Name. ________________________________ **Student Admn. No.:** _______________________	**Printed Pages:01**

School of Computing Science & Engineering
Backlog Examination, June 2023

[Programme: B.Tech **] [Semester:** IV **] [Batch:]**

Course Title: Network Security **Course Code: CSCS2041**	**Max Marks: 100** **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.	Differentiate between Active attacks and Passive Attacks.	**K1**	CO1	5
2.	Compare stream cipher with block cipher with an example.	**K2**	CO2	5
3.	What are the disadvantages of double DES?	**K1**	CO1	5
	SECTION-B (40 Marks) **10 Marks each**			
4.	What are the web-based attacks?	**K1**	CO1	10
5.	Explain the process of deriving eighty 64-bitwords from 1024 bits for processing of a single block and discuss single round function in SHA-512 algorithm. Show the values of W16, W17, W18 and W19.	**K3**	CO3	10
6.	Explain IP Security protocols in detail.	**K3**	CO3	10
7.	Discuss the various principles involved in private and public key cryptography. OR Discuss any four Substitution Technique and list their merits and demerits	**K4**	CO3	10
	SECTION-C (45 Marks) **15 Marks each**			
8.	Discuss the services provided by PGP services?	**K4**	CO3	15
9.	Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and N=5.	**K6**	CO4	15
10	How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components. OR Analyze the Cryptographic algorithms used in S/MIME and Explain S/MIME certification processing.	**K5**	CO4	15