Seat No. : _____

AF-106

April-2018

B.Sc., Sem.-VI

SE-311 : Mathematics

(Elective Course)

(Convex Analysis and Probability Theory)

Time : 3 Hours] **[Max. Marks : 70**

Instructions : (i) Notations are usual everywhere.
(ii) Figures to the right indicate marks of the question.

1. (a) Define convex set and affine set. Also explain each of them by an example. **9**

OR

Define convex hull of a set.
Also provide examples of convex sets , non-convex sets and Illustrate an example of a convex hull of a subset of R^2.

(b) Show that the function $f : R \to R$ defined as $f(x) = x^2$ is monotonically increasing on $[0, \infty)$ and decreasing on $(-\infty , 0]$ **9**

OR

Show that the function $f : R \to R$ defined as $f(x) = x^3$ is a convex function on $[0, \infty)$ whereas concave on $(-\infty , 0]$

2. (a) Define following terms : **9**
Null and Certain Events, axiomatic definition of probability. Also, state the probabilities of null and certain events.

OR

Define following terms :
(i) Sample space, (ii) Event, (iii) Elementary event, (iv) Mutually Exhaustive events

(b) Using the addition rule of probability for two events A and B defined on a finite sample space such that P[A] = 0.35, P[B] = 0.45 and $P[A \cup B] = 0.65$, then find the probability of following events : **9**

(i) $\overline{B}$, (ii) $\overline{A} \cap \overline{B}$ (iii) $\overline{A \cup B}$, (iv) $\overline{A} \cap B$, if events A and B are independent

OR

Two balanced dice are thrown once, simultaneously. Find the probability of the following events :
(i) 2 on a first die and odd number on a second die.
(ii) Even number on first die and a multiple of 3 on second die.
(iii) Sum of numbers on two dice is 7.
(iv) Sum of numbers on two dice is divisible by 5.

3. (a) State the mean and variance of binomial distribution.

A X follows binomial distribution, with parameters n and p, and mean and variance of a random variable X are 9 and 6 respectively, then find n and p. Also, find P (X=1), P(X<2). **9**

OR

A random variable X follows Poisson distribution with parameter m, such that P(X=1) = P(X=2), then find parameter m and also find P(X=0), P(X<3), P(X>2).

(b) For a normal distribution, state its probability distribution function. Also, state mean, variance, mode and median of normal distribution. **9**

OR

During a typical football game, injuries are expected and are treated as a random variable, following a Poisson distribution. A coach can expect 3.2 injuries. Find the probability that the team will have at most 1 injury in this game.

4. Attempt any **eight** of the following questions in short : **16**

(a) Define monotonically increasing and decreasing functions on an interval I.

(b) State the Intermediate Value Theorem.

(c) Define Convex and concave functions on an interval I.

(d) If $A = \{(x, y) \in R^2 / x^2 + y^2 = 4\}$ then find the convex hull of A.

(e) Two coins are tossed, find the probability that exactly one head appears.

(f) State the independence of two events.

(g) In a manufacturing process, defective units produced are denoted by a random variable X. State the distribution of a random variable X.

(h) Define conditional probability.

(i) For two mutually exclusive events A, B on a finite sample space S, $P(\bar{A} \mid B) = 1$. Do you agree ? If yes, justify.

(j) State the theorem on total probability.

Seat No. : _____

AF-106

April-2018

B.Sc., Sem.-VI

SE-311 : Mathematics

(Elective Course)

(Cryptography)

Time : 3 Hours] **[Max. Marks : 70**

Instructions : (i) **All** the questions are compulsory.
(ii) Right hand side figure indicate marks of the question.

1. (a) Is $(\mathbb{Z}_n, +_n, .n)$ a Ring ? Justify. Also check whether $(\mathbb{Z}_{50}, \oplus_{50}, \odot_{50})$ is a Ring or not. Note that here $\oplus$ and $\odot$ are defined as: $a \oplus b = a._{50} b$ and $a \odot b = a +_{50} b$. **9**

OR

Explain extended Euclidian algorithm and illustrate it with example.

(b) Obtain the value of x that satisfies following four congruence : **9**

$x \equiv 1(\text{mod } 2), x \equiv 2(\text{mod } 3), x \equiv 3(\text{mod } 5), x \equiv 4(\text{mod } 7)$

OR

Explain Shank's Algorithm, find the discrete logarithm of 431 (mod 37) with respect to the base 13.

2. (a) Define cryptanalysis. A cipher text obtained using the shift cipher is given below. Do the cryptanalysis and obtain the plain text.

"PSTBQJILJNXUTBJW". **9**

OR

Discuss Modern Cryptography.

(b) Explain Affine cipher. Transform the text "All that glitters is not gold" using linear relation $y = 2x + 3$. **9**

OR

Define Hill cipher. Encrypt the plaintext "KILL" using Hill cipher. Use the encrypt matrix $\begin{bmatrix} 9 & 5 \\ 4 & 7 \end{bmatrix}$.

