53 (CS 603) INSC

2012 C
2013
(May)

INFORMATION SECURITY

Paper : CS 603

Full Marks : 100

Pass Marks : 30

Time : Three hours

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

*Answer **any five** questions.*

FIRST HALF

1. *(a)* Briefly define a ring. Consider the set $S = \{a, b\}$ with addition and multiplication defined by the tables 3+3=6

+	a	b
a	a	b
b	b	a

×	a	b
a	a	b
b	a	b

Is S a ring ? Justify your answer.

Contd.

(b) Find the integers $\times$ such that $2\times3=6$

(i) $5 \times \equiv 4 \pmod 3$

(ii) $7 \times \equiv 6 \pmod 5$

(iii) $9 \times \equiv 8 \pmod 7$

(c) Prove the following : $4+4=8$

(i) $[(a \bmod n)\ (b \bmod n)] \bmod n = (ab) \bmod n$

(ii) $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

2. (a) Explain Euclid's Algorithm. Using Euclid's algorithm determine $4+4+4=12$

(i) *gcd* (24140, 16762)

(ii) *gcd* (4655, 12075)

(b) Why is $gcd(n, n+1) = 1$ for two consecutive integers n and $n+1$ 4

(c) Suppose that $m = qn + r$ with $q > 0$ and $0 \le r < n$. Show that $m/2 > r$. 4

3. (a) What are the roles of the public and private key in public key crypto system ? Explain RSA. $4+4 = 8$

(b) Perform encryption and decryption using the RSA algorithm for the following : 4×3=12

(i) $p = 3$; $q = 11$, $e = 7$; M = 5

(ii) $p = 5$; $q = 11$, $e = 3$; M = 9

(iii) $p = 7$; $q = 11$, $e = 17$; M = 8

4. (a) Why it is important to study the Feistel Cipher ? Draw the general Cipher Structure. 3+5=8

(b) What is the difference between

(i) A block Cipher and a stream cipher

(ii) Confusion and Diffusion

4+4 = 8

(c) Draw the F box of DES algorithm. 4

SECOND HALF

5. (a) What are IP Sec ? Give examples of applications of IP Sec. 2+4=6

(b) Mention *any four* benefits of IP Sec. What services are provided by IP Sec ?

4+4=8

(c) Draw the IP Sec Security Scenerio. What is a replay attack ? 3+3=6

6. (a) Construct a playfair matrix with the key largest. Using the following playfair matrix 4+6=10

M	*F*	*H*	*I/J*	*K*
U	*N*	*O*	*P*	*Q*
Z	*V*	*W*	*X*	*Y*
E	*L*	*A*	*R*	*G*
D	*S*	*T*	*B*	*C*

encrypt this massage :

"MUST SEE YOU OVER CADOGAN WEST. COMING AT ONCE".

(b) What is affine Caesar Cipher ? Consider $a = 3$ and $b = 15$, using the affine Caesar cipher encrypt "CITK". 2+4=6

(c) Find the inverse of the following :

(i) Additive inverse – 25 mod 26

(ii) Multiplicative Imverse 9 mod 26 2+2=4

7. Write short notes on : (***any five***) 4×5=20

(i) Brute force attack

(ii) Abelian Group

(iii) Fermat's Theorem

(iv) Digital Signature

(v) Timing attack

(vi) Man in the midelle attack

(vii) SSL (Secure Socket Layer)
