**POORNIMA UNIVERSITY, JAIPUR**

**END SEMESTER EXAMINATION, APRIL 2023**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **2BT4138** | Roll No. | Total Printed Pages: 2 |
| **2BT4138** |  |
| B. Tech. II Year IV- Semester (Main/Back) End Semester Examination, April 2023  **(CE / CC / AIDS / CS)** | |
| **BCECCE4102 : Information System Security** | | | |

# Time: **3** Hours. Total 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.--------------------------Nil--------------------** **2.------------------Nil-----------------------**

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **UNIT-I (CO1)** | **Marks** | **Bloom Level** |
| **Q.1** | **(a)** | Propagating Cipher Block Chaining(PCBC) encryption is given by the equation  C*n* = E(*K*,[*Cn*-1 XOR *Pn*-1 XOR *Pn*])  Find out the decryption equation and draw neat figure for both encryption and decryption. (P0 can be considered as NULL) | **(6)** | **Apply** |
|  |  |  |  |  |
|  | **(b)** | Suppose that, in PCBC mode, blocks Ci and Ci+1 are interchanged during transmission. Show that this affects only the decrypted blocks Pi and Pi+1 but not subsequent blocks. | **(6)** | **Apply** |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.2** | **(a)** | Show the encryption of “ I JUST LOVE BEING AT A29 AND AT C345 using playfair cipher with key as: “ADDRESS0275”. | **(6)** | **Apply** |
|  |  |  |  |  |
|  | **(b)** | We consider double encryption of a private-key algorithm in order to increase the security, such that: *y* = *e*2(*e*1(*M*)). Assume two ciphers are given as:  *e*1(*x*) = *a*1*:x* + *b*1  *e*2(*z*) = *a*2*:z* + *b*2  Show that there is a single cipher *e*3(*M*) = *a*3*:M* + *b*3 which performs exactly the same encryption (and decryption) as the combination *e*2(*e*1(*M*)). | **(6)** | **Apply** |
|  |  |  |  |  |
|  |  | **UNIT-II (CO2)** |  |  |
|  |  |  |  |  |
| **Q.3** | **(a)** | Why X.509 certificate is required in authentication? Draw neat diagram of X.509 v3. What is the role of CA? Explain. | **(6)** | **Understand** |
|  |  |  |  |  |
|  | **(b)** | Describe details of one round of DES? | **(6)** | **Understand** |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.4** | **(a)** | Assume a public key for RSA encryption given by the pair (n=143*,e=*11).  (i) Find the private key to the given public key.  (ii) Decrypt V , use ASCII values of letter(A=65) | **(6)** | **Apply** |
|  |  |  |  |  |
|  | **(b)** | Describe details of one round of AES? | **(6)** | **Understand** |
|  |  |  |  |  |
|  |  | **UNIT-III (CO3)** |  |  |
| **Q.5** | **(a)** | How Diffie Hellman algorithm is vulnerable to Man in the Middle attack? Describe in detail. | **(6)** | **Apply** |
|  |  |  |  |  |
|  | **(b)** | Write short notes on  (i) covert channel (ii) Buffer overflow | **(6)** | **Understand** |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.6** | **(a)** | Write short notes on  (i) Salami Attack (ii) TOCTOU | **(6)** | **Understand** |
|  |  |  |  |  |
|  | **(b)** | Discuss the purpose of all keys used in Kerberos version 4.0 | **(6)** | **Understand** |
|  |  |  |  |  |
|  |  | **UNIT-IV (CO4)** |  |  |
|  |  |  |  |  |
| **Q.7** | **(a)** | Why do we need dual signature in SET? How does it work? | **(6)** | **Understand** |
|  |  |  |  |  |
|  | **(b)** | How master key is generated in SSL? | **(6)** | **Understand** |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.8** | **(a)** | Draw neat diagram of (Cardholder sends) **Purchase Request message** in SET and explain in detail. | **(6)** | **Understand** |
|  |  |  |  |  |
|  | **(b)** | How 3D secure protocol works? Explain with neat diagram. | **(6)** | **Understand** |
|  |  |  |  |  |
|  |  | **UNIT V (CO5)** |  |  |
|  |  |  |  |  |
| **Q.9** | **(a)** | What is the basic concept of Traffic Flow Security? Explain with an example. | **(6)** | **Understand** |
|  |  |  |  |  |
|  | **(b)** | Write short notes on  (i) Honeypot (ii) IDS | **(6)** | **Understand** |
|  |  |  |  |  |
|  |  | **OR** |  |  |
|  |  |  |  |  |
| **Q.10** | **(a)** | With neat diagram describe how PGP provides both authentication and confidentiality service together. | **(6)** | **Remember** |
|  |  |  |  |  |
|  | **(b)** | Differentiate between application level gateway and circuit level gateway. | **(6)** | **Remember** |