C 61498 **(Pages 2)**

Name..

Reg. No.......................................

SIXTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, APRIL 2014

(2009 Scheme)

CS/PTCS 09 L01—INFORMATION SECURITY

(Regular/Supplementary/Improvement)

Time : Three Hours Maximum : 70 Marks

Part A

Short answer questions (one/two sentences).

1. Decipher the following cipher text using brute force attack :

   AYGLCPS NLZNRIFNEIHR AIAECE. (Hint: Algorithm - Rail fence)

2. What are the characteristics of good ciphers ?

3. What are the requirements of authentication function ?

4. What are the two modes in which the IPsec ESP service can be used ?

5. How does the operating system protect the password file ?

(5 × 2 = 10 marks)

Part B

Answer any **four** *questions.*
Analytical/Problem solving questions.

6. Consider a plain text alphabet G. Using the RSA algorithm and the values as E = 3, D = 11 and N = 15, find out what this plain text alphabet encrypts to and verify that upon decryption, it transforms back to G.

7. Compare the different versions of Secure Hash Algorithm.

8. Draw the DSS approach to generate Digital Signature of a message.

9. Explain the major issues in the design of a distributed intrusion detection system.

10. Explain the different classes of message authentication function.

11. Explain how CAPTCHA can be used to provide security for Hard AI Problems.

(4 × 5 = 20 marks)

Turn over

Part C

Answer section (a) **or** *section* (b) *of each questions.*
Descriptive / Analytical / Problem solving questions.

12. (a) Consider a Diffie-Hellman scheme with a common prime q = 353 and a primitive root α = 3. Users A and B have private keys X_A =17, X_B = 21 respectively. Assume user D is the intruder. If user D has private keys X_{D1} = 18 and X_{D2} = 31, find Y_A, YB. YD_1, YD_2. What is the shared secret key K_1 and K_2 ? Explain the diagram.

Or

(b) Discuss the variety of ways in which a Hash function (H) can be used to provide message authentication and mention the requirements of a Hash code.

13. (a) What are the various kinds of attacks on password ? Explain any three attacks with an example for each.

Or

(b) Explain Firewalls in detail. How Screened Host Firewall Systems is different from Dual-homed Host Firewalls and Screened Subnet Firewalls (with DMZ).

14. (a) Explain the two approaches in which the IPSec ESP service can be used? Explain with neat diagram.

Or

(b) Explain in detail about the ticketing mechanism in Kerberos that is used for providing authentication.

15. (a) Explain the software based attacks and also discuss in detail about the software recovery engineering methods.

Or

(b) Mention the methods by which an operating system can be trusted and explain the issues involved in operating system security functions.

(4 × 10 = 40 marks)