Reg. No.												

Question Paper Code	12626

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2024

Sixth Semester

Artificial Intelligence and Data Science

20AIEL605 – FOUNDATION OF CRYPTOGRAPHY

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

	Marks	K – Level	CO
1. Brief about Cryptography.	2	K1	CO1
2. List out the goals of Cryptography.	2	K1	CO1
3. State the difference between Stream Cipher and Block Cipher.	2	K1	CO2
4. Illustrate the stream cipher working method.	2	K1	CO2
5. State the difference between Active and Passive attacks in the cryptography.	2	K1	CO3
6. In which method the passive attack follow up their data?	2	K1	CO3
7. State about the Random Oracle Model in cryptography.	2	K1	CO4
8. List the different types of Key Exchange protocols available in cryptography.	2	K1	CO4
9. Brief about El-Gamal Encryption algorithm.	2	K1	CO5
10. Illustrate about RSA.	2	K1	CO5

PART - B (5 × 16 = 80 Marks)

Answer any Five Questions

11. Explain in detail about Symmetric key cryptography.	16	K2	CO1
12. Extend briefly about the four attack models of cryptography.	16	K2	CO1
13. Summarize about the stream cipher with an example and its limitations.	16	K2	CO2
14. Describe about message integrity and authenticity in detail.	16	K2	CO3
15. Explain in detail about Message Authentication Code.	16	K2	CO3
16. Interpret about commitment schemes in cryptography and brief in detail.	16	K2	CO4
17. Discuss about public key encryption in detail.	16	K2	CO5
18. Develop an El Gamal Public key encryption in the network channel and explain the process.	16	K2	CO5