

University of Mumbai
Examinations Summer 2022

Time: 2 hour 30 minutes

Max. Marks: 80

| | |
|------------|--|
| Q1. | Choose the correct option for following questions. All the Questions are compulsory and carry equal marks |
| 1. | The principle of ensures that the sender of a message cannot later deny sending of the message |
| Option A: | Authentication |
| Option B: | Non repudiation |
| Option C: | Access control |
| Option D: | Integrity |
| 2. | Rail Fence Technique is an example of |
| Option A: | Substitution |
| Option B: | Transposition |
| Option C: | product cipher |
| Option D: | Caesar cipher |
| 3. | The number of symmetric keys needed for one to one communication between 8 people is |
| Option A: | 256 |
| Option B: | 32 |
| Option C: | 28 |
| Option D: | 8 |
| 4. | For the Knapsack: {1 6 8 15 24}, find the plain text code if the ciphertext is 39 |
| Option A: | 10010 |
| Option B: | 11101 |
| Option C: | 10101 |
| Option D: | 00111 |
| 5. | The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not |
| Option A: | Authenticated |
| Option B: | Joined |
| Option C: | Submit |
| Option D: | Separate |
| 6. | What is honey pot attack? |
| Option A: | dummy device put into the network to attract attackers |
| Option B: | single line threat |
| Option C: | IP spoofing bypass |
| Option D: | recognition attack |
| 7. | Which is not a component of Public key infrastructure (PKI)? |
| Option A: | Client |
| Option B: | CRL |
| Option C: | CA |
| Option D: | KDC |

| | |
|-----------|--|
| 8. | The attack in which the attacker aims at exhausting the targeted server's resources. |
| Option A: | Phishing attack |
| Option B: | DoS attack |
| Option C: | Website scripting attack |
| Option D: | SQL injection attack |
| 9. | Secure Hash Algorithm -1 (SHA-1) has a message digest of |
| Option A: | 160 bits |
| Option B: | 512 bits |
| Option C: | 628 bits |
| Option D: | 820 bits |
| 10. | Which of the following is considered as the unsolicited commercial email? |
| Option A: | Virus |
| Option B: | Malware |
| Option C: | Spam |
| Option D: | Adware |

| | |
|-----------|---|
| Q2 | |
| A | Solve any Two 5 marks each |
| i. | Explain the relationship between Security Services and Mechanisms in detail. |
| ii. | Explain ECB and CBC modes of block cipher. |
| iii. | Define non-repudiation and authentication. Show with example how it can be achieved. |
| B | Solve any One 10 marks each |
| i. | Elaborate the steps of key generation using the RSA algorithm. In RSA system the public key (E, N) of user A is defined as (7,187). Calculate $\Phi(N)$ and private key 'D'. What is the cipher text for M=10 using the public key. |
| ii. | Discuss DES with reference to following points 1. Block size and key size 2. Need of expansion permutation 3. Role of S-box 4. Weak keys and semi weak keys 5. Possible attacks on DES |

| | |
|-----------|---|
| Q3 | |
| A | Solve any Two 5 marks each |
| i. | What are properties of hash function? Explain role of hash function in security. |
| ii. | Explain working of TGS in Kerberos. |
| iii. | List and explain various types of attacks on encrypted message. |
| B | Solve any One 10 marks each |
| i. | Why are digital certificates and signatures required? What is the role of digital signature in digital certificates? Explain any one digital signature algorithm. |
| ii. | What is the need for message authentication? List various techniques used for message authentication. Explain any one of them. |

| | |
|------------|--|
| Q4. | |
|------------|--|

| | | |
|----------|--|----------------------|
| A | Solve any Two | 5 marks each |
| i. | Explain handshake protocol in SSL. | |
| ii. | Explain buffer overflow attack. | |
| iii. | List various Software Vulnerabilities. How vulnerabilities are exploited to launch an attack. | |
| B | Solve any One | 10 marks each |
| i. | How does PGP achieve confidentiality and authentication in emails? | |
| ii. | How is security achieved in Transport and Tunnel modes of IPSEC? Explain the role of AH and ESP. | |