M.Sc.(CS) (Sem-IV) July-2023

Computer Science : Paper II -Specialization- Track B: Cyber & Information Security-II

Time : 2 Hours **Total Marks : 60**

N.B.

(1) All questions are compulsory.

(2) Figures to the right indicate full marks.

(3) Assume additional data if necessary but state the same clearly.

(4) Symbols have their usual meanings and tables have their usual standard design unless stated otherwise.

(5) Use of calculators and statistical tables are allowed.

Q1	Attempt Any two of the following.	**12**
a	Define the following term i) Prime Number ii) Greatest Common Divisor	**6**
b	Explain Chinese Remainder Theorem	**6**
c	Explain Euclidean Algorithm	**6**
d	What is quadratic residue? Find the quadratic residue of 7.	**6**
Q2	Attempt Any two of the following.	**12**
a	Explain the broad working of DES	**6**
b	Suppose m=6 and the keyword is CIPHER and the plaintext is the string THISCRYPTOSYSTEMISNOTSECURE Encrypt using Vigenère Cipher.	**6**
c	Write a short note on SHA.	**6**
d	Define HMAC? Write advantages and disadvantages of HMAC.	**6**
Q3	Attempt Any two of the following.	**12**
a	What are the possible attacks on RSA?	**6**
b	State the RSA Algorithm. Explain with an example	**6**
c	Explain the Solovay-Stressen Algorithm.	**6**
d	What is Public Key Infrastructure? Explain PKIX Architectural Model.	**6**

Q4	Attempt Any two of the following.	**12**
a	State and explain the Diffie Hellman Key Exchange Algorithm.	**6**
b	Discuss the Station-to-station protocol.	**6**
c	Write a note of Certificate Lifecycle.	**6**
d	What is MTI Key Agreement	**6**

Q5	Attempt Any two of the following.	**12**
a	Write a short note on Pretty Good Privacy Services.	
b	Explain the various Algorithm Modes	
c	State and explain the application of Congruences.	
d	Explain the Miller-Rabin Algorithm.	