Course Code	PCS21E08J	Course Name	CRYPTOGRAPHY AND NETWORK SECURITY	Course Category	D	Discipline Elective Courses	L	T	P	C
							3	0	2	4

Pre-requisite Courses	Nil	Co-requisite Courses	Nil	Progressive Courses	Nil
Course Offering Department	Computer Science	Data Book / Codes/Standards		Nil	

Course Learning Rationale (CLR):	The purpose of learning this course is to:	Learning		
		1	2	3
		Level of Thinking (Bloom)	Expected Proficiency (%)	Expected Attainment (%)
CLR-1 :	*To become familiar with objective of research*			
CLR-2 :	*To get exposed to resources for research*			
CLR-3 :	*To learn art of writing and presentation*			
CLR-4 :	*To study about the data collection*			
CLR-5 :	*To learn about analysis and inference*			

Course Learning Outcomes (CLO):	At the end of this course, learners will be able to:				Program Learning Outcomes (PLO)														
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
					Fundamental Knowledge	Application of Concepts	Link with Related Disciplines	Procedural Knowledge	Skills in Specialization	Ability to Utilize Knowledge	Skills in Modeling	Analyze, Interpret Data	Investigative Skills	Problem Solving Skills	Communication Skills	Analytical Skills	PSO 1	PSO 2	PSO 3
CLO-1 :	*Have a thorough understanding of steps involved in research preparation and planning*	3	80	70	L	H	-	H	L	-	-	-					-	-	-
CLO-2 :	*Perform literature review and case study*	3	85	75	M	H	L	M	L	-	-	-					-	-	-
CLO-3 :	*Learn the basics of academic writing and presentation*	3	75	70	M	H	M	H	L	-	-	-					-	-	-
CLO-4 :	*Learn the basics of data collection*	3	85	80	M	H	M	H	L	-	-	-					-	-	-
CLO-5 :	*Knowledge about analysis and inference*	3	85	75	H	H	M	H	L	-	-	-					-	-	-

Duration (Hour)		15	15	15	15	15
S-1	SLO-1	*Overview on Symmetric Cipher Model*	*Overview on Block ciphers and the data encryption standard*	*Basic knowledge of Network security – Authentication Application*	*IP Security Overview*	*Overview on System Security*
	SLO-2	*Conventional encryption model*	*Block Cipher Principles*	*Design of function F*	*Triple DES*	*AES cipher*
S-2	SLO-1	*Overview on Classical Encryption Techniques*	*The strength of DES*	*Kerberos*	*IP Security Architecture*	*Intruders*
	SLO-2	*Substitution ciphers*	*Stream ciphers*	*S- box design*	*Cipher block chaining mode*	*AES algorithm*
S-3	SLO-1	*Brief on Symmetric Cipher Model*	*The Data Encryption Standard*	*Kerberos Authentication Service*	*Authentication Header*	*Intrusion Detection*
	SLO-2	*Transposition techniques*	*Feistal cipher*	*Groups*	*Examples*	*AES encryprion*
S4-5	SLO-1	*Laboratory 1: Perform encryption, decryption using the following substitution techniques i)Ceaser cipher*	*Laboratory 4:vi) Vigenere Ciphers*	*Laboratory 7: Apply DES algorithm for practical applications*	*Laboratory 10: Implement the SIGNATURE SCHEME - Digital Signature Standard.*	*Laboratory 13: Apply AES algorithm for practical applications*
S-6	SLO-1	*Techniques involved in – Cryptography*	*Describe the procedure of DES Encryption*	*Overview on Electronic Mail Security*	*Encapsulating Security Payload*	*Password Management*
	SLO-2	*Rotor machines*	*Diffusion*	*Rings*	*Examples*	*AES decryption*
S-7	SLO-1	*Principles involved in - Cryptanalysis*	*Describe the procedure of DES Decryption*	*Operational Description*	*Combining Security Associations*	*Discuss on Malicious Software*

