This question paper contains 1 printed page. Your Roll No.....

1735 A

MCA / IV Sem.

Paper MCA – 402 – Information Security

(Admissions of 2009 and onwards)

Time : 2 hours Maximum Marks :50

Write your Roll No. on the top immediately on receipt of this question paper.
Attempt all questions.
Attempt each question on a fresh page & all parts of a question together.

1	(a)	Enlist 4 properties of hash functions to be used for information security applications. With the help of a block diagram, explain the construction of a keyed one-way hash function.	6
	(b)	Explain how quasigroups are used in the design of cryptographic schemes. Use a 3x3 Latin square.	4
2	(a)	Give a brief description of the Data Encryption Standard (DES) & explain the functioning of one round using a Feistel network.	6
	(b)	Design a key distribution protocol enabling two principals to communicate with the help of a third party to effect an introduction. Use standard notations.	4
3	(a)	How are confusion & diffusion ensured in the design of AES. Name 2 standards/commercial systems that use AES.	6
	(b)	Perform the following operations on all elements of GF(5) (i) Multiplication (ii) Additive inverse.	4
4	(a)	For p=3 & q=11 in RSA, identify a suitable key pair and show the process of encryption & decryption for plaintext x = 2.	5
	(b)	Which one-way function has been used in Diffie-Hellman key exchange protocol? For n = 29 and g = 2, show how Tanu & Manu derive a common secret key by communicating over a public channel.	5
5		Attempt any <u>two</u> of the following:	
	(a)	Explain with the help of a block diagram how message signing and verification are carried out for the PGP standard.	5
	(b)	How is the design of multimedia encryption schemes different from that of normal data encryption? Explain three primitives used in the design of multimedia encryption schemes.	5
	(c)	Compute (i) 7^{13} mod 47 (ii) 4^{18} mod 17 using efficient techniques . Show intermediate steps.	5

100