COURSE INFORMATION SHEET

Course: CRYPTOGRAPHY, NETWORK SECURITY AND CYBER LAW	**Semester: 6**
Course Code: 17CS61	**Course Type: Regular**
Lecture Hours / Week: 4 Hours/Week	**Scheme: 2017**
Exam Hours / Exam Marks: 3 Hrs / 60 Marks	**Credits: 4**
Corresponding Lab Course Code: --NA--	**Lab Course Name: --NA--**

SYLLABUS:

Module No.	Details	Hours
Module 1	Introduction - Cyber Attacks, Defence Strategies and Techniques, Guiding Principles, Mathematical Background for Cryptography - Modulo Arithmetic's, The Greatest Comma Divisor, Useful Algebraic Structures, Chinese Remainder Theorem, Basics of Cryptography - Preliminaries, Elementary Substitution Ciphers, Elementary Transport Ciphers, Other Cipher Properties, Secret Key Cryptography – Product Ciphers, DES Construction.	10
Module 2	Public Key Cryptography and RSA – RSA Operations, Why Does RSA Work?, Performance, Applications, Practical Issues, Public Key Cryptography Standard (PKCS), Cryptographic Hash - Introduction, Properties, Construction, Applications and Performance, The Birthday Attack, Discrete Logarithm and its Applications - Introduction, Diffie-Hellman Key Exchange, Other Applications.	10
Module 3	Key Management - Introduction, Digital Certificates, Public Key Infrastructure, Identity–based Encryption, Authentication–I - One way Authentication, Mutual Authentication, Dictionary Attacks, Authentication – II – Centalised Authentication, The Needham-Schroeder Protocol, Kerberos, Biometrics, IPSecSecurity at the Network Layer – Security at Different layers: Pros and Cons, IPSec in Action, Internet Key Exchange (IKE) Protocol, Security Policy and IPSEC, Virtual Private Networks, Security at the Transport Layer - Introduction, SSL Handshake Protocol, SSL Record Layer Protocol, OpenSSL. Text-1:Chapter :6-2 to 6-08 (Excluding 6-4),5-9 to 5-17(Excluding 5-15),12- 1,12-2,12-4,12-6,10-1,10-3	10

Module 4	IEEE 802.11 Wireless LAN Security - Background, Authentication, Confidentiality and Integrity, Viruses, Worms, and Other Malware, Firewalls – Basics, Practical Issues, Intrusion Prevention and Detection - Introduction, Prevention Versus Detection, Types of Instruction Detection Systems, DDoS Attacks Prevention/Detection, Web Service Security – Motivation, Technologies for Web Services, WS- Security, SAML, Other Standards.	10
Module 5	IT act aim and objectives, Scope of the act, Major Concepts, Important provisions, Attribution, acknowledgement, and dispatch of electronic records, Secure electronic records and secure digital signatures, Regulation of certifying authorities: Appointment of Controller and Other officers, Digital Signature certificates, Duties of Subscribers, Penalties and adjudication, The cyber regulations appellate tribunal, Offences, Network service providers not to be liable in certain cases, Miscellaneous Provisions.	10
	TOTAL HOURS	**50**

TEXT BOOKS / REFERENCE BOOKS:

Text / Reference	Book Title / Author / Publication / Edition
Text 1	Cryptography, Network Security and Cyber Laws – Bernard Menezes, Cengage Learning, 2010 edition (Chapters-1,3,4,5,6,7,8,9,10,11,12,13,14,15,19(19.1- 19.5),21(21.1-21.2),22(22.1-22.4),25
Ref 1	Cryptography and Network Security- Behrouz A Forouzan, DebdeepMukhopadhyay, Mc-GrawHill, 3rd Edition, 2015
Ref 2	Cryptography and Network Security- William Stallings, Pearson Education, 7th Edition
Ref 3	Cyber Law simplified- VivekSood, Mc-GrawHill, 11th reprint , 2013
Ref 4	Cyber security and Cyber Laws, Alfred Basta, Nadine Basta, Mary brown, ravindrakumar, Cengage learning

COURSE PRE-REQUISITES

Course Code	Course Name	Description	Sem
17CS52	COMPUTER NETWORKS	Basics of Computer Networks	5

COURSE OBJECTIVES

SL No	Course Objectives
1	Explain the concepts of Cyber security
2	Illustrate key management issues and solutions.
3	Familiarize with Cryptography and very essential algorithms
4	Introduce cyber Law and ethics to be followed.

