Ref No:

SRI KRISHNA INSTITUTE OF TECHNOLOGY,BANGALORE

COURSE PLAN

Academic Year 2019-20

Program:	B E – Computer Science & Engineering
Semester :	6
Course Code:	17CS61
Course Title:	Cryptography Network Security and Cyber Laws
Credit / L-T-P:	4 / 4-0-0
Total Contact Hours:	50
Course Plan Author:	Nagarathna C

Academic Evaluation and Monitoring Cell

No. 29, Chimny hills, Hesarghtta Road, Chikkabanavara
Bangalore – 560090, Karnataka, India
Phone/Fax: +91-08023721315/ 23721477
www.skit.org.in

Table of Contents

Note : Remove “Table of Content” before including in CP Book
Each Course Plan shall be printed and made into a book with cover page
Blooms Level in all sections match with A.2, only if you plan to teach / learn at higher levels

A. COURSE INFORMATION

1. Course Overview

Degree:	BE	Program:	CS
Semester:	6	Academic Year:	2019-20
Course Title:	CRYPTOGRAPHY ,NETWORK SECURITY AND CYBER LAW	Course Code:	17CS61
Credit / L-T-P:	4-0-0	SEE Duration:	180 Minutes
Total Contact Hours:	50	SEE Marks:	80 Marks
CIA Marks:	30	Assignment	1/Module
Course Plan Author:	Nagarathna C	Sign ..	Dt:
Checked By:	Dhananjay V	Sign ..	Dt:
CO Targets	CIA Target : ..... %	SEE Target:	..... %

Note: Define CIA and SEE % targets based on previous performance.

2. Course Content

Content / Syllabus of the course as prescribed by University or designed by institute. Identify 2 concepts per module as in G.

Module	Content	Teaching Hours	Identified Module Concepts	Blooms Learning Levels
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 (5,5)	-Crypto analysis GCD -Block cipher product cipher	L3 Apply,
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 (5,5)	-Block cipher product cipher -Two Key techniques	L4 ANALYZE
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, I**PSec**- Security 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.	10 (5,5)	-Digital signature protocols -Security protocols, keys interchange	L3 Apply,
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 (5,5)	-802.11 protocol filters -Wireless security web security	L3 Apply,
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	10 (5,5)	-E- records cyber security -Ethics &	L2 Understand,

	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.		Responsibilities	
-	**Total**	**50**	-	-

3. Course Material

Books & other material as recommended by university (A, B) and additional resources used by course teacher (C).

1. Understanding: Concept simulation / video ; one per concept ; to understand the concepts ; 15 – 30 minutes
2. Design: Simulation and design tools used – software tools used ; Free / open source
3. Research: Recent developments on the concepts – publications in journals; conferences etc.

Modules	Details	Chapters in book	Availability
A	**Text books (Title, Authors, Edition, Publisher, Year.)**	-	-
1, 2, 3, 4, 5	Cryptography, Network Security and Cyber Laws – Bernard Menezes, Cengage Learning, 2010 edition		In Lib / In Dept
B	**Reference books (Title, Authors, Edition, Publisher, Year.)**	-	-
1, 2,3	Cryptography and Network Security- Behrouz A Forouz an, Debdeep Mukhopadhyay, Mc-GrawHill, 3rd Edition, 2015	?	In Lib
1,2,3	Cryptography and Network Security- William Stalling s, Pearson Education, 7 th Edition		In Library
5	Cyber Law simplified- Vivek Sood, Mc-GrawHill, 11 th reprint , 2013		In Library
5	Cyber security and Cyber Laws, Alfred Basta, Nadine Basta, Mary brown, ravindra kumar, Cengage learning		In Library
C	**Concept Videos or Simulation for Understanding**	-	-
C1	https://youtube.be/ucA7lblaeFs – 20 min		
C1	https://youtube.be/ucA7lblaeFs – 35 min		
C2	https://youtube./nmPa5sfrrU – 19 min		
C2	https://youtube.be/DfsV2YeuSSo – 18 min		
C3	https://sllideplayer.com/slide/4647972/		
C3	https://youtube.be/DfsV2YeuSSo – 18 min		
C4	https://sllideplayer.com/slide/4647972/		
C4	https://youtube.be/ucA7lblaeFs		
C5	http://cyberlawclinic.net		
C5	http://cyberlawclinic.net		
D	**Software Tools for Design**	-	-
E	**Recent Developments for Research**	-	-
	Secure file storage on cloud using cryptography https://irjet.net/archives/V5/i3/IRJJET-V513475		
F	**Others (Web, Video, Simulation, Notes etc.)**	-	-
1	http://www.diginotes.in/notescsesem6.html		
2	https://www.youtube.com/watch?v=akEr8cUAd5g		

4. Course Prerequisites

Refer to GL01. If prerequisites are not taught earlier, GAP in curriculum needs to be addressed. Include in Remarks and implement in B.5.
Students must have learnt the following Courses / Topics with described Content . . .

