RAN-2303080304040005

RAN-2303080304040005

M.Sc. (Sem. - IV) Examination September - 2025

Mathematics : Partition Theory and Cryptography (Paper - PGMTH : 4044)

Time: 3 Hours] **[Total Marks: 70**

સૂચના : / Instructions

(1) ઉપરોક્ત દર્શાવેલ વિગતો ઉત્તરવહી પર અવશ્ય લખવી.
Fill up strictly the above details on your answer book

(2) Attempt all questions.

(3) Follow usual notations and conventions.

(4) Use of non-programmable scientific calculator is permitted.

Seat No.:

Student's Signature

Q.1. For $|x| < 1$, prove that **(14)**
$\Pi_{m \geq 1} (1 - x^m) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \bullet\bullet\bullet$.

OR

Q.1. **Answer the following:** **(14)**

(1) prove that $p(n,k) = q\left(n + \frac{k(k-1)}{2}, k\right)$. Explain the same using suitable example.

(2) Derive the generating function for the partition function $p(n)$.

Q.2. **Answer any TWO of the following:** **(14)**

(1) State and prove Durfee's identity for $p(n)$.

(2) State and prove the Euler's recursion formula for $p(n)$. Use it to compute the value of $p(10)$.

(3) Explain what you mean by two-line partition of a natural number n. Hence obtain all such partitions for $n = 8$.

Q.3. **Answer any TWO of the following:** **(14)**

(1) Explain the method of encrypting and decrypting a message using Autokey Cipher. Hence encipher the message EARLY DAYS with seed Q.

(2) The ciphertext ALXWU has been enciphered using the Hill's cipher and the congruences $C_1 \equiv 4P_1 + 11P_2 \ (mod\ 26)$, $C_2 \equiv 3P_1 + 8P_2 \ (mod\ 26)$. Derive the plaintext message.

(3) Explain the method of encrypting and decrypting a message using Vignére Cipher. Hence encipher the message TROPHY with the key word DUBAI.

Q.4. **Answer any TWO of the following:** **(14)**

(1) Explain ElGamal Cryptosystem for encrypting messages based on discrete logarithmic problem.

(2) An RSA cryptosystem uses two prime numbers 3 and 13 to generate the public key = 3. What is the value of cipher text for a plain text F?

(3) A user of the knapsack cryptosystem has the sequence 3,5,11,20,41 as an encryption key. If the user's private key involves the modulus $m = 85$ and multiplier $a = 44$, then determine the secret ciphertext for the plain text message LION.

Q.5. Answer any TWO of the following: **(14)**

(1) What do you mean by active and passive attacks? Explain in detail about the following attacks: (i) Brute Force attack (ii) Known plaintext attack.

(2) Explain what you mean by superincreasing sequence. Hence explain algorithm to solve knapsack problem $V = a_1x_1 + a_2x_2 + \cdots + a_nx_n$; where $\{a_i\}$ for $i = 1,2, \ldots , n$ is a superincreasing sequence of integers.

(3) Show that $p(n,k)$ is the coefficient of x^n in $\prod_{m=1}^{k} x^k (1 - x^m)^{-1}$.

———————