Reg. No.												

Question Paper Code	12287

B.E. / B.Tech - DEGREE EXAMINATIONS, NOV / DEC 2023

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.	Why is Cryptography important?	*2,K1,CO1*
2.	Write down the advance application of cryptography.	*2,K1,CO1*
3.	How does the Stream Cipher Work?	*2,K1,CO2*
4.	Where the Pseudo Random Function is Used? And How?	*2,K1,CO2*
5.	In which method the passive attack follow up their data?	*2,K1,CO3*
6.	State the limitation of Message Authentication Code.	*2,K1,CO3*
7.	What is the Random Oracle Model in cryptography?	*2,K1,CO4*
8.	What are all the different types of Key Exchange protocols available in cryptography?	*2,K1,CO4*
9.	List out the vulnerabilities of the DHKE algorithm.	*2,K1,CO5*
10.	What is Diffie Hellman Key Exchange algorithm?	*2,K1,CO5*

PART - B (5 × 16 = 80 Marks)

Answer any Five questions

11.	Illustrate about any three historical ciphers.	*16,K2,CO1*
12.	Explain briefly about the four attack models of cryptography.	*16,K2,CO1*
13.	Explain in detail about single message security and multi message security.	*16,K2,CO2*
14.	Discuss about stream cipher with an example and its limitations.	*16,K2,CO2*
15.	Illustrate and sketch the architecture of HMAC with a neat diagram.	*16,K3,CO3*
16.	Explain in detail about the Random Oracle Model.	*16,K2,CO4*
17.	Explain in detail about Authenticated encryption.	*16,K2,CO4*
18.	Develop an El Gamal Public key encryption in the network channel and explain the process.	*16,K3,CO5*