Code : 061505

B.Tech. 5th Semester Exam., 2013

INFORMATION SECURITY

Time : 3 hours *Full Marks* : 70

Instructions :

(i) Marks are indicated in the right-hand margin.

(ii) There are ***NINE*** *questions in this paper.*

(iii) Attempt ***FIVE*** *questions in all.*

(iv) Question No. ***1*** *is compulsory.*

1. Explain any *seven* of the following terms : 2×7=14

(a) Cryptology

(b) Cryptographer

(c) Cipher text

(d) Decryption

(e) Logic bomb

(f) DMZ

(g) Spoofing

(h) Masquerading

(i) Intrusion

(j) Sniffing

2. *(a)* Explain the working of RC4 algorithm

(b) Differentiate between the following

(i) Block cipher and Stream cipher

(ii) Passive security threat and Active security threat 8+6=14

3. *(a)* What are the two problems with the one-time pad?

(b) Explain the working of DES cipher clearly mentioning the number of bits in key, subkey and plaintext block. 5+9=14

4. *(a)* Describe the buffer overflow attack and the measures which can be taken to control it.

(b) What do you understand by MALWARE? Explain the different categories of it. 7+7=14

5. *(a)* Explain the working of asymmetrical cryptography.

(b) Define cryptanalysis. What is the difference between a mono-alphabetic and a poly-alphabetic cipher? 6+8=14

6. Explain any two information security models and discuss their benefits. 14

7. *(a)* Discuss the characteristics of symmetrical algorithms.

   (b) Explain the working of digital signature. 7+7=14

8. *(a)* What does it mean to say that a system is 'trusted'? Do you agree that "only a trusted system can break your security"? Why or why not?

   (b) Give two reasons why NGSCB attestation is necessary. 8+6=14

9. Suppose that Bob's knapsack private key is (3, 5, 10, 23) and $m^{-1} = 6$, and that the modulus is $n = 47$.

   (a) Find the plaintext for the ciphertext $C = 20$. Give your answer in binary.

   (b) Find the plaintext for the ciphertext $C = 29$. Give your answer in binary.

   (c) Find m and the public key. 5+5+4=14

★ ★ ★