X/D/TZ

Reg. No: 23BCE2093

Final Assessment Test – April 2026

VIT
Vellore Institute of Technology

Course: BCSE309L - Cryptography and Network Security

Class NBR(s): 1923/1928/1931/1932/1934/1935/1936/1938/1941/1943/1946/1948/1950/1954/1959/1982/2478 Slot: B1+TB1

Time: Three Hours Max. Marks: 100

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

COs	CO Statements
CO1	To know the fundamental mathematical concepts related to security.
CO2	To understand concept of various cryptographic techniques.
CO3	To apprehend the authentication and integrity process of data for various applications.
CO4	To know fundamentals of Transport layer security, web security, E-Mail Security and IP Security.

BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)

Answer ALL Questions
(10 X 10 = 100 Marks)

1. Use the Extended Euclidean Algorithm to: CO1 BL3
   - Find gcd(867,255) [6]
   - Express it in the form ax+by [2]
   - Determine whether a modular inverse exists [2]

2. a) Find 7^{100} mod 13 using Fermat's theorem. [5] CO1 BL3
   b) Determine all primitive roots modulo 9. [5]

3. A user applies Elliptic Curve Cryptography with curve: CO2 BL3
   $y^2 \equiv x^3+3x+5 \pmod{19}$. Find all points on the curve and verify any two points that belongs to the curve.

4. A user applies SHA-512 to a message "**SECURITY**". Calculate first 16 words and Compute the next words W16 to W19. Show all intermediate steps. CO2 BL4

5. In a university network, students access multiple services (email, library, database) using a single login through Kerberos. Describe the authentication process and explain how Kerberos achieves Single Sign-On (SSO). Illustrate the role of AS, TGS, and service servers. CO3 BL2

6. A branch office communicates with headquarters over the internet using IPsec in tunnel mode. Explain how ESP protects the entire IP packet and ensures secure communication. Describe the sequence of encapsulation and decapsulation. CO4 BL2

7. A company uses Pretty Good Privacy for secure email communication between employees. Explain how PGP ensures Confidentiality, Integrity and Authentication. Describe the sequence of operations involved. CO4 BL3

8. A banking system provides online transaction services to customers. Due to increasing cyber threats such as phishing, unauthorized access, and denial-of-service attacks, the bank plans to deploy a robust firewall architecture. Explain how firewall design principles can be applied in this scenario and discuss the role of access control policies and filtering mechanisms. CO4 BL4

9.a) A sender wants to send a plaintext **"89ABCDEF01234567"** to a receiver through a social network. He/she applies Data Encryption Standard algorithm for encryption and uses the key as **"0F15 71C9 47D9 E859"**. Show the key generated for the first two rounds. CO2 BL3

Permuted Choice Table

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

Expansion Permutation Table

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

OR

9.b) A sender wants to encrypt the plaintext PT=[3 1 4 1] using RC4 algorithm with the Key=[1 5 9 2]. Perform KSA and PRGA, and generate the ciphertext. CO2 BL3

10.a) A person uses the ElGamal digital signature scheme for authentication. Consider the following parameters: prime number p=37, generator g=2, private key x=11, and a randomly chosen integer k=13. The message to be signed is m=9. Generate the digital signature pair (r,s) using the ElGamal digital signature algorithm and verify the correctness of the signature. CO3 BL3

OR

10.b) A user wants to digitally sign a message using the Digital Signature Algorithm. Consider the parameters: prime numbers p=47, q=23, generator g=4, private key x=7, and a randomly chosen integer k=5. The message to be signed is m=12. Generate the digital signature pair (r,s) and verify the correctness of the signature. CO3 BL3

⇔⇔⇔ **X/D/TZ** ⇔⇔⇔