Seat No. : _______________

AF–107

April–2016

B.Sc., Sem.–VI

311 : Mathematics
(Convex Analysis and Probability Theory)
(Elective Course)

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

Instructions : (1) Notations are usual everywhere.

(2) Figures to the right indicate marks of the question.

1. (a) Define convex set and affine set. Aiso give an example of each of them. **9**

OR

Define monotonically increasing and decreasing functions on an interval I. Also show that the function f : R → R defined as $f(x) = x^2$ is monotonically increasing on $[0, \infty)$ and decreasing on $(-\infty, 0]$.

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

Also show that the function f : R → R defined as $f(x) = x^3$ is a convex function on $[0, \infty)$ whereas concave on $(-\infty, 0]$ **9**

OR

If the polynomial function f : R → R is defined as $f(x) = x^4 + 2x^3 - 36x^2 + 62x + 5$ then check double differentiability of f.

Also discuss the convexity/concavity of the function f.

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∪B] = 0.65, then find the probability of following events :

(i) $\bar{B}$, (ii) $\bar{A} \cap \bar{B}$ (iii) $\overline{A \cup B}$, (iv) $\bar{A} \cap B$ if events A and B are independent. **9**

OR

(b) 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 Hyper Plane and Convex hull of a set.

(b) State the Intermediate Value Theorem

(c) Give examples each one of convex and non-convex sets of R^2

(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–107

April–2016

B.Sc., Sem.–VI

311 Mathematics
Cryptography (Theory)
(Elective Course)

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

Instructions : (1) **All** questions are compulsory.

(2) Figures to right indicate full marks for the question.

1. (a) State and prove the Fermat's Little Theorem. **9**

OR

If n is a fixed positive integer and a, b, c, d are integer, then prove that the following :

(a) $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n} \Leftrightarrow a - b \equiv 0 \pmod{n}$.

(b) $a \equiv a(\text{mod } n)$

(c) $a \equiv b(\text{mod } n)$ and $b \equiv c(\text{mod } n) \Leftrightarrow a \equiv c(\text{mod } n)$.

(b) Obtain all the primitive elements of Z_{37}. **9**

OR

Using Shank's Algorithm, find the discrete logarithm of 15 (mod 29) with respect to the base 2.

2. (a) (i) Discuss Modern cryptography. **9**

(ii) Discuss relation between Hill cipher and Permutation cipher.

OR

Define Shift cipher and Substitution cipher. A ciphertext obtained using the shift cipher is given below. Do the cryptanalysis and obtain the plaintext.: TEXQHFKALCZXHBPELRIATBEXSB–XIFZB.

(b) (i) Suppose that affine cipher $E(x) = (ax + b) \pmod{26}$ enciphers s as U and o as A. Find a and b.

(ii) Using Vigenere cipher with MKGANDHI as the key : If you accept your limitations you go beyond them. **9**

OR

(i) Encrypt the following text using the permutation cipher scheme of $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$ *"Attitude Can Change Your Life"*.

(ii) Encrypt the plaintext given below using Hill cipher. "*Gujarati*". Use the encryption matrix $\begin{bmatrix} 9 & 5 \\ 4 & 7 \end{bmatrix}$ **9**

3. (a) Alice selects p = 23 and c = 5 and convey the same to Bob. Alice selects a = 8 and Bob selects b = 19. What is private key exchange between them using the DH algorithm ? Show how Eve mounts an attack using Shank's algorithm and wrenches the private key shared between Alice and Bob. **9**

OR

Define Trapdoor function. Discuss Birthday Paradox.

(b) Alice and Bob select the prime number p = 17 with g = 6 as a primitive elements. Alice select a random number a = 5 as private key, computes her public key and sends it to Bob; Bob uses b = 9 as the ephemeral key to mail a message m = 13 to Alice. Show the full transaction including the recovery of massage key using ElGamal Public–Key cryptosystem. **9**

OR

With p = 11, q = 13, e = 7 and m = 9. Show that the complete transaction conforming to the RSA cryptosystem.

4. Attempt any **eight**. Do as directed: **16**

(i) In cryptography, what is cipher ?

(a) Algorithm for performing encryption and decryption
(b) Encrypted message
(c) Both (a) and (b)
(d) None of the mentioned

(ii) Cryptanalysis is used

(a) to find some insecurity in a cryptographic scheme
(b) to increase the speed
(c) to encrypt the data
(d) none of the mentioned

(iii) Let L be the least common multiple of 175 and 105. Among all of the common divisors $x > 1$ of 175 and 105, let D be the smallest. Which is correct of the following ?

(a) D = 5 and L = 1050
(b) D = 5 and L = 35
(c) D = 7 and L = 525
(d) D = 5 and L = 525
(e) D = 7 and L = 1050

(iv) The ________ is the original message before transformation.

(a) ciphertext
(b) plaintext
(c) secret–text
(d) none of the above

(v) A(n) ________ algorithm transforms plaintext to ciphertext.

