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

IV B.Tech I Semester Regular Examinations, November - 2016

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & 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) Use Caesar cipher with key =15 to encrypt the message “Hello”. [4]

   b) What is differential cryptanalysis? [4]

   c) Solve the congruence $x^2 \equiv 7 \bmod 13$. [4]

   d) Distinguish between message integrity and message authentication. [4]

   e) Write the authentication dialogue exchanged between a user and authentication server in Kerberos V4? [3]

   f) Who are treated as intruders on a network? [3]

PART–B *(3x16 = 48 Marks)*

2. a) What are the tools available for session hijacking? Explain briefly how they work. [8]

   b) Determine the security services required to counter various types of Active and Passive attacks. What are the common C-functions that give raise to buffer overflow? [8]

3. a) Describe the round function of CAST block Cipher. Explain the encryption algorithm of CAST. [10]

   b) Explain the Key Scheduling of CAST. How many S-boxes are used by CAST? [6]

4. a) Explain Miller Rabins Primality Testing. Use the same to test the primality of 271, 341. Use base 2. [8]

   b) What are discrete logarithms? Explain how are they used in Public Key Cryptography? [8]

5. a) Explain the compression of Secure Hash Algorithm. [10]

   b) What are the requirements of hash functions? [6]

6. a) What is the need for security services at transport layer of Internet Protocol? [8]

   b) Explain the four protocols defined by Secure Socket Layer. [8]

7. a) Explain the methods used for statistical anomaly detection. [8]

   b) What are the services provided by IPSec? Where can be the IPSec located on a network? [8]

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

IV B.Tech I Semester Regular Examinations, November - 2016

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & 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

*****

<u>PART–A</u> *(22 Marks)*

1. a) Using Hill Cipher to encipher the message "we live in a insecure world". Use the key $\begin{bmatrix} 03 & 02 \\ 05 & 07 \end{bmatrix}$ [4]

   b) What are the weaknesses of DES? [4]

   c) Solve the congruence $x^5 \equiv 11 \bmod 17$. [4]

   d) Explain an attack to which MAC is vulnerable. How to make MAC more secure? [4]

   e) What are the components of $\text{Ticket}_{\text{TGS}}$ and Ticket_{v}? [3]

   f) What is meant by IP Spoofing? [3]

<u>PART–B</u> *(3x16 = 48 Marks)*

2. a) How are local variables put on the stack? How is stack used to pass arguments through to a function? How all this adds up to allow an overflowed buffer to take control of the machine and execute an attacker's code? Explain with examples. [10]

   b) What are transposition ciphers? [6]

3. a) Give the structure of AES. Explain how Encryption/Decryption is done in AES. [10]

   b) Define OFB and list its advantages and disadvantages. [6]

4. a) Explain Chinese Remainder Theorem. Using CRT find 'x' from the equations $x \equiv 7 \bmod 13$ and $x \equiv 11 \bmod 12$ [8]

   b) What are the attacks that are possible on RSA? [8]

5. a) Give the structure of HMAC. List out the design objectives of HMAC. Explain the benefits/advantages of HMAC over other hash based schemes. [10]

   b) Compare HMAC with CMAC. [6]

6. a) Explain the authentication procedures defined by X.509 certificate. Illustrate the concept of 'certificate chain' for verification of digital signature on X.509 certificate. [8]

   b) What are the main features of Kerberos Version 5? [8]

7. a) Write briefly about the signature based Intrusion Detection Systems. [8]

   b) What is Transport mode and Tunnel mode? Explain about the scope of AH and ESP in these modes? [8]

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

IV B.Tech I Semester Regular Examinations, November - 2016

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & 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) Use Vigenere Cipher with key HEALTH to encrypt the message "Life is full of surprises". [4]
   b) How is meet in the middle attack done in 2-DES? [4]
   c) For which value of n, does the group G= < Z_n*, x> have primitive roots: 17, 20, 38 and 50. [4]
   d) What is Birthday Attack on Digital Signatures? [4]
   e) What is Radix-64 text encoding? [3]
   f) How is replay attack prevented by IPSec? [3]

PART–B *(3x16 = 48 Marks)*

2. a) Write briefly the categories of attacks. What are the x.800 listed attacks? [8]
   b) Write briefly about ARP attack and session hijacking. [8]

3. a) Explain the round transformation of IDEA. Also explain the key scheduling of IDEA. [10]
   b) How is expansion permutation function done in DES? [6]

4. a) Explain ElGamal Crypto System with examples. [12]
   b) Discuss the security of ElGamal Crypto System. [4]

5. a) Describe the steps in finding the message digest using SHA-512 algorithm. What is the order of finding two messages having the same message digest? [10]
   b) Explain the benefits/advantages of HMAC over other hash based schemes. [6]

6. a) What are the content types provided by S/MIME? Explain. [8]
   b) How is an enveloped data MIME entity prepared? Write the steps. [8]

7. a) Explain about Host based Intrusion Detection Systems in brief. [8]
   b) What are the different combinations of Security Association on a network? [8]

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

IV B.Tech I Semester Regular Examinations, November - 2016

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science & 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 phishing? [4]
   b) Distinguish between diffusion and confusion. [4]
   c) Find the value of ϕ(100) and ϕ (80) [4]
   d) What is message authentication? How is it different from message integrity? [4]
   e) What are the keys used by PGP? [3]
   f) What are the contents of a Security Association? [3]

PART–B *(3x16 = 48 Marks)*

2. a) What is the relation between security mechanisms and attacks? Explain. [8]
   b) Discuss about SQL injection techniques briefly. [8]

3. a) How do you convert a block cipher into a stream cipher by using the Cipher Feedback (CFB) mode? Explain. [8]
   b) What is a Feistel Cipher? Name the Ciphers that follow Feistel Structure. [8]

4. a) Describe Chinese Remainder Theorem and explain its application. [10]
   b) What is the cipher text if the plain text is 63 and public key is 13? Use RSA algorithm. [6]

5. a) What are the requirements of cryptographic hash functions? [6]
   b) Describe the digital signature schemes DSS, Schnorr and ElGamal. [10]

6. a) Why does PGP compress the message? What are the reasons for compressing the signature but before encryption? [8]
   b) Give the summary of cryptographic algorithms used by S/MIME. [8]

7. a) What is an audit record? What is the use of audit record in intrusion detection? [8]
   b) Describe the architecture of IPSec. [8]