SUBJECT CODE : CS/MC/SI64

B. C. A. DEGREE EXAMINATION, APRIL 2012
SIXTH SEMESTER

REG. NO. _____

COURSE   :   MAJOR CORE
PAPER   :   SECURITY ISSUES IN INFORMATION TECHNOLOGY
TIME   :   30 MINUTES   MAX. MARKS: 20

SECTION-A   **(20 X 1 = 20)**

TO BE ANSWERED ON THE QUESTION PAPER ITSELF

I. Choose the correct answer:

1. Information has _____when it is free from mistakes and has the value that the end user expects
   (a) confidentiality   (b) authenticity   (c) accuracy   (d) integrity

2. Protecting data in _____ are critical aspects of information security
    (a) motion   (b) rest   (c) motion and Rest   (d) different state

3. _____ is the risk that remains to the information asset even after the existing control has been applied
   (a) Residual risk   (b) Control risk   (c) Non residual risk   (d) None of these

4. _____ is the process by which an attacker changes the format and timing of their activity to avoid being detected by IDPS
   (a) Tuning   (b) Masking   (c) Phreaking   (d) Evasion

5. _____is the process of attracting attention to a system by placing tantalizing information into key location
   (a) Enticement   (b) Entrapment   (c) Sag   (d) Back hack

6. _____authenticate the cryptographic key embedded in the certificate.
   (a) Digital certificate   (b) Digital signature   (c) DSS   (d) DA

7. _____ is the finger print of the author's message which is compared with the recipient's locally calculated hash of the same message.
   (a) Message digest   (b) Message authentication code
   (c) Secure hash standard   (d) DGP

8. RFP means _____
   (a) Request For Project   (b) Ready For Proposal
   (c) Ready For Project   (d) Request For Proposal

..2

II. Fill up the blanks:

9. In a _____ a hacker uses his personal computers to break in to a system.

10. _____ works directly with data owners and responsible for storage, maintenance, protection of the information.

11. _____allows the attacker to access the system at will with special privileges,

12. _____is a technique used to gain unauthorized access to computers.

13. _____ is the control approach that attempt to shift risk to other assets, other processes or other organization.

14. _____ plan addresses the preparation for recovery from disaster.

15. _____ can detect and prevent intrusion by active response.

16. Hiding information within images is called_____.

III. State True or False:

17. Mitigation is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.

18. Packet filtering firewall is also called proxy server.

19. Web clients use Digital Certificate to authenticate the user.

20. The tracking process is commonly implemented using a _____.

∗∗∗∗∗∗∗

SUBJECT CODE : CS/MC/SI64

B. C. A. DEGREE EXAMINATION, APRIL 2012
SIXTH SEMESTER
COURSE   :   MAJOR CORE
PAPER   :   SECURITY ISSUES IN INFORMATION TECHNOLOGY
TIME   :   2½ HOURS   MAX. MARKS: 80

SECTION – B
Answer any eight questions: **(8 x 5 = 40)**

1. List the components of an information system.

2. Write a note on (a) trespass

                    (b) vandalism

                    (c) Timing attack.

3. What are kerberos? Explain.

4. Brief a note on VPN.

5. Explain about Vernam cipher method.

6. How does public key algorithm work?

7. Explain planning and risk assessment.

8. Explain about steganography.

9. Discuss on "Sys sp".

10. How can you accomplish the goal of Readiness and Review domain?

SECTION – C
Answer any four questions: **(4 x 10 = 40)**

11. Explain different types of attacks.

12. Discuss on Risk Control Strategies.

13. Explain different processing mode of firewalls.

14. Briefly explain IDPS detection methods.

15. State and explain Cryptographic tools.

16. Give clear details on External Monitoring domain.

✳✳✳✳✳✳✳