

Total No. of Questions :6]

SEAT No. :

P286

[Total No. of Pages :2

Oct./BE/ Insem. - 604

B.E. (Information Technology)

INFORMATION AND CYBER SECURITY

(2015 Pattern) (Semester-I)

Time : 1 Hour]

[Max. Marks :30

Instructions to the candidates:

- 1) *Solve Q.1 or Q.2, Q.3 or Q.4 and Q.5 or Q.6.*
- 2) *Draw neat diagrams wherever necessary.*
- 3) *Figures to the right indicate full marks.*

Q1) a) Categories different attacks. Differentiate between Active and passive attacks. [4]

b) Explain different security goals (Security Services) in detail. [6]

OR

Q2) a) What is an IDS? What are different types and different methods of IDS. [6]

b) Write short note on Security threats and vulnerabilities. [4]

Q3) a) Determine the value of X using Chinese remainder theorem. [4]

$$X=1 \pmod{5} \quad X=6 \pmod{7} \quad X=8 \pmod{11}$$

b) Explain ECB,CBC,CFB and OFB modes of operation with neat diagram. [6]

OR

Q4) a) Let the given data be-two prime numbers $p=7$, $q=11$, Plain text=8 and public key $e=17$. Using RSA algorithm perform encryption and decryption. [5]

b) Explain ElGamal encryption algorithm with example. [5]

P.T.O.

Q5) a) How AH and ESP protocols works under transport and tunnel mode.[6]

b) What is Digital certificate? Explain X.509 with neat diagram. [4]

OR

Q6) a) What problem was Kerberos designed to address? Explain its working. [8]

b) What is Digital signature and how it works? [2]

