Mahindra University, Hyderabad

École Centrale School of Engineering
Minor-I Examinations

SE23UCAM020

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

Date: 25/02/2025 **Start Time: 10:00 AM**
Time Duration: 1.5 Hours **Max. Marks: 20**

Instructions:

1) There are 5 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 3(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.

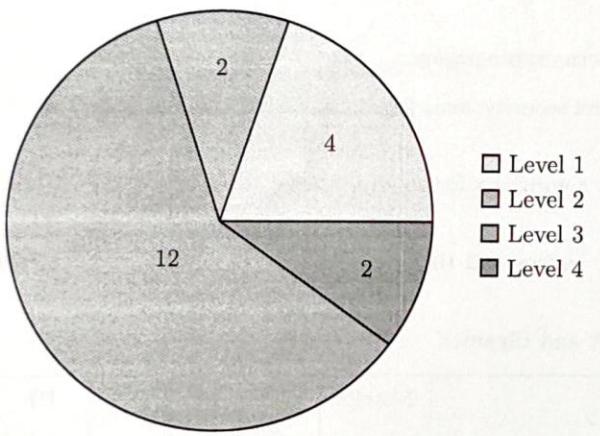
CO 4: Understand the mathematical foundations of elliptic curves and their applications in cryptography such as El-Gamal cryptosystems based on elliptic curves.

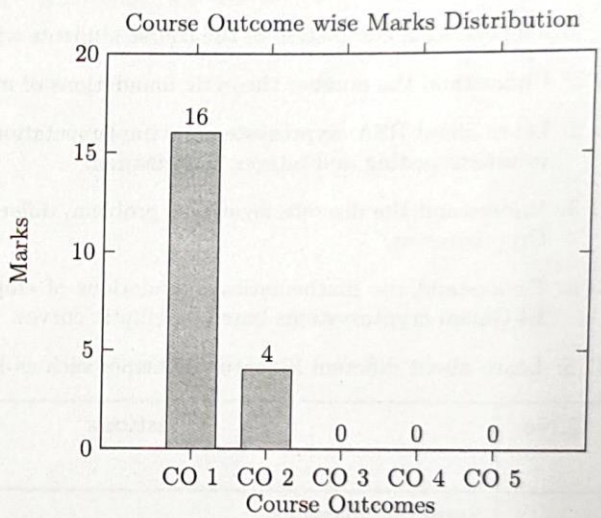
CO 5: Learn about different Signature Schemes such as RSA and Elgamal.

Q.No.	Questions	Marks	CO	BL	PO	PI Code
1	State the following: (a) Kerckhoff's Principle. (b) Primitive Root Theorem. (c) Fermat's Little Theorem. (d) Prime Number Theorem.	4	CO1	L1	PO1	1.1.1
2	(a) Using Extended Euclidean algorithm find $100^{-1} \pmod{143}$. (b) Using Fast Powering Algorithm compute $5^{248} \pmod{1000}$.	2+2	CO1	L3	PO1	1.1.2

Q.No.	Questions	Marks	CO	BL		
3	(a) Let $m \geq 1$ and a be integers. Prove that $ab \equiv 1 \pmod{m}$ for some integer b if and only if $gcd(a, m) = 1$. (b) Suppose that $m \equiv 1 \pmod{b}$, where m and b are positive integers. What integer between 1 and $m-1$ is equal to $b^{-1} \pmod{m}$?	2+2	CO1	L2, L4	PO1	
4	Bob's RSA public key cryptosystem has modulus $n = 247$ and encryption exponent $b = 7$. Alice sends Bob the ciphertext $c = 90$. Unfortunately, Bob has chosen too small a modulus. Help Eve in decrypting Alice's message.	4	CO2	L3	PO1	1.3.1
5	Solve the following simultaneous systems of congruences using Chinese Remainder Theorem. $x \equiv 4 \pmod{10}$, $x \equiv 7 \pmod{21}$, and $x \equiv 9 \pmod{11}$.	4	CO1	L3	PO1	1.1.2

Bloom's Level 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