WEST BENGAL UNIVERSITY OF TECHNOLOGY

CS-801D

CRYPTOGRAPHY AND NETWORK SECURITY

Time Allotted: 3 Hours — Full Marks: 70

The questions are of equal value.
The figures in the margin indicate full marks.
Candidates are required to give their answers in their own words as far as practicable.

GROUP A
(Multiple Choice Type Questions)

1. Answer *all* questions. 10×1 = 10

(i) ________ ensures that a message was received by the receiver from the actual sender and not from an attacker.

[✓ (A) Authentication] (B) Authorization
(C) Integration (D) None of these

(ii) Which of the following is a passive attack?

[✓ (A) Masquerade] (B) Replay
(C) Denial of service [✓ (D) Traffic analysis]

(iii) In public-key cryptography, ____________ key is used for encryption

[✓ (A) public] [✓ (B) private]
(C) both (A) and (B) (D) shared

(iv) Which of the following is a monoalphabetic cipher?

[✓ (A) Caesar cipher] (B) Autokey cipher
(C) Vigenere cipher (D) All of these

(v) In polyalphabetic cipher, the characters in plaintext have a ________ relationship with the characters in ciphertext

(A) one-to-one [✓ (B) one-to-many]
(C) many-to-one (D) many-to-many

(vi) ________ is based on the idea of hiding the relationship between the ciphertext and the key

(A) Diffusion (B) Confusion
[✓ (C) Both (A) and (B)] (D) None of these

(vii) There are __________ encryption rounds in IDEA.

(A) 5 (B) 16
(C) 10 [✓ (D) 8]

(viii) In asymmetric-key cryptography, how many keys are required for each communicating party?

[✓ (A) 2] (B) 3
(C) 4 (D) 1

(ix) A ______ is used to verify the integrity and authenticity of a message

(A) Decryption algorithm [✓ (B) Message digest]
(C) MAC (D) Both (B) and (C)

(x) RSA __________ be used for digital signatures

[✓ (A) can] (B) cannot
(C) must (D) must not

GROUP B
(Short Answer Type Questions)

Answer any *three* questions. 3×5 = 15

2. (a) Explain the differences between asymmetric and symmetric key cryptographies. 3
   (b) What is meant by IP sniffing and IP spoofing? 2

3. Explain active attack and passive attack with example. 5

4. What type of key is generated or exchanged by using Diffie-Hellman key exchange algorithm? Justify your answer. 5

5. Differentiate between transport and tunnel modes of operation of IPsec. 5

6. How is S-HTTP different from SSL? 5

GROUP C
(Long Answer Type Questions)

Answer any *three* questions. 3×15 = 45

7. (a) Write down RSA algorithm. 5
   (b) In a RSA system, the public key of a user is 17 and N = 187. What will be the private key of this user? 6
   (c) Is it possible to combine symmetric key and asymmetric key cryptography so that better of the two can be combined? 4

8. (a) How digital signatures can be generated? 5
   (b) Compare and contrast MD5 and SHA-1 algorithms. 5
   (c) Why is the SSL layer positioned between the application layer and transport layer? 3
   (d) What are the problems associated with clear text password? 2

9. (a) What is Algorithm mode? Describe Cipher Block Chaining (CBC) mode. 2+4
   (b) Discuss the vernam cipher. 3
   (c) State and explain how IDEA works. 6

10. (a) Discuss the basic principle of security. 4
   (b) Distinguish between substitution and transposition cipher. 5
   (c) Discuss different types of firewall with neat diagram. 6

11. (a) Write short notes on any *three* of the following: 3×5
   (a) Biometric Authentication
   (b) Message digest
   (c) DES
   (d) Public key infrastructure
   (e) PGP