MAY - 18

Q. P. Code: 24643

(3 Hours) [Total Marks:80]

1. Question No. 1 is compulsory.
2. Attempt any three out of the remaining five questions.
3. Assume suitable data if necessary
4. Figures to right indicate full marks.

Q.1	(a)	What is the purpose of S-boxes in DES? Explain the avalanche effect?	[05]
	(b)	Give examples of replay attacks. List three general approaches for dealing with replay attacks.	[05]
	(c)	Why is the segmentation and reassembly function in PGP(Pretty Good Privacy) needed?	[05]
	(d)	List and explain various types of attacks on encrypted message.	[05]
Q.2	(a)	What is the need for message authentication? List various techniques used for message authentication. Explain any one.	[10]
	(b)	Explain Kerberos protocol that supports authentication in distributed system.	[10]
Q.3	(a)	What characteristics are needed in secure hash function? Explain the operation of secure hash algorithm on 512 bit block.	[10]
	(b)	What is a nonce in key distribution scenario? Explain the key distribution scenario if A wishes to establish logical connection with B. A and B both have a master key which they share with itself and key distribution center.	[10]
Q.4	(a)	Why E-commerce transactions need security? Which tasks are performed by payment gateway in E-commerce transaction? Explain the SET (Secure Electronic Transaction) protocol.	[10]
	(b)	In RSA system the public key of a given user e=7 & n=187.	[10]

2F4A7267688055B483146CAF0560042A

1) What is the private key of this user?
2) If the intercepted CT=11 and sent to a user whose public key e=7 & n=187. What is the PT?
3) Elaborate various kinds of attacks on RSA algorithm?

Q.5 **(a)** How can we achieve web security? Explain with example. **[10]**

(b) Use Hill cipher to encrypt the text "short". The key to be used is "hill". **[10]**

Q.6 **(a)** Explain IPSec protocol in detail. Also write applications and advantages of IPSec. **[10]**

(b) Differentiate between i) MD-5 and SHA ii) Firewall and IDS. **[10]**

****

2F4A7267688055B483146CAF0560042A