TE (I.T.) Rev. SEM VI
Information & N/w Security

may 2014
13/05/14

[REVISED COURSE]

QP Code : MV-18098

TIME - 3 Hrs **Marks – 100**

Note:

1. **Question 1 is compulsory.**
2. **Answer any 4 out of the remaining questions.**

Q.1 a) Among the fundamental challenges in Information security are confidentiality, integrity, and availability (CIA). Give an example where Confidentiality is required, but not integrity. Give an example where integrity is required, but not confidentiality. Give an example where availability is the overriding concern . **(5)**

b) Encrypt the message "We are all together"
using a double transposition cipher with 4 rows and 4 columns, using the row permutation

(1,2,3,4) -----→ (2,4,1,3)

And the column permutation

(1,2,3,4) ----→(3,1,2,4) **(5)**

c) What is the difference between authentication and non-repudiation? **(5)**

d) Why is it a good idea to hash passwords that are stored in a file? What is a "salt" and why should a salt be used whenever passwords are hashed? **(5)**

Q.2a) Explain key generation, encryption and decryption in the RSA algorithm **(10)**
b) Identify security issues due to protocol weakness in following protocols **(10)**
1) CSMA/CD 3) Ethernet with MTU 1500

Q.3 a) Explain Birthday Problem? Suppose hash function generates 12 bit output. If you hash 2^{10} randomly selected messages, how many collisions would you expect to find? **(10)**

b) Explain Kerberos operation in detail **(10)**

Q.4 a) Explain key generation, encryption and decryption in the RSA algorithm **(10)**
b) Explain following Attacks **(10)**
1) Buffer overflow attack 2) Salami Attack

Q.5 **a)** What are the three aspects of a 3-factor authentication **(05)**
b) What are the possible attacks on the password, Explain each in detail ? **(05)**
c) What is Access Control? How it is different from Availability? **(05)**
d) Write a note on firewall **(05)**

Q.6 a) What is primary advantage of SSL over IPSec? What is primary advantage of IPsec over SSL? **(05)**

b) 'Strength of DES depends on the S-boxes in DES'- Comment on the statement **(05)**

c) Write a note on CAPTCHA **(05)**

d) What is the difference between Digital signature and Digital Certificate **(05)**

Q.7 Write a short note on **(5 X 4 = 20)**

a) Session Hijacking
b) Risk Analysis
c) Web Server Vulnerability
d) Honey pot