Code No: 07A60503 R07

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, HYDERABAD
B. Tech III Year II Semester Examinations, May/June, 2013
Information Security
(Computer Science and Engineering)

Time: 3 hours **Max. Marks: 80**

Answer any five questions
All questions carry equal marks

- - -

1.a) What are the different security attacks and services? Explain them.
b) Explain the following attacks:
i) ARP attack
ii) Man-in-the-middle attack. [8+8]

2.a) How the hash function is generated using SHA-512?
b) Discuss in detail the process of encryption and decryption in AES algorithm. [8+8]

3.a) Explain about X.509 directory service.
b) What is Public key cryptography? Explain RSA algorithm with the help of an example. [8+8]

4. Discuss the services of PGP with neat figures. [16]

5. Explain the packet formats of Tunnel mode and Transport mode for AH and ESP Header. [16]

6.a) Discuss the protocol architecture of SSL.
b) How web security is provided by SSL and TLS. [8+8]

7.a) Discuss the types of Viruses.
b) Explain in detail about SNMP. [8+8]

8. What are the design principles of Firewalls? Explain the different types of firewalls. [16]

****

Code: 13A05702 **R13**

B.Tech IV Year I Semester (R13) Supplementary Examinations June 2017

CRYPTOGRAPHY & NETWORK SECURITY

(Computer Science and Engineering)

Time: 3 hours Max. Marks: 70

PART – A

(Compulsory Question)

*****

1 Answer the following: (10 X 02 = 20 Marks)

(a) Find the plaintext for the given Cipher text with Key K = 3.
Using Ceaser Cipher. Cipher Text : GUDSMDEGXONDODP

(b) Define Avalanche Effect.

(c) Determine the Numbers which are Relatively Prime to 21 by using Euler Totient Function.

(d) Differentiate conventional and public key encryption.

(e) Give the requirements for a Hash Function.

(f) Define MAC (Message Authentication Code).

(g) Differentiate forward and reverse certificates.

(h) What is S/MIME?

(i) Sketch neatly the SSL protocol stack.

(j) What are the benefits of IPSec?

PART – B

(Answer all five units, 5 X 10 = 50 Marks)

UNIT – I

2 Write short notes on security mechanisms.
Explain in detail about the steps involved in DES.

OR

3 Explain in detail about AES.
Give an account on different block cipher modes of operation.

UNIT – II

4 Perform Encryption and Decryption using the RSA algorithm.
p = 3 q = 11 e = 7 M = 5

OR

5 Explain in detail about Elgamal Cryptosystem and Chinese Remainder theorem.

UNIT – III

6 With an example, explain in detail about Secure Hash Algorithm.

OR

7 Explain in detail about HMAC and Digital Signature Standard..

UNIT – IV

8 Sketch neatly and briefly explain about Public Key Infrastructure.

OR

9 Explain in detail about Kerberos.

UNIT – V

10 Explain in detail about SSH and SSL record protocol transmission.

OR

11 Explain in detail about IP Security Policy.

*****

Code :R7411206

R7

IV B.Tech I Semester(R07) Supplementary Examinations, May/June 2011
INFORMATION SECURITY
(Common to Information Technology, Computer Science & Systems Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE questions
All questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) What are the different security services that are available ? Explain.
   (b) Write short notes on:
      i. UDP hijacking and
      ii. ARP attacks.
2. (a) What are the essential ingredients of a symmetric cipher ?
   (b) Briefly explain Electronic code Book (ECB).
   (c) Write notes on Key distribution approaches of message Authentication.
3. (a) Define Digital signature.
   (b) In what order should the signature function and the confidentiality function be applied to a message and why ?
   (c) Explain X0509 directory Authentication service.
4. (a) What are the five principal services provided by php?
   (b) Explain RSA algorithm.
5. (a) Explain IP Sec Documents with a neat diagram.
   (b) Write notes on ESP.
6. (a) What are the key features of SET ?
   (b) Write notes on SSL.
7. (a) List and briefly define three classes of intruders.
   (b) What is the role of compression and encryption in the operation of a virus.
   (c) Write short notes on SNMPrz.
8. (a) List three design goals of a firewall.
   (b) Explain packet filter router.
   (c) Define reference monitor what is the difference between subject and object of a access control.

⋆ ⋆ ⋆ ⋆ ⋆