3. (a) Prisha selects p = 23 and c = 5 and convey the same to Bharti. Prisha selects a = 6 and Bharti selects b = 15. What is private key exchange between them using the DH algorithm ? Show how Meera mounts an attack using Shank's algorithm and wrenches the private key shared between Prisha and Bharti. **9**

OR

Explain the Pollard's ρ algorithm for Discrete logarithm.

(b) Prisha and Bharti select the prime number 17 with g = 6 as a primitive element. Bharti selects a random number k = 5 as the private key, computes him key and send it to Prisha; Prisha uses $x = 9$ as the private key to mail a message M = 13 to Bharti. Show the full transaction including the recovery of message by Bharti using ElGamal Public-key cryptosystem. **9**

OR

Explain RSA algorithm with a suitable example.

4. Do as Directed. Attempt any **eight** in short : **16**

(1) State Fermat's Little Theorem.

(2) State Euler's theorem.

(3) Give atleast two differences between shift cipher and permutation cipher.

(4) Give an example each of a monoalphabetic cryptosystem and a polyalphabetic cryptosystem.

(5) What is the fundamental theorem of arithmetic ?

(6) Is 10 a primitive root of 21 ?

(7) Define Trapdoor function.

(8) What is probability that atleast two share a birthday from group of n people ?

(9) Which cipher replaces one character with another character ?

(10) Define Euler's Phi function.

Seat No. : _____

AF-106

April-2018

B.Sc., Sem.-VI

SE-311 : Mathematics

(Operation Research)

Time : 3 Hours] **[Max. Marks : 70**

Instructions: (1) **All** the questions are compulsory.
(2) Notations and Terminology are standard.
(3) Figures to the right indicates the full marks.

1. (a) Derive the EOQ (Economic Order Quantity) Model in which Demand Rate is constant. **9**

OR

Explain the order level lot size (OLLS) system.

(b) Find out the most economic batch quantity of a product on a machine, if the production rate of that item on the machine is 200 pieces per day and the demand is uniform at the rate of 100 pieces per day. The ordering cost is 200 per batch and the cost of holding one item in inventory is 0.81 per day. How will the batch quantity vary if the production rate is infinite ? **9**

OR

The demand for an item in a company is 18,000 units per year, and the company can produce the item at a rate 3,000 per month. The cost of one set-up is ₹ 500 and the holding cost of one unit per month is ₹ 0.15. The shortage cost of one unit is ₹ 20.00 per month. Determine the optimum manufacturing quantity and the number of shortages. Also, determine the manufacturing time and time between two set-up.

2. (a) Explain the basic differences between PERT and CPM. **9**

OR

Explain the terms in brief : (1) Float (2) Activities

(b) Consider the following network activity and their duration : **9**

Activity	A	B	C	D	E	F	G	H	I	J
Immediate Predecessor	—	—	A	A	A	C	D	B, E	H	F, G, I
Duration (months)	4	1	2	3	2	1.5	1.5	2.5	1.5	1

(1) Construct the Project network.

(2) Determine the critical path.

OR

Consider the following network activity and their duration :

Activity	A	B	C	D	E	F	G	H
Immediate Predecessor	—	—	A	B	A	C, D	C, D, E	F
Duration	3	6	4	3	4	5	3	1

(1) Construct the CPM network.

(2) Compute the total floats and free floats for non-critical path.

3. (a) Explain the Principles of Dominance. **9**

OR

State and Prove Necessary and Sufficient Condition for the existence of a saddle point.

(b) Find the optimum strategy and value of the game of the following Pay-off matrix using Matrix method. **9**

	Player B			
Player A	B_1	B_2	B_3	B_4
A_1	3	2	4	0
A_2	3	4	2	4
A_3	4	2	4	0
A_4	0	4	0	8

OR

Find the optimum strategy and value of the game of the following Pay-off matrix using the method of oddments :

	Player B			
Player A	B_1	B_2	B_3	B_4
A_1	–1	2	3	0
A_2	–4	–1	–1	0
A_3	–1	1	1	–4
A_4	4	–1	2	–7

4. Attempt any **eight** : **16**

1. Define : (1) Pure strategy (2) Mixed strategy.
2. Give Full form of PERT and CPM.
3. Define: (1) Merge Event (2) Burst Event.
4. Explain: Fair game with illustration.
5. Give Formula to find optimum order quantity and cycle time for EOQ model with finite replenishment rate.

6. Develop a network :

Activity	A	B	C	D
Immediate Predecessor	–	–	A	B

7. Define: (1) Lead time (2) Cycle time.

8. Give an example of pay-off matrix for game without saddle point.

9. Explain (Any two) types of cost, related to the inventory system.

10. Find the range of values of p and q that will render the entry (2, 2) a saddle point for the game :

Player A	B_1	B_2	B_3
A_1	2	4	5
A_2	10	7	q
A_3	4	p	6