PSG COLLEGE OF TECHNOLOGY, COIMBATORE
DEPARTMENT OF APPLIED MATHEMATICS AND COMPUTATIONAL SCIENCES
M.Sc. CYBER SECURITY

23XC52 – CRYPTANALYSIS

CONTINUOUS ASSESSMENT TEST 2 Date: 28-10-2025

Total marks: 40 21 Duration: 1 hr 30mins

INSTRUCTIONS:

1. Answer **ALL** questions. Each question carries 20 Marks.
2. Subdivision (a)(i), (a)(ii) carries 2 marks each, subdivision (b) carries 6 marks each and subdivision (c) carries 10 marks each.
3. Course Outcome Table :

Qn.1	CO4	Qn.2	CO5

1. (a) (i) What are the steps involved in proving the security of the cryptosystem using the method of provable security? 1 [BTL1]

(ii) What are the applications of pairing-based cryptography? 2 [BTL3]

(b) What is Lattice-Reduction? What are the fundamental steps involved in Lattice-Reduction Attack? 2 [BTL4]

(c) Idealize the ElGamal encryption scheme suitable for providing provable security. Further, prove the security of scheme using random oracle model. [BTL5]
4

2. (a) (i) Distinguish between message authentication and entity authentication. [BTL1]
2

(ii) Does the protocol given below withstands Lowe's attack? If so, give the reason why the attack is not possible. If not, demonstrate the attack and provide an improvement. [BTL3]

$$A \rightarrow B : N_A$$
$$B \rightarrow A : sig_B(N_A)$$

(b) Consider the following protocol [BTL4]

$$A \rightarrow S : M_1 = \{A, S, B, e(NA)\}$$
$$S \rightarrow B : M_2 = \{S, B, A\}$$
$$B \rightarrow S : M_3 = \{B, S, A, e(NB)\}$$
$$S \rightarrow A : M_4 = \{S, A, B, v(NA, NB)\}$$
$$S \rightarrow B : M_5 = \{S, A, B, v(NA, NB)\}$$

The main aim of this protocol is to distribute session keys for mobile communications. The unary constant $e(\cdot)$ denotes a standard encryption

function that only the Server is able to invert, and the binary constant $v(\cdot)$ stands for bit-wise exclusive-or. Demonstrate the protocol fails to enforce agent authentication. 3

(c) (i) Describe the Needham – Schroeder Protocol for symmetric and asymmetric cryptosystems. Further, detail the possible attacks on the schemes and improvements made on them. [BTL5]

(OR)

(ii) Carryout the formal analysis of Needham-Schroeder shared key protocol in BAN logic.

****