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

23XC52 – CRYPTANALYSIS

CONTINUOUS ASSESSMENT TEST 1 **Date: 26-08-2025**

Total marks: 40 **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	CO1	Qn.2	CO2

1. (a) (i) What are the fundamental components of a security system? What are the attacks threatening them? [BTL1]

(ii) What is MD-strengthening? Why it is required in the construction of hash function? [BTL3]

(b) Write a short note on the following attacks: Known plaintext attack, Chosen plaintext attack and Chosen cipher text attack. Also mention in all the three attacks, how do the attacker gets the plaintext, ciphertext pairs? [BTL4]

(c) (i) Explain Eratosthenes's sieve algorithm to list all the prime numbers up to a given bound. In addition, discuss its time and space complexities. Further, make possible improvement and reduce its time complexity. [BTL5]

(OR)

(ii) Explain segmented sieve algorithm with suitable case study and demonstrate its advantage in the reduction of space complexity over Eratosthenes's sieve algorithm.

2. (a) (i) What are the challenges in mounting algebraic and correlation attacks in non-linear shift registers? [BTL1]

(ii) In ORYX cipher, although there is a register X, what is the need for the registers A and X? How their specific contribution in the cipher differ? [BTL3]

(b) State and prove Shannon's theorem. Write the attack game definition of Semantic security. [BTL4]

(c) Define feedback polynomial, output polynomial and cube polynomial for a non-linear shift register. Further, explain the cube attack on NLFSR in detail. [BTL5]