PSG COLLEGE OF TECHNOLOGY, COIMBATORE - 641 004

Department ofApplied Mathematics and Computational Sciences

MSc TCS & Sem 5

CONTINUOUS ASSESSMENT TEST 2 Date: 28.10.2025

23XT52- Computational Number Theory and Cryptography

Time: 1 Hour 30 min. **Maximum Marks: 40**

INSTRUCTIONS:

1. Answer **ALL**questions. Each question carries 20 Marks.
2. Subdivision (a) carries 3 marks each, subdivision (b) carries 7 marks each and subdivision (c) carries 10 marks each.
3. Course Outcome Table :

Qn.1	CO.3	Qn.2	CO.4

1.a) i) What is the cipher text corresponding to the RSA plain text $C = 10$, when RSA values are $n = 35, and\ e = 5$? [BTL3]

ii) Justify whether a known-message attack is feasible on the ElGamal cryptosystem. [BTL3]

b) Write any three potential attacks on RSA cryptosystem. [BTL2]

c) Write the Elliptic curve encryption and decryption process. Suppose Bob selects $p = 67$ and the elliptic curve $y^2=x^3+2x+3$ over $GF(13)$. He also selects his secret key as $d = 4$ and $g = (2,22)$. Find out the corresponding public key. [BTL3]

2. a) i) What is MAC? What is the difference between a MAC and a hash function? [BTL2]

ii) What is dictionary attack on password authentication? [BTL2]

b) Explain merkle damgard hash function. Also, assume we have a very simple message digest. The message digest is just one number between 0 and 25. The digest is initially set to 0. The cryptographic hash function adds the current value of the digest to the value of the current character (between 0 and 25). Addition is in modulo 26. What is the value of the digest if the message is "HELLO"? [BTL3]

c) Compute the private key and sign the message "5" using RSA signature scheme with the given values $p = 7, q = 11$ and $e = 7$.
Also compute the ELGamal signature for the given values $e_1 = 10,\ d = 3$ $p = 19,\ M = 17\ and\ r = 5$. [BTL3]