Modules	Course Code	Course Name	Topic / Description	Sem	Remarks	Blooms Level
1	15MAT41	Mathematics	To know the importance of learning theories and strategies in Mathematic	1,2		L2 Understand
2	15cs52	Computer Networks	OSI LAYERS , Connection-Oriented Transport TCP, IPv6,A Brief foray into IP Security, Network Support for Multimedia	5	-	L2 Understand
3	15CS43	Design and Analysis of Algorithm	Basic knowledge of algorithms	4		L2
					-	
-						
-						

5. Content for Placement, Profession, HE and GATE

The content is not included in this course, but required to meet industry & profession requirements and help students for Placement, GATE, Higher Education, Entrepreneurship, etc. Identifying Area / Content requires experts consultation in the area.
Topics included are like, a. Advanced Topics, b. Recent Developments, c. Certificate Courses, d. Course Projects, e. New Software Tools, f. GATE Topics, g. NPTEL Videos, h. Swayam videos etc.

Modules	Topic / Description	Area	Remarks	Blooms Level
1	Advance Encryption Algorithm	Higher Study	Gap A seminar on AES algorithm	L3 Apply
2	RC4 & RC5	Gate	Gap A seminar on RC4 & RC5	L3 Apply
2	SHA-II & SHA-III	Higher Study	Gap A seminar on SHA-II & III	L3 Apply
3	MAC and HMAC	Higher Study & Industries	A seminar on HMAC	L3 apply
-				
-				

B. OBE PARAMETERS

1. Course Outcomes

Expected learning outcomes of the course, which will be mapped to POs. Identify a max of 2 Concepts per Module. Write 1 CO per Concept.

Modules	Course Code.#	Course Outcome **At the end of the course, student should be able to . . .**	Teach. Hours	Concept	Instr Method	Assessment Method	Blooms' Level
1	17CS61.1	Apply the basics of Cryptography techniques for enhancing the security	5	Basic concepts of cryptography	Lecture / PPT,	Assignment, seminar	L3
1	17CS61.2	Analyze Cryptography algorithms and its need to various applications	5	Key management	Lecture / PPT, proble	Assignment, seminar	L4

				techniques	m solving		
2	17CS61.3	Apply different Authentication mechanisms and make use of Security protocols	10	Authentication and security protocols	Discussion, lecture, ppt	Presentation, assignment	L3
3	17CS61.4	Identify different security technologies to secure WLAN	10	Web service security	Lecture, discussion	Assignment, slip test	L3
4	17CS61.5	Awareness about the existing Cyber Laws and Ethics in security issues	10	Cyber laws	Discussion, lecture , PPT	Seminar and assignment	L2
-	**-**	**Total**	**50**	**-**	**-**	**-**	**L2-L4**

2. Course Applications

Write 1 or 2 applications per CO.
Students should be able to employ / apply the course learnings to . . .

Modules	Application Area Compiled from Module Applications.	CO	Level
1	Used in secure communication: encrypting communications between us and another system.	CO1	L3
1	Manage the security of applications and systems in depth so that you can detect vulnerabilities as early as possible	CO1	L3
2	securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures.	CO1	L3
2	Blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.	CO1	L3
3	Digital signatures can be used to authenticate the source of messages.	CO2	L4
3	Securing electronic mail (*Privacy Enhanced Mail, Pretty Good Privacy* [PGP]), network management (*Simple Network Management Protocol Version 3*[SNMPv3]), Web access (Secure HTTP, *Secure Sockets Layer* [SSL]), and others.	CO2	L4
4	Wireless LAN provides a solutions complete network visibility to help successfully manage a network's wireless life cycle.	CO3	L3
4	Some standard provides a framework for encrypting and decrypting entire XML documents or just portions of an XML document.	CO4	L3
5	The goal of E-commerce technology is to give a secure, convenient and immediate payment facility to the users over the Internet.	CO5	L2

3. Mapping And Justification

CO – PO Mapping with mapping Level along with justification for each CO-PO pair.
To attain competency required (as defined in POs) in a specified area and the knowledge & ability required to accomplish it.

Modules	Mapping		Mapping Level	Justification	Level
-	**CO**	**PO**		**-**	**-**
1	**CO1**	PO1	3	Students will get to know about the maths behind the cryptographic algorithm which can contribute to the basic engineering knowledgeAND ALSO Knowledge of cryptography in building the solutions to data encrypting and decrypting	L3
1	CO1	PO2	2	Using the knowledge in basic maths students can analyze and formulate solutions for some problems.AND ALSO Only if students know the existing cryptographic algorithms they can formulate new one doing problem analysis.	L2
1	CO1	PO3	-	No design and development content. NO mapping	-

