LECTURE PLAN

Institute/Department	UNIVERSITY INSTITUTE OF ENGINEERING (UIE)	**Program**	**Bachelor of Engineering - Computer Science & Engineering (CS201)**
Master Subject Coordinator Name:	Puneet Kaur	**Master Subject Coordinator E-Code**:	**E6913**
Course Name	Information Security and Cryptography	**Course Code**	**20CST-354**

Lecture	Tutorial	Practical	Self Study	Credit	Subject Type
3	0	0	0	3.0	T

Course Type	Course Category	Mode of Assessment	Mode of Delivery
Program Core	Graded (GR)	Theory Examination (ET)	Theory (TH)

Mission of the Department	MD1: To provide practical knowledge using state-of-the-art technological support for the experiential learning of our students. MD2: To provide an industry-recommended curriculum and transparent assessment for quality learning experiences. MD3: To create global linkages for interdisciplinary collaborative learning and research. MD4: To nurture an advanced learning platform for research and innovation for students’ profound future growth. MD5: To inculcate leadership qualities and strong ethical values through value-based education.
Vision of the Department	“To be recognized as a leading Computer Science and Engineering department through effective teaching practices and excellence in research and innovation for creating competent professionals with ethics, values, and entrepreneurial attitude to deliver service to society and to meet the current industry standards at the global level.”

Program Educational Objectives(PEOs)	
PEO1	PEO1 Graduates of the Computer Science and Engineering will contribute to the Nation’s growth through their ability to solve diverse and complex computer science and engineering problems across a broad range of application areas. (PEO1 is focused on Problem Solving)
PEO2	PEO2 Graduates of the Computer Science and Engineering will be successful professionals, designing and implementing Products & Services of global standards in the field of Computer Science & Engineering, becoming entrepreneurs, Pursuing higher studies & research. (PEO 2 is focused on Professional Success)
PEO3	PEO3 Graduates of the Computer Science and Engineering Program will be able to adapt to changing scenario of dynamic technology with an ability to solve larger societal problems using logical and flexible approach in decision making. (PEO 3 is focused on Attaining Flexibility and Adaptability)

Program Specific OutComes(PSOs)	
PSO1	PSO1 Exhibit attitude for continuous learning and deliver efficient solutions for emerging challenges in the computation domain.
PSO2	PSO2 Apply standard software engineering principles to develop viable solutions for Information Technology Enabled Services (ITES).

Program OutComes(POs)	
PO1	PO1 Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals and an engineering specialization to the solution of complex engineering problems.
PO2	PO2 Problem analysis: Identify, formulate, review research literature and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences and engineering sciences.
PO3	PO3 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.
PO4	PO4 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.
PO5	PO5 Modern tool usage: Create, select, and apply appropriate techniques, resources and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
PO6	PO6 The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7	PO7 Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development
PO8	PO8 Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO9	PO9 Individual or teamwork: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO10	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
PO11	PO11 Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as member and leader in a team, to manage projects and in multidisciplinary environments.
PO12	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 to technological change.

Text Books

Sr No	Title of the Book	Author Name	Volume/Edition	Publish Hours	Years
1	Cryptography and Network Security	William Stallings	6th edition	Pearson Education	March 2013
2	Network Security	2. Charlie Kaufman, Radia Perlman and Mike Specine	-	Prentice Hall of India	2002

Reference Books

Sr No	Title of the Book	Author Name	Volume/Edition	Publish Hours	Years
1	Cryptography & Network Security	Behrouz A. Ferouzan	-	Tata MC Graw Hill	-
2	Internet Security: Cryptographic Principles	Man Young Rhee	-	Wiley Publications	-
3	Security in Computing	Charles Pfleeger	4th edition	Prentice Hall of India	-
4	Internet Security Protocols	Ulysess Black	-	Pearson Education Asia	-
5	Network Security	Charlie Kaufman and Radia Perlman, Mike Speciner	Second edition	Private Communication in Public World”,PHI.	-
6	Network Security Essentials (Applications and Standards)	William Stallings	4th	Pearson Education	2012

Course OutCome

SrNo	OutCome
CO1	Analyze the number theory, classical encryption techniques and block ciphers.
CO2	Understand and analyze public-key cryptography, encryption standards, RSA, and other public-key cryptosystems.
CO3	Design hash functions, MAC algorithms and digital signatures.
CO4	Explore best security practice and system security such as authentication schemes, firewall characteristics and configurations.
CO5	Demonstrate and examine the various encryption techniques to secure data in transit across network.

