Total No. of Questions : 12]

SEAT No. :

P840

[Total No. of Pages : 3

[4458]-791

B.E. (Information Technology) (Semester - I)

INFORMATION ASSURANCE & SECURITY

(2008 Course)

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

Instructions to the candidates:

1) ***Answers Question 1 or 2, 3 or 4, 5 or 6 from Section-I and Question 7 or 8, 9 or 10, 11 or 12 from Section-II.***
2) ***Answers to the two sections should be written in separate answer books.***
3) ***Neat diagrams must be drawn wherever necessary.***
4) ***Figures to the right indicate full marks.***
5) ***Assume suitable data, if necessary.***

SECTION - I

Q1) a) Differentiate between the following: **[8]**

i) Active and Passive attacks.

ii) Authentication and Authorization.

b) Using Euclidean algorithm calculate GCD (48, 30) and GCD (105, 80). **[8]**

OR

Q2) a) Explain Fermat's Little Theorem and solve the following using the same: **[8]**

i) 15^{18} mod 17

ii) 5^{27} mod 13

b) Illustrate the use of polynomials for secret sharing. **[8]**

Q3) Describe the modes of operation (ECB,CBC,CFB,OFB & CTR mode) with the help of block diagram. **[16]**

OR

Q4) a) Calculate Cipher text using RSA algorithm. Given data is as follows :- Prime numbers P,Q as 13,17 and the plain text to be sent is 12. Assume public key (e) as 19. **[8]**

b) Discuss and compare linear cryptanalysis and differential cryptanalysis. **[8]**

P.T.O.

Q5) a) Discuss key management with respect to following issues: **[10]**

i) Key generation.

ii) Key distribution.

iii) Key Updation.

b) Explain one way and mutual authentication. **[8]**

OR

Q6) a) How the Digital Certificate creation takes place? Enlist the contents of digital certificate. **[10]**

b) Explain Public key infrastructure X.509 with the help of architectural block diagram. **[8]**

SECTION - II

Q7) a) What is IPSEC? How does AH and ESP differ while working under Tunnel mode and Transport mode? **[10]**

b) As we know that social networking chat applications are relayed chats and there is no security from service providers. Considering this, Alice and Bob want to chat from their computers with security in peer to peer fashion. Explain with diagram how to achieve this in application layer, network layer and SSL. **[8]**

OR

Q8) a) Discuss SSL with respect to four phases. **[10]**

i) Establish security capabilities.

ii) Server authentication and key exchange.

iii) Client authentication and key exchange.

iv) Finish.

b) What do you mean by Internet key exchange protocol? Explain its different phases. **[8]**

Q9) a) Describe the types of smart cards and explain the advantages and disadvantages of smart card. **[8]**

b) Draw and explain the implementation context for PDCA cycle in ISO 27001. **[8]**

OR

Q10) a) With the help of block diagram describe the process of mobile payments. **[8]**

b) Considering current context of internet banking or internet based payment systems, explain with diagram, the use of mobile phone as an additional measure to enhance authentication process. (Hint: OTP-one time password) **[8]**

Q11) Write short notes on (Any four) : **[16]**

a) Electronic evidence.

b) Internet fraud.

c) Identity Theft.

d) Computer Forensics.

e) Cyber Terrorism.

OR

Q12) a) Explain Indian IT laws in detail. **[8]**

b) Illustrate Industrial Espionage in IT industry. **[8]**