53 (IT 702) ISCL

2014

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** questions from **eight**.*

1. *(a)* State the advantages of public key cryptography over secret key cryptography. Differentiate Block ciphers from Stream Ciphers. 4+4

   (b) Define Cryptanalysis. Explain the following Cryptanalytic attack briefly 2+6

   (i) Known Plaintext attack

   (ii) Ciphertext only attack

   (iii) Chosen plaintext attack.

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

2. (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) 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 requirements of one-way hash function design. 2+3+3

3. (a) A single bit error occurs in exactly one block of Ciphertext during transmission. How will this effect the recovery of plaintext in each of the following modes ? 6

ECB, CBC, CFB, OFB

(b) What is digital signature ? How will you verify it ? 4+2+4

(c) Explain HMAC structure briefly. 4

4. *(a)* Explain RSA algorithm. Perform encryption and decryption using RSA algorithm for $P = 17, q = 11, e = 7, M = 88$. 5+5

(b) In MD5 algorithm, what is the number of padding bits if the length of the original message is 2590 bits ? Do we need padding if the length of the original message is multiple of 512bits. 2+2

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

5. *(a)* In Kerberos Version 4, describe scenario of authentication in an open network environment by using Authentication Server (AS) Scenario, AS and Traffic Granting Server (TGS) Scenario, full service Kerberos Scenarios, briefly. 3+4+5

(b) How are transport and tunnel modes used in Encapsulating Security Paylead (ESP) service ? 4+4

6. *(a)* Why is 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

(b) What is session hijacking ? How does it differ from spoofing ? 4+2

(c) Compare and contrast Pretty Good Privacy (PGP) and S/MIME. 6

7. *(a)* What are IP see ? Mention *any four* benefits of IP see. 2+4

(b) Describe SHA-512 algorithm briefly. 4

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

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

(i) Fiestal Cipher

(ii) FEAL

(iii) Intrusion Detection System

(iv) Man-in-the Middle attack

(v) 3DES

(vi) Session Key

(vii) Buffer overflow.
