| Reg. No | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

# B.Tech DEGREE EXAMINATION, JUNE 2024

Fifth & Sixth Semester

## 18CSE381T - CRYPTOGRAPHY

*(For the candidates admitted during the academic year 2018-2019 to 2021-2022)*

**Note:**

i. **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

ii. **Part - B** and **Part - C** should be answered in answer booklet.

**Time: 3 Hours** **Max. Marks: 100**

**PART - A (20 × 1 = 20 Marks)** — Answer **all** Questions

| | | Marks | BL | CO |
|---|---|---|---|---|
| 1. | Ensuring the confidential information is not disclosed to unauthorized individual is called as,<br>(A) Data breach (B) Data confidentiality<br>(C) Data integrity (D) Data availability | 1 | 1 | 1 |
| 2. | Name the type of active attack when one entity pretends to be a different entity.<br>(A) Traffic analysis (B) Replay<br>(C) Masquerade (D) Release of message content | 1 | 2 | 1 |
| 3. | What is the process that uses mathematical algorithm and transforms data into a form that is not readily intelligible?<br>(A) Encipherment (B) Digital signature<br>(C) Access control (D) Hashing | 1 | 2 | 1 |
| 4. | The method of inserting bits into gaps in a data stream to frustrate traffic analysis attempts is called as,<br>(A) Encryption (B) Notarization<br>(C) Traffic analysis (D) Traffic padding | 1 | 1 | 1 |
| 5. | Find the 8-bit word related to the polynomial $x^6 + x^5 + x^2 + x + 1$.<br>(A) 00010011 (B) 11000110<br>(C) 00100110 (D) 01100111 | 1 | 3 | 2 |
| 6. | What is $\Phi(37)$?<br>(A) 2 (B) 3<br>(C) 36 (D) 37 | 1 | 5 | 2 |
| 7. | What is the relationship between two integers, when their only common positive integer factor is 1?<br>(A) Primitive root (B) Relatively prime<br>(C) Distributive (D) Commutative | 1 | 3 | 2 |
| 8. | Solve -11mod7.<br>(A) 2 (B) 4<br>(C) 3 (D) 6 | 1 | 5 | 2 |
| 9. | The strategy that seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key is called as,<br>(A) Confusion (B) Diffusion<br>(C) Encryption (D) Decryption | 1 | 1 | 3 |
| 10. | The key size in DES algorithm is<br>(A) 36 bits (B) 48 bits<br>(C) 56 bits (D) 66 bits | 1 | 1 | 3 |

| | | | | |
|---|---|---|---|---|
| 11. | A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext. Identify the effect.<br>(A) Raman effect (B) Zero day effect<br>(C) Paradox effect (D) Avalanche effect | 1 | 2 | 3 |
| 12. | Pick the type of block cipher mode that is used for satellite communication.<br>(A) Electronic Code Book (B) Cipher Block Chaining<br>(C) Output Feedback mode (D) Cipher Feedback mode | 1 | 3 | 3 |
| 13. | In public key cryptosystem, the key that is used to perform decryption to ensure the confidentiality is<br>(A) Shared key (B) Private key<br>(C) Public key (D) Secret key | 1 | 1 | 4 |
| 14. | The type of attack that depends on the running time of the decryption algorithm is,<br>(A) Zero day attack (B) Brute force attack<br>(C) Mathematical attack (D) Timing attack | 1 | 2 | 4 |
| 15. | Pick the algorithm that enables two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages.<br>(A) Elgamal cryptosystem (B) Diffie Hellman key exchange<br>(C) RSA (D) DES | 1 | 2 | 4 |
| 16. | Solve. $11^5$ mod 19.<br>(A) 7 (B) 1<br>(C) 3 (D) 11 | 1 | 5 | 4 |
| 17. | Any modification to a sequence of messages between parties, including insertion, deletion, and reordering is called as,<br>(A) Content modification (B) Timing modification<br>(C) Sequence modification (D) Source repudiation | 1 | 1 | 3 |
| 18. | Which function accepts a variable-length block of data M as input and produces a fixed-size hash value h=H(M)?<br>(A) Encryption (B) Polynomial arithmetic<br>(C) MAC function (D) Hash function | 1 | 1 | 4 |
| 19. | When a hash function is used to provide message authentication, the hash function value is often referred to as,<br>(A) message digest (B) digram<br>(C) key (D) secret key | 1 | 1 | 4 |
| 20. | Which of the following is the cryptographic checksum?<br>(A) Message Authentication Code (B) Digital Signature<br>(C) Hash (D) Private key | 1 | 2 | 3 |

**PART - B (5 × 4 = 20 Marks)**

Answer **any 5** Questions

| | | Marks | BL | CO |
|---|---|---|---|---|
| 21. | With a neat diagram, explain the network security model. | 4 | 1 | 1 |
| 22. | Using the extended Euclidean algorithm, find the multiplicative inverse of 1234 mod 4321. | 4 | 3 | 2 |
| 23. | Differentiate Cipher Feedback Mode and Output Feedback Mode. | 4 | 4 | 3 |
| 24. | Explain the significance of RSA algorithm. | 4 | 1 | 4 |
| 25. | Discuss the applications of cryptographic hash functions. | 4 | 4 | 4 |
| 26. | Find x for the given set of congruent equations using Chinese Remainder Theorem. $x \equiv 1 \pmod 5$; $x \equiv 1 \pmod 7$; $x \equiv 3 \pmod{11}$; | 4 | 5 | 2 |

| | | Marks | BL | CO |
|---|---|---|---|---|
| 27. | Encrypt the plain text "cryptography" with key "monarchy" using Playfair cipher. Briefly explain its rules. | 4 | 5 | 1 |

**PART - C (5 × 12 = 60 Marks)**

Answer **all** Questions

| | | Marks | BL | CO |
|---|---|---|---|---|
| 28. | (a) Briefly discuss about the various security services and security mechanisms. | 12 | 3 | 1 |
| | **(OR)** | | | |
| | (b) Encrypt the plain text "networks" using Hill cipher. [key: ciphering]. | | | |
| 29. | (a) Construct the addition and multiplication tables for GF($2^3$) using Polynomial Arithmetic Modulo ($x^3 + x + 1$). | 12 | 5 | 2 |
| | **(OR)** | | | |
| | (b) Brief out Fermat's and Euler's theorem with an example and proof. With an example state Fermat's method of primality testing. | | | |
| 30. | (a) Describe the Data Encryption Standard (DES) algorithm with the overview and single round function diagrams. | 12 | 2 | 3 |
| | **(OR)** | | | |
| | (b) Explain in detail the key generation ,encryption and decryption process with appropriate equations of Blowfish algorithm. | | | |
| 31. | (a) Summarize the RSA algorithm and encrypt the message M=88 using RSA algorithm. Use p=17, q=11, e=7. | 12 | 5 | 4 |
| | **(OR)** | | | |
| | (b) Show the secret key exchange process using Diffie Hellman key exchange algorithm. Perform Key exchange based on the use of the prime number $q = 353$ and a primitive root , $\alpha = 3$. A and B select private keys $X_A = 97$ and $X_B = 233$, respectively. | | | |
| 32. | (a) Explain in detail about the SHA-512 algorithm with an example. | 12 | 3 | 3 |
| | **(OR)** | | | |
| | (b) Discuss the process of generating and verifying digital signatures using ElGamal Digital Signature Scheme.q=19, $\alpha$=10, $X_A$=16, K=5. | | | |

* * * * *