**POORNIMA UNIVERSITY, JAIPUR**

**END SEMESTER EXAMINATION, April 2023**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **4BT2123** | Roll No. | Total Printed Pages: 2 |
| **4BT2123** |  |
| B. Tech. II Year IV Semester (Back) End Semester Examination, April 2023 | |
| **BCE04108: Cryptography Fundamentals** | | | |

# Max. Time: **3**Hours. Max. Marks: **60**

Min. Passing Marks: **21**

Attempt **five** questions selecting one question from each Unit. There is internal choice from Unit I to Unit V. Marks of each question or its parts are indicated against each question / parts. Draw neat sketches wherever necessary to illustrate the answer. Assume missing data suitably (if any) and clearly indicate the same in the answer.

Use of following supporting material is permitted during examination for this subject.

# **1.----------------------------------------------** **2.-----------------------------------------**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **UNIT-I (CO1)** | **Marks** | **Bloom Level** |
|  |  |  |  |  |
| **Q.1** | **(a)** | How polyalphabetic cipher differs from monoalphabetic cipher? Describe with suitable Example. | **(6)** | **Analyzing** |
|  |  |  |  |  |
|  | **(b)** | Compare confusion and diffusion in cryptography. How rail fence cipher works? How it is different from Caesar Cipher. Show with suitable example. | **(6)** | **Analyzing** |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.2** | **(a)** | Are there any other ciphers that are available, other than the Caesar cipher? Summerize in detail. | **(6)** | **Analyzing** |
|  |  |  |  |  |
|  | **(b)** | Convert the plain text **LEARNING** into cipher text with **MONARCHY** key by using playfair cipher. | **(6)** | **Evaluating** |
|  |  |  |  |  |
|  |  | **UNIT-II (CO2)** |  |  |
|  |  |  |  |  |
| **Q.3** | **(a)** | Calculate public key and private key pair of asymmetric key cryptography by using RSA algorithm.  **P=7, Q=13**  Also show the encryption and decryption process. | **(6)** | **Evaluating** |
|  |  |  |  |  |
|  | **(b)** | Describe MD5 message digest algorithm in details with suitable steps and block diagrams. | **(6)** | **Understanding** |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.4** | **(a)** | How 56-bit key is converted into 48-bit key in DES Algorithm. Show key transformation process. | **(6)** | **Evaluating** |
|  |  |  |  |  |
|  | **(b)** | How Elliptical curve cryptography algorithm effects on key length as compared to other algorithms? Compare it with suitable table. | **(6)** | **Applying** |
|  |  |  |  |  |
|  |  | **UNIT-III (CO3)** |  |  |
|  |  |  |  |  |
| **Q.5** | **(a)** | Alice and Bob want to communicate securely. How they will agree on same symmetric key to exchange their messages. Explain the algorithm with suitable example that implements key exchange. | **(6)** | **Applying** |
|  |  |  |  |  |
|  | **(b)** | What do you mean by key revocation? What are the reasons for a certificate can be revoked? State in detail. | **(6)** | **Understanding** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.6** |  | Key management is helpful to handle the cryptographic keys. Justify your answer. Also Draw the phases of key management life cycle and explain each phase in detail. | **(12)** | **Analyzing** |
|  |  |  |  |  |
|  |  | **UNIT-IV (CO4)** |  |  |
|  |  |  |  |  |
| **Q.7** | **(a)** | If you want to exchange the information securely between a web browser and a web server. Which protocol you will use to achieve two basic security services like authentication and confidentiality? Explain the working of that protocol in detail. | **(6)** | **Applying** |
|  |  |  |  |  |
|  | **(b)** | What do you mean by cryptography Vulnerabilities? List the classification of Vulnerabilities. | **(6)** | **Understanding** |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.8** | **(a)** | Describe the working of Kerberos network authentication protocol in detail with suitable diagram. | **(6)** | **Understanding** |
|  |  |  |  |  |
|  | **(b)** | Identify and explain a network that is constructed using public wires usually the internet to connect remote users or regional offices to a company's private, internal network. What Security mechanisms are provided by that security model? | **(6)** | **Evaluating** |
|  |  |  |  |  |
|  |  | **UNITV (CO5)** |  |  |
|  |  |  |  |  |
| **Q.9** | **(a)** | What are the key aspects related to authentication? How biometric based authentication does takes place? Describe the suitable steps with proper diagram. | **(6)** | **Analyzing** |
|  |  |  |  |  |
|  | **(b)** | Identify the need of Single Sign On for authentication? How SSO window works? What are the possible reasons to look for a SSO solution? | **(6)** | **Analyzing** |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.10** | **(a)** | Which method is used for keeping sensitive information in email communication & accounts secure against unofficial access, loss, or compromise. Illustrate with proper explanation. | **(6)** | **Analyzing** |
|  |  |  |  |  |
|  | **(b)** | Identify the problems with clear text password and message digest of passwords? How these problems are solved by adding randomness in password based authentication. | **(6)** | **Analyzing** |