Lingaya's Vidyapeeth

Deemed-to-be-University u/s 3 of UGC Act 1956, Government of India
NAAC ACCREDITED
Approved by MHRD / AICTE / PCI / BCI / COA / NCTE
Nachauli, Jasana Road, Faridabad- 121002 (Haryana)
Website: www.lingayasvidyapeeth.edu.in | Ph: 0129-2598200-05

COURSE PLAN & COURSE DATA SHEET

PROGRAM: B.TECH	DEGREE: 3+2
COURSE: CRYPTOGRAPHY AND NETWORK SECURITY	SEMESTER: 6TH CREDITS: 3
COURSE CODE: CS-306 REGULATION:	COURSE TYPE: CORE
COURSE AREA/DOMAIN: CS-356	CONTACT HOURS: 3+1 (Tutorial) hours/Week.
CORRESPONDING LAB COURSE CODE (IF ANY):	LAB COURSE NAME (IF ANY):CNS Lab

PROGRAM EDUCATIONAL OBJECTIVES:

SYLLABUS:

UNIT	DETAILS	HOURS
I	ATTACKS ON COMPUTERS & COMPUTER SECURITY: Introduction; The need of Security ; Security Approaches; Principal of Security; Types of Attacks, CRYPTOGRAPHY : Introduction; Plain Text & Cipher Text; Substitution Techniques; Transposition Techniques; Types of Cryptography; Steganography; Symmetric Key Algorithm: Algorithm Types and Modes, DES; Asymmetric Key Algorithm: RSA, Digital Signatures	12
II	DIGITAL CERTIFICATES AND PUBLIC KEY INFRASTRUCTURE: Digital Certificates ; Private Key Management; The PKIX Model ; Public Key Cryptography Standards; Creating Digital certificates using Java	7
III	INTERNET SECURITY PROTOCOLS: Introduction; Secure Socket Layer(SSL); Secure Electronic Transaction (SET); Electronic Money; Email security; Wireless application protocol (WAP); Security in GSM: Security in 3G	7
IV	USER AUTHENTICATION AND KERBEROS: Introduction, Authentication Basics; Passwords; Authentication Tokens; Certificate Based Authenticaton; Biometric Authentication; Kerberos	7
V	NETWORK SECURITY, FIREWALL AND VPN: Introduction, Firewalls: Types of Firewalls ; IP Security; Virtual Private Network; Intrusion, CASE STUDIES ON NETWORK SECURITY : Introduction ; secure Inter branch payment transactions; Denial of Service attacks; IP Spoofing attacks; Contract Signing; Secret Splitting ; Virtual elections	7
	TOTAL HOURS	40

Teacher Centric Approach **TC1: Chalk and Talk, TC2: PPT, TC3: Video Lectures TC4: Blended learning**
Learner Centric Approach: **LC1: Assignment. LC2: Mini project. LC3: Quiz/Class test. LC 4: Seminar on recent trends.** **LC5: Group Task. LC6: Others**

DETAILED SESSION PLAN

Lecture session/ Number	Topics to be covered	CO addressed	Teacher Centric Approach	Learner Centric Approach	References	Relevance with POs and PSOs
1.	Unit 1- Introduction about		TC1	LC1,LC3	T1/T2/R1/W1	
2.	Need of security, Principles of		TC1	LC1,LC3	T1/T2/R1/W1	
3.	Different security approaches		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
4.	Introduction to attacks and its		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
5.	Passive attacks and its types		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
6.	Active attacks and its types		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
7.	Quiz based assignment - 1		TC1	LC1,LC3	T1/T2/R1/W1	
8.	Introduction to cryptography		TC1	LC1,LC3	T1/T2/R1/W1	
9.	Types of cryptography and		TC1,TC2	LC1,LC3	T1/T2/R1/W1	
10.	Substitution techniques and its		TC1	LC1,LC3	T1/T2/R1/W1	
11.	Substitution techniques and its		TC1	LC1,LC3	T1/T2/R1/W1	
12.	Transposition techniques and its		TC1	LC1,LC3	T1/T2/R1/W1	
13.	Transposition techniques and its		TC1	LC1,LC3	T1/T2/R1/W1	
14.	Algorithm Types and Modes		TC1	LC1,LC3	T1/T2/R1/W1	

