Code No: **R41051** **R10** **Set No. 1**

IV B.Tech I Semester Regular/Supplementary Examinations, Nov/Dec - 2015

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
*****

1 a) Determine the security mechanisms required to provide various types of security services. [8]

b) How packet blocking and Route Table modification is done as part of TCP Session Hijacking? [7]

2 Give the overall structure of the AES encryption process. Describe the sequence of transformations in each round and showing the corresponding decryption function. [15]

3 a) Use Fermat's theorem to find a number between 0 and 72 with congruent to 9794 modulo 73. [8]

b) What are discrete logarithms? Explain their use in public key algorithms. [7]

4 Users A and B use Diffie-Hellman key exchange scheme using prime q=71 and primitive root α =2.

a) User A has private key Xa=5, What is A's public key Ya?
b) User B has private key Xb=12, what is B's public key Yb?
c) What is the shared secret key? [15]

5 a) What are the services provided by digital signatures? Explain if the following are provided
i) Source Authentication, ii) Data Integrity and iii) Source Non-Repudiation. [9]

b) What is Birthday Attack on Digital Signatures? Can it be performed by an 'Outsider'? [6]

6 a) Explain how email messages are protected using S/MIME signing and encryption? [10]

b) What is Radix 64 format? What is its use in PGP? [5]

7 a) Write some of the applications of IPSec. [7]

b) Differentiate the packet structure of ESP and AH. [8]

8 a) Give the taxonomy of malicious programs. Define each one. [8]

b) What are the different types of viruses? How do they get into the systems? [7]

Code No: **R41051** **R10** **Set No. 2**

IV B.Tech I Semester Regular/Supplementary Examinations, Nov/Dec - 2015

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
****

1 a) Why and where do format string vulnerabilities exist? How are they fixed? [8]

b) Discuss about buffer injection techniques briefly. [7]

2 a) Give the structure of Output Feedback Mode? Explain the advantages and disadvantages of OFB. [7]

b) What is double DES? What kind of attack on double DES makes it useless? [8]

3 a) What two assertions are made by Chinese Remainder Theorem? Demonstrate each assertion. [8]

b) What is Euler's Totient Function? Find the value of $\phi(37)$. [7]

4 a) What is an elliptic curve? Explain encryption in this context. [8]

b) Explain about the strength of RSA. [7]

5 a) List the generally accepted requirements for a cryptographic hash function. Explain each requirement. [6]

b) Explain Digital signature scheme (DSS) and Digital Signature Algorithm (DSA) in detail. [9]

6 a) Give the format for X.509 certificate. How are users certificates obtained? [8]

b) Explain the authentication services provided by X.509. [7]

7 a) Describe about SSL secure communication and SSL authentication. [8]

b) Describe in general how online payment processing is done. [7]

8 a) What is a firewall? What is the need for firewalls? What is the role of firewalls in protecting networks? [8]

b) What is a worm? Name some known worms. [7]

Code No: **R41051** **R10** **Set No. 3**

IV B.Tech I Semester Regular/Supplementary Examinations, Nov/Dec - 2015

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
*****

1 a) Define threat and attack. What is the difference between both? List some examples of attacks which have arisen in real world cases. [8]

b) Describe the mechanisms for preventing and detecting hijacking problems. [7]

2 a) Compare the substitution method in DES and AES. Why do we need only one substitution table in AES, but several in DES? [8]

b) What are the merits of Output-Feedback (OFB) as compared to Cipher Feedback (CFB)? [7]

3 a) What is a primitive root? Find all the primitive roots of 25. [8]

b) What is the difference between an index and a discrete logarithm? [7]

4 a) What are the ingredients of public key encryption scheme? Show with a diagram. Explain the encryption scheme. [7]

b) Perform encryption and decryption using the RSA algorithm P = 3, q = 11, e = 7, M = 5. [8]

5 Describe the steps in message digest generation in Secure Hash Algorithm in detail. [15]

6 a) Write note on PGP session keys, public/private key rings and passphrase keys. [8]

b) What are the similarities and differences between S? MIME and PGP? [7]

7 a) What does SSL handshake establish? How is it performed? [8]

b) What services are provided by IPSec? Explain. [7]

8 a) What is a application level gateway? What are the advantages and disadvantages of application gateways? [8]

b) Explain the need for trusted systems. [7]

Code No: **R41051** **R10** **Set No. 4**

IV B.Tech I Semester Regular/Supplementary Examinations, Nov/Dec - 2015

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & Engineering and Information Technology)

Time: 3 hours **Max. Marks: 75**

Answer any FIVE Questions
All Questions carry equal marks
****

1 a) What is meant by Denial of Service (DOS), Spoofing & Phishing? Explain. [8]

b) Explain Hill cipher with an example. [7]

2 a) Describe Encryption and decryption functions Triple DES. Compare its strength with DES. [10]

b) How are keys generated in Cast-128 algorithm? [5]

3 a) Given 2 as a primitive root of 29, construct a table of discrete logarithms, and use it to solve the congruence: $x^7 \equiv 17(mod\ 29)$ [8]

b) Use Euler's theorem to find a number between 0 and 28 with congruent to 6 modulo 35. [7]

4 a) Define some Elliptic curves on real numbers. Give the description of addition on those elliptic curves. [8]

b) In what way Diffie Hellman key exchange algorithm prone to man in the middle attack? Explain. [7]

5 a) What is the difference between weak and strong collision resistance? [8]

b) Describe the various modes of arbitrated digital signatures. [7]

6 a) Explain how authentication is performed in Kerberos. [8]

b) Enumerate the differences between Kerberos Version 4 and 5. [7]

7 List the scope and requirements of SET. Explain the participants of SET and their relationship. [15]

8 a) What is meant by stateful packet inspection? What are the advantages and disadvantages? [8]

b) Compare the features of host based IDS and network based IDS. Why, when and where to use host based IDS? [7]