Lecture Plan Preview-Theory

Unit No	LectureNo	ChapterName	Topic	Text/ Reference Books	Pedagogical Tool**	Mapped with CO Numer (s)
1	1	Introduction and Number theory	The OSI security architecture	,T-Network Security,R-Internet Security: Cryptograph	Instructor Lead WorkShop,PPT	CO1
1	2	Introduction and Number theory	Services, Mechanisms and attacks	,T-Network Security,R-Internet Security: Cryptograph	Instructor Lead WorkShop,PPT	CO1
1	3	Introduction and Number theory	Network security model	,T-Cryptography and Network Secur,T-Network Security,R-Internet Security: Cryptograph	PPT	CO1
1	4	Introduction and Number theory	Symmetric cipher model	,T-Network Security,R-Internet Security: Cryptograph	PPT	CO1
1	5	Introduction and Number theory	Substitution techniques	,T-Network Security,R-Internet Security: Cryptograph	PPT	CO2
1	6	Introduction and Number theory	Transposition techniques	,T-Cryptography and Network Secur,R-Internet Security: Cryptograph	PPT	CO2
1	7	Introduction and Number theory	Steganography	,T-Network Security,R-Internet Security: Cryptograph,R-Security in Computing	PPT	CO2
1	8	Introduction and Number theory	Groups, Rings, Fields	,T-Cryptography and Network Secur,T-Network Security,R-Cryptography &amp; Network Securit,R-Internet Security Protocols,R-Internet Security: Cryptograph,R-Network Security,R-Network Security Essentials (A,R-Security in Computing	PPT	CO2
1	9	Introduction and Number theory	Euclid's algorithm	,T-Cryptography and Network Secur,R-Internet Security: Cryptograph	PPT	CO2
1	10	Introduction and Number theory	Fermat's and Euler's theorem	,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO2
1	11	Introduction and Number theory	The Chinese remainder theorem	,T-Cryptography and Network Secur,R-Internet Security: Cryptograph	PPT	CO3
1	12	Block ciphers	Data Encryption Standard-Block cipher principles	,T-Network Security,R-Internet Security: Cryptograph	PPT	CO3
1	13	Block ciphers	Blowfish-RC5 algorithm	,T-Network Security,R-Internet Security: Cryptograph	PPT	CO3
1	14	Block ciphers	Advanced Encryption Standard (AES)	,T-Cryptography and Network Secur,R-Security in Computing	PPT	CO5
1	15	Block ciphers	Triple DES	,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO3
2	16	Public key crptography	Principles of public key cryptosystems	,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO3
2	17	Public key crptography	The RSA algorithm	,T-Cryptography and Network Secur,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO3
2	18	Public key crptography	Key management	,T-Network Security,R-Security in Computing	PPT	CO3
2	19	Public key crptography	Diffie Hellman Key exchange	,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO2

