PSG COLLEGE OF TECHNOLOGY, COIMBATORE - 641 004

Department of Applied Mathematics and Computational Sciences

MSc TCS & Sem 5

CONTINUOUS ASSESSMENT TEST 1 Date: 26.08.2025

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. Subdivisions (a)(i) and (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	CO.1	Qn.2	CO.2

1. a) i) Evaluate $3^{87} \bmod 43$. [BTL3]

   ii) Evaluate $11^{7} \bmod 17$ by square and multiply method [BTL3]

   b) Analyze whether 389 is a prime number or a composite number using Miller Rabin algorithm. [BTL4]

   c) Determine whether or not the following linear systems are solvable: If solvable, compute the smallest positive integer x such that $x \equiv 2 \pmod 4$; $x \equiv 2 \pmod 7$; *and* $x \equiv 1 \pmod 9$. Also, solve $63x \equiv 70 \pmod{77}$ [BTL4]

2. a) i) What is cipher text only attack? Give an example for it. [BTL2]

   ii) John is reading a mystery book involving cryptography. In one part of the book, the author gives a ciphertext "CIW" and two paragraphs later the author tells the reader that this is a shift cipher and the plaintext is "yes". In the next chapter, the hero found a tablet in a cave with "XVIEWWWI" engraved on it. John immediately found the actual meaning of the ciphertext. What type of attack did John launch here? Also compute the plaintext. [BTL4]

   b) Encrypt the plaintext "June" using Hill cipher (KP $\pmod{26} \equiv C$) with the key $\begin{pmatrix} 2 & 3 \\ 3 & 6 \end{pmatrix}$. Also compute the inverse key. [BTL3]

   c) Explain Advanced Encryption Standard with all round functions in detail. [BTL4]