53 (IT 702) ISCL

2015

INFORMATION SECURITY AND CYBER LAWS

Paper : IT 702

Full Marks : 100

Time : Three hours

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

Answer ***any five (5)*** *questions out of* ***eight (8).***

1. *(a)* Define Cryptanalysis. Explain the following Cryptanalytic attack briefly 2+6

   (i) Known plaintext attack.

   (ii) Ciphertext only attack.

   (iii) Chosen plaintext attack.

   (b) Compare and contrast symmetric key cryptography. How the best can be taken from the both and combined to give a best solution ? 4+2

(c) Define the three security goals, distinguish between active and passive attacks with suitable examples. 2+4

2. (a) Explain RSA algorithm. Perform encryption and decryption using RSA algorithm for

$$P = 17, q = 11, C = 7, M = 88.$$

6+4

(b) State the advantages of public key cryptography. Differentiate Block ciphers from stream cipher. 5+5

3. (a) What are the different ways of distributing keys ? What is the need of key exchange ? Describe the Diffe-Hellman key exchange algorithm. 4+2+6

(b) Describe SHA-512 algorithm briefly. 4

(c) Why it is easier to hijack a UDP session than a TCP session ? Give your points in favour of this. 4

4. (a) What is an one-way function ? Do you think that one-way function is an integral part of modern cryptography ? If so, why ? Give *at least three* important requirement of one way-hash function design. 2+3+3

(b) What is the purpose of S/MIME? Compare and contrast Pretty Good Privacy (PGP) and S/MIME. 4+4

(c) What do you mean by Feistel cipher structure? 4

5. (a) What is digital signature? How will you verify it? Give the basic structure of digital signature. 4+2+4

(b) List out the characteristics of a good firewall implementation. How is a circuit gateway differ from an application gateway? 5+5

6. (a) What are the different security mechanism reommended by ITU (International Telecommunication Union) in their X·800 recommended, describe them briefly. 8

(b) In man-in-the-middle attack, even we send our information by using SSL technique, the attacker can also read our information, why? Describe it with the help of appropriate figures. 4

(c) Explain the following : 4+4

(i) Message Authentication Code (MAC)

(ii) Hash based Message Code (HMAC)

7. *(a)* In Kerberos Version4, describe scenario of authentication in an open network environment by using Authentication Server (AS) scenario, AS and traffic Granting Server (TGS) scenario, fuel service Kerberos scenarios, briefly. 3+4+5

(b) Why SSL layer positioned between Application and Transport layer? Discuss the following sub protocols of SSL 2+6

(i) Handshake Protocol

(ii) Record Protocol

(iii) Alert Protocol.

8. Write short notes on : ***(any five)*** 5×4

(i) Message Integrity

(ii) Sniffing

(iii) Intrusion Detection System

(iv) IPSec

(v) Denial of Service

(vi) Session Key

(vii) Buffer overflow.
