Department of _____

Subject Name: _____ **Subject Code:** _____

SEM : **DIV :** **ACADEMIC YEAR :**

Faculty : _____

Module-1 Question Bank

SL#	Question	CO	Level	Marks
1	Explain the principles of Public Key Cryptography. Compare symmetric and asymmetric cryptography.	CO2	L2	**5**
2	Explain the applications and requirements of Public Key Cryptosystems.	CO2	L2	**5**
3	Explain Public Key Cryptanalysis and the common attacks on public-key algorithms.	CO2	L2	**10**
4	Explain the RSA algorithm with a neat flowchart. Discuss its security and computational aspects.	CO2	L2	**5**
5	Using RSA, let p = 17, q = 11, e = 7. Find the public/private keys and encrypt & decrypt the message M = 88.	CO2	**L3**	**10**
6	Explain the Diffie–Hellman Key Exchange algorithm with a neat diagram.	CO2	L2	**10**
7	Using Diffie–Hellman, let q = 23, α = 5, XA = 6, XB = 15. Find the shared secret key.	CO2	**L3**	**10**
8	Explain the Man-in-the-Middle (MITM) attack on Diffie–Hellman. How can it be prevented?	CO2	L3	**10**
9	Explain Elliptic Curve Cryptography (ECC). Why is ECC considered more secure than RSA for the same key size?	CO2	L2	**5**
10	Explain the Elliptic Curve Diffie–Hellman (ECDH) key exchange process with a neat diagram.	CO2	L2	**10**
11	Explain Linear Congruential Generator (LCG) and Blum Blum Shub (BBS) Generator. Compare their advantages and limitations.	CO2	L2	**10**
12	For the Linear Congruential Generator, generate the first five random numbers using X_0 = 7, a = 5, c = 3, m = 16.	CO2	L3	**10**

Faculty Signature