SEMESTER VI

Subject Code	Subject Name (Theory course)	Category	L	T	P	C
AI23611	SECURE SYSTEMS ENGINEERING	PC	3	0	0	3

OBJECTIVES:	
•	To Able to know the fundamentals of secure systems.
•	To Understand the basic cryptography and key management techniques.
•	To Able to build and evaluate trusted system.
•	To Explore different auditing mechanisms and Network security.
•	To Learn the various security systems.

UNIT I	INTRODUCTION TO SECURE SYSTEMS	9
An overview of Computer Security – Access Control matrix – Foundational results Security Policies – Confidentiality policies – Hybrid policies.		
UNIT II	**BASIC CRYPTOGRAPHY AND KEY MANAGEMENT**	**9**
Classical Crypto systems: Transposition ciphers, Substitution ciphers, Data Encryption Standard Public Key cryptography: RSA – Cryptographic checksums: HMAC – Key Management: Key Exchange, Cryptographic key infrastructure – Digital Signature.		
UNIT III	**INTRODUCTION TO ASSURANCE AND EVALUATING SYSTEMS**	**9**
Assurance and Trust – Building secure and trusted systems: Life cycle, Waterfall life cycle model, Prototyping Evaluating Systems: Role of formal evaluation, TCSEC requirements, classes, processes, impact. FIPS requirements, Security levels, impact.		
UNIT IV	**AUDITING AND NETWORK SECURITY**	**9**
Auditing: Anatomy of an auditing system, Designing an auditing system, auditing mechanisms. Network Security: Introduction, Policy Development, Network Organization anticipating attacks.		
UNIT V	**SYSTEM SECURITY, USER SECURITY AND PROGRAM SECURITY**	**9**
System Security: Introduction, Policy, Networks. User Security: Policy, Access, Processes. Program Security: Introduction, Requirements and policy, Design, Refinement and Implementation.		
	Contact Hours : 45	

COURSE OUTCOMES: On completion of the course, the students will be able to	
•	Identify the different secure systems and policies.
•	Apply cryptography and key management techniques to design a secure system.
•	Design and evaluate secure trusted system.
•	Apply different auditing mechanisms and ensure network security.
•	Apply various security systems for real time problem.

TEXT BOOKS:	
1	Ross Anderson ,Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition, Kindle Edition, 2021
2	RON ROSS, Systems Security Engineering, Special Publications,2016

REFERENCES:	
1	John Musa D, Software Reliability Engineering, 2nd Edition, Tata McGraw-Hill, 2005.
2	Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead, Software Security Engineering: A Guide for Project Managers, Addison Wesley, 2008
3	Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition,WILEY,2008

Web links
https://www.isms.online/iso-27002/control-8-27-secure-system-architecture-and-engineering-principles/
https://csrc.nist.gov/projects/systems-security-engineering-project

CO – PO – PSO mapping

COs	POs												PSOs		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
AI23611.1	2	2	2	2	2	-	-	-	-	-	1	2	2	3	3
AI23611.2	2	2	2	2	2	-	-	-	-	-	1	2	2	3	3
AI23611.3	2	2	2	2	2	-	-	-	-	-	2	2	3	3	3
AI23611.4	2	2	2	2	2	-	-	-	-	-	2	2	3	3	3
AI23611.5	2	2	2	2	2	-	-	-	-	-	2	2	3	3	3
Average	2	2	2	2	2	-	-	-	-	-	1.4	2	2.6	2.8	2.8

Correlation levels 1, 2 or 3 are as defined below:
1: Slight (Low) 2: Moderate (Medium) 3: Substantial (High)
No correlation: "-"