Duration (Hour)		15	15	15	15	15
	SLO-2	*Stegnography*	*Confusion*	*Fields*	*Digital Signature Standard*	*Transformation*
S-8	SLO-1	*Substitution Techniques- Caesar Cipher*	*Feistal description alg*	*Cryptographic Keys*	*Key Management*	*Viruses*
	SLO-2	*Block Cipher*	*Examples*	*Examples*	*RSA Algortihm*	*Related Threats*
S9-10	SLO-1	*Laboratory 2: ii) playfair cipher*	*Laboratory 5: Perform encryption and decryption using following transposition techniques. Rail fence*	*Laboratory 8: example on DES*	*Laboratory 11: Apply RSA algorithm for practical applications.*	*Laboratory 14: example on AES*
S-11	SLO-1	*Monoalphabetic Ciphers*	*Differential and Linear Cryptanalysis*	*Public-Key Management*	*Overview on Web Security*	*Virus Counter measures*
	SLO-2	*Playfair Cipher*	*Examples*	*Double DES*	*Meet in the middle attack*	*Examples*
S-12	SLO-1	*Hill Cipher*	*Block Cipher Design Principles*	*S/MIME (Secure/Multipurpose Internet Mail Extension)*	*Web Security Considerations*	*Overview on Firewall*
	SLO-2	*Polyalphabetic Ciphers, One-Time Pad*	*Key generation*	*Key Rings*	*Secure Socket Layer*	*Diffie-Hellman Key Exchange algorithm*
S-13	SLO-1	*Overview of Transposition Techniques*	*Principles of Public-Key Cryptosystems*	*S/MIME Functionality*	*Transport Layer Security*	*Firewall Design Principles*
	SLO-2	*Steganography*	*The RSA Algorithm*	*S/MIME Messages, Certificate processing*	*Secure Electronic Transaction*	*Trusted Systems*
S 14-15	SLO-1	*Laboratory 3: iii) Hill Cipher*	*Laboratory 6: ii. Row & Column Transformation*	*Laboratory 9: Calculate the message digest of a text using the SHA-1 algorithm.*	*Laboratory 7: example on RSA*	*Laboratory 15: Implement the Diffie-Hellman Key Exchange algorithm*

Learning Resources	1. Anderson B.H., Dursaton and Poole, M : Thesis and assignment writing, Wiley Eastern 1997 2. Bordens, K. S. and Abbott, B.B : Research design and Methods, Mc Graw Hill, 2008 3. Leedy, P. . : Practical Research – Planning and design, Ninth Edition, Pearson, 2010	4. Walpole, R.A., Myers, R.H., Myers, S.L. and Ye, King : Probability and Statistics for Engineers and Scientists, Pearson Prentice Hall, Pearson Education Inc., 2012 5. Kothari, C.K. [2004], 2.e, Research Methodology – Methods and Technique3s [New Age International, New Delhi] 6. Ganesan R, Research Methodology for Engineers , MJP Publishers, Chennai. 2016

Learning Assessment

Bloom's Level of Thinking		Continous Learning Assessment(50% Weightage)								Final Examination (50% weightage)	
		CLA – 1 (10%)		CLA – 2 (10%)		CLA – 3 (20%)		CLA – 4# (10%)			
		Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice	Theory	Practice
Level 1	Remember	20%	20%	15%	15%	15%	15%	15%	15%	15%	15%
	Understand										
Level 2	Apply	20%	20%	20%	20%	20%	20%	20%	20%	20%	20%
	Analyze										
Level 3	Evaluate	10%	10%	15%	15%	15%	15%	15%	15%	15%	15%
	Create										
	Total	100 %		100 %		100 %		100 %		100%	

CLA – 4 can be from any combination of these: Assignments, Seminars, Short Talks, Mini-Projects, Case-Studies, Self-Study, MOOCs, Certifications, Conf. Paper etc

Course Designers		
Experts from Industry	**Experts from Higher Technical Institutions**	**Internal Experts**
Mr. S. Karthik, Assistant Consultant, Tata Consultancy Services	Dr.S.Sasikala, Associate Professor and Head, Dept. of Computer Science, University of Madras	Dr Kalpana
		Mrs.P.Yogalakshmi