53 (CS 717) CRNS

2014

CRYPTOGRAPHY AND NETWORK SECURITY

Paper : CS 717

Full Marks : 100

Time : Three hours

The figures in the margin indicate full marks for the questions.

*Answer **any 10** questions out of **12.***

FIRST HALF

1. *(a)* Differentiate between SECRET KEY versus PUBLIC KEY cryptography. 2+8=10

(b) Consider a Hill Cipher $m = 3$ (block size = 3) with key K shown below

$$K = \begin{pmatrix} 25 & 3 & 7 \\ 5 & 9 & 21 \\ 11 & 8 & 13 \end{pmatrix}$$

(i) What is the Ciphertext corresponding to the plaintext = (VOW) ?

(ii) What is the plaintext corresponding to the Ciphertext = (TQX) ?

2. *(a)* Do each of the following inverses exist ? If yes, what are they ? If no, explain why not ?

(i) $102^{-1} \pmod{411}$

(ii) $77^{-1} \pmod{411}$

(b) Check whether 14 is a generation of the group $\langle Z^*457, {}^*457 \rangle$

(c) Consider the field $GF(2^4)$. Let the field multiplication be performed module the irreducible polynomial

$$x^4 + x + 1$$

Compute $(1010)^{-1}$.

(d) An integer $n, 0 \leq n \leq 210$, satisfies the following set of congruences

$$n \bmod 5 = 4$$

$$n \bmod 6 = 3$$

$$n \bmod 7 = 2$$

What is n ? 4+2+2+2=10

3. *(a)* What is public key cryptosystem ?

(b) Explain RSA.

(c) Perform encryption and decryption using RSA algorithm for the following parameter $p = 3, q = 11, c = 7$ and $M = 5$.

(d) In a public key cryptosystem using the RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5, n = 35$. What is the plaintext M ? 2+4+2+2=10

4. *(a)* Explain El Gamal Encryption Algorithm.

(b) A block of plaintext has been encrypted using El Gamal encryption algorithm. Assume that $p = 977, g = 3$ and the recipient's public key = 477. What is the plaintext corresponding to the ciphertext $C_1 = 108$ and $C_2 = 562$? 6+4=10

5. *(a)* What do you understand by an Elliptic Curve Cryptography ? 2+4+4=10

(b) Let $A=(2, 4)$ and $B=(8, 5)$ be two points on the EC

$$Y^2 = x^3 + 2x + 4$$

Over F_{13}.

(i) Compute $A+B$?

(ii) Compute $2A$?

(c) Explain EC over binary fields ?

2+4+4=10

6. (a) In an Elliptic Curve of the binary field $GF(2^4)$, the multiplicative group of this field has 15 elements (all 4 bits binary strings except 0000). It turns out that $g = 0010$ is a generator of this group where field multiplication is defined using the irreducible polynomial $x^4 + x^3 + 1$. Check whether (g^{13}, g^{12}) is a point on the Elliptic curve $y^2 + xy = x^3 + gx^2 + g^4$.

(b) Explain Discrete Logarithm Problem on Elliptic Curves. 6+4=10

SECOND HALF

7. *(a)* Explain centralized authentication system using public key cryptography.

   (b) Explain Needham Schroedom Protocol with the possible attacks (*any one* version).

   4+6=10

8. *(a)* What is IPSec ?

   (b) Company policy requires two hosts *A* and *B*, in two different branches of an organization to communicate securely over the internet using the IPSec. Which of the *four* options would be most appropriate *AH* in transport mode, AH in tunnel mode, ESP in transport mode or ESP in tunnel mode ?

   (i) Explain your choice

   (ii) Show all the headers that are inserted in communication and the scope of authentication, integrity checking and encryption

   (iii) Is it necessary/possible to double encrypt a packet between *A* and *B* ? Explain.

   2+8=10

9. *(a)* Write short notes on the following Internet Scanning Worms

(i) Code Red

(ii) Slammer.

(b) Explain the Simple Epidemic Worm Propagation Model. 6+4=10

10. *(a)* What are BOTNETS ?

(b) How does a second generation Botnets work in a P2P networks ? Explain with representation diagram.

(c) A web worms always execute on the users browser. Yes *or* No ? Explain. 2+6+2=10

11. *(a)* What do you understand by vulnerability ?

(b) Explain *any four* important vulnerability classes in the field of security.

(c) Explain *any one* defence strategy and technique. 2+5+3=10

12. Write short notes on : ***(any two)*** 5+5=10

(a) Kerberos

(b) Trojans

(c) Digital Signature

(d) Buffer Overflow.
