Mahindra University, Hyderabad

École Centrale School of Engineering
Minor-II Examinations

Program: B. Tech. Branch: CM Year: II Semester: II
Subject: Number Thoery & Cryptography (MA2209)

Date: 15/04/2025 Start Time: 02:00 PM
Time Duration: 1.5 Hours Max. Marks: 20

Instructions:

1) There are 4 questions, all of which are compulsory.
2) Justify your answer wherever required.
3) You can earn up to 2 additional marks beyond the full score by solving Question 4(b).

Course outcomes (COs)

Upon successful completion of the course students will

CO 1: Understand the number theoretic foundations of modern cryptography.

CO 2: Learn about RSA cryptosystem, its implementation and security considerations. Learn different algorithms for primality testing and integer factorization.

CO 3: Understand the discrete logarithm problem, different algorithms for solving it, and learn about the ElGamal Cryptosystem.

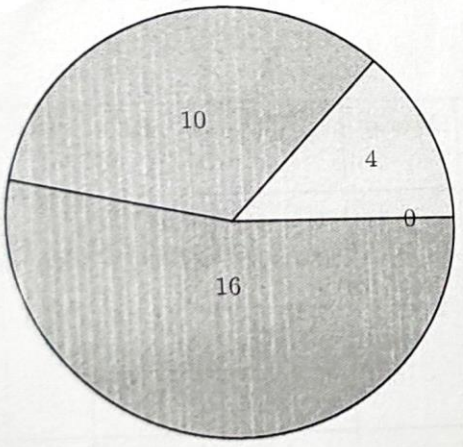
CO 4: Understand the mathematical foundations of elliptic curves and their applications in cryptography such as El-Gamal cryptosystems based on elliptic curves.

CO 5: Learn about different Signature Schemes such as RSA and Elgamal.

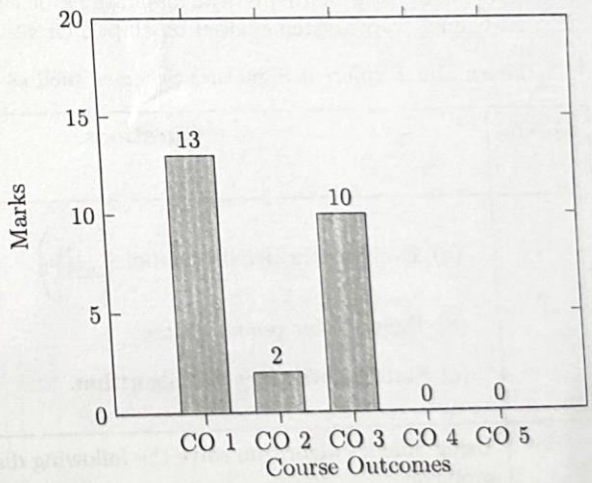
Q.No.	Questions	Marks	CO	BL	PO	PI Code
1	(a) Evaluate the Jacobi symbol $\left(\frac{7411}{9283}\right)$. (b) Define Euler pseudo prime. (c) State Solovay-Strassen algorithm.	2+2+2	CO1, CO2	L1, L3	PO1	1.1.1
2	Using Shank's algorithm solve the following discrete logarithm problem: $2^x \equiv 5 \mod 61$. OR State and prove Euler's Criterion for quadratic residue modulo p, where p is a prime.	5	CO3/CO1	L3/L2	PO1	1.1.2

Q.No.	Questions	Marks	CO	BL	PO	C
3	Alice and Bob agree to use the prime $p = 67$ and the primitive root $g = 7$ for the communications using the ElGamal public key cryptosystem. Bob chooses $a = 12$ as his private key. (a) What is the value of his public key A? (b) Alice encrypts the message $m = 12$ using the ephemeral key $k = 3$. What is the ciphertext (c_1, c_2) that Alice sends to Bob? (c) Verify that Bob gets back the original message $m = 12$ from the ciphertext (c_1, c_2) using his private key. OR Suppose that p is a prime and $\alpha \in Z_p^*$. Prove that α is a primitive element modulo p if and only if $\alpha^{(p-1)/q} \not\equiv 1 \mod p$ for all primes q dividing $p-1$.	(1+2+2)/5	CO3	L3/L2	PO1	1.1.2
4	(a) Let p be an odd prime and let g be a primitive root modulo p. Prove that a has a square root modulo p (i.e., there exists b such that $b^2 \equiv a \mod p$) if and only if its discrete logarithm $\log_g(a)$ modulo p is even. (b) Let p be a prime satisfying $p \equiv 3 \mod 4$. Let a be an integer such that a has a square root modulo p. Use (a) to prove that $b = a^{(p+1)/4} \mod p$ is a square root of a.	1.5+2.5	CO1	L3	PO1	1.3.1

Bloom's Level wise Marks Distribution



Course Outcome wise Marks Distribution



BL – Bloom's Taxonomy Levels:
1 – Remembering, 2 – Understanding, 3 – Applying, 4 – Analysing, 5 – Evaluating, 6 – Creating

CO – Course Outcomes

PO – Program Outcomes

PI Code – Performance Indicator Code

End of exam