1	CO1	PO4	1	The knowledge in the mathematics behind the subject helps students to do research on developing new overcoming the demerits of the existing one AND Only if students know the existing cryptographic algorithms they can conduct investigations of complex problems and provide valid conclusions.	L2
1	CO1	PO5	2	The knowledge in maths will help in formulating new algorithms.	L2
1	CO1	PO6	-	No mapping for engineer and society	-
1	CO1	PO7	-	No matching for environment and sustainability	-
1	CO1	PO8	-	No matching for ethical principles	-
1	CO1	PO9	-	No mapping for individual and team work	-
1	CO1	PO10	-	No mapping for communication.	-
1	CO1	PO11	-	No mapping for Demonstrating knowledge and understanding of Engg principles	-
1	CO1	PO12	1	Lifelong learning is required for encryption and decryption of data using mathematical concept of cryptography	L3
2	**CO2**	PO1	3	Apply different key management techniques to achieve the cryptographic objectives like confidentiality and authentication	L3
2	CO2	PO2	2	classification of keys based on their intended use, techniques for the distribution of public keys, architectures supporting automated key updates in distributed systems, and the roles of trusted third parties requires the knowledge of key management	L2
2	CO2	PO3	-	To design a symmetric and asymmetric key management techniques requires the knowledge of key management	L2
2	CO2	PO4	3	Analyze Identity based encryption scheme with RSA encryption procedure requires the basic knowledge of cryptography	L2
2	CO2	PO5	-	Apply modern encryption methods which are used for public key encryption.	L3
2	CO2	PO6	-	No mapping for engineer and society	-
2	CO2	PO7	-	No matching for environment and sustainability	-
2	CO2	PO8	--	No matching for ethical principles	-
2	CO2	PO9	-	No mapping for individual and team work	-
2	CO2	PO10	-	No mapping for communication.	-
2	CO2	PO11	-	No matching for demonstrating knowledge and understanding of Engg principles	-
2	CO2	PO12	1	Learning in the context of technology changes	L2
3	**CO3**	PO1	3	Apply various algorithm and protocols to solve network issues	L3
3	CO3	PO2	2	Students will be able to analyze various security requirements and come up with the security protocol for each requirement	L4
3	CO3	PO3	2	Students know the existing network security applications they can develop new one understanding the problems of the existing ones	L2
3	CO3	PO4	1	Having knowledge on the existing protocols will help them in conducting further investigations on the security requirement	L4
3	CO3	PO5	-	No modern tool usage . No mapping	-
3	CO3	PO6	-	No mapping for engineer and society	-
3	CO3	PO7	-	No matching for environment and sustainability	-
3	CO3	PO8	-	No matching for ethical principles	-
3	CO3	PO9	-	No mapping for individual and team work	-
3	CO3	PO10	-	No mapping for communication.	-
3	CO3	PO11	-	No matching for demonstrating knowledge and understanding of Engg principles	-
3	CO3	PO12	1	Learning in the context of technology changes	L2

4	**CO4**	PO1	3	Knowledge of TCP/IP is required to apply the protocols to authenticate the data.	L3
4	CO4	PO2	3	Identifying different protocols which should be applied to secure the data requires the knowledge of TCP/IP protocols	L4
4	CO4	PO3			
4	CO4	PO4	2	Investigating different authentication protocols using digital signatures and biometric authentication	L4
4	CO4	PO5	1	Having knowledge on the existing security mechanisms like access control,passwords etc will help them in choosing the appropriate technique in meeting the specific security requirement	L2
4	CO4	PO6	-	No mapping for engineer and society	-
4	CO4	PO7	-	No matching for environment and sustainability	-
4	CO4	PO8	-	No matching for ethical principles	-
4	CO4	PO9	-	No mapping for individual and team work	-
4	CO4	PO10	-	No mapping for communication.	-
4	CO4	PO11	-	No matching for demonstrating knowledge and understanding of Engg principles	-
4	CO4	PO12	-	Learning in the context of technology changes	L2
5	**CO5**	PO1	2	Apply various cyber laws and rules while designing a applications	L3
5	CO5	PO2	-	No mapping for problem analysis	-
5	CO5	PO3	-	No design and development	
5	CO5	PO4	-	No investigation & interpretation content. No mapping	-
5	CO5	PO5	-	No tool content. No mapping	-
5	CO5	PO6	3	Apply the laws and acts on real world application will impact on society since heavy usage of computer & mobile	L3
5	CO5	PO7	2	There Will Be Mild Interference With environment & sustainability.	L2
5	CO5	PO8	3	Apply the cyber laws that regulates Internet in the process of sending data or exchanging information around the globe	L3
5	CO5	PO9	1	Effective team work or individual hands on practice makes Confident about concept	L2
5	CO5	PO10	1	Effective communication on engineering activities will be the part of every activities	L2
5	CO5	PO11	-	No matching for demonstrating knowledge and understanding of Engg principles	-
5	CO5	PO12	2	Learning in the context of technology changes. Recognizing the laws and acts to validate the electronic contracts, electronic signatures, data security, blocking of websites etc. requires the knowledge of Internet laws and cyber acts.	L2

4. Articulation Matrix

CO – PO Mapping with mapping level for each CO-PO pair, with course average attainment.

