Lesson Plan & Work-done Diary for AY: 2024-25, EVEN Semester

Course with Code: Cryptography & Network Security [BCS703]					Faculty: Ms. Ambika V		Semester & Section: VII	
Class No.	Date planned (DD/MM)	Topics to be covered	TLP Planned	ClassNo.	Date of Conduction (DD/MM)	Topics Covered	TLP Executed	Remarks if any deviation
MODULE-1								
1.		Introduction to the course, A model for Network Security	PPT Chalk & Talk	1				
2.		Symmetric cipher model	PPT Chalk & Talk	2				
3.		Caesar Cipher, Monoalphabetic Cipher	PPT Chalk & Talk	3				
4.		Playfair Cipher	PPT Chalk & Talk	4				
5.		Hill Cipher	PPT Chalk & Talk	5				
6.		Polyalphabetic Ciphers, One time pad	PPT Chalk & Talk	6				
7.		Steganography	PPT Chalk & Talk	7				
8.		Traditional Block Cipher structures	PPT Chalk & Talk	8				
9.		data Encryption Standard (DES), A DES Example	PPT Chalk & Talk	9				
10.		The strength of DES, Block cipher design principles	PPT, Socrative app	10				

Course with Code: Cryptography & Network Security [BCS703]				Faculty: Ms. Ambika V				Semester & Section: VII	
Class No.	Date planned (DD/MM)	Topics to be covered	TLP Planned	Class No.	Date of Conduction (DD/MM)	Topics Covered	TLP Executed	Remarks if any deviation	
MODULE-2									
1.		Linear Congruential Generators	PPT Chalk & Talk	1					
2.		Blum Blum Shub Generator	PPT Chalk & Talk	2					
3.		Principles of public key cryptosystems-Public key cryptosystems	PPT Chalk & Talk	2					
4.		Applications for public key cryptosystems	PPT Chalk & Talk	4					
5.		Requirements for public key cryptography, Public key Cryptanalysis	PPT Chalk & Talk	5					
6.		The RSA algorithm: Description of the Algorithm	PPT Chalk & Talk	6					
7.		Computational aspects, The Security of RSA	PPT Chalk & Talk	7					
8.		Diffie-Hellman key exchange: The Algorithm	PPT Chalk & Talk	8					
9.		Key exchange Protocols, Man-in-the-middle Attack	PPT Chalk & Talk	9					
10.		Analog of Diffie-Hellman key Exchange	PPT Chalk & Talk	10					
11		Elliptic Curve Encryption/Decryption	PPT Chalk & Talk	11					
12		Security of Elliptic Curve Cryptography	PPT Chalk & Talk	12					

Course with Code: Cryptography & Network Security [BCS703]				Faculty: Ms. Ambika V			Semester & Section: VII	
Class No.	Date planned (DD/MM)	Topics to be covered	TLP Planned	Class No.	Date of Conduction (DD/MM)	Topics Covered	TLP Executed	Remarks if any deviation
MODULE-3								
1.		Applications of Cryptographic Hash functions	PPT Chalk & Talk	1				
2.		Two simple Hash functions	PPT Chalk & Talk	2				
3.		Symmetric key distribution using symmetric encryption	PPT Chalk & Talk	3				
4.		Symmetric key distribution using asymmetric encryption	PPT Chalk & Talk	4				
5.		Symmetric key distribution using asymmetric encryption	PPT Chalk & Talk	5				
6.		Distribution of public keys	PPT Chalk & Talk	6				
7.		X.509 Certificates	PPT Chalk & Talk	7				
8.		Public Key Infrastructures	PPT Chalk & Talk	8				

Course with Code: Cryptography & Network Security [BCS703]				Faculty: Ms. Ambika V				Semester & Section: VII	
Class No.	Date planned (DD/MM)	Topics to be covered	TLP Planned	Class No.	Date of Conduction (DD/MM)	Topics Covered	TLP Executed	Remarks if any deviation	
MODULE-4									
1.		Remote user authentication principles	PPT Chalk & Talk	1					
2.		Kerberos	PPT Chalk & Talk	2					
3.		Remote user authentication using asymmetric encryption	PPT Chalk & Talk	3					
4.		Web security consideration	PPT Chalk & Talk	4					
5.		Transport layer security	PPT Chalk & Talk	5					
6.		Transport layer security	PPT Chalk & Talk	6					
7.		Email Threats and comprehensive email security	PPT Chalk & Talk	7					
8.		S/MIME	PPT Chalk & Talk	8					
9.		S/MIME	PPT Chalk & Talk	9					
10.		Pretty Good Privacy	PPT Chalk & Talk	10					

Course with Code: Cryptography & Network Security [BCS703]				Faculty: Ms. Ambika V			TLP Executed	Semester & Section: VII
Class No.	Date planned (DD/MM)	Topics to be covered	TLP Planned	Class No.	Date of Conduction(DD/MM)	Topics Covered	TLP Executed	Remarks if any deviation
MODULE-5								
1.		Domain keys Identified Mail	PPT Chalk & Talk	1				
2.		Domain keys Identified Mail	PPT Chalk & Talk	2				
3.		IP Security: IP Security overview	PPT Chalk & Talk	3				
4.		IP Security: IP Security overview	PPT Chalk & Talk	4				
5.		IP Security Policy	PPT Chalk & Talk	5				
6.		Encapsulating Security Payload	PPT Chalk & Talk	6				
7.		Encapsulating Security Payload	PPT Chalk & Talk	7				
8.		Combining security associations	PPT Chalk & Talk	8				
9.		Combining security associations	PPT Chalk & Talk	9				
10.		Internet key exchange.	PPT Chalk & Talk	10				

	Activity	Planned	Actual	Remarks
1	Theory Classes	50		
2	Assignments/ Quizzes/Self-study	2		
3	Tutorials/ Extra classes	2		
4	Internal Assessments	3		
5	ICT based Teaching (% of usage in Curriculum)	100		

Planning	Execution
Faculty Signature:	Faculty Signature:
HoD Signature:	HoD Signature: