53 (IT 702) ISCL

2017

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 out of* ***eight***.

1. *(a)* What do you mean by cryptanalysis? Explain the following cryptanalytic attack briefly : 2+6

   (i) Known plaintext attack

   (ii) Ciphertext only attack

   (iii) Chosen plaintext attack.

   (b) Define *three* security goals, distinguish between passive active attacks with suitable examples. 3+4

(c) Why it is easier to hijack a UDP session than a TCP session? Give your points in favour of this. 5

2. (a) Define Discrete Logarithm. 5

(b) What are the drawback of 3-DES? Describe various steps of encryption and decryption in AES algorithm. 2+8

(c) If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate? 5

3. (a) What is the role of public key and private key in public key crypto system? 4

(b) Perform encryption and decryption using the RSA algorithm for the following : 4×3

(i) $P = 3, q = 11, e = 7, M = 5$

(ii) $P = 5, q = 11, e = 3, M = 9$

(iii) $P = 7, q = 11, e = 17, M = 8$

(c) State the advantage of public key cryptography over secret key cryptography. 4

4. (a) Why it is important to study Feistel Cipher ? Explain the function F of DES algorithm. 4+6

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

(c) What is Avalanche effect ? Why it is an important criterion for encryption ? 4

5. (a) In a Diffie-Hellman key exchange, let the prime number be 353 and one of its primitive root be 3 and let A and B select their secret keys $X_A = 97$ and $X_B = 233$. Compute public key and common secret key of A and B. 7

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

(b) Describe SHA-512 algorithm briefly. 5

6. (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

7. (a) What is IPSec and explain the *two* modes of IPSec operation? 3+6

(b) Mention *any four* benefits of IPSec. What types of security services are provided by IPSec? 4+4

(c) Using Euclid's algorithm find GCD (105, 66). 3

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

(i) Man-in-the middle attack

(ii) Intrusion Detection System

(iii) Digital Signature

(iv) Session Key

(v) HMAC

(vi) Secure Socket Layer (SSL).
