53 (IT 702) INSC

2016

INFORMATION SECURITY & 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 out of **Eight**.*

1. *(a)* State the advantage of Public Key Cryptography over Secret Key Cryptography. Differentiate Block ciphers from Stream ciphers. 5+5

   (b) What do you mean by Security Services? Explain various types of Security Services of X.800 architecture. 2+8

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

   (i) Known plaintext attack

(ii) Ciphertext only attack

(iii) Chosen plaintext attack.

(b) 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 :

ECB, CBC, CFB, OFB. 8

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

3. (a) Explain RSA algorithm with $p = 83$, $q = 107$ and $m = 234$. Show the complete translation conforming to the RSA algorithm. 6+4

(b) Define Primitive root. Given that 2 is a primitive root of 19. Determine all other primitive roots of 19. 2+4

(c) What is the difference between authentication and non-repudiation ? 4

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

(b) Consider a Diffie-Hellman Scheme with a common prime number 11 and a primitive root $\alpha = 2$. 6

(i) if user A has public key $Y_A = 9$, what is A's Private key ?

(ii) if user B has public key $Y_B = 3$, what is shared secret key K ?

(c) Define discrete logarithm. 2

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

6. (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 a Replay attack ? How can this be prevented ? 2+3

(c) What are IPsec ? Mention *any four* benefits of IPsec. 3+4

7. (a) Differentiate between Circuit-level and Application-level firewalls. 4

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

(i) Handshake protocol

(ii) Record protocol

(iii) Alert protocol

(c) How are transport and tunnel modes used in IPsec Encapsulating Security Protocol (ESP) Service ? 4+4

8. (a) Describe SHA-512 algorithm briefly. 5

(b) Write short notes on : ***(any three)*** 3×5

(i) Avalanche effect

(ii) FEAL

(iii) Digital Signature

(iv) IDS

(v) HMAC.
