Total number of printed pages–5

53 (CS 603) INSC

2015

INFORMATION SECURITY

Paper : CS 603

Full Marks : 100

Time : Three hours

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

Question ***No. 1*** *is* ***compulsory****, answer* ***any five*** *from the rest.*

1. *(a)* What are substitution cipher, transposition cipher and block cipher ? 6

   (b) Explain the Encryption and Decryption algorithm of Cacsar Cipher. 4

   (c) What do you understand by confusion and diffusion in cryptography ? 4

   (d) What do you understand by DoS and Replay Attack ? 4

(e) What is cryptanalysis and explain the Ciphertext only Attack? 5

(f) Explain one time pad with example. 2

2. *(a)* What do you understand by Modular Arithmetic? Explain with an example. 3

(b) Show that if $c|a$ (meaning c divides a) and $c|b$ (c divides b) then c also divides d $(c|d)$ where $d = gcd\ (a, b)$ 4

(c) Prove that 6

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

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

(d) Calculate *gcd* (100, 506). 2

3. *(a)* What do you understand by symmetric cipher? 2

(b) What is DES and why we need it? 4

(c) Explain DES encryption and decryption algorithm with proper diagram. 9

4. *(a)* Explain how entities involved in a communication can be able to distribute the keys in the symmetric cipher model. 10

   (i) By considering a Key Distribution Centre

   (ii) By decentralized way (No KDC)

   (b) Can you find a security vulnerability in the key distribution scenario of the above question while you consider using KDC and give a proper way or method to secure it? 5

5. *(a)* What is Asymmetric Key Cipher? 2

   (b) What do you understand by Euler Totient function? 2

   (c) Why are prime numbers important in cryptography? 2

   (d) Calculate 9

   (i) Perform encryption and decryption using the RSA algorithm for $p=17$; $q=31$; $e=7$; $M=2$;

   (ii) In a public key system using RSA, you intercept the ciphertext $c=10$ sent to a user whose public key is $e=5$, $n=35$. What is the plaintext M?

(iii) In an RSA system, the public key of a given user is $e=31$, $n=3599$. What is the private key of this user?

6. (a) What is IPSec? 2

(b) Explain the IPSec protocol. 8

(c) Explain Digital Signature algorithm. 5

7. Write short notes on : ***(any three)*** 5×3=15

(a) DNS Spoofing

(b) Phishing

(c) Web Worm

(d) Kerberos

8. (a) What do you understand by MITM (Man In the Middle) attack? Explain with neat diagram? 4

(b) What is ARP Spoofing? 3

(c) In a LAN Network there are two machines (*A* and *B*) communicating with each other. Meanwhile another machine (*C*) which is thought to be attacker attacks the ARP caches of both the machines. 8

(i) Explain with neat diagram how can the attacker *C* poisons the ARP caches of *A* and *B*.

(ii) Show how the poisoning of ARP caches leads to MITM.

[Hint : Consider MAC address of $A : aa : aa : aa : aa : aa : aa :$, MAC address of $B : bb : bb : bb : bb : bb : bb :$ and MAC address of $C : cc : cc : cc : cc : cc : cc :$. Consider any valid IP addresses for these machines.]

———————