Enrolment No. _________

AHMEDABAD UNIVERSITY

SCHOOL OF ARTS & SCIENCES

UNDERGRADUATE PROGRAMMES

2025-2026 MONSOON SEMESTER

END SEMESTER EXAMINATION

MAT215 ELEMENTARY NUMBER THEORY & CRYPTOGRAPHY

Date: 01-12-2025	Total Marks: 20
Time: 11.00 am – 01.00 am	No. of printed pages: 03

General Instructions:

1. Students must carry their identity card during the examination.
2. No break is allowed during the examination under any circumstances. In case of an emergency, with prior permission of the invigilator and an escort, a break of maximum five minutes is allowed.
3. No unauthorized devices, such as mobile phones, any kind of watches, other gadgets, or any kind of material is allowed on person.
4. Any violation of examination rules and an intent of malpractice will lead to strict disciplinary action, including a possible expulsion from the university.

Questions

1. **Each of the following questions is worth 1 mark. Attempt any two.**

   (a) Let p and q be distinct primes. Determine all integers of the form $n = p^9$ and $n = p^4 q$ whose Euler totient value is $\varphi(n) = 48$.

   (b) Let n be a positive integer. Determine all values of n for which the number of positive divisors of n is equal to 6.

   (c) Compute the following values:$\sigma(100)$, $\tau(100)$ and $\varphi(100)$.

2. **Each of the following questions is worth 2 marks. Attempt any two.**

   (a) Prove that an integer is divisible by 7 if and only if the number obtained by subtracting twice the last digit from the number formed by removing the last digit is divisible by 7. (For example $203 \to 20 - 2 \cdot 3 = 14$, which is divisible by 7.)

   (b) A plaintext letter T is encrypted to K, and plaintext letter H is encrypted to R using an affine cipher $E(n) = an + b \pmod{26}$. Determine the values of a and b.

   (c) Prove that if $\gcd(x, n) > 1$, then x is not invertible modulo n. In other words, show that no integer y can satisfy $xy \equiv 1 \pmod{n}$ when x and n are not relatively prime.

3. **Each of the following questions is worth 3 marks. Attempt any two.**

   (a) The length of a message encrypted with a permutation cipher provides a powerful clue, as the length of the permutation must divide the length of the message. Imagine the sender knows this and decides to add a couple of garbage letters at the end of the message so that the new message's length is no longer a multiple of the true key. Discuss the value of this method. Would something like this help protect a message encrypted with a Vigenere cipher from the Kasiski test?

   Further, a friend of ours wants to send us a message. Worried that a permutation cipher may not provide enough security, she decides to apply two permutations. Which provides more security, two permutations of length 10 or one permutation of length 10 and one of length 7?

   (b) The greatest disadvantage of the one-time pad is that you need to have a large text. As it can be impractical to carry a large text with you, there are several options. One is to use an agreed-upon document, which may be accessible through the internet. Here, however, is another idea. Let a_1 be any integer in $\{1,2,\ldots,25\}$ and shift the first letter of the text by a_1. Let $a_2 = a_1^2 \pmod{26}$, and shift the second letter by a_2. We continue, and let$a_k = a_{k-1}^2 \pmod{26}$ and shift the k^{th}letter by a_k. We can create as long a pad as needed, simply by taking more and more terms. We get different pads by choosing different starting values, and now all we need to do is remember that starting value and the fact that we square modulo 26 to get the next shift. Is this a good system? Why or why not?

   (c) Consider an n-bit LFSR. Assume two states, say the i^{th} and j^{th} states, are identical. Why must the pattern repeat? How is the length of the period of the pattern related to i and j?

Further, what is the longest possible period of repetition of a 4-bit LFSR register? Of a 5-bit LFSR register? Of an n-bit LFSR register?

4. **Each of the following questions is worth 4 marks. Attempt any two.**

(a) The first step of KidRSA creates an integer M from integers a, b by setting $M = ab - 1$. Prove that you can find infinitely many pairs of integers (a, b) where each of these is at least 2 and M is the square of an integer.

Can you find infinitely many pairs of integers (a, b) where each is at least 2 and M is a multiple of 1701?

(b) Prove that each positive integer x has one and only one base b expansion.

(c) Suppose Alice is sending Bob an important message. She wants Bob to be convinced the message originates from her, so she uses her public/private keys. Bob now knows, as this is publicly available, that $(e_{\text{Alice}}, n_{\text{Alice}})$ and a message $m^{d}\text{Alice} \pmod{n_{\text{Alice}}}$. Is this enough information for Bob to deduced_{Alice}?

What would be the consequences if he could determine d_{Alice}?

In RSA, we needed to assume the message m was relatively prime to n. Use the Chinese Remainder Theorem to show that the RSA Theorem also holds if m is not relatively prime to n; i.e., if $n = pq$ is the product of two distinct primes and$ed \equiv 1 \pmod{\varphi(n)}$, then $m^{ed} \equiv m \pmod{n}$.

5. **(Bonus Question)** Prove that all Carmichael numbers are odd, and they must have at least three distinct prime factors.