buffer Flow attack, Distributed Denial of service attack | 1 | CO3 |
| 22 | Design of Substitution Boxes (S-Boxes), Weak authentication | 1 | CO3 |
| 23 | Hash Functions , Security of Hash Functions, | 2 | CO3 |
| 24 | Secure Hash Algorithm | 1 | CO3 |
| 25 | Authentication applications, Kerberos, | 2 | CO3 |
| 26 | IP security, Pretty Good Privacy (PGP), | 2 | CO3 |
| 27 | Web Security Light weight cryptography for mobile devices | 1 | CO3 |
| 28 | Side channel attacks. | 1 | CO3 |
| 29 | System security, Security Standards, , | 2 | CO4 |
| 30 | Intruders, and Viruses, | 1 | CO4 |
| 31 | Firewalls, Malicious software, | 2 | CO4 |
| 32 | Intrusion Detection System, | 2 | CO4 |
| 33 | Trusted Systems, | 1 | CO4 |
| 34 | Virus Counter measures, | 1 | CO4 |
| 35 | Authentication Strategies. | 1 | CO4 |

**LESSON PLANNING**

**Cryptography and Network Security**

**Paper code ETIT-403**