-	-	Course Outcomes	Program Outcomes														-
Modules	CO.#	**At the end of the course student should be able to . . .**	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	Level
1	CO1	Apply the basics of Cryptography techniques for enhancing the security	3	2	-	1	2	-	-	-	-	-	-	3	2			3
2	CO2	Analyze Cryptography algorithms and its need to various applications	3	2	-	3	-	-	-	-	-	-	-	3		1		3
3	CO3	Apply different Authentication mechanisms and make use of Security protocols	3	2	2	-	-	-	-	-	-	-	-	3		1		3
4	CO4	Identify different security technologies to secure WLAN	3	3	-	2	-	-	-	-	-	-	-	3		1		3
5	CO5	Awareness about the existing	2	-	-	-	-	3	2	3	1	1	-	1		1		3

		Cyber Laws and Ethics in security issues																	
		AVG	**2.8**	**1.8**	**1**	**1.2**	**1**	**3**	**2**	**3**	**1**	**1**	**-**	**2.6**	**2**	**1**	**-**	**-**
-		**Average attainment (1, 2, or 3)**																	
-	*PO, PSO*	*1.Engineering Knowledge; 2.Problem Analysis; 3.Design / Development of Solutions; 4.Conduct Investigations of Complex Problems; 5.Modern Tool Usage; 6.The Engineer and Society; 7.Environment and Sustainability; 8.Ethics; 9.Individual and Teamwork; 10.Communication; 11.Project Management and Finance; 12.Life-long Learning; S1.Software Engineering; S2.Data Base Management; S3.Web Design*																	

5. Curricular Gap and Content

Topics & contents not covered (from A.4), but essential for the course to address POs and PSOs.

Modules	Gap Topic	Actions Planned	Schedule Planned	Resources Person	PO Mapping
1	Cryptosystem	Should understand before cyber attacks		self	L3
1	Basic cryptography	Should understand cryptography		self	L3
3	MD 5 Algorithm	Should understand before SHA		Self	L3
4	ISO Layres security	Should understand before network layers security		Dr KSJ	L3
4	Dos	Should understand before DDos		Dhananjaya	L3

6. Content Beyond Syllabus

Topics & contents required (from A.5) not addressed, but help students for Placement, GATE, Higher Education, Entrepreneurship, etc.

Modules	Gap Topic	Area	Actions Planned	Schedule Planned	Resources Person	PO Mapping
5	Cyber laws	Placement, GATE, Higher Study, Entrepreneurship.	Presentation by students & Mini Project	May 1st week	NVLN Prasad Advocate	
1	Network Security	Placement, GATE, Higher Study, Entrepreneurship.	Presentation	April 3rd week	Lokesh H D .	
5	Cyber security	Placement, GATE, Higher Study, Entrepreneurship.	Presentation	May 1st week	NVLN Prasad Advocate	

C. COURSE ASSESSMENT

1. Course Coverage

Assessment of learning outcomes for Internal and end semester evaluation. Distinct assignment for each student. 1 Assignment per chapter per student. 1 seminar per test per student.

Modules	Title	Teach. Hours	No. of question in Exam						CO	Levels
			CIA-1	CIA-2	CIA-3	Asg	Extra Asg	SEE		
1	Introduction	10	2	-	-	1	1	2	CO1	L3
2	Public Key Cryptography and RSA	10	2	-	-	1	1	2	CO2	L4
3	Key Management	10	-	2	-	1	1	2	CO3	L3
4	IEEE 802.11 Wireless LAN Security	10	-	2	2	1	1	2	CO4	L3
5	IT act	10	-	-	2	1	1	2	CO5	L2
-	**Total**	**54**				**5**	**5**	**10**	**-**	**-**

2. Continuous Internal Assessment (CIA)

Assessment of learning outcomes for Internal exams. Blooms Level in last column shall match with A.2.

Modules	Evaluation	Weightage in Marks	CO	Levels
1, 2	CIA Exam – 1	30	CO1, CO2	L3,L4
3, 4	CIA Exam – 2	30	CO3,CO4	L3,L3
5	CIA Exam – 3	30	CO5	L2
1, 2	Assignment - 1	05	CO1, CO2	L3,L4
3, 4	Assignment - 2	05	CO3,CO4	L3,L3
5	Assignment - 3			
1, 2	Seminar - 1	10	CO5	L2
3, 4	Seminar - 2		-	-
5	Seminar - 3		-	-
1, 2	Quiz - 1	05	CO1, CO2	L3,L4
3, 4	Quiz - 2	05	CO3,CO4	L3,L3
5	Quiz - 3		-	-
1 - 5	Other Activities – Mini Project	-		
	Final CIA Marks	**40**	**-**	**-**

D1. TEACHING PLAN - 1

Module - 1

Title:	INTRODUCTION	Appr Time:	10 Hrs
a	***Course Outcomes***	-	**Blooms**
-	The student should be able to:	-	**Level**
1	Apply the basics of Cryptography techniques for enhancing the security	CO1	L3
b	***Course Schedule***	-	-
Class No	**Module Content Covered**	**CO**	**Level**
1	**Introduction** - Cyber Attacks, Defence Strategies and Techniques,	CO1	L3
2	Guiding Principles, Mathematical Background for Cryptography -	CO1	L3
3	Modulo Arithmetic's, The Greatest Comma Divisor,	CO1	L3
4	Useful Algebraic Structures, Chinese Remainder Theorem,	CO1	L3
5	Basics of Cryptography - Preliminaries,	CO1	L3
6	Elementary Substitution Ciphers	CO1	L3
7	Elementary Transport Ciphers Other Cipher Properties	CO1	L3
8	Secret Key Cryptography –	CO1	L3
9	Product Ciphers	CO1	L3

