

13/05/2025 MCA SEM-II (NEP-2020) INFO.SECURITY QP CODE: 10081322

(2 Hours)

Total Marks: 50

Note:

- Question number Q1 is compulsory
- Attempt any two questions out of Q2 to Q5

		Marks	Course Outcome	Bloom's Level
			CO	BL
Q1	a. Explain SAML assertion.	[05]	CO3	BL2
	b. Describe the various principles of information security	[05]	CO1	BL2
	c. Discuss MD5.	[05]	CO2	BL4
	d. Discuss Inference.	[05]	CO4	BL2
Q2	a. Discuss SSL protocol along with its sub protocols.	[08]	CO3	BL2
	b. If public key E=5 for p=13 and q=19, find its correspond private key.	[07]	CO2	BL4
Q3	a. Discuss one round of DES	[08]	CO2	BL4
	b. Explain PGP protocol.	[07]	CO3	BL2
Q4	a. Calculate the GCD using extended Euclidean algorithm along with S and T	[08]		
	i. 1071 and 462		CO2	BL4
	ii. 119 and 544			
	b. Discuss the OS security.	[07]	CO4	BL2
Q5	a. What is firewall? Discuss its type with advantages and disadvantages.	[08]	CO3	BL2
	b. Discuss the steps used for certificate creation. How digital certificate can be verified?	[07]	CO2	BL4