COURSE OUTCOMES

CO No.	On completion of this course, students will be able to:	RBT Level / Cognitive Level
17CS61.1	Understand cryptography basics, algorithms and mathematical background for cryptography.	L2 Understand
17CS61.2	Analyze the important cryptographic algorithms.	L4 Analyze
17CS61.3	Understand key management issues and algorithms.	L2 Understand
17CS61.4	Understand security issues in Wireless LAN and web.	L2 Understand
17CS61.5	Understand cyber security and need of cyber Laws.	L2 Understand

CO-PO-PSO MAPPING

CO No.	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
17CS61.1	2	2	-	-	-	-	-	-	-	-	-	-	1	1	-
17CS61.2	2	2	-	1	-	-	-	-	-	-	-	1	2	2	-
17CS61.3	2	2	-	-	-	-	-	-	-	-	-	1	2	2	-
17CS61.4	2	1	-	-	-	-	-	-	-	-	-	1	2	2	-
17CS61.5	2	1	-	-	-	1	-	-	-	-	-	1	-	-	-
17CS61	**2.0**	**1.6**	-	**1.0**	**-**	**1.0**	**-**	**-**	**-**	**-**	**-**	**1.0**	**1.8**	**1.8**	**-**

CO-PO-PSO JUSTIFICATION

CO No.	PO/PSO	CL	Justification
17CS61.1	PO1	2	Moderately mapped as students can understand the concepts of modulus operation, encryption and decryption techniques in cryptography.
	PO2	2	Moderately mapped as students can compare and contrast alternative solutions to select the best encryption and decryption techniques.
	PSO1	1	Slightly mapped as students apply the concepts of cryptography to secure the application software.
	PSO2	1	Slightly mapped as students apply the concepts of cryptography to secure the system software such as operating systems, compilers and debuggers.
17CS61.2	PO1	2	Moderately mapped as students can apply mathematical models to secure applications against different types of attacks.
	PO2	2	Moderately mapped as students can compare and contrast alternative solutions to select the best encryption and decryption techniques.
	PO4	1	Slightly mapped as students can develop different cryptographic algorithms to secure applications against different types of attacks.
	PO12	1	Slightly mapped as students can use the concepts of cryptography in application and system software.
	PSO1	2	Moderately mapped as students apply the concepts of cryptography to secure the application software.
	PSO2	2	Moderately mapped as students apply the concepts of cryptography to secure the system software such as operating systems, compilers and debuggers.
17CS61.3	PO1	2	Moderately mapped as students can understand the concepts public, private keys, symmetric and asymmetric keys.
	PO2	2	Moderately mapped as students can apply mathematical models to public, private keys, symmetric and asymmetric keys.
	PO12	1	Slightly mapped as students can use the concepts of keys in encryption and decryption algorithms.
	PSO1	2	Moderately mapped as students apply the concepts of cryptography to secure the application software.
	PSO2	2	Moderately mapped as students apply the concepts of cryptography to secure the system software such as operating systems, compilers and debuggers.
17CS61.4	PO1	2	Moderately mapped as students can identify different security issues in wireless LAN and web applications.

	PO2	1	Slightly mapped as students can compare and contrast alternative solutions to secure wireless LAN and web applications.
	PO12	1	Slightly mapped as students can use the concepts of cryptography in securing web applications.
	PSO1	2	Moderately mapped as students apply the concepts cryptography to secure the application software.
	PSO2	2	Moderately mapped as students apply the concepts cryptography to secure the system software such as operating systems, compilers and debuggers.
17CS61.5	PO1	2	Moderately mapped as students can use the concepts of cryptography in framing cyber laws.
	PO2	1	Slightly mapped as students can compare and contrast alternative solutions to develop cyber security.
	PO6	1	Slightly mapped as students can understand the cyber laws and IT act for protecting public.
	PO12	1	Slightly mapped as students can use the concepts of cryptography in cyber security.

GAPS IN THE SYLLABUS TO MEET INDUSTRY/PROFESSIONAL REQUIREMENTS:

SL No.	Description	Proposed Action
1		

TOPICS BEYOND SYLLABUS/ADVANCED TOPICS/DESIGN:

SL No.	Description
1	Implementation of RSA, AES, DES and Diffie Hellman key exchange algorithms.

WEB SOURCE REFERENCES:

SL No.	Web References
1	https://www.javatpoint.com/cyber-security-tutorial
2	https://www.meity.gov.in/content/information-technology-act-2000

DELIVERY / INSTRUCTIONAL METHODOLOGIES:

SL No.	Delivery Methodology	Tick Appropriate
1	Chalk and Talk	✓
2	Student Assignment	✓
3	Student Seminar	✓

4	LCD Projectors / Smart Boards	✓
5	Student Project / Lab Sessions	-
6	Additional Courses	-

ASSESSMENT METHODOLIES: DIRECT

SL No.	Assessment Methodology	Tick Appropriate
1	Assignment	✓
2	Internal Assessment / Model Exams	✓
3	Student Seminar	✓
4	University Exams	✓
5	Student Lab Practices	-
6	Student Mini / Major Projects	-
7	Certification Courses / Online Test / Quiz (MOOC /NPTEL/ Others)	✓
8	Add-on Courses	-
9	Others (If any)	-

ASSESSMENT METHODOLIES: INDIRECT

SL No.	Assessment Methodology	Tick Appropriate
1	Assessment of Course Outcomes (Course Feedback)	✓
2	Student Feedback on Faculty (Twice)	✓
3	Assessment of Student Mini / Major Project by Experts	-
4	Others	-

Prepared by: **Approved by:**

(Ashwini M & Jagadamba A) **(H.o.D)**