2	20	Hash Functions and digital signatures	Authentication requirement	,T-Network Security,R-Security in Computing	PPT	CO2
2	21	Hash Functions and digital signatures	Authentication function – MAC	,T-Cryptography and Network Secur,R-Cryptography &amp; Network Securit	PPT	CO2
2	22	Hash Functions and digital signatures	Hash function	,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO2
2	23	Hash Functions and digital signatures	Security of hash function and MAC	,T-Cryptography and Network Secur,R-Cryptography &amp; Network Securit	PPT	CO1
2	24	Hash Functions and digital signatures	MD1, MD4	,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO2
2	25	Hash Functions and digital signatures	MD5	,T-Cryptography and Network Secur,R-Cryptography &amp; Network Securit	PPT	CO3
2	26	Hash Functions and digital signatures	SHA512	,T-Network Security,R-Cryptography &amp; Network Securit,R-Internet Security: Cryptograph	PPT	CO3
2	27	Hash Functions and digital signatures	HMAC – CMAC	,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO3
2	28	Hash Functions and digital signatures	Digital signature	,T-Cryptography and Network Secur,R-Cryptography &amp; Network Securit	PPT	CO3
2	29	Hash Functions and digital signatures	authentication protocols	,T-Network Security,R-Security in Computing	PPT	CO2
2	30	Hash Functions and digital signatures	DSS	,T-Network Security,R-Security in Computing	PPT	CO3
2	31	Hash Functions and digital signatures	EI Gamal	,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO1
2	32	Hash Functions and digital signatures	Surprise test	,T-Cryptography and Network Secur,T-Network Security,R-Cryptography &amp; Network Securit,R-Internet Security Protocols,R-Internet Security: Cryptograph,R-Network Security,R-Network Security Essentials (A,R-Security in Computing	Case Study	CO3
2	33	Security Practice and System security	Authentication applications	,T-Cryptography and Network Secur,T-Network Security,R-Cryptography &amp; Network Securit,R-Security in Computing	PPT	CO5
3	34	Security Practice and System security	Kerberos	,T-Network Security,R-Security in Computing	PPT	CO3
3	35	Security Practice and System security	Authentication services	,T-Network Security,R-Cryptography &amp; Network Securit,R-Internet Security: Cryptograph	PPT	CO1
3	36	Security Practice and System security	Internet Firewalls for Trusted System	,T-Network Security,R-Cryptography &amp; Network Securit	PPT	CO3
3	37	Security Practice and System security	Roles of Firewalls, Types of firewalls	,T-Network Security,R-Security in Computing	PPT	CO4
3	38	Security Practice and System security	Intruder – Intrusion detection system	,T-Network Security,R-Security in Computing	PPT	CO3

3	39	Security Practice and System security	Firewall designs ,Virus and related threats.	,T-Network Security,R-Security in Computing	PPT	CO4
3	40	E-Mail Security	Security Services for E-mail-attacks possible through E-mail – establishing keys privacy authentication of the source	,T-Network Security,R-Security in Computing	PPT	CO3
3	41	E-Mail Security	Message Integrity-Privacy-S/MIME	,T-Cryptography and Network Secur,R-Cryptography &amp; Network Securit	PPT	CO2
3	42	IP Security and Web Security	Overview of IPsec – IP address and IPv6-Authentication Header	,T-Network Security,R-Cryptography &amp; Network Securit,R-Internet Security: Cryptograph	PPT	CO4
3	43	IP Security and Web Security	SSL Architecture and its layers	,T-Cryptography and Network Secur,T-Network Security,R-Cryptography &amp; Network Securit,R-Internet Security Protocols,R-Internet Security: Cryptograph,R-Network Security,R-Network Security Essentials (A,R-Security in Computing	PPT	CO5
3	44	Public key crptography	Revision	,T-Cryptography and Network Secur,T-Network Security,R-Cryptography &amp; Network Securit,R-Internet Security Protocols,R-Internet Security: Cryptograph,R-Network Security,R-Network Security Essentials (A,R-Security in Computing	Case Study	CO5
3	45	E-Mail Security	Revision	,T-Cryptography and Network Secur,T-Network Security,R-Cryptography &amp; Network Securit,R-Internet Security Protocols,R-Internet Security: Cryptograph,R-Network Security,R-Network Security Essentials (A,R-Security in Computing	Case Study	CO5

Assessment Model

Sr No	Assessment Name	Exam Name	Max Marks
1	20EU01	External Theory	60
2	20EU01	Assignment	10
3	20EU01	Attendance Marks	2
4	20EU01	Mid-Semester Test-1	40
5	20EU01	Quiz	4
6	20EU01	Surprise Test	12
7	20EU01	Mid-Semester Test-2	40

CO vs PO/PSO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	1	NA	NA	2	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
CO2	1	3	2	1	NA	NA	NA	NA	NA	NA	NA	NA	NA	2
CO3	1	3	2	1	NA	NA	NA	NA	NA	NA	NA	NA	NA	2
CO4	2	2	1	1	NA	NA	NA	NA	NA	NA	NA	NA	NA	2
CO5	2	2	2	1	NA	NA	NA	NA	NA	NA	NA	NA	NA	3
Target	1.4	2.5	1.75	1.2	NA	NA	NA	NA	NA	NA	NA	NA	NA	2.25