

DEPARTMENT OF COMPUTER SCIENCE & DESIGN

Lesson Plan & Work-done Diary for AY: 2026 (ODD Semester)

Course with Code: Cryptography and Network Security – BCS703				Faculty: Darshini Y			Semester : 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
BRIDGE COURSE								
1		Concepts of Cryptography	PPT	1				
2			PPT	2				
3			PPT	3				
4			PPT	4				
		Module-1						
1		A model for Network Security, Classical encryption techniques	PPT	1				
2		Symmetric cipher model, Substitution ciphers-Caesar Cipher	PPT	2				
3		Monoalphabetic Cipher, Playfair Cipher	PPT	3				
4		Hill Cipher	PPT	4				
5		Polyalphabetic Ciphers	PPT	5				
6		One time pad, Steganography	PPT	6				
7		Block Ciphers and Data Encryption Standards: Traditional Block Cipher structures	PPT	7				
8		Data Encryption Standard (DES)	PPT	8				
9		A DES Example	PPT	9				
10		The strength of DES, Block cipher design principles.	PPT	10				



DEPARTMENT OF COMPUTER SCIENCE & DESIGN

Course with Code: Cryptography and Network Security – BCS703				Faculty: Darshini Y			Semester : 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		Pseudorandom number Generators: Linear Congruential Generators	PPT	1				
2		Blum Blum Shub Generator	PPT	2				
3		Principles and Applications for public key cryptosystems	PPT	3				
4		Requirements for public key cryptography, Public key Cryptanalysis	PPT	4				
5		The RSA algorithm: Description of the Algorithm,	PPT	5				
6		Computational aspects, The Security of RSA.	PPT	6				
7		Diffie-Hellman key exchange: The Algorithm	PPT	7				
8		Key exchange Protocols, Man-in-the-middle Attack, Elliptic Curve Cryptography	PPT	8				
9		Analog of Diffie-Hellman key Exchange	PPT	9				
10		Security of Elliptic Curve Cryptography	PPT	10				



DEPARTMENT OF COMPUTER SCIENCE & DESIGN

Course with Code: Cryptography and Network Security – BCS703				Faculty: Darshini Y			Semester : 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	1				
2		Two simple Hash functions	PPT	2				
3		Key management and distribution - KDC	PPT	3				
4		Key management and distribution	PPT	4				
5		Symmetric key distribution using symmetric encryption	PPT	5				
6		Symmetric key distribution using asymmetric encryption	PPT	6				
7		Distribution of public keys	PPT	7				
8		X.509 Certificates - Format	PPT	8				
9		X.509 Certificates	PPT	9				
10		Public Key Infrastructure	PPT	10				



DEPARTMENT OF COMPUTER SCIENCE & DESIGN

Course with Code: Cryptography and Network Security – BCS703				Faculty: Darshini Y			Semester : 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	1				
2		Kerberos – version 4	PPT	2				
3		Kerberos – version 4 and 5	PPT	3				
4		Kerberos continuation	PPT	4				
5		Remote user authentication using asymmetric encryption	PPT	5				
6		Web security consideration, Transport layer security	PPT	6				
7		Transport layer security	PPT	7				
8		Email Threats and comprehensive email security	PPT	8				
9		S/MIME	PPT	9				
10		S/MIME, Pretty Good Privacy	PPT	10				





DEPARTMENT OF COMPUTER SCIENCE & DESIGN

Course with Code: Cryptography and Network Security – BCS703					Faculty: Darshini Y			Semester : 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 - Strategy	PPT	1					
2		IP Security overview , Domain keys Identified Mail	PPT	2					
3		IP Security Policy	PPT	3					
4		IP Security Policy – Traffic Processing	PPT	4					
5		Encapsulating Security Payload – Header format	PPT	5					
6		Encapsulating Security Payload format	PPT	6					
7		Combining security associations	PPT	7					
8		Internet key exchange – Header format and message exchanges	PPT	8					
9		Internet key exchange continuation	PPT	9					
10		Revision	PPT	10					





DEPARTMENT OF COMPUTER SCIENCE & DESIGN

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