

<http://www.rgpvonline.com>

CS-7101(GS)/CS-7201(NGS)

B.E. VII Semester

Examination, December 2013

Network & Web Security (Elective)

Time : Three Hours

Maximum Marks : 70/100

Note: Attempt one question from each unit, including subparts.
All questions carry equal marks.

Unit - I

1. a) Explain the following terms
 - i) Sniffing
 - ii) Snooping
 - iii) Spoofing
 - iv) Phishing
- b) What do you mean by intrusion? Explain types of IDS detection techniques.

OR

2. a) Explain the following:
 - i) Monypots
 - ii) Active attacks
 - iii) System Integrity verifiers
- b) What are the key principles of security? What are various security mechanism to achieve security goals?

Unit - II

3. a) i) While DES keys are 64 bites long, but its effective key length is only 56 bits, why?

ii) What is the most security-critical component of DES round function. Give brief description of this component.

- b) On the elliptic curve over the real numbers $y^2 = x^3 - 36x$, Let $P = (-3.5, 9.5)$ and $Q = (-2.5, 8.5)$. Find $P+Q$ and $2P$.

OR

4. a) Given the key "GYBNQKURP" apply the hill cipher to the plain text "ACT" to show how encryption and decryption are performed and prove authenticity.
- b) Define Avalanche effect and completeness effect. Also discuss the strength of DES with regard to these.

Unit - III

5. a) Why has there been an interest in developing a message authentication code derived from a cryptographic hash function as apposed to one derived from a symmetric cipher?
- b) Explain briefly about MD5 message digest algorithm.

OR

6. a) What do you understand by Secure Hash Algorithm (SHA)? Describe the logic of SHA-1.
- b) Write the digital signature algorithm (DSA) of digital signature standard. Give reasons behind choice of various parameters of the algorithm.

Unit - IV

7. a) What is virus? Explain different types of viruses.
- b) Write short notes on following:
- i) FTP Trojan.

ii) Search Engine Phishing.

iii) TCP/IP hijacking.

OR

8. a) What are the differences between threat and attack? Explain classification of security attacks.
- b) What do you mean by Denial of service? Write various denial of service attacks. Explain any two.

Unit - V

9. a) What do you mean by firewall? When the system administrator trusts the internal users. What types of firewall is to be used? What are its advantages and disadvantages?
- b) Write short notes on following (any two)
- i) Trusted system
- ii) IP Security.
- iii) Classes of Hacker.

OR

10. a) Explain working of packet filtering router firewall.
- b) What do you understand by web security? What are various web security protocol? Explain any one.

<http://www.rgpvonline.com>