53 (IT 702) INSC

2018

INFORMATION SECURITY AND CYBER LAW

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* ***seven.***

1. Answer the following questions : 10×2

   (i) What is the difference between Asymmetric and Symmetric encryption ?

   (ii) What are the requirements for a Hash function ?

   (iii) What is the role of session key in public key schemes ?

   (iv) What is digital signature ?

(v) What is denial of service attack?

(vi) Compare Substitution and Transposition techniques.

(vii) What is discrete logarithm?

(viii) Define cryptanalysis.

(ix) Define primitive root.

(x) Define integrity and non-repudiation.

2. (a) Define *three* security goals. Distinguish between active and passive attacks with suitable examples. 3+4

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

(c) What is replay attack? How can this be prevented? 3+2

3. (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 requirements at one-way-hash function design. 3+3+3

(b) State the advantage of using Cipher Block Chaining (CBC) mode over Electronic Code Book (ECB) mode. 4

(c) What are the important features of Advanced Encryption Standard (AES) ? How does AES differ from DES ? 4+3

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

(b) Kerberos uses three different kinds of secret keys : the login key, the ticket-granting key and session key. Explain the need for each of these keys. In particular, how the security offered by the Kerberos is weakened if we made use of just the login key or just the session key and login key instead of three keys. 6+4

5. (a) In a Diffie-Hellman-Key-Exchange Algorithm. Let 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 $X_B = 223$. Compute public key common secret key of A and B. 8

(b) Compare and contrast S/MIME and PGP protocols. 6

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

6. (a) Are DES and AES block ciphers? Give reasons. 4

(b) List out the characteristics of good firewall implementation. How is a circuit gateway different from an application gateway? 10

(c) Justify the inclusion of SSL layer in between application layer and transport layer. 6

7. (a) What is IPSec and what are the *two* modes of IPSec operation? What type of security services are provided by IPSec? 2+2+4

(b) Explain HMAC structure briefly. 4

(c) Write short notes on ***any two*** of the following : 4+4

(i) Digital Signature

(ii) Intrusion detection system

(iii) MAC

(iv) pseudo.random sequence.
