Name. _____	**Printed Pages:01**
Student Admn. No.: _____	

School of _____

Backlog Examination, June 2023

[Programme: B.Sc. CS**] [Semester:** IV **] [Batch:]**

Course Title: CRYPTOGRAPHIC AND NETWORK SECURITY	**Max Marks: 100**
Course Code: BSCS2470	**Time: 3 Hrs.**

Instructions:

1. *All questions are compulsory.*
2. *Assume missing data suitably, if any.*

		K Level	COs	Marks
	SECTION-A (15 Marks) 5 Marks each			
1.	Define web-based attacks.	K1	CO1	5
2.	Define Euler's Theorem.	K1	CO1	5
3.	Explain intrusion detection system.	K2	CO2	5
	SECTION-B (40 Marks) 10 Marks each			
4.	Illustrate TCP session hijacking and UDP hijacking	K2	CO2	10
5.	Construct RSA Algorithm and Estimate the encryption and decryption values for the RSA algorithm parameters.	K3	CO2	10
6.	Compare stream cipher with block cipher with examples	K4	CO3	10
7.	Analyze the OSI security architecture. OR Analyze classical encryption techniques with symmetric cipher mode	K4	CO3	10
	SECTION-C (45 Marks) 15 Marks each			
8.	List-out IP Security protocols in detail.	K4	CO3	15
9.	Explain Cryptographic algorithms used in S/MIME and Explain S/MIME certification processing	K5	CO4	15
10	Discuss Triple DES and its applications OR Solve decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5.	K6	CO4	15