Total No. of Questions : 10]

SEAT No : □

P 3125

[Total No. of Pages :2

[5154]-691

B.E.(Information Technology)

INFORMATION AND CYBER SECURITY

(2012 Course) (414453)

Time : 2½ Hours] ***[Max. Marks : 70***

Instructions to the candidates:

1) ***Answers Question 1 or 2, 3 or 4, 5 or 6, 7 or 8 and 9 or 10.***
2) ***Neat diagrams must be drawn whenever necessary.***
3) ***Figures to the right indicate full marks.***
4) ***Assume suitable data, if necessary.***

Q1) a) Compute the inverse of 17 in mod 23 arithmetic. Show steps clearly. **[6]**

b) State Euler's theorem. **[4]**

OR

Q2) a) Show with proper working that 13 is a primitive root of 19. **[6]**

b) In Diffie-Hellman key exchange between two parties A and B where A picks his secret as 9 and B picks his secret as 6. Apply 13 as the primitive root of 19, for this Diffie-Hellman exchange and show the shared secret. Show the math working steps clearly. **[4]**

Q3) a) What do you mean by cryptanalysis. Mention the applications of public key cryptography. **[6]**

b) List out the problems of one time pad. **[4]**

OR

Q4) a) Write down the purpose of S-box in DES. **[6]**

b) Give the types of attacks with examples. **[4]**

Q5) Consider the following threats to web security and describe how each is countered by particular feature of SSL. **[16]**

a) Brute force attacks.
b) Known plaintext attacks.
c) Replay attacks.
d) Man-in-the-middle attacks.
e) Password sniffing.
f) IP spoofing.
g) IP hijacking.
h) SYN flooding.

OR