53 (CS 603) INSC

2016

INFORMATION SECURITY

Paper : CS 603

Full Marks : 100

Time : Three hours

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

*Question number **1** is compulsory and attempt **any six** form the rest.*

1. Explain briefly (Answer within **60** words each) : 4×10=40

   (a) What is the difference between compression and encryption ?

   (b) If you had to both encrypt and compress data during transmission, which would you do first, and why ?

   (c) In public-key cryptography you have a public and a private key, and you often perform both encryption and signing functions. Which key is used for which function ?

(d) What is the difference between Diffie-Hellman and RSA ?

(e) What do you understand by a Format String Vulnerability attack ?

(f) What is the difference between a threat and vulnerability ?

(g) What is Phising and Spoofing ?

(h) Think about our CIT Kokrajhar Network. We use cyberoam as a proxy server. What are the advantage and disadvantage of using this proxy server ?

(i) Sometimes we see https instead of http in some of the websites. What is the reason behind this ?

(j) Can you identify *any four* strong points of Linux in the security point of view ?

2. (a) What do you understand by Authentication and Authorization ?

(b) Explain the buffer overflow attack.

5+5=10

Or

(c) What do you mean by CSS (Cross Site Scripting) attack ? How to prevent this ?

(d) Have you heard CSRF (Cross Site Scripting Request Forgery) ? What is it ? How to prevent CSRF ?

5+5=10

3. (a) What do you understand by modular arithmetic ?

(b) Prove

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

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

5+5=10

4. (a) Explain the Euclid algorithm for finding the greatest common divisor with an example.

(b) Explain the extended algorithm for finding the multiplicative inverses with an example.

5+5=10

5. (a) Find the following :

(i) $-200 \bmod 31$

(ii) $gcd(102, 1026)$

(b) Find the multiplicative inverses of the following :

(i) $(30)^{-1} \bmod 31$

(ii) $(-100)^{-1} \bmod 47$

5+5=10

6. *(a)* Given $f(x) = x^6 + x^5 + 3x^3 + 2x^2 + 4$ and $g(x) = x^3 + 2x^2 + 1$ where field multiplication are performed in modulo of 7. Find

(i) $f(x) \times g(x)$

(ii) $gcd[f(x), g(x)]$

(b) Prove $a \equiv b(\text{mod } n)$ and $b \equiv c(\text{mod } n)$ imply $a = c(\text{mod} n)$. 3+4+3=10

7. *(a)* What do you understand by Chinese Remainder Theorem ?

(b) Given following three equations

$X = 2 \text{mod} 3$

$X = 4 \text{mod} 5$

$X = 5 \text{mod} 7$

Find X ?

4+6=10

8. *(a)* Dexter wants to set up his own public and private keys using RSA. He choose $p = 23$ and $q = 19$ with $e = 283$. Compute the public key.

(b) Consider a situation where Alice and Bob want to communicate securely using RSA Algorithm. Can you device a scenario where both the parties can be able to communicate with each other without having doubt on each other ? (Explain within **60** words).

5+5=10