15.	DES algorithm	TC1	LC1,LC3	T1/T2/R1/W1
16.	RSA algorithm	TC1	LC1,LC3	T1/T2/R1/W1
17.	Digital Signatures	TC1,TC2	LC1,LC3	T1/T2/R1/W1
18.	Unit 2- Introduction to	TC1	LC1,LC3	T1/T2/R1/W1
19.	Private key management	TC1	LC1,LC3	T1/T2/R1/W1
20.	The PKIX Model	TC1	LC1,LC3	T1/T2/R1/W1
21.	Public Key Cryptography	TC1,TC2	LC1,LC3	T1/T2/R1/W1
22.	Creating Digital certificates using	TC1,TC2	LC1,LC3	T1/T2/R1/W1
23.	Creating Digital certificates using	TC1,TC2	LC1,LC3	T1/T2/R1/W1
24.	Quiz based assignment - 2	TC1	LC1,LC3	T1/T2/R1/W1
25.	Unit 4- Introduction to	TC1,TC2	LC1,LC3	T1/T2/R1/W1
26.	Secure Socket Layer(SSL)	TC1	LC1,LC3	T1/T2/R1/W1
27.	Secure Electronic Transaction(SET)	TC1	LC1,LC3	T1/T2/R1/W1
28.	Electronic Money	TC1,TC2	LC1,LC3	T1/T2/R1/W1
29.	Email security	TC1,TC2	LC1,LC3	T1/T2/R1/W1
30.	Wireless application	TC1	LC1,LC3	T1/T2/R1/W1
31.	Security in GSM: Security in 3G	TC1,TC2	LC1,LC3	T1/T2/R1/W1
32.	Unit 4- Introduction to	TC1,TC2	LC1,LC3	T1/T2/R1/W1
33.	Authentication Basics: Passwords	TC1	LC1,LC3	T1/T2/R1/W1
34.	Authentication Tokens	TC1	LC1,LC3	T1/T2/R1/W1
35.	Certificate Based Authentication	TC1,TC2	LC1,LC3	T1/T2/R1/W1
36.	Biometric Authentication	TC1,TC2	LC1,LC3	T1/T2/R1/W1
37.	Kerberos – introduction and	TC1,TC2	LC1,LC3	T1/T2/R1/W1
38.	Quiz based assignment - 3	TC1	LC1,LC3	T1/T2/R1/W1
39.	Introduction, Firewalls	TC1	LC1,LC3	T1/T2/R1/W1
40.	Types of Firewalls	TC1	LC1,LC3	T1/T2/R1/W1

41.	IP Security		TC1,TC2	LC1,LC3	T1/T2/R1/W1
42.	Virtual Private Network: Intrusion		TC1	LC1,LC3	T1/T2/R1/W1
43.	secure Inter branch payment		TC1,TC2	LC1,LC3	T1/T2/R1/W1
44.	Denial of Service attacks: IP Spoofing		TC1	LC1,LC3	T1/T2/R1/W1
45.	Contract Signing; Secret Splitting :		TC1	LC1,LC3	T1/T2/R1/W1

TEXT/REFERENCE BOOKS:

T/R	BOOK TITLE/AUTHORS/PUBLICATION
1	Stallings William, "Cryptography and Network Security", 4th Edition, Prentice-Hall, Englewood Cliffs, 2006 Behrouz A. Forouzan "Cryptography and Network Security", TMH
2	Behrouz A. Forouzan "Cryptography and Network Security", TMH
3	Atul Kahate , "Cryptography and Network Security", 3rd Edition, Tata Mcgraw Hill.
4	Mani Subramanian, "Network Management Principles & Practices", Addison Wesley, 1999
5	Kauffman C., Perlman R. and Spenser M., "Network Security", 2nd Edition, Prentice Hall, 2002

 # WEB SOURCE REFERENCES (W):

1	https://www.tutorialspoint.com/information_security_cyber_law/network_security.htmL
2	
3	
4	
5	
6	
7	

COURSE PRE-REQUISITES:

C.CODE	COURSE NAME	DESCRIPTION	SEM
CS-306	**CRYPTOGRAPHY AND NEYWORK SECURITY**	**3-0-0**	**6TH**

COURSE OBJECTIVES:

1	The main objective behind this course is to learn about the various network attacks and preventing attacks. This course is designed to cover Application security, Network security, Web security etc.
2	Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
3	Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges.
4	Data Communications and Computer Networks, Computer Programming, Data Structures, Prime Number Theory

COURSE OUTCOMES:

S.NO	DESCRIPTION	PO(1..12) MAPPING	PSO(1..3) MAPPING
Cxxx.1	Understand and analyze public-key cryptography, RSA and other public-key cryptosystems	PO1,PO2,PO3	PSO1,PSO2,PSO3
Cxxx.2	Analyze and design hash and MAC algorithms, and digital signatures.	PO1,PO2,PO12	PSO1,PSO2,PSO3
Cxxx.3	Design network application security schemes, such as PGP, S/ MIME, IPSec, SSL, TLS, HTTPS, SSH, etc.	PO1,PO2,PO3,PO12	PSO2,PSO3
Cxxx.4	Understand key management and distribution schemes and design User Authentication Protocol	PO1,PO2,PO3,PO6,PO12	PSO1,PSO2,PSO3
Cxxx.5	Know about Intruders and Intruder Detection mechanisms, Types of Malicious software, Firewall Characteristics, Types of Firewalls, Firewall Location and Configurations	PO1,PO2,PO3,PO6,PO12	PSO1,PSO2,PSO3
COURSE OVERALL PO/PSO MAPPING:			

