**Course Code:** 20CS1001 **R20**

**SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR**
**(AUTONOMOUS)**
Siddharth Nagar, Narayanavanam Road – 517583

**QUESTION BANK (DESCRIPTIVE)**

**Subject with Code:** Cryptography & Data Security (20CS1001)
**Course & Branch:** B.Tech – CIC
**Regulation:** R20
**Year & Sem:** II-B.Tech & II-Sem

## UNIT – I
## INTRODUCTION TO SECURITY CONCEPTS
## A MODEL FOR CRYPTOGRAPHY CONCEPTS AND TECHNIQUES

| | | | | |
|---|---|---|---|---|
| **1** | | Explain in detail about passive attacks and active attacks. | **[L2][CO1]** | **[12M]** |
| **2** | **a.** | What is meant by security services? Explain various security services listed inX.800? | **[L1][CO1]** | **[6M]** |
| | **b.** | Differentiate Substitution and Transposition techniques. | **[L3[CO1]** | **[6M]** |
| **3** | **a.** | Examine the properties of Security Mechanisms. | **[L3][CO1]** | **[8M]** |
| | **b.** | Compare Encryption and Decryption Process. | **[L4][CO1]** | **[4M]** |
| **4** | **a.** | Classify possible types of attacks in cryptography? | **[L2][CO1]** | **[8M]** |
| | **b.** | Write short note on linear and differential cryptanalysis | **[L1][CO1]** | **[4M]** |
| **5** | **a.** | Describe Symmetric and Asymmetric key cryptography techniques. | **[L2][CO1]** | **[7M]** |
| | **b.** | Summarize the relation between key range and key size in cryptography? | **[L2][CO1]** | **[5M]** |
| **6** | **a.** | Simplify various non-cryptographic vulnerabilities. | **[L4][CO1]** | **[6M]** |
| | **b.** | What is security approaches? Explain various methods of security approaches? | **[L1][CO1]** | **[6M]** |
| **7** | | Explain any three Substitution Techniques with example. | **[L2][CO1]** | **[12M]** |
| **8** | **a.** | Discuss in detail about Denial of services (DOS), Spoofing and Phishing attacks? | **[L2][CO1]** | **[6M]** |
| | **b.** | Infer the Principles of security in data security? | **[L2][CO1]** | **[6M]** |
| **9** | **a.** | Illustrate different types of transposition techniques in detail. | **[L3][CO1]** | **[6M]** |
| | **b.** | Discuss Play fair cipher in Detail. | **[L2][CO1]** | **[6M]** |
| **10** | | Indicate any three Symmetric key cipher techniques. | **[L2][CO1]** | **[12M]** |

**Course Code:** 20CS1001 **R20**

## UNIT – II
## CONVENTIONAL ENCRYPTION

| | | | | |
|---|---|---|---|---|
| **1** | **a.** | Illustrate Conventional encryption model. | **[L3][CO2]** | **[6M]** |
| | **b.** | State and explain the principles of public key cryptography? | **[L1][CO2]** | **[6M]** |
| **2** | | Describe Hill cipher and Monoalphabetic ciphers in detail | **[L2][CO2]** | **[12M]** |
| **3** | **a.** | Explain Double &Triple DES with keys. | **[L2][CO2]** | **[8M]** |
| | **b.** | Derive Ceasar cipher algorithm, encrypts the message using the key "POLYMORPHIC" and Key k=3. | **[L3][CO2]** | **[4M]** |
| **4** | | Summarize one time pad and Polyalphabetic cipher methods with example. | **[L4][CO2]** | **[12M]** |
| **5** | **a.** | Explain Rail fence Technique and Row Columnar techniques. | **[L2][CO2]** | **[6M]** |
| | **b.** | Categorize any two Substitution Techniques in symmetric key cryptography. | **[L4][CO2]** | **[6M]** |
| **6** | **a.** | Establish Affine cipher Encryption and Decryption process using the keyword "MONARCHY" and keys a=3, b=5. | **[L3][CO2]** | **[7M]** |
| | **b.** | Compare conventional key with public key encryption. | **[L5][CO2]** | **[5M]** |
| **7** | | Demonstrate single round DES with neat sketch. | **[L2][CO2]** | **[12M]** |
| **8** | | Write short notes on block cipher principles? Explain the block cipher modes of operation. | **[L1][CO2]** | **[12M]** |
| **9** | **a.** | Infer the Principles of Stream Cipher and Block cipher. | **[L2][CO2]** | **[6M]** |
| | **b.** | Discuss key distribution in detail. | **[L2][CO2]** | **[6M]** |
| **10** | | Examine the general structure of DES with neat sketch. | **[L4][CO2]** | **[12M]** |

