BHAI GURDAS INSTITUTE OF ENGINEERING & TECHNOLOGY

Department of Computer Science and Engineering

LESSON PLAN

Subject Name: - Network Security & cryptography **Subject Code: - BTCS 701-18**

Year: -2023 **Semester: - 6th**

Lecture No.	Unit	Date/Week	Topic	Teaching Aids	References
1	1	5 Days	Introduction to Cryptography	Projector, chalk, green board, duster	Text Book , Notes
2			Security Threats		
3			Active and Passive attacks		
4			Conventional Encryption Model		
5			CIA model		
6	2	5 Days	Modular Arithmetic		
7			Euclidean and Extended Euclidean algorithm		
8			Euclidean and Extended Euclidean algorithm		
9			Prime numbers		
10			Fermat and Euler's Theorem		
11	3	12 Days	Dimensions of Cryptography		
12			Classical Cryptographic Techniques Block Ciphers		
13			Feistal Cipher Structure		
14			Simplifies DES, DES, Double and Triple DES		
15			Block Cipher design Principles		
16			Modes of Operations Public-Key Cryptography		
17			Principles Of Public-Key Cryptography		
18			, RSA Algorithm		
19			Diffie-Hellman Key Exchange		
20			Diffie-Hellman Key Exchange		
21			Elgamal Algorithm		
22			Elliptic Curve Cryptography		
23	4	6 Days	Introduction to Hash and MAC Algorithms		
24			Authentication Requirement		
25			Message Authentication Code		
26			Hash Functions,Security Of Hash Functions And Macs,		
27			MD5 Message Digest Algorithm		
28			Secure Hash Algorithm, Digital Signatures		
29	5	7 Days	Threats in networks		
30			Network Security Controls – Architecture		

31			Strong Authentication, Access Controls		
32			Wireless Security		
33			Traffic flow security		
34			Design and Types of Firewalls, Personal Firewalls		
35			IDS, Email Security – PGP, S/MIME		