COURSE OUTCOMES VS POs MAPPING (DETAILED; HIGH:3; MEDIUM:2; LOW:1)**:**

S.NO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
Cxxx.1	2	1	1	-	-	-	-	-	-	-	-	-	1	2	3
Cxxx.2	1	2	-	-	-	-	-	-	-	-	-	2	1	2	1
Cxxx.3	1	1	2	-	-	-	-	-	-	-	-	1	-	1	2
Cxxx.4	2	1	2	-	-	2	-	-	-	-	-	1	1	2	2
Cxxx.5	1	2	1	-	-	1	-	-	-	-	-	2	1	1	2
Cxxx*															

** For Entire Course, PO & PSO Mapping*

POs & PSO REFERENCE:

PO 1	**Engineering Knowledge:** Apply the knowledge of mathematics, science, engineering and Application fundamentals, and an engineering and Application specialization to the solution of complex engineering problems.	PO7	**Environment and sustainability**: Understand the impact of professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.	PSO 1	Professional Skills: An ability to understand the basic concepts in Electronics & Communication Engineering and to apply them to various areas, like Electronics, Communications, Signal processing, VLSI, Embedded systems etc., in the design and implementation of complex systems.

PO 2	**Problem Analysis:** Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.	PO8	**Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of engineering practice.	PSO 2	Problem-Solving Skills: An ability to solve complex Electronics and communication Engineering problems, using latest hardware and software tools, along with analytical skills to arrive cost effective and appropriate solutions.
PO 3	**Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations	PO9	**Individual and teamwork**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.	PSO 3	Successful Career and Entrepreneurship: An understanding of social-awareness & environmental-wisdom along with ethical responsibility to have a successful career and to sustain passion and zeal for real-world applications using optimal resources as an Entrepreneur.
PO 4	**Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.	PO10	**Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.		
PO 5	**Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and	PO11	**Project management and finance**: Demonstrate knowledge and understanding of the engineering and		

	modelling to complex engineering activities with an understanding of the limitations.		management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.		
PO 6	**The engineer and society**: Apply reasoning informed by contextual knowledge to assess societal, health, safety, legal and cultural issues, and the consequent responsibilities relevant to the professional engineering practice.	PO12	**Life-long learning:** Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.		

COs VS POs MAPPING JUSTIFICATION:

S.NO	PO/PSO MAPPED	LEVEL OF MAPPING	JUSTIFICATION
Cxxx.1			
Cxxx.2			
Cxxx.3			
Cxxx.4			
Cxxx.5			
Cxxx*			

GAPS IN THE SYLLABUS - TO MEET INDUSTRY/PROFESSION REQUIREMENTS, POs & PSOs:

SNO	DESCRIPTION	PROPOSED ACTIONS
1		
2		
3		
4		
5		

PROPOSED ACTIONS: TOPICS BEYOND SYLLABUS/ASSIGNMENT/INDUSTRY VISIT/GUEST LECTURER/NPTEL ETC

 # TOPICS BEYOND SYLLABUS/ADVANCED TOPICS/DESIGN:

1	
2	

3	
4	
5	
6	
7	

DELIVERY/INSTRUCTIONAL METHODOLOGIES:

☐ CHALK & TALK	☐ STUD. ASSIGNMENT	☐ WEB RESOURCES	☐ NPTEL/OTHERS
☐ LCD/SMART BOARDS	☐ STUD. SEMINARS	☐ ADD-ON COURSES	☐ WEBNIARS

ASSESSMENT METHODOLOGIES-DIRECT

☐ ASSIGNMENTS	☐ STUD. SEMINARS	☐ TESTS/MODEL EXAMS	☐ UNIV. EXAMINATION
☐ STUD. LAB PRACTICES	☐ STUD. VIVA	☐ MINI/MAJOR PROJECTS	☐ CERTIFICATIONS
☐ ADD-ON COURSES	☐ OTHERS		

ASSESSMENT METHODOLOGIES-INDIRECT

☐ ASSESSMENT OF COURSE OUTCOMES (BY FEEDBACK, ONCE)	☐ STUDENT FEEDBACK ON FACULTY (TWICE)
☐ ASSESSMENT OF MINI/MAJOR PROJECTS BY EXT. EXPERTS	☐ OTHERS

 # INNOVATIONS IN TEACHING/LEARNING/EVALUATION PROCESSES:

. Learning Through Interactivity

2. The Shift from Physical to eTextbooks

3. Focus on Accessible Education

4. Higher Measurability of Learning Effectiveness

5. Leverage a Single, Unified Platform

Prepared by
(Ms.SHIVANI BANSAL)

Approved by
(HOD)

 # Additionally, the details to be compiled separately by the Departmental Coordinator for the entire Department.