Code No: **RT41051** **R13** **Set No. 1**

IV B.Tech I Semester Regular/Supplementary Examinations, October/November - 2017

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any THREE questions from Part-B

*****

PART–A *(22 Marks)*

1. a) What is meant by ARP poisoning? [4]
   b) Write about the application of DES in CBC mode. [4]
   c) What is meant by relative prime? Give an example. [3]
   d) What is the role of Key Distribution centre? [3]
   e) List out web security threats. [4]
   f) What is meant by intrusion detection? [4]

PART–B *(3x16 = 48 Marks)*

2. a) Briefly define the monoalphabetic cipher. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher? [8]
   b) What is Buffer Overflow? What are the tasks in exploiting the overflowable Buffer? [8]

3. Write about the CAST-128 key expansion, encryption and Decryption functions. [16]

4. a) Use discrete logarithm properties to solve the following equation $x5 \equiv 11 \bmod 17$. Using quadratic residues solve $x2 \equiv 5 \bmod 11$. [8]
   b) Given p=19, q=23, and e=3 Use RSA algorithm to find n, $\phi(n)$ and d. [8]

5. a) Give the structure of HMAC. Explain the applications of HMAC. [8]
   b) Write short notes on Digital Signature Algorithm. [8]

6. a) What protocols comprise SSL? What is the difference between an SSL connection and an SSL session? [8]
   b) Explain about SSL Handshake protocol. [8]

7. a) Write briefly about techniques used for Statistical anomaly detection. [10]
   b) What are the contents of an audit record? [6]

Code No: **RT41051** **R13** **Set No. 2**

IV B.Tech I Semester Regular/Supplementary Examinations, October/November - 2017

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any THREE questions from Part-B
*****

PART–A *(22 Marks)*

1. a) What is the role ARP in Ethernet switching? [4]
   b) What is the role of S-Box in DES? [4]
   c) What is a ring and a commutative ring? Differentiate. [4]
   d) What are the criterion of cryptographic hash function? [3]
   e) What are the requirements of Kerberos? [4]
   f) What are the different categories of intruders? [3]

PART–B *(3x16 = 48 Marks)*

2. a) Construct a Playfair matrix with the key largest. encrypt this message: MEET ME AT THE TOGA PARTY [8]
   b) List and explain the security mechanisms defined by X.800. [8]

3. Write about the following in AES cipher:
   Substitute Bytes Transformation
   ShiftRows Transformation
   MixColumns Transformation
   AddRound Key Transformation [16]

4. Write about key generation, encryption and decryption in ElGamal Cryptosystem. [16]

5. a) Give the structure of CMAC. What is the difference between CMAC and HMAC? [8]
   b) Describe the attacks on digital signatures. [8]

6. a) In S/MIME, how does a receiver find out what cryptographic algorithms the sender has used when receives an S/MIME message. [8]
   b) Explain about the trust mechanism and certificates used by PGP and S/MIME. [8]

7. a) Write short notes on Signature based IDS. [8]
   b) What are the basic approaches of building Security Associations? [8]

Code No: **RT41051** **R13** **Set No. 3**

IV B.Tech I Semester Regular/Supplementary Examinations, October/November - 2017

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any THREE questions from Part-B
*****

PART–A *(22 Marks)*

1. a) What is meant by UDP Session Hijacking? [4]
   b) What is a product cipher? [3]
   c) Mention the values of Multiplication modulo 7 from 0 to 6. [4]
   d) What is the difference between Hash function and Message Authentication Code? [4]
   e) List the transfer encodings used in S/MIME. [4]
   f) What services are provided by IPSec? [3]

PART–B *(3x16 = 48 Marks)*

2. a) Explain about Hill Cipher. Consider the plaintext "paymoremoney" and use the encryption key: K=$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$. Find the cipher text. [8]
   b) What is SQL Injection? Illustrate how is it performed with an example. [8]

3. a) What are the various block cipher design principles? Explain how different cryptographic algorithms use Fiestel Cipher Structure? [8]
   b) How is key expansion done in Blowfish? [8]

4. a) Let q=353 and α=3. Xa=97, Xb=233. Use Diffie Hellman Key exchange algorithm to find Ya, Yb and Secret key K. [8]
   b) Describe about public and private keys in ECC system and explain about security of ECC. [8]

5. a) Describe the process involved in digital signatures. Explain about different digital signatures. [8]
   b) Write about HMAC algorithm. What need to be done to speed up HMAC algorithm? [8]

6. Write about the following with respect to PGP:
   (i) Cryptographic algorithms used by PGP
   (ii) Compression in PGP
   (iii) Steps involved in PGP message generation. [16]

7. Write notes on:
   a)Encapsulating Security Payload.
   b) Transport and Tunnel Mode
   c) ISAKMP [16]

Code No: **RT41051** **R13** **Set No. 4**

IV B.Tech I Semester Regular/Supplementary Examinations, October/November - 2017

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any THREE questions from Part-B
*****

PART–A *(22 Marks)*

1. a) What is man in the Middle Attack? [4]
   b) What is avalanche effect? [3]
   c) Define the terms Ring, Group, Field. [4]
   d) What is the difference between message integrity and message authentication. [4]
   e) What is meant by PKI? [4]
   f) What is replay attack? [3]

PART–B *(3x16 = 48 Marks)*

2. a) Explain the various active attacks? What security mechanisms are suggested to counter attack active attacks? [8]
   b) What are the different transposition techniques? Explain. [8]

3. Describe about IDEA encryption and decryption. Write the applications which use IDEA. [16]

4. a) Explain about Euclidean algorithm for Greatest Common Divisor. [8]
   b) Define elliptic curves and explain their application in cryptography. [8]

5. Give the structure of SHA-512 compression function. Explain the structure of each round. Is Man in the Middle attack possible on SHA-512 [16]

6. a) What are the different servers used in Kerberos? Explain the role of each one. [8]
   b) What are the differences between Kerberos 4 and Kerberos 5. [8]

7. a) How is the behavior of an intruder found? [8]
   b) Explain about IPSec architecture and Security associations. [8]