Register Number: ……………………..

B.E/B.TECH DEGREE EXAMINATIONS: NOV/DEC 2013

Sixth Semester

ITY110: CRYPTOGRAPHY & NETWORK SECURITY

(Common to IT & CSE)

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. The assurance that data received are exactly as sent by an authorized entity is known as
a) Authentication b) Integrity
c) Confidentiality d) Non repudiation

2. How many keys are used in triple encryption?
a) Two b) Three
c) One d) Both a) and b)

3. □ (41) = ?
a) 35 b) 40
c) 42 d) 18

4. $y^2 = x^3 + ax + b$ represents
a) Elliptic curves b) Sinusoidal curves
c) Beizer curves d) Trapezoidal curves

5. For any given block ***x***, it is computationally infeasible to find ***y*** ≠ ***x*** with H(***y***) = H(***x***). This property is known as
a) One-way b) Weak collision resistance
c) Strong collision resistance d) Moderate collision resistance

6. MD5 Algorithm takes as input a message of
a) 2^{15} b) 2^{32}
c) Arbitrary length d) 2^{64}

7. Kerberos relies on
a) Asymmetric encryption b) Authentication
c) Symmetric encryption d) Digital signature

8. PGP provides
a) Confidentiality and Authentication b) Confidentiality and Authorization
c) Confidentiality and Non-repudiation d) Confidentiality and Encryption

9. ___________ are designed to divert an attacker from accessing critical systems
a) Kerberos b) Honeypots
c) Passwords d) Firewalls

10. ___________ propagates itself from system to system
a) Virus b) Worm
c) Trojan Horse d) Zombie

PART B (10 x 2 = 20 Marks)

11. What are the two difficulties with one-time pad?
12. What is a Meet-in-the-middle-attack?
13. What is the zero point of an elliptic curve?
14. What is a nonce?
15. Differentiate between message authentication code and a one-way hash function.
16. What are the properties a digital signature should have?
17. What do you mean by realm in Kerberos?
18. What protocols comprise SSL?
19. What is a salt in the context of Unix password management?
20. List some weaknesses of a Packet-filtering router.

PART C (5 x 14 = 70 Marks)

21. a) (i) Explain Polyalphabetic cipher with an example (8)
(ii) What is Steganography? Give examples. (6)

(OR)

b) Write the evaluation criteria needed for AES.

22. a) (i) Perform encryption and decryption using RSA algorithm for the following: (10)
p = 5 ; q = 11 ; e = 3; M = 9
(ii) Write the requirements for public key cryptography. (4)

(OR)

b) (i) Users A and B use the Diffie-Hellman key exchange technique a common prime (10)
q = 71 and a primitive root α = 7.
If user A has private key, $X_a = 5$, what is A's Public key Y_a?
(ii) Write about the significance of timing attacks. (4)

23. a) Illustrate message authentication code with neat sketches.

(OR)

b) Design and implement HMAC algorithm with neat diagrams.

24. a) Explain the significance of encapsulating security payload with its format.

(OR)

b) Discuss the steps involved in the SSL record protocol transmission in web security.

25. a) Illustrate the different types of approaches to intrusion detection.

(OR)

b) (i) Mention the various capabilities and limitations of a firewall. (7)
(ii) Explain the different firewall configurations in detail. (7)

****