Program: BE

|  |  |  |  |
| --- | --- | --- | --- |
| Date | 23 June 2025 | Maximum Marks | 50 |
| Course Code | **CS362AI** | Duration | 90 min |
| 6th Sem | VI Semester | CIE-III | |
| **Network Programming and Security** | | | |

|  |  |  |
| --- | --- | --- |
|  | **QUIZ** |  |
| 1 | The left half becomes the new right half in the next round, and the previous right half is combined with the output of the round function using XOR to become the new left half—thus both halves influence the final output. | 2 |
| 2 | S-boxes in DES provide non-linearity and confusion by converting 6-bit inputs into 4-bit outputs. This transformation helps resist cryptanalysis techniques like linear and differential attacks. | 2 |
| 3 | A public-key cryptosystem must have computationally easy key generation, encryption, and decryption, but the private key should be infeasible to derive from the public key. | 2 |
| 4 | **A = g^a mod p = 3^6 mod 17 = 729 mod 17 = 16** So, A sends **16** to B. | 2 |
| 5 | SSL/TLS use **digital certificates** issued by trusted Certificate Authorities (CAs). During the **TLS handshake**, the server presents its certificate, and the client **verifies the server’s identity** using the CA’s public key, ensuring authentication and preventing impersonation. | 2 |
| **Sl. No.** | **Test Questions** | **M** |
| 1a | Single round explanation – 6 Marks  Advantages – 2 Marks  Disadvantages – 2 Marks | **10** |
| 2.a | * Each user has a pair of keys: public and private. * The public key is shared openly, while the private key is kept secret. * Messages encrypted with the public key can only be decrypted with the private key. * It must be computationally infeasible to determine the private key from the public key. * Ensures confidentiality, integrity, authentication, and non-repudiation. | **5** |
| 2.b |  | **5** |
| 3.a | * **Public-key cryptanalysis** aims to break the system by deriving the private key from the public key. * Common attacks include:   + **Mathematical attacks** (e.g., factoring large numbers in RSA).   + **Timing attacks** (analyzing time taken for operations).   + **Chosen ciphertext attacks** (feeding chosen inputs to see outputs).   + **Man-in-the-middle attacks** (in key exchange protocols). * Proper key sizes and secure implementations are essential to prevent such attacks. | **5** |
| 3.b |  | **5** |
| 4 | * Algorithm 3 Marks * Key exchange protocol – 3 Marks * Man in the middle attack – 4 marks | **10** |
| 5 | * Introduction to https – 2 Marks * Basic concepts of SSL/TLS – 2 marks * **Steps in HTTPS Handshake – 4 Marks** * Security Services Provided – 2 Marks | **10** |

**Course Outcomes**

|  |  |
| --- | --- |
| CO1 | Explore the variety of network programming concepts and protocols. |
| CO2 | Analyse the interoperability of networking protocols and its usage. |
| CO3 | Design the client/server communication on Unix platforms. |
| CO4 | Investigate & Design the cryptographic algorithms to ensure secure transfer of secret keys and encryption/decryption of messages. |
| CO5 | Demonstrate Network Programming and Cryptographic algorithms to solve real-world problems. |

**Blooms’ taxonomy**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| L1 | L2 | L3 | L4 | L5 | L6 | CO1 | CO2 | CO3 | CO4 | CO5 | CO6 |
| 14 | 20 | 16 | - | - | - | 19 | 16 | 15 | - | - | - |