	Harcourt Butler Technical University Kanpur			II MID SEM (2023-24)
Branch	**MCA**		Program	**MCA**
Course Name	**Cryptography and Network Security**		Semester	**IV**
Course Code	**ECA-582**		Year	**II**
Time:	**1.00 Hr**		Maximum Marks	**15**
Knowledge Level (KL)	**K1:** Remembering	**K3:** Applying		**K5:** Evaluating
	K2: Understanding	**K4:** Analyzing		**K6:** Creating

Note: Answer All Questions

Q. No	Questions	Marks	COs	KL
1	Consider a Diffie- Hellman scheme with a common prime q=11 and primitive root α=2. (a) If user A has public key Y_A=9, what is A's private key X_A? (b) If user B has public key Y_B=3, what is the shared secret key K, shared with A?	3	CO2	K3
2	Discuss about Birthday Attack on hash code?	3	CO3	K2
3	Describe the MD5 message digest algorithm.	3	CO3	K2
4	Explain Digital Signature Standard algorithm with diagram.	4	CO3	K2
5	What are the five main services provided by Pretty Good Privacy (PGP)?	2	CO4	K2

Course Outcomes	**CO1**	Understand and deploy cryptographic technique to secure data in networks
	CO2	Analyze the vulnerabilities in any computing systems and design a security solution.
	CO3	Understand and use standard algorithms for confidentiality, integrity and authenticity.
	CO4	Apply various key distribution and management schemes in network system.
	CO5	Apply security protocols in various IT applications.