

Code No: RT41051

**R13**

**Set No. 1**

IV B.Tech I Semester Regular/Supplementary Examinations, Oct/Nov - 2018

**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) Differentiate between Active attacks and Passive Attacks. [4]
- b) Compare stream cipher with block cipher with an example. [4]
- c) Define Euler's theorem and list out its applications. [4]
- d) What are the requirements of the cryptographic hash functions? [3]
- e) What are the services provided by PGP services? [4]
- f) Illustrate the services provided by IPSec. [3]

**PART-B** (3x16 = 48 Marks)

- 2 a) Discuss the various principles involved in private and public key cryptography. [8]
- b) Discuss any four Substitution Technique and list their merits and demerits. [8]
- 3 a) Explain in detail Feistel Block Cipher structure with neat sketch. [8]
- b) Write a note on Block Cipher Design Principles. [8]
- 4 a) State and Describe Fermat's theorem. [8]
- b) Perform decryption and encryption using RSA algorithm with  $p=3$ ,  $q=11$ ,  $e=7$  and  $N=5$ . [8]
- 5 a) Write and explain the digital signature algorithm. [8]
- b) Illustrate in detail about the message authentication code and its requirements. [8]
- 6 How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components. [16]
- 7 a) Explain in detail the operation of Internet Key Exchange with an example. [8]
- b) Explain in detail about Host-Based Intrusion Detection Systems [8]

Code No: RT41051

**R13**

**Set No. 2**

IV B.Tech I Semester Regular/Supplementary Examinations, Oct/Nov - 2018

**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) List few examples for transposition cipher. [4]
- b) Write a note on decryption. [4]
- c) Write short note on Elgamal encryption. [4]
- d) Formulate the types of attacks addressed by message authentication. [3]
- e) Why E-mail compatibility function is needed in PGP? [4]
- f) Write short note on tunnel mode in IP security. [3]

**PART-B** (3x16 = 48 Marks)

- 2 a) What is a Cyber Threat? Write about Most Common Sources of Cyber Threats in detail [8]
- b) What is a Phishing attack? Explain various Phishing techniques with suitable example. [8]
- 3 a) Explain the generation sub key and S Box from the given 32-bit key by Blowfish. [10]
- b) Mention the strengths and weakness of DES algorithm. [6]
- 4 a) Identify the possible threats for RSA algorithm and list their counter measures. [8]
- b) Briefly explain Deffie Hellman key exchange with an example. [8]
- 5 a) With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than  $2^{128}$  bits and produces as output a 512 bit message digest. [8]
- b) Write down the steps involved in Elgamal Digital Signature Scheme used for authenticating a person. [8]
- 6 a) Describe the SSL Specific protocol – Handshake action in detail [8]
- b) Analyze the Cryptographic algorithms used in S/MIME. [8]
- 7 a) Draw the IP security authentication header and describe the functions of each field. [8]
- b) Explain in detail about Network-Based Intrusion Detection Systems. [8]

Code No: **RT41051**

**R13**

**Set No. 3**

**IV B.Tech I Semester Regular/Supplementary Examinations, Oct/Nov - 2018**

**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 cryptography? [4]
- b) Discuss about encryption. [4]
- c) Define Fermat Theorem. [4]
- d) What are the properties that a digital signature should have? [3]
- e) What is Kerberos? What are the uses? [4]
- f) What is Internet key management in IPsec? [3]

**PART-B (3x16 = 48 Marks)**

- 2 a) Discuss Format String Vulnerability and Prevention with suitable example. [8]
- b) What is session hijacking in cyber security? Discuss ARP poisoning attack. [8]
- 3 a) Draw the general structure of DES. Explain the encryption and decryption process. [8]
- b) Discuss in detail block cipher modes of operation. [8]
- 4 a) State and explain Euler's theorem. [8]
- b) Write a note on Elliptic Curve Cryptography. [8]
- 5 a) What characteristics are needed in secure hash function? Write about the security of hash functions and MACs. [8]
- b) Differentiate digital signature from digital certificate. [8]
- 6 a) Explain Secure Electronic transaction with neat diagram. [8]
- b) Draw and explain PGP Cryptographic function for Authentication. [8]
- 7 a) What is transport mode and tunnel mode authentication in IP? Describe how ESP is applied to both these modes. [8]
- b) Write a note on Signature based IDS. [8]

Code No: RT41051

**R13**

**Set No. 4**

**IV B.Tech I Semester Regular/Supplementary Examinations, Oct/Nov - 2018**

**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) Compare Substitution and Transposition techniques. [4]
- b) What is a block cipher? [4]
- c) List the properties of Euler's theorem. [4]
- d) Define weak collision property of a hash function. [3]
- e) What is the role of Ticket Granting Server in inter realm operations of Kerberos? [4]
- f) Write about ESP? [3]

**PART-B (3x16 = 48 Marks)**

- 2 a) Explain in detail Man in the Middle Attacks. [8]
- b) Write about Security Mechanisms in cryptography. [8]
- 3 a) Discuss various transformation functions of AES. [8]
- b) Write a note on Block Cipher Design Principles. [8]
- 4 Users A and B use the Diffie Hellman key exchange technique, a common prime  $q=11$  and a primitive root  $\alpha=7$ .  
(a) What is the shared secret key? Also write the algorithm.  
(b) How man in middle attack can be performed in Diffie Hellman algorithm. [16]
- 5 a) With a neat flowchart, Show how MD5 process a single 512 bit block. [8]
- b) Give a brief notes on X.509 authentication services. [8]
- 6 a) Explain in detail S/MIME certification processing. [8]
- b) Write the methodology involved in computing the keys in SSL/TLS protocol. [8]
- 7 a) Describe IP security Architecture. [8]
- b) Explain in detail about Network-Based Intrusion Detection Systems. [8]