Reg. No. : | | | | | | | | | | |

R 3413

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2007.

Sixth Semester

Information Technology

IT 1352 — CRYPTOGRAPHY AND NETWORK SECURITY

(Regulation 2004)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are the problems with the one-time pad?

2. What is avalanche effect?

3. What is the use of traffic padding?

4. List the properties of Euler's Phi.

5. List the advantages and disadvantages of symmetric and asymmetric key cryptography.

6. Find the GCD of (1130, 1004).

7. What is message authentication code?

8. What is the difference between weak and strong collision resistance?

9. What services are provided by IP sec?

10. What is honeypots?

annauniv portal.blogspot.com

PART B — (5 × 16 = 80 marks)

11. (a) (i) Explain in detail the transformations take place in AES encryption procedure. (12)

(ii) Explain the playfair cipher with an example. (4)

Or

(b) Decrypt the Hill cipher LVWADSOWVCIY where the ciphertext VC and YH correspond to the plaintext en and th respectively. (16)

12. (a) (i) Users A and B use the Diffie–Hellman key exchange technique, a common prime $p = 71$ and a primitive root $g = 7$ are used. If user A has private key $XA = 5$, what is A's public key YA? If user B has private key $XB = 12$, what is B's public key YB? What is the shared secret key? (12)

(ii) In RSA system, the public key of a given user is $e = 31$, $n = 3599$, what is the private key of this user? (4)

Or

(b) Discuss in detail the different ways of distribution of public keys. (16)

13. (a) (i) Describe the block chaining technique. (10)

(ii) List and brief the different attacks identified across a network. (6)

Or

(b) (i) Discuss the security of HMAC. (10)

(ii) Write and explain the digital signature algorithm. (6)

14. (a) Discuss the different types of authentication procedures. (16)

Or

(b) (i) What are the key features of SE? Explain. (8)

(ii) What protocols comprise SSL? Explain any two of them. (8)

15. (a) Discuss in detail the packet-filtering router firewall. (16)

Or

(b) (i) List and brief, the different generations of antivirus software. (6)

(ii) Discuss on Behavior-Blocking software. (10)

annaunivportal.blogspot.com