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)* Define Cryptanalysis. Explain the following cryptanalytic attacks briefly. 2+6

   (i) Ciphertext only attack

   (ii) Known plaintext attack

   (iii) Chosen plaintext attack.

   (b) Describe the DES encryption algorithm. What is avalanche effect in DES decryption ? 6+2

(c) What is denial service attack? 4

2. (a) State the advantage of public key cryptography over secret key cryptography. Differentiate block ciphers from stream ciphers. 5+4

(b) A block cipher operates on block of fixed length, often 64 or 128 *bits*. How output feedback (OFB) mode makes a block cipher into a synchronous stream cipher? 5

(c) What is digital signature? What requirements should a digital signature scheme satisfy? 3+3

3. (a) Explain RSA algorithm. In RSA crypto system has $p = 13$, $q = 11$ and $e = 5$

(i) Find decryption key d

(ii) Encrypt 85

(iii) Decrypt ciphertext 2. 6+6

(b) While DES keys are 64 *bit* long, but its effective key length is only 56 *bits*, why? 4

(c) What is a reply attack? How can it be prevented? 2+2

4. *(a)* How are transport and tunnel mode used in IPsec Encapsulating Security Payload (ESP) Service ? 4+4

(b) A Feistel cipher is a block cipher with a particular structure. Explain briefly basic encryption and decryption operations of it. 8

(c) Why session keys are required ? What are the advantages ? 2+2

5. *(a)* Explain the Diffie-Hellman algorithm for establishing a shared secret over an unprotected communication channel. Provide an example to illustrate the working of this algorithm. 6+4

(b) Why is SSL layer positioned between the application layer and transport layer ? Discuss the following sub-protocols of SSL 4+6

(i) Handshake Protocol

(ii) Record Protocol

(iii) Alert Protocol.

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 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 function design. 3+2+3

7. *(a)* Differentiate between Circuit-level and Application-level firewalls. 6

(b) Show and explain HMAC structure. 6

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

8. *(a)* What is the difference between authentication and non-repudiation? 5