**UE22EC342BA1: Cryptography (4-0-0-0-4)**

**RR: Dr. SSM**

**EC: Prof. SGH 74 (Teaching) + 10(A/H/P)= 84 slots**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Class**  **#** | **Chapter Title/Reference Literature** | **Topics to be Covered** | **% of Portion Covered** | |
| **Individual** | **Cumulative** |
|  | **Introduction:** | Cryptography, | 1.19 |  |
|  | Text book 1: 1.1 | Security Goals, | 1.19 |  |
|  | Text book 1: 1.1 | Attacks on information systems by adversaries, | 1.19 |  |
|  | Text book 1: 1.2 | Threat analysis | 1.19 |  |
|  | Text book 1: 1.3 | Security services and Mechanisms. | 1.19 |  |
|  | Text book 1: 1.3 | Security services and Mechanisms. | 1.19 |  |
|  | Text book 2: 1.1 | Cryptanalysis, and Steganography | 1.19 |  |
|  | Text book 2: 1.2 | OSI security Architecture, | 1.19 |  |
|  | Text book 2: 1.5 | Model for network Security, Symmetric Cipher Model | 1.19 |  |
|  | Text book 2: 1.6 | Traditional ciphers | 1.19 |  |
|  | **Number Theory:** Text book 1:2.1 | Integer Arithmetic, | 1.19 |  |
|  | Text book 1:2.1 | Euclid’s greatest common divisor algorithm. | 1.19 |  |
|  | Text book 1:2.1 | Extended Euclid’s algorithm. | 1.19 |  |
|  | Text book 1:2.1 | Linear Diophantine Equation | 1.19 |  |
|  | Text book 1:2.1 | Modular Arithmetic, | 1.19 |  |
|  | Text book 1:2.2 | Additive inverse and multiplicative inverse | 1.19 |  |
|  | Text Book 1: 2.2 | Matrices | 1.19 |  |
|  | Text Book 1: 4.1, | Linear congruence | 1.19 |  |
|  | Text Book 1: 4.1 | Numerical on linear congruence | 1.19 |  |
|  | Text Book 1: 9.1, | Chinese remainder theorem. | 1.19 |  |
|  | Text Book 1: 9.1, | Numerical on Chinese remainder theorem. | 1.19 | 25 |
| **UNIT 2** | | | | |
|  | Text Book 1: 9.2, | Block ciphers, stream ciphers and Product ciphers. | 1.19 |  |
|  | Text Book 1: 9.4 | Block ciphers, stream ciphers and Product ciphers | 1.19 |  |
|  | Text Book 1: 3.1 | Kirchhoff’s principle: Key domain, Entropy of key. | 1.19 |  |
|  | Text Book 1: 3.2 | Substitution cipher and Transposition cipher | 1.19 |  |
|  | Text book 1:5.1, | Modern block ciphers | 1.19 |  |
|  | Text book 1:6.2 | Shannon’s principles of confusion and diffusion. | 1.19 |  |
|  | Text Book 1: 6.2 | Data Encryption Standard (DES): | 1.19 |  |
|  | Text Book 1: 6.4 | DES Structure, | 1.19 |  |
|  | Text Book 1: 7.2- | Multiple DES, | 1.19 |  |
|  | Text Book 1:7.6, | DES Security Analysis. | 1.19 |  |
|  | Text Book 1:8.1 | Advanced Encryption Standard (AES): Transformations, | 1.19 |  |
|  | Text Book 1:8.1 | Advanced Encryption Standard (AES): Transformations, | 1.19 |  |
|  | Text Book 1:8.1 | Advanced Encryption Standard (AES): Transformations, | 1.19 |  |
|  | Text Book 1:8.1 | Advanced Encryption Standard (AES): Transformations, | 1.19 |  |
|  | Text Book 1:8.1 | Key expansion, AES Security analysis. | 1.19 |  |
|  | Text Book 1:8.2 | Use of Modern block ciphers Techniques (ECB, CBC, CFB, OFB, and CTR) to use block to encrypt large files. | 1.19 |  |
|  | **One-Way Hash (OWH) Functions:** Text book 1:9.3 | one-way hash functions | 1.19 |  |
|  | Text book 1:9.3 | pre-image resistance, second-preimage resistance and | 1.19 |  |
|  | Text book 1:9.3 | collision-resistance) via birthday theorems; | 1.19 |  |
|  | Text book 1:9.3 | Message authentication via Message Authentication Codes (MAC): | 1.19 |  |
|  | Text book 1:9.3 | HMAC, NMAC, CMAC. | 1.19 | 50 |
| **Unit 3** | | | | |
|  | Text Book 1: 9.1, | Euler’s Totient Function | 1.19 |  |
|  | Text Book 1: 9.1, | Euler’s theorem, and Fermat’s theorem | 1.19 |  |
|  | Text Book 1: 9.1, | Euler’s theorem, and Fermat’s theorem | 1.19 |  |
|  | Text Book 1: 9.1, | Asymmetric Key Cryptography (AKC): | 1.19 |  |
|  | Text book 1:9.3 | Introduction and RSA crypto-system. | 1.19 |  |
|  | Text book 1:9.6. | Message Integrity and Random Oracle Model. | 1.19 |  |
|  | Text book 1:9.6 | Cryptography hash functions: | 1.19 |  |
|  | Text book 1:10.2, | Introduction to hash, SHA- 512 and Whirlpool*.* | 1.19 |  |
|  | Text book 1: 10.4 | Attacks on digital signatures. | 1.19 |  |
|  | Text book 1: 12.1- 12.4 | Digital signature algorithms (RSA). | 1.19 |  |
|  | Text book 1:13.4 | El-Gamal, Digital Signature Algorithm. | 1.19 |  |
|  | Text book 1:13.5 | Schnorr, Digital Signature Algorithm. | 1.19 |  |
|  | Text book 1:13.5 | Applications of digital signatures. | 1.19 |  |
|  | Text book 1:13.5 | Digital Signatures via One Time Signature (OTS). | 1.19 |  |
|  | Text book 1:13.6 | Entity authentication via smart-cards, passwords. | 1.19 |  |
|  | Text book 1:13.6 | Biometrics, Challenge-response protocols. | 1.19 |  |
|  |  | A/H/P | 1.19 |  |
|  |  | A/H/P | 1.19 |  |
|  |  | A/H/P | 1.19 |  |
|  |  | A/H/P | 1.19 |  |
|  |  | A/H/P | 1.19 | 75 |
| Unit 4 | | | | |
|  |  | Internal structure of OWH functions: Compression functions | 1.19 |  |
|  | Text book 1:14.3 | SHA-512, Applications of OWH functions: Message integrity | 1.19 |  |
|  | Text book 1:14.3 | Passwords, and Biometrics. zero-knowledge protocols, | 1.19 |  |
|  | Text book 1:14.4 | Challenge-response protocols, | 1.19 |  |
|  | Text book 1:14.5 | 2-factor authentication via One Time Passwords (OTPs), | 1.19 |  |
|  | Text book 1:15.1 | Zero-knowledge protocols, | 1.19 |  |
|  | Text book 1:15.2 | Authenticated Key Exchange Protocols: | 1.19 |  |
|  | Text book 1:15.3 | 2-factor authentication via One Time Passwords (OTPs). | 1.19 |  |
|  | Text book 1:17.1 | Diffie-Hellman Key Exchange, | 1.19 |  |
|  | Text book 1:17.1 | Station To Station (STS) protocol, | 1.19 |  |
|  | Text book 1:17.1 | Key Management in the Kerberos system | 1.19 |  |
|  | Text book 1:17.1 | Key Management in the Kerberos system | 1.19 |  |
|  | Text book 1:17.1 | Digital Certifying Authority (CA), | 1.19 |  |
|  | Text book 1:17.1 | Certificate Revocation List (CRL). | 1.19 |  |
|  | Text book 1:17.1 | Secure Sockets Layer (SSL) protocol, Secret splitting techniques: Attacks | 1.19 |  |
|  | Text book 1:17.1 | Defense mechanisms on Internet-based systems; Systems Security | 1.19 |  |
|  |  | A/H/P | 1.19 |  |
|  |  | A/H/P | 1.19 |  |
|  |  | A/H/P | 1.19 |  |
|  |  | A/H/P | 1.19 |  |
|  |  | A/H/P | 1.19 | 100 |

