

Course	: MSCCS	Date	: 19/02/2026
Subject Code	: MSCCS-104	Time	: 11:30AM TO 01:45PM
Subject Name	: Computational Number Theory and Cryptography	Duration	: 02.15 Hours
		Max. Marks	: 70

Answer the following (Attempt any three) (30)

- Answer the following (Attempt any four) (20)**

- Part – A (Multiple Choice Questions) (10)**

- 1 Euler's theorem is a generalization of:
A Fermat's Little Theorem
B Wilson's Theorem
C CRT
D None
- 2 If $n = pq$ in RSA, the modulus n should be:
A A square
B Product of two primes
C Odd number
D Even number
- 3 In Miller-Rabin test, if a witness exists, the number is:
A Prime
B Composite
C Even
D Unknown
- 4 Jacobi symbol is useful in:
A Encryption
B Hashing
C Primality testing
D Key exchange

- 5 Public key in ElGamal is:
A x B $y = g^x \text{ mod } p$
C k D $H(m)$
- 6 CRT is used in RSA to:
A Improve speed B Encrypt faster
C Avoid keys D Solve hash collisions
- 7 Fermat's Little Theorem is applicable if:
A a and n are co-prime B $a > n$
C a divides n D $a < 1$
- 8 RSA is a type of:
A Symmetric B Asymmetric
C Hybrid D None
- 9 $\text{GCD}(60, 48) = ?$
A 4 B 6
C 12 D 24
- 10 IFF identity scheme is used by:
A Universities B Corporates
C National labs D Schools

Part – B (Do as Directed)

(10)

- 1 Write binary of 19.
- 2 $\phi(9) = ?$
- 3 Simplify $2^5 \text{ mod } 7$.
- 4 Mention one cryptographic application of GCD.
- 5 Convert 21 in base-2.
- 6 Find GCD of 35 and 15.
- 7 Name one primality testing algorithm.
- 8 Identify: Is 143 prime?
- 9 What is output of $\phi(13)$?
- 10 RSA: $p=5, q=11$, find n .