(a) encryption
(b) decryption
(c) either (a) or (b)
(d) neither (a) nor (b)

(vi) A _______ cipher replaces one character with another character.

(a) substitution
(b) transposition
(c) either (a) or (b)
(d) neither (a) nor (b)

(vii) The ________ cipher is the simplest monoaphabetic cipher. It uses modular arithmetic with a modulus of 26.

(a) transposition
(b) additive
(c) shift
(d) none of the above

(viii) A combination of an encryption algorithm and a decryption algorithm is called a ________.

(a) cipher
(b) secret
(c) key
(d) none of the above

(ix) The result of –7(mod 12) is:

(a) –7
(b) 12
(c) 5
(d) –5

(x) The art of breaking the code is:

(a) Cryptosystem
(b) Steganography
(c) Cryptography
(d) Cryptanalysis

Seat No. : _______________

AF–107

April–2016

B.Sc., Sem.–VI

311 : Mathematics
(Elective Course)

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

Instructions : (1) **All** the questions are compulsory.

(2) Notations and terminologies are standard.

(3) Figure to the right indicate the full marks.

1. (a) Explain economic order quantity (EOQ) model with constant rate of demand. Find optimum inventory, total cost and the optimum cycle time for this model. **9**

OR

Explain EOQ model with shortages. Find minimum cost for this model.

(b) A product is to be manufactured on a machine. Ordering cost per order = ₹ 30, purchase cost per unit = ₹ 0.10, Inventory holding cost per unit per annum = ₹ 0.05, production rate = 1,00,000 units/year, demand rate = 10,000 units/year. Determine the economic manufacturing quantity. **9**

OR

The demand for a certain item is 16 units per period. Unsatisfied demand causes a shortage cost of ₹ 0.75 per unit per short period. The cost of initiating purchasing action is ₹ 15 per purchase and the holding cost is 15% of average inventory valuation per period. Item cost is ₹ 8 per unit. Find the minimum cost and purchase quantity.

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

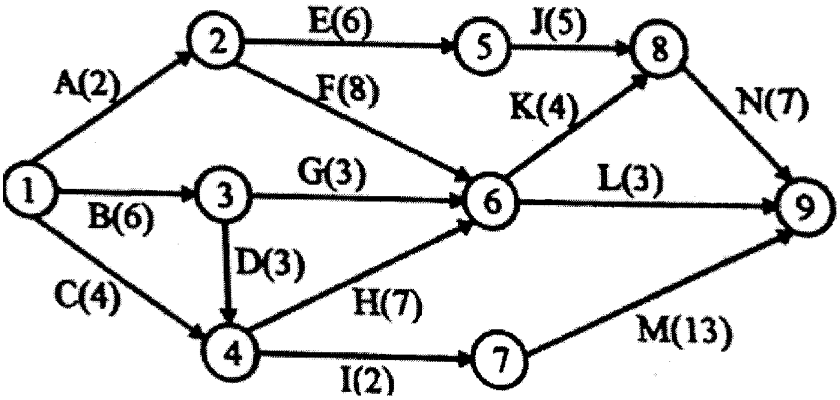
OR

A small project consists of 13 activities which take place and time for completion according as follows:

Activity	A	B	C	D	E	F	G	H	I	J	K	L	M
Immediate Predecessor	–	A	B	A	D	E	–	G	H,J	–	A	C,K	I,L
Duration	6	4	7	2	4	10	2	10	6	13	9	3	5

Draw a project network. Determine the critical path.

2. (b) Indicate the critical path. Find the total float and free float for all activities. Also verify that the total float of all activities in the critical path are zero. **9**



OR

Consider the following information activities required for a project. Draw a network diagram.

Activity	A	B	C	D	E	F	G	H	I	J	K	L
Predecessors	–	–	–	A	A	E	B	B	D,F	C	H,J	G,I,K

3. (a) Explain the dominance principal. **9**

OR

Solve the following 3 × 3 game by the method of oddments.

Player B

		B_1	B_2	B_3
Player A	A_1	3	1	1
	A_2	1	1	5
	A_3	1	4	1

(b) Solve the following game. **9**

Player B

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

OR

3. (b) For the game with the following pay off matrix, determine the optimum strategies and the value of the game by simplex method.

Player B

		B_1	B_2	B_3
Player A	A_1	2	–2	3
	A_2	–3	5	–1

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

(1) Define holding cost, shortage cost.

(2) Define lead time, demand.

(3) What is the carrying cost in EOQ model with finite replacement rate if production rate = demand rate ?

(4) Given the following information, develop a network.

Activity	**Immediate predecessor**
A	–
B	–
C	A
D	B

(5) Define total float, free float.

(6) Define two person zero sum game.

(7) Define strategy.

(8) Solve the following game :

Player B

		B_1	B_2	B_3	B_4
Player A	A_1	8	–2	9	–3
	A_2	6	5	6	8
	A_3	–2	4	–9	5

(9) Define network.

(10) Define ordering cost.