MCC/22/M.SC./SEM.-III/MTM/1

*Total pages: 03*

**PG (CBCS)**
**M.SC. Semester- III Examination, 2023**
**MATHEMATICS**
**PAPER: MTM 303**
**(STOCHASTIC PROCESS AND REGRESSION AND CRYPTOGRAPHY)**

**Full Marks: 50** **Time: 2 Hours**

The figures in the right-hand margin indicate full marks.
Candidates are required to give their answers in their own words as far as practicable.

**Write the answer for each unit in separate sheet**

## MTM 303.1: STOCHASTIC PROCESS AND REGRESSION

### GROUP-A

1. Answer any **TWO** of the following questions: 2×2=4

a) Define transition graph with transition matrix of a Markov chain.
b) Define Gauss-Markov linear model.
c) Define Markov chain with an example.
d) Prove that $1-r_{1.23}^2=(1-r_{12}^2)(1-r_{13.2}^2)$

### GROUP-B

2. Answer any **TWO** of the following questions: 2×4=8

a) Prove that the state j is persistent iff $\sum_{n=0}^{\infty} P_{jj}^{(n)}=\infty$.
b) Find the regression of $X_1$ on $X_2$ and $X_3$ given in the following results:

| Trait | Mean | Standard Deviation | $r_{12}$ | $r_{23}$ | $r_{31}$ |
|---|---|---|---|---|---|
| $X_1$ | 28.02 | 4.42 | +0.80 | --- | --- |
| $X_2$ | 4.91 | 1.10 | --- | -0.56 | --- |
| $X_3$ | 594 | 85 | --- | --- | -0.40 |

Where $X_1=seed\ per\ acre; X_2=Rainfall\ in\ inches; X_3=Accumulated\ temperature\ above\ 42^0\ F.$

c) State and prove Chapman- Kolmogorov Equation.
d) Let,$\{X_n, n\geq 0\}$be a Markov chain having state space $S=\{1,2,3,4\}$ and transition matrix $P=\begin{pmatrix} \frac{1}{3} & \frac{2}{3} & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

Identify the state as transient, persistent, ergodic.

P.T.O

## GROUP-C

3. Answer any **ONE** of the following questions: 1×8=8

a) Find the probability generating function for birth and death process when rate of birth and death are respectively $n\lambda$ and $n\mu$, where n is the population size at any time t. Assume that the initial population size is i.

b) Let $\{X_n, n \geq 0\}$ be branching process. Show that $m = E(X_1) = \sum_{k=0}^{\infty} kp_k$ and $\sigma^2 = Var(X_1)$, then $E(X_n) = m^n$ and $Var(X_n) = \begin{cases} \frac{m^{n-1}(m^n-1)}{m-1}\sigma^2, if\ m \neq 1 \\ n\sigma^2, if\ m = 1 \end{cases}$.

[Internal Assessment-05]

## MTM 303.2: CRYPTOGRAPHY

## GROUP-A

1. Answer any **TWO** of the following questions: 2×2=4

a) In Rabin Cryptosystem, let the public key $n = 517$ and plaintext is 17. What is Ciphertext?

b) What is the Ciphertext of "**MIDNAPORE CITY COLLEGE**" using Caesar Cipher?

c) Solve the equation $x^2 \equiv 6\ mod(10)$ and then find the Legendre symbol $\left(\frac{6}{10}\right)$.

d) Let $\mathbb{P}, \mathbb{C}, \mathbb{K}$ denote plaintext space, ciphertext space and key space respectively. In Shift Cipher $\mathbb{P} = \mathbb{C}$ and $\mathbb{K} = \mathbb{Z}_{26}$. Suppose the key for shift cipher is $k = 11$ and plaintext is 22. Then what is the ciphertext?

## GROUP-B

2. Answer any **TWO** of the following questions: 2×4=8

a) Use the Playfair cipher with key **diskjockey** to encrypt the string of plaintext: **the phone is bugged.**

b) i) Suppose that $\pi$ is the following permutation of $\{1, 2, 3, \dots, 8\}$:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 6 & 2 & 7 & 3 & 8 & 5 \end{pmatrix}.$$

Compute the permutation $\pi^{-1}$.

ii) Decrypt the following ciphertext, for a Permutation Cipher with $m = 8$, which was encrypted using the key $\pi$:

**TGEEMNELNNTDROEOAAHDOETCSHAEIRLM**

c) Let Block be a block cipher consisting of two rounds of a feistel cipher having block length 8 with the session keys $k_1, k_2$ such that $k = k_1||k_2$ be the secret key. Suppose the complex function $F$ used in the feistel cipher is simple $XOR$ with the session key. That is, $F(m', k') = m' \oplus k'$ for input string $m'$ and session key $k'$. Find the ciphertext $Block(m, k)$ where the message $m = 10100101$ and the secret key $k = 11001010$.

P.T.O

d) i) Evaluate 7503 mod 81.

ii) Consider Substitution cipher with key:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| X | N | Y | A | H | P | O | G | Z | Q | W | B | T | S | F | L | R | C | V | M | U | E | K | J | D | I |

Encrypt the plaintext:

**math is the only place where truth and beauty mean same thing**

iii) Verify the above example that substitution cipher is monoalphabetic.

## GROUP-C

3. Answer any **ONE** of the following questions: 1×8=8

a) Consider the following Playfair array:

| | | | | |
|---|---|---|---|---|
| B | A | R | M | G |
| U | E | I/J | T | N |
| H | O | S | D | W |
| Y | L | P | C | F |
| K | Q | V | X | Z |

i) Encrypt the plaintext: **HAPPY DAYS**

ii) Decrypt the ciphertext: **TERCSUBW**

b) i) Define Polyalphabetic cipher with example.

ii) In Vigenere Cipher, consider key $k = (2,8,15,7,4,17)$.

- Encrypt the plaintext: **this cryptosystem is not secure**
- Decrypt the ciphertext: **i love math teacher**

[Internal Assessment- 05 Marks]

******