**Name:**

**Enrolment No:**

**UPES**

**End Semester Examination, DEC 2024**

| | |
|---|---|
| **Course:** IT DATA SECURITY | **Semester: V** |
| **Program:** B.TECH CSE+CSF | **Time : 03 hrs.** |
| **Course Code:** CSSF3025 | **Max. Marks: 100** |

**Instructions:**

## SECTION A
**(5Qx4M=20Marks)**

| S. No. | | Marks | CO |
|---|---|---|---|
| Q 1 | **Define** the concept of data security and **explain** why it is critical for organizations. | **4** | **CO1** |
| Q 2 | **Describe** the different types of data security threats commonly encountered in the modern era. | **4** | **CO2** |
| Q 3 | **List and explain** any two threat techniques specifically targeting wireless networks. | **4** | **CO2** |
| Q 4 | **Explain** the purpose of data provenance in cloud security and its importance. | **4** | **CO3** |
| Q 5 | **Define** data mobility and **discuss** the importance of security for data-in-transit. | **4** | **CO4** |

## SECTION B
**(4Qx10M= 40 Marks)**

| | | | |
|---|---|---|---|
| Q 6 | **Discuss** various database security countermeasures and **explain** their significance in preventing data breaches. | **10** | **CO2** |
| Q 7 | **Discuss** the various elements that organizations should consider to build an effective data security mechanism. | **10** | **CO1** |
| Q 8 | For p=11 and q=19 . Apply RSA algorithm where Cipher message =80 and thus find the plain text.<br>**OR**<br>Suppose that two parties A and B wish to setup a common key (D-H) between themselves using the Diffie-Hellman Key exchange technique. They agree on 7 as the modulus and 3 as | **10** | **CO3** |

| | | | |
|---|---|---|---|
| | the primitive root. Party A chooses 2 and Party B chooses 5 as their respective secrets. Their D-H Key is. | | |
| Q 9 | Let ECC equation is $y^2 = x^3 + 2x + 2$ (mod 17) is given<br>P= (5,1) and Q= (6,3) .Calculate the value of 5P. | **10** | **CO3** |
| **SECTION-C**<br>**(2Qx20M=40 Marks)** | | | |
| Q 10 | **Analyze** and **compare** various types of data security threats, such as malware, cryptographic, and web application threats. **Evaluate** how each threat impacts an organization and the significance of countermeasures for each type. | **20** | **CO1** |
| Q 11 | For NOMAD Framework define and explain following<br>A. Client Management Service<br>B. Cloud Storage Service<br>C. NOMAD operational overview.<br>**OR**<br>Given that two prime no's p and q are 5 and 7 respectively for paillier homomorphic encryption. Perform Encryption and decryption for message (m1=10 and m2=20). Let assume µ=1 and random value r1=3 and r2=4. | **20** | **CO4** |