10	DES Construction.	CO1	L3
c	**Application Areas**	**CO**	**Level**
1	Used in secure communication: encrypting communications between us and another system.	CO1	L3
2	Manage the security of applications and systems in depth so that you can detect vulnerabilities as early as possible	CO1	L3
d	**Review Questions**	-	-
1	What is addition, multiplication and multiplicative and additive inverses modulo 8?	CO1	L3
2	Find gcd(21,300) using Euclid's algorithm.	CO1	L3
3	State Euler,s theorem	CO!	L2
4	Why modular arithmetic has been used in cryptography	CO1	L2
5	State and explain Chinese remainder theorem with an example	CO1	L3
6	List ans explain the cyber attacks	CO1	L2
7	Explain defence strategies and techniques.	CO1	L2
8	Explain all the guiding principles in security practice	CO1	L2
9	Explain rings with an examples	CO1	L3
10	Define cryptography	CO1	L2
11	Explain types of attacks	CO1	L2
12	Explain Product ciphers	CO1	L2
13	Define DES and Explain the DES construction	CO1	L3
e	**Experiences**	-	-
1			
2			

Module – 2

Title:	Public Key Cryptography and RSA	Appr Time:	10 Hrs
a	***Course Outcomes***	-	**Blooms**
-	The student should be able to:	-	**Level**
1	Analyze Cryptography algorithms and its need to various applications	CO2	L4
2			
b	***Course Schedule***	-	-
Class No	**Module Content Covered**	**CO**	**Level**
11	Public Key Cryptography and RSA – RSA Operations,	CO2	L3
12	Why Does RSA Work?, Performance,	CO2	L4
13	Applications, Practical Issues,	CO2	L4
14	Public Key Cryptography Standard (PKCS),	CO2	L4
15	Cryptographic Hash - Introduction, Properties	CO2	L3
16	Construction, Applications and Performance,	CO2	L4
17	The Birthday Attack	CO2	L2
18	Discrete Logarithm and its Applications	CO2	L2
19	Introduction, Diffie-Hellman Key Exchange	CO2	L2
20	Other Applications.	CO2	L2
c	**Application Areas**	**CO**	**Level**
1	securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures.	CO2	L4
2	Blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.	CO2	L4

d	**Review Questions**	CO2	-
14	Explain the RSA operations with example.	CO2	L3
15	Why does RSA works.	CO2	L3
16	List and explain the performance parameters of RSA	CO2	L4
17	Explain the side channel and other attacks.	CO2	L2
18	Explain Public Key Cryptography Standard (PKCS).	CO2	L2
19	Explain Generic Cryptographic hash construction	CO2	L3
20	Explain the applications of Hash	CO2	L2
21	Explain Birthday Attack	CO2	L2
22	Solve using RSA algorithm p=11, q=5,e=3 PT=9	CO2	L3
23	Explain Diffe- Hellman Key exchange	CO2	L2
e	**Experiences**	-	-
1			
2			

E1. CIA EXAM – 1

a. Model Question Paper - 1

Crs Code:	17CS61	Sem:	VI	Marks:	30	Time:	75 minutes
Course:	Cryptography and Network Security And Cyber Law						

-	-	**Note: Answer any 2 questions, each carry equal marks.**	**Marks**	**CO**	**Level**
1	a	Explain the extended euclids algorithm pseudocode along with illustration of this example b=79 and c= 12	7	CO1`	L3
	b	Explain DES algorithm(along with round function)./ orExplain Fiestel cipher structure.	8	CO1	L2
2	a	Consider the group <Z 13,*13>, is it a cyclic group. check whether 2 is a generator of Z 13.	7	CO1	L3
	b	Explain the types of elementary substitution ciphers with example.	8	CO1	L3
3	a	Perform encryption and decryption using RSA algorithms for prime numbers p=3,q=11,e=3,and message = 011101011.	7	CO2	L3
	b	Define hashing.Illustrate the properties of cryptographic hash with a neat figure.	8	CO2	L2
4	a	Perform encryption and decryption using El Gamal algorithm for a plaintext message 3 and assume p=11,g=2,receipeints private key a=5,and random number chosen by sender is 7 .	8	CO2	L3
	b	Define hashing.I llustrate the properties of cryptographic hash with a neat figure.	7	CO2	L2

b. Assignment -1

Note: A distinct assignment to be assigned to each student.