**Text Books:**

1. “Cryptography and Network Security”, Behrouz A. Forouzan and Debdeep Mukhopadhyay, 3rd Edition, Tata McGraw-Hill, 2010.

**Reference Books:**

1. “Cryptography and Network Security”, William Stalling, Pearson Education, 7th Edition, 2017.
2. “Computer Networking: A Top Down Approach”, James Kurose and Keith Ross, 5th Edition, Pearson, 2012.
3. “Cryptography and Network Security”, AtulKahate, TMH, 2003.
4. “A Computational Introduction to Number Theory and Algebra”, Cambridge University Press, Victor Shoup, 2005.
5. “Handbook of Applied Cryptography, CRC Press”, Alfred Menezes, Paul, Oorschot, and Scott Vanstone, 1996.

**Assessment plan:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Event** | **Portion** | **Marks** | | **Mode** |
| A/H/P |  | 10 (A/H/P 1-10) | | **Coding, Report** |
| ISA 1 | Units 1 and 2 | 40 | Scaled to 20 | **Hybrid mode** |
| ISA 2 | Units 3 and 4 | 40 | **Hybrid mode** |
| **Total ISA** | | **50** | |  |
| ESA – Theory | Units 1, 2, 3, 4 | 100 | Scaled to 50 | **Hybrid mode** |
| **Total ESA** |  | **50** |  |  |
| **Total ISA + ESA** |  | **100** | |  |