Total No. of Questions : 12]

SEAT No. :

P3336

[Total No. of Pages : 2

[5254]-180-A

B.E. (Computer)

INFORMATION SECURITY

(2008 Pattern) (Elective - IV)

Time : 3 Hours] *[Max. Marks : 100*

Instructions to the candidates:

1) ***All questions are compulsory.***
2) ***Figures to the right indicate full marks.***

SECTION - A

Q1) a) What is confidentiality? Explain any one algorithm to implement confidentiality. **[9]**

b) Explain any one algorithm to implement classical cryptography. **[9]**

OR

Q2) a) Describe different policies of security in detail. **[9]**

b) What is information security? Discuss lifecycle of security in detail. **[9]**

Q3) a) Differentiate private and public key cryptography. **[8]**

b) What is IDEA? Explain idea in detail. **[8]**

OR

Q4) a) Explain DES algorithm & with suitable diagram in detail. **[8]**

b) Discuss different issues of cryptography. **[8]**

Q5) a) Explain ECC encryption algorithm in detail. **[8]**

b) Discuss different issues of generation of key. **[8]**

OR

Q6) a) What is DH? Explain DH. algorithm in short. **[8]**

b) Discuss uses of number theory in different algorithm for cryptography. **[8]**

P.T.O.

SECTION - B

Q7) a) Define MAC. Discuss applications of MAC in information security. **[9]**

b) What is PKI? Explain PKI in detail. **[9]**

OR

Q8) a) What is HMAC? Explain algorithm of HMAC in detail. **[9]**

b) Define DSA. Explain DSA algorithm in detail. With suitable diagram. **[9]**

Q9) a) What is SSL? Discuss SSL with application. **[8]**

b) What is IPSEC? What are different applications of IPSEC. **[8]**

OR

Q10)a) Define TLS. Discuss TLS with applications. **[8]**

b) What is IDS? Enlist different types of IDS with explanation. **[8]**

Q11)a) Enlist and explain different security services. **[8]**

b) Define PGP. Describe PGP in detail. **[8]**

OR

Q12)Write a short notes on following (any four) **[16]**

a) PGP

b) PEM

c) S/MIME

d) Standards of information security.

e) Information security architecture