D2. TEACHING PLAN - 2

Module – 3

Title:	Key Management	Appr Time:	10 Hrs
a	***Course Outcomes***	-	**Blooms**
-	The student should be able to:	-	**Level**
1	Apply different Authentication mechanisms and make use of Security protocols	CO3	L3
2			L3

b	***Course Schedule***		
Class No	**Module Content Covered**	**CO**	**Level**
21	**Key Management** - Introduction, Digital Certificates,	CO3	L2,L3
22	Public Key Infrastructure, Identity–based Encryption,	CO3	L3
23	Authentication–I - One way Authentication, Mutual Authentication	CO3	L3
24	Dictionary Attacks, Authentication – II – Centalised Authentication,	CO3	L3
25	The Needham-Schroeder Protocol, Kerberos, Biometrics,	CO3	L3
26	PSec- Security at the Network Layer – Security at Different layers	CO3	L2,L3
27	I: Pros and Cons, IPSec in Action, Internet Key Exchange (IKE) Protocol,	CO3	L3
28	Security Policy and IPSEC, Virtual Private Networks,	CO3	L3
29	Security at the Transport Layer - Introduction, SSL Handshake Protocol	CO3	L3
30	SSL Record Layer Protocol, OpenSSL.	CO3	L3
c	**Application Areas**	**CO**	**Level**
1	Classify various Algorithms and protocols to be used at various TCP/IP Layers & to operate Digital Signature in Real World Situation	CO3	L3
2	Students will be able analyze protocols for various security objectives with cryptographic tools	CO3	L3
d	**Review Questions**	CO3	-
24	Explain the types of PKI Architecture.	CO3	L2
25	Explain the identity-based encryption.	CO3	L2
26	explain mutual authentication methods(	CO3	L3
27	Demonstrate the working of a Kerberos protocol with a neat figure.	CO3	L3
28	Explain Needham Schroeder protocol version 1 and 2 along with the attacks launched on these versions.	CO3	L3
29	Explain IPSec protocols in transport mode with a neat diagram.	CO3	L3
30	Explain IKE phase 1 main mode protocol with description of messages exchanged between the entities.	CO3	L2
31	Explain SSL handshake protocol. /how a client and a server communicate using SSL handshake protocol	CO3	L2
32	Explain SSL record layer protocol with a neat figure.	CO3	L3
e	**Experiences**	-	-
1			
2			

Module – 4

Title:	IEEE 802.11 Wireless LAN Security	Appr Time:	10 Hrs
a	***Course Outcomes***	-	**Blooms**
-	The student should be able to:	-	**Level**
1	Identify different security technologies to secure WLAN	CO4	L3
2			
b	***Course Schedule***		
Class No	**Module Content Covered**	**CO**	**Level**
31	**IEEE 802.11 Wireless LAN Security** - Background, Authentication,	CO4	L2
32	Confidentiality and Integrity, Viruses, Worms, and Other Malware,	CO4	L2
33	Firewalls – Basics, Practical Issues,	CO4	L2
34	Intrusion Prevention and Detection - Introduction,	CO4	L3
35	Prevention Versus Detection,	CO4	L3
36	Types of Instruction Detection Systems,	CO4	L3
37	DDoS Attacks Prevention/Detection,	CO4	L3
38	Web Service Security – Motivation,	CO4	L3
39	Technologies for Web Services,	CO4	L3

40	WS- Security, SAML, Other Standards.	CO4	L3
c	**Application Areas**	**CO**	**Level**
1	Wireless LAN provides a solutions complete network visibility to help successfully manage a network's wireless life cycle.	CO4	L2
2	Some standard provides a framework for encrypting and decrypting entire XML documents or just portions of an XML document.	CO4	L3
d	**Review Questions**	CO4	-
33	Explain the infrastructure of WLAN/wireless LAN .	CO4	L2
34	Explain key hierarchy and four way handshake protocol in 802.11i	CO4	L2
35	Explain the classification /types of firewalls based on the processing modes.	CO4	L2
36	Explain IP traceback using Probablistic Packet marking and packet logging with an example.	CO4	L3
37	Explain entities involved in web services	CO4	L3
38	Explain XML signature elements and sub elements with an example code	CO4	L3
e	**Experiences**	-	-
1			
2			

E2. CIA EXAM – 2

a. Model Question Paper - 2

Crs Code:	17CS61	Sem:	6	Marks:	30	Time:	75 minutes
Course:	Cryptography and Network Security And Cyber Law						

-	-	**Note: Answer any 2 questions, each carry equal marks.**	**Marks**	**CO**	**Level**
1	a	Explain the format of X.509 certificate with a neat figure.	7	CO3	L2
	b	Explain one-way authentication method OR password-based authentication technique.	8	CO3	L2
2	a	Explain IKE phase 1 main modeprotocol with description of messages exchanged between the entities.	7	CO3	L3
	b	Explain SSL handshake protocol. /how a client and a server communicate using SSL handshake protocol	8	CO3	L3
3	a	Explain the infrastructure of WLAN/wireless LAN .	7	CO4	L2
	b	Explain the significance of DMZ in placement of firewall with a neat diagram.	8	CO4	L3
4	a	Explain IP traceback using Probablistic Packet marking and packet logging with an example.	7	CO4	L3
	b	Explain XML signature elements and sub elements with an example code	8	CO4	L3

b. Assignment – 2

Note: A distinct assignment to be assigned to each student.