**Course Code:** 20CS1001 **R20**

## UNIT – III
## ASYMMETRIC KEY CIPHERS

| | | | | |
|---|---|---|---|---|
| **1** | **a.** | Explain the RSA algorithm. Compute cipher text for M=88, p=17, q=11, e=7. | **[L2][CO3]** | **[8M]** |
| | **b.** | Write about the strength of RSA? | **[L1][CO3]** | **[4M]** |
| **2.** | | Compute Cipher text for Plain text =”DECRYPTION”, P=11, D=3, E1=2, R=4(Random Integer) plain text=7,using Elgamal Cryptography. | **[L3][CO3]** | **[12M]** |
| **3** | **a.** | Illustrate the structure of Diffie-Hellman Key Exchange and Calculate Diffie-Hellman Key Exchange algorithm using keys q=7,$X_a$ =3, $X_b$=4, α=2. | **[L4][CO3]** | **[7M]** |
| | **b.** | Establish Digital Signature Algorithm using RSA. | **[L3][CO3]** | **[5M]** |
| **4** | | Generalize the structure of DSA and its algorithms. | **[L2][CO3]** | **[12M]** |
| **5** | **a.** | Infer the concept of Elgamal Cryptography algorithm. | **[L2][CO3]** | **[8M]** |
| | **b.** | List out the possible attacks on RSA Algorithm. | **[L1][CO3]** | **[4M]** |
| **6** | **a.** | Examine the structure of X448 key exchange and its algorithms. | **[L3][CO4]** | **[7M]** |
| | **b.** | Explain the concepts of Random Bit Generation. | **[L2][CO4]** | **[5M]** |
| **7** | | Demonstrate the Structure of AES and its transformations. | **[L2][CO4]** | **[12M]** |
| **8** | | Discuss about key scheduling and round transformation of IDEA. | **[L2][CO4]** | **[12M]** |
| **9** | **a.** | Evaluate the structure of blowfish algorithm and list out the merits and Demerits. | **[L1][CO4]** | **[8M]** |
| | **b.** | Derive the concepts of Stream ciphering in asymmetric key ciphers. | **[L3][CO4]** | **[4M]** |
| **10** | | Discuss any one Asymmetric Key cipher algorithms with example. List out the advantages and disadvantages. | **[L3][CO4]** | **[12M]** |

**Course Code:** 20CS1001 **R20**

## UNIT – IV
## INTRODUCTION TO DATA SECURITY & IDS SECURITY

| | | | | |
|---|---|---|---|---|
| **1** | | What is security attack? Explain different Types of Security attacks? | **[L2][CO5]** | **[12M]** |
| **2** | | Examine the types, process & tools of Vulnerability assessment? | **[L4][CO5]** | **[12M]** |
| **3** | **a.** | Explain Vulnerability and its types? | **[L2][CO5]** | **[6M]** |
| | **b.** | Enumerate security goals and its methods. | **[L1][CO5]** | **[6M]** |
| **4** | | Discuss Hash Functions and Two Simple Hashing functions in detail. | **[L2][CO5]** | **[12M]** |
| **5** | | Design elliptic curve architecture and its functions briefly. | **[L6][CO5]** | **[12M]** |
| **6** | **a.** | Define Non-malicious Program errors and identify Buffer overflow in Non-malicious Program errors. | **[L3][CO5]** | **[7M]** |
| | **b.** | Evaluate the types and characteristics of Data Integrity. | **[L5][CO5]** | **[5M]** |
| **7** | **a.** | Infer in detail about Time-of-check to Time-of-use Errors. | **[L2][CO5]** | **[6M]** |
| | **b.** | Describe Hash funtions.List out the features and properties of hash functions. | **[L2][CO5]** | **[6M]** |
| **8** | | Classify various types of viruses in IDS Security. | **[L4][CO5]** | **[12M]** |
| **9** | **a.** | Define firewall? Examine the need for firewalls and role of firewalls inprotecting networks. | **[L4][CO5]** | **[8M]** |
| | **b.** | Summarize (i) Salami attack.<br>(ii) Trap Door | **[L2][CO5]** | **[4M]** |
| **10** | | Illustrate various types of malicious software viruses. | **[L3][CO5]** | **[12M]** |

**Course Code:** 20CS1001 **R20**

## UNIT – V
## IP SECURITY & DIGITAL SIGNATURES

| | | | | |
|---|---|---|---|---|
| **1** | | Sketch neatly and summarize IP security Architecture in detail. | **[L3][CO6]** | **[12M]** |
| **2** | | Generalize Authentication header and its modes of operation in detail. | **[L6][CO6]** | **[12M]** |
| **3** | **a.** | Justify briefly about combining Security Associations. | **[L5][CO6]** | **[8M]** |
| | **b.** | Distinguish between Digital Signature and Digital Certificate. | **[L4][CO6]** | **[4M]** |
| **4** | | Infer the characteristics, working and components of Encapsulating security payloads. | **[L2][CO6]** | **[12M]** |
| **5** | **a.** | Discuss Model of Digital Signature and Encryption with Digital Signature. | **[L2][CO6]** | **[6M]** |
| | **b.** | Differentiate between SHA1 and SHA2 | **[L4][CO6]** | **[6M]** |
| **6** | | Define Digital signature. Write down the steps followed in creating digital signature. List the Benefits and drawbacks of digital signatures. | **[L1][CO6]** | **[12M]** |
| **7** | **a.** | Illustrate the steps involved in DSA Algorithm. | **[L3][CO6]** | **[6M]** |
| | **b.** | Examine the Proof of Digital signature algorithm. | **[L3][CO6]** | **[6M]** |
| **8** | | Explain various types of Authentication Protocols and its advantages and disadvantages. | **[L2][CO6]** | **[12M]** |
| **9** | | Discuss about Digital Signature Standard approach. Identify the benefits and Problems of DSS. | **[L2][CO6]** | **[12M]** |
| **10** | **a.** | Describe the steps taken to ensure security, signing the Digest in Digital Signature algorithm. | **[L2][CO6]** | **[6M]** |
| | **b.** | Examine Secure Hash Algorithm and applications. | **[L4][CO6]** | **[6M]** |

**Prepared by:Dr.R.Elankavi /CSE**