Extra (IT)

CS/B.Tech/Even/IT/8th Sem/IT-801D/2014

2014

Cryptography & Network Security

Time Alloted : 3 Hours *Full Marks : 70*

The figure 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. Choose the correct alternatives for the following:

10x1=10

i) The four primary security principles related to a message are

(a) confidentiality, authentication, integrity and non-repudiation

(b) confidentiality, access control, non-repudiation and integrity

(c) authentication, authorization, non-repudiation and availability

(d) availability, access control, authorization and authentication

ii) Book Cipher is also called as

(a) Rail Fence Technique

(b) One-time pad

(c) Mono-alphabetic Cipher

(d) Running Key Cipher

iii) Conversion of cipher text into plain text is called as

(a) encryption (b) decryption
(c) cryptography (d) cryptanalyst

iv) Redundancy of plain text increases by.

(a) Confusion
(b) Diffusion
(c) Both confusion and diffusion
(d) Neither confusion nor diffusion

v) Bits contain in DES encrypts blocks.

(a) 32 (b) 56 (c) 64 (d) 128

vi) SSL layer is located between

(a) transport layer, network layer
(b) application layer, transport layer
(c) data link layer, physical layer
(d) network layer, data link layer

vii) Firewall is a specialized form of a

(a) bridge (b) disk (c) printer (d) router

viii) Application gateways are packet filters that.

(a) less secure than (b) more secure than
(c) equally secure to (d) slower

ix) In asymmetric key cryptography keys are required per communicating

(a) 2 (b) 3 (c) 4 (d) 5

x) If A and B want to communicate securely with each other, B must not know

(a) X's private key (b) X's public key
(c) B's private key (d) B's private key

GROUP - B

(Short Answer Type Questions)

Answer any *three* of the following. 3x5=15

2. What is the difference between passive and active security threats? 5

3. Explain **Simple Columnar Transposition Technique** of symmetric encryption. Convert the text "WEST BENGAL UNIVERSITY OF TECHNOLOGY" with the key value 31254. 5

4. (a) What is a meet-in-the-middle attack?

(b) Why is the middle portion of 3DES a decryption rather than an encryption? 2+3

5. What are the properties that a digital signature should have? 5

6. (a) Discuss about the four basic principles related to the security of a message.

(b) What is availability? 4+1

GROUP - C

(Long Answer Type Questions)

Answer any *three* of the following. 3x15=45

7. a. What do you mean by network security explain with a suitable model.

b. What is Brute-force attack? Explain.

c. What is Worm? What is the difference between Worm and Virus?

d. What are the key principles of security? 4+4+(2+2) +3

8. a. What are the key requirements of message digest?

b. What are the problems with exchanging of public keys?

c. Explain RSA algorithm.

d. "Symmetric key cryptography is faster than Asymmetric key cryptography"- Justify.

3+3+6+3

9. a. What is the purpose of the S-boxes in DES?

b. In the public-key system using RSA, you intercept the cipher text CT=10 sent to a user whose public key is E=5, N=35. What is the plain text PT?

c. What are the roles of the public and private key?

d. In an RSA system, the public key of a given user is E=31, N=3599. What is the private key of the user?

2+4+3+6

10. a. Why is the SSL layer positioned between Application layer and Transport layer?

b. Name the four key steps in the creation of a Digital certificate. How is SHTTP different from SSL?

c. What are the problems associated with clear text passwords?

4+4+3+4

11. Write short notes of any three of the following.

5x3

a) Kerberos

b) S/MIME

c) Firewall

d) DNS spoofing

e) Secure Electronic Transaction (SET)