**ICT 4102 INFORMATION & WEB SECURITY**

**Syllabus**

|  |  |  |  |
| --- | --- | --- | --- |
| **Unit** | **Topics** | **Sections** | **Text Book** |
| Introduction to Information and Network Security | Computer Security Concepts | S 1.1 | Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings |
| The OSI Security Architecture | S 1.2 |
| Security Attacks | S 1.3 |
| Security Services | S 1.4 |
| Security Mechanisms | S 1.5 |
| A Model for Network Security | S 1.6 |
| Symmetric-Key Ciphers | Kerckhoff’s principle | F 3.1 | Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings;  Cryptography and Network Security (4th Edition)  by Behrouz A.Forouzan, McGraw-Hill |
| Substitution ciphers | F 3.2; S 2.1 2.2 |
| Transposition ciphers | F 3.3 ; S 2.3 |
| Stream and block ciphers | F 3.4 ; S 3.1 |
| DES | F 6 .2; S 3.2 3.3 |
| AES | F 7.1 ; S 5.2 5.5 |
| Use of modern block ciphers | F 5.1 |
| Mathematical Tools of Symmetric Cryptography | Modular arithmetic | F 2.2, S 4.3 | Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings;  Cryptography and Network Security (4th Edition)  by Behrouz A.Forouzan, McGraw-Hill |
| Linear Congruence | F 2.4 |
| Algebraic structures | F 4.1 |
| GF fields | F 4.2,S 4.4 |
| Mathematical Tools for Asymmetric Cryptography | Primes | F 9.1 | Cryptography and Network Security (4th Edition)  by Behrouz A.Forouzan, McGraw-Hill |
| Primality testing | F 9.2 |
| Factorization | F 9.3 |
| CRT | F 9.4 |
| Quadratic congruence | F 9.5 |
| Exponentiation and logarithm | F 9.6 |
| Asymmetric-Key Cryptography | Introduction | F 10.1 | Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings;  Cryptography and Network Security (4th Edition)  by Behrouz A.Forouzan, McGraw-Hill |
| RSA Cryptosystems | F 10.2;  S 9.1 9.2 |
|  | Rabin | F 10.3 |
| ElGamal | F 10.4 S 10.2 |
| ECC | F 10.5 S10.4 |
| Message Integrity and Message Authentication | Message integrity | F 11.1 | Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings;  Cryptography and Network Security (4th Edition)  by Behrouz A.Forouzan, McGraw-Hill |
| Random Oracle model | F 11.2 |
| Message authentication | F 11.3 S 12.1 |
| Hash function | F 12.1 S 11.4 |
| SHA-512 | F 12.2 S 11.5 |
| Whirlpool | F 12.3 |
|  | Digital signature schemes: RSA  ElGamal  Schnorr  ECC  Digital Signature Standard | F 13.5 S 13.1 -13.4 | Cryptography and Network Security (4th Edition)  by Behrouz A.Forouzan, McGraw-Hill ;  Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings |
| Attacks on digital signature | F 13.4 |
| User Authentication | Passwords | F 14.1 | Cryptography and Network Security (4th Edition)  by Behrouz A.Forouzan, McGraw-Hill ;  Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings |
| Challenge-response | F 14.2 |
| Zero-knowledge | F 14.3 |
| Biometrics | F 14.4 -14.5 |
| Key Management | KDC | F 15.1 | Cryptography and Network Security (4th Edition)  by Behrouz A.Forouzan, McGraw-Hill ;  Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings |
| Kerberos | F 15.2 |
| Public key distribution: CA | F 15.3 |
| PKI | F 15.4 |
| Email Security | PGP | S 18.1 | Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings; |
| S/MIME | S 18.2 |
| Transport Layer Security | Web Security Considerations | S 16.1 | Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings;  Cryptography and Network Security (4th Edition)  by Behrouz A.Forouzan, McGraw-Hill |
| Secure Socket Layer and  Transport Layer Security | S 16.2 16.3; F 17.1 17.4 |
| HTTPS | S 16.4 |
| SSH | S 16.5 |
| Overview, IP Security Policies | Overview | S 19.1 | Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings; |
| IP Security Policies | S 19.2 |
| Wireless Network Security | Wireless LAN overview | S 17.1 | Cryptography and Network Security: Principles and Practice (5th Edition)  by William Stallings; |
| Wireless LAN Security | S 17.2 |