D3. TEACHING PLAN – 3

Module – 5

Title:	IT act aim and objectives	Appr Time:	10 Hrs
a	***Course Outcomes***	-	**Blooms**
-	The student should be able to:	-	**Level**
1	Awareness about the existing Cyber Laws and Ethics in security issues	L2	L2
2			L2
b	***Course Schedule***		
Class No	**Module Content Covered**	**CO**	**Level**
41	**IT act aim and objectives**, Scope of the act, Major Concepts,	CO5	L2
42	Important provisions, Attribution, acknowledgement,	CO5	L2

43	and dispatch of electronic records,	CO5	L2
44	Secure electronic records and secure digital signatures,	CO5	L2
45	Regulation of certifying authorities: Appointment of Controller and Other officers,	CO5	L2
46	Digital Signature certificates, Duties of Subscribers,	CO5	L2
47	Penalties and adjudication,	CO5	L2
48	The cyberregulations appellate tribunal,	CO5	L2
49	Offences, Network service providers not to be liable in certain case	CO5	L2
c	**Application Areas**	**CO**	**Level**
1	The goal of E-commerce technology is to give a secure, convenient and immediate payment facility to the users over the Internet.	CO5	L2
d	**Review Questions**	-	-
39	Explain any four important provisions of IT act 2000	CO5	L2
40	Discuss the penalties and adjudication under section 43 IT act 2000 for a) Damage to computer, computer system b) Failure to protect data. c) Failure to furnish information return	CO5	L2
41	Define the following terms: 1. Certifying Authority b)Addressee c) Digital signature d)Public key	CO5	L2
42	Explain offense ,punishments ,penalties under IT act 2000.	CO5	L2
43	Explain aim and objectives of IT act 2000.	CO5	L2
7	**Experiences**	-	-
1			
2			

E3. CIA EXAM – 3

a. Model Question Paper - 3

Crs Code:	17CS61	Sem:	VI	Marks:	30	Time:	75 minutes
Course:	Cryptography and Network Security And Cyber Law						

-	-	**Note: Answer any 2 questions, each carry equal marks.**	**Marks**	**CO**	**Level**
1	a	Describe the role of certifying authority with regard to issuing digital certificate and Representation upon issuance,suspension .	7	CO5	L2
	b	Describe the duties of subscriber under the section 40, 41, and 42 of IT act 2000	8	CO5	L2
2	a	Discuss the penalties and adjudication under section 43 IT act 2000 for a) Damage to computer, computer system b) Failure to protect data. c) Failure to furnish information return	10	CO5	L2
	b	Who is a controller? Outline his functions as a controller.	5	CO5	L2
3	a	Explain offense ,punsishments ,penalties under IT act 2000.	7	CO5	L2
	b	Describe the duties of subscriber under the section 40, 41, and 42 of IT act 2000	8	CO5	L2
4	a	Define the following terms: 1. Certifying Authority b)Addressee c) Digital signature d)Public key	8	CO5	L2
	b	Describe the role of certifying authority with regard to issuing digital certificate and Representation upon issuance,suspension .	7	CO5	L2

b. Assignment – 3

Note: A distinct assignment to be assigned to each student.

F. EXAM PREPARATION

1. University Model Question Paper

Course:	Cryptography and Network Security And Cyber Law	Month / Year	2015

Crs Code:	17CS61	Sem:	6	Marks:	80	Time:	180 minutes

-	Note	Answer all FIVE full questions.	Marks	CO	Level
1	a	List and explain the various types of vulnerabilities with common cyber attacks	8	CO1	L2
	b	Encrypt the plaijn text “cryptography” using hill cipher technique with key matrix K=[9 4] [5 7]	8	CO1	L3
		OR			
2	a	Distinguish between: a)[confusion and diffusion ciphers. b)?Block cipher and stream cipher	8	CO1	L2
	b	With neat diagram schematic explain single round of DES encryption model.	8	CO1	L2
3	a	In RSA system, it is given p=3, q=11,l=7 and M= 5 Find the cipher text ‘C’ and also find the message ‘m’ from decryption	8	CO2	L3
	b	Define Hash Function. Explain the construction of generic cryptography Hash	8	CO2	L2
		OR			
4	a	With a neat diagram explain the proccess of computing Hash function using SHA-1 algorithm	8	CO2	L2
	b	Explain the working of Diffie-Hellman key exchange protocol	8	CO2	L2
5	a	What is digital certificate? Explain the X.509 digital certificate format	8	CO3	L2
	b	Distinguish working of Diffie-Hellman key exchange protocol	8	CO3	L3
		OR			
6	a	Assume a client ‘C’ wants to communicate with server ‘S’ using kerberos protocol. How can it be achived	8	CO3	L3
	b	What is secure socket layer? Explain SSL handshake protocols	8	CO3	L2
7	a	What is intrusion detection system(IDS)? Explain different types of IDS.	6	CO4	L2
	b	Explain how 802.11i provides message confidentiality and integrity.	5	CO4	L3
		OR			
	c	Explain the characteristics of virus and worm	5	CO4	L2
8	a	What is WS-security? Explain the various types of WS-security	5	CO4	L2
	b	Explain the prevention and detection methods on DDOS attack.	6	CO4	L3
	c	List and explain any two technologies used for web services.	5	CO7	L3
9	a	List and explain the objectives and scope of IT Act	8	CO5	L2
	b	Explain the process of issuing digital signature certificate and revocation of digital certificate by certifying authority	8	CO5	L2
		OR			
10	a	Explain he various offences and punishment on cyber crime	8	CO5	L2
	b	Explain the process of attribution, acknowledgement and dispatch of electronic record	8	CO5	L2

