DEPARTMENT OF COMPUTER SCIENCE AND ENGG.
NATIONAL INSTITUTE OF TECHNOLOGY, TIRUCHIRAPPALLI.

RETEST

CSPC 63 Principles of Cryptography

22/04/25

Time: 60 mins

ANSWER ALL THE QUESTIONS

MAX: 20 Marks
4 * 5 = 20 marks

1. State and explain Euler's theorem. With examples, explain how it is useful. $a^{\phi(n)} \equiv 1 \bmod n$

2. Use a Playfair Cipher to encipher the message " The key is hidden under the door pad". The secret key can be made by filling the first and part of the second row with the word " GUIDANCE" and filling the rest of the matrix with the rest of the alphabet.

3. What are Galois fields? Explain the significance of Galois fields in AES.

4. (a) In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to an user whose public key is $e = 5$, $n = 35$. What is the plaintext M? (3)

   (b) In ElGamal, what happens when C1 and C2 are swapped during the transmission? (2)

******