Department of Information Technology

LESSON PLAN

Subject: Information Security **Subject code: OE-IT-D410A**

Session: 2022-23 **Semester: VIII**

SNo	Topic	No. of Lectures required	CO Covered	Teaching Methodology
1	**Unit-1** Introduction, The need for security	1	CO1	
2	Security approaches, Principles of security	1		
3	Types of Security attacks, Security services	2		
4	Security Mechanisms	1		
5	A model for Network Security	1		
6	Cryptography: Concepts and Techniques: Introduction, plain text and cipher text	2		
7	substitution techniques, transposition techniques	2		
8	symmetric and asymmetric key cryptography, stegnography, key range and size	2		
9	**Unit 2** Symmetric key Ciphers**:** Block Cipher principles	1	CO2	
10	Differential and Linear cryptanalysis	1		
11	Block cipher modes of operation	1		
12	Stream ciphers, RC4	1		
13	Location and placement of encryption function, Key distribution.	1		
14	Asymmetric key Ciphers: Principles of public key crypto systems,	1		
15	RSA	2		
16	Diffie Hellman	1		
17	ECC	1		
18	**Unit 3** Message Authentication Algorithms and Hash Functions	2	CO3	
19	Authentication requirements, Functions, Message authentication codes	1		
20	Hash Functions, Secure hash algorithm, HMAC, CMAC	1		
21	Digital signatures, knapsack algorithm	1		
22	Authentication Applications: Kerberos, X.509 Authentication Service	1		
23	Public – Key Infrastructure, Biometric	2		

	Authentication.			
24	**Unit 4** E-Mail Security: Pretty Good Privacy	1	CO4	
25	S/MIME.	1		
26	Web Security: Web security considerations,	1		
27	Secure Socket Layer	1		
28	Transport Layer Security,	1		
29	Secure electronic transaction	1		
30	Intruders . Intrusion detection	2		
31	password management	1		
32	virus and related threats	1		
33	Firewall design principles, types of firewalls.	2		