**ACADEMIC YEAR: 2022-2023**

**YEAR:** III **SEMESTER:** II

**SUBJECT NAME**: CRYPTOGRAPHY AND NETWORK SECURITY **REGULATION**: R20

**QUESTION BANK**

**UNIT-1**

|  |  |  |  |
| --- | --- | --- | --- |
| Q. No | Question | Marks | Cognitive level |
| 1 | Explain the three security goals | **5M** | **L1** |
| 2 | Explain about Cryptographic Attacks | **10M** | **L1** |
| 3 | Explain about security services | **5M** | **L1** |
| 4 | Explain about security mechanisms | **10M** | **L1** |
| 5 | Write and explain about Euclidean algorithm | **5M** | **L1** |
| 6 | Explain the extended Euclidean algorithm. Find gcd (a, b) and  the values of s and t for given a=161 and b=28 | **10M** | **L3** |
| 7 | State and prove the properties of modular arithmetic binary  Operations | **5M** | **L1** |
| 8 | Using the extended Euclidean algorithm, find gcd(291, 42)  And the values of s and t | **5M** | **L2** |
| 9 | Distinguish between passive and active security attacks. Name  some passive attacks. Name some active attacks | **10M** | **L2** |
| 10 | Find the particular and the general solutions to the following  linear Diophantine equation. 25x + 10y = 15 | **5M** | **L3** |
| 11 | Define the following terms i) Modulo operator, ii) Congruence | **5M** | **L1** |
| 12 | Find all solutions to linear equation: 3x ≅ 4 (mod 5) | **5M** | **L3** |

**UNIT-2**

|  |  |  |  |
| --- | --- | --- | --- |
| Q. No | Question | Marks | Cognitive level |
| 1 | Define the following terms with suitable examples   1. Group 2. Ring 3. Field | **10M** | **L1** |
| 2 | Write short notes on Substitution and Permutation | **5M** | **L1** |
| 3 | Briefly explain about symmetric key cryptography. | **5M** | **L1** |
| 4 | Explain in detail Fiestel Block Cipher structure with neat sketch. Distinguish between a Feistel and a non-Feistel block cipher | **10M** | **L1, L3** |
| 5 | Explain about Round Function in Data Encryption Standard. | **5M** | **L1** |
| 6 | Explain about different transformations in Advanced Encryption  Standard. | **5M** | **L1** |
| 7 | Explain DES cryptography in detail | **10M** | **L1** |
| 8 | Briefly explain about CAST algorithm | **10M** | **L1** |
| 9 | Explain about general structure of AES algorithm | **10M** | **L1** |
| 10 | Explain about Blowfish algorithm | **10M** | **L1** |
| 11 | Explain IDEA algorithm. | **10M** | **L1** |
| 12 | Explain about Design Criteria and Properties of DES | **5M** | **L1** |

**UNIT-3**

|  |  |  |  |
| --- | --- | --- | --- |
| Q. No | Question | Marks | Cognitive level |
| 1 | Define Euler’s Phi-Function. Explain briefly about Fermat’s  theorem with examples | **10M** | **L1** |
| 2 | Difference between Symmetric key cryptography and asymmetric  cryptography. | **5M** | **L1** |
| 3 | Explain briefly about Eluer’s theorem with examples | **5M** | **L1** |
| 4 | What is meant by primality testing? Explain about deterministic algorithms and probabilistic algorithms for  primality test. | **10M** | **L1** |
| 5 | Explain the Pollard rho Method for factorization. Explain about Chinese reminder theorem and its application. | **10M** | **L1** |
| 6 | Given the super increasing tuple b=[7,11,23,43,87,173,357], r=41, and modulus n=1001, encrypt and decrypt the letter using the knapsack cryptosystem. Use [7 6 5 1 2 3 4] as the permutation  table. | **10M** | **L1** |
| 7 | Find the value of x for the following sets of congruence using  the Chinese reminder theorem. x  2 mod 7 and x  3 mod  9 | **5M** | **L3** |
| 8 | Explain about Discrete logarithm with the properties. | **5M** | **L1** |
| 9 | Find the result of 312 mod 11 and 5 -1 mod 23.  Given p=19, q=23, and e=3. Use RSA algorithm to find n, Ø(n) and  d. | **10M** | **L3** |
| 10 | Explain in detail about RSA Key generation, encryption and  decryption process | **10M** | **L1** |
| 11 | Explain in detail about Rabin Cryptosystem | **10M** | **L1** |
| 12 | Explain about Elliptic Curve Cryptography in detail. | **10M** | **L1** |
| 13 | Explain about ElGamal Cryptosystem in detail | **10M** | **L1** |

**UNIT-4**

|  |  |  |  |
| --- | --- | --- | --- |
| Q. No | Question | Marks | Cognitive level |
| 1 | What is Message Authentication code? Explain its functions and  basic uses. | **5M** | **L1** |
| 2 | Distinguish between Message Integrity and Message  Authentication. | **5M** | **L2** |
| 3 | Explain about HMAC algorithm with a neat diagram | **10M** | **L1** |
| 4 | Explain about CMAC algorithm | **10M** | **L1** |
| 5 | Discuss Secure Hash Algorithm in detail | **10M** | **L2** |
| 6 | What is KDC? Explain with neat diagrams | **10M** | **L1** |
| 7 | What are the methods used to distribute the symmetric key?  Explain | **10M** | **L1** |
| 8 | Discuss how public key is distributed in Asymmetric key  Cryptography | **10M** | **L2** |
| 9 | Explain about Digital Signature algorithm in detail | **10M** | **L2** |
| 10 | What is Kerberos protocol and explain in detail. | **10M** | **L2** |
| 11 | Describe Certificate Authority and X.509 Certificate. | **10M** | **L2** |

**UNIT-5**

|  |  |  |  |
| --- | --- | --- | --- |
| Q. No | Question | Marks | Cognitive level |
| 1 | What is PGP. Discuss about its services | **10M** | **L1** |
| 2 | Discuss how PGP key rings are maintained by the user. | **10M** | **L2** |
| 3 | Describe how trust in PGP is achieved using web of trust model | **10M** | **L2** |
| 4 | Explain how email messages are protected using S/MIME  signing and encryption? | **10M** | **L1** |
| 5 | Draw and discuss the Architecture of IPSec | **10M** | **L2** |
| 6 | Differentiate the packet structure of ESP and AH. | **10M** | **L2** |
| 7 | Explain about SSL protocol in detail | **10M** | **L1** |
| 8 | What is the use of SSL protocol? Explain SSL record protocol  operation with SSL record format. | **10M** | **L1** |
| 9 | Explain Advantages and Disadvantages of Packet Filters, Circuit-  Level Firewalls, and Application Layer Firewalls | **10M** | **L2** |
| 10 | What is a firewall? What is the need for firewalls? What is the  role of firewalls in protecting networks? | **10M** | **L2** |