2. SEE Important Questions

Course:	Cryptography and Network Security And Cyber Law					Month / Year	
Crs Code:	17CS61	Sem:	6	Crs Code:	17CS61	Sem:	6

	Note	Answer all FIVE full questions. All questions carry equal marks.	-	-	
Module	Qno.		Marks	CO	Year
1	1	Explain the motives of launching cyber attacks.	8	Co1	
1	2	Explain the types of attacks/common attacks launched /high profile attacks.	8	CO1	
1	3	Define vulnerability. Explain the types of vulnerabilities in the domain of Security.	8	CO1	
1		Briefly explain the defence strategies and techniques deployed to overcome network attacks.	8	CO1	

1	4	Explain access control,authentication and authorization.	8	CO1	
1	5	Explain the guiding principles in security practice.	8	CO1	
11	6	Explain the properties of modulo arithmetic.	7	CO1	
1		Solve using euclids algorithm for gcd(161,112)	8	CO1	
1	7	Explain the extended euclids algorithm pseudocode along with illustration of this example b=79 and c= 12 Or Find the inverse of 12 modulo 79.	8	CO1	
1	8	Define group and explain the properties of group.	8	CO1	
1	9	Define lagranges theorem,eulers, fermats little theorem.	8	CO1	
1	10	Consider the group <Z 13,*13>, is it a cyclic group. check whether 2 is a generator of Z 13.	7	CO1	
1	11	Explain Chinese remainder theorem.	5	CO1	
1	12	Define a)cryptography b) ciphertext c) encryption d)decryption e)kerchoffs principle.	10	CO1	
1	13	Bring out the difference between secret key cryptography and public key cryptography.	6	CO1	
2	14	Explain known ciphertext attack with a pseudocode.	6	CO1	
2	15	Explain the types of elementary substitution ciphers with example.	8	CO1	
2	16	Explain monoalphabetic ciphers with example.	6	CO1	
2	17	Explain all polyalphabetic ciphers methods with an example.	8	CO1	
2	18	Explain hill cipher ,vigenere cipher and one time pad cipher methods with example.	8	CO1	
2	19	What are transposition ciphers. explain the working of it with an example	8	CO1	
2	20	Differentiate between confusion and diffusion.	6	CO1	
2	21	Write a note on stream and block cipher.	5	CO1	
2	22	Demonstrate the working of a product cipher with a neat figure. OR Explain Three Round SPN Network	8	CO1	
2	23	Explain DES algorithm(along with round function)./ orExplain Fiestel cipher structure.	7	CO1	
2	24	Explain S- box implementation using table look up,(substitution in round function)	6	CO1	
2	25	Explain RSA operations/ RSA key generation/algorithm/RSA encryption and decryption	5	CO2	
2	26	Perform encryption and decryption using RSA algorithms for prime numbers p=3,q=11,e=3,and message = 011101011.	8	CO2	
2	27	Explain RSA applications and performance.	5	CO2	
2	28	Explain weak and strong collision attack.	5	CO2	
2	29	Define hashing.Illustrate the properties of cryptographic hash with a neat figure.	8	CO2	
2	30	Explain attack complexity OR weak collision and strong collision resistance with a pseudocose/program	6	CO2	
2	31	Explain the computation of generic cryptographic hash with a neat figure	7	CO2	
2	32	Explain MAC / message authentication code. // (refer notes :explain the introduction part of HMAC)	5	CO2	
2	33	Explain HMAC OR (Hash Based Message Authentication Code).	6	CO2	
2	34	Explain the computation of hash using SHA-1 OR SECURE HASH ALGORITHM -1.	7	CO2	
2	35	Explain birthday analogy and attack.	5	CO2	
2	36	Perform encryption and decryption using El Gamal algorithm for a plaintext message 3 and assume p=11,g=2,receipeints private key a=5,and random number chosen by sender is 7 .	8	CO2	
2	37	Explain man in the middle attack on Diffie hellman key exchange	6	CO2	

		algorithm.			
3	38	Explain the format of X.509 certificate with a neat figure.	6	CO3	
3	39	Explain public key infrastructure or functions of PKI	7	CO3	
3	40	Explain authentication and key agreement using session key.	6	CO3	
3	41	Explain Needham Schroeder protocol version 1 and 2 along with the attacks launched on these versions.	8	CO3	
3	42	Demonstrate the working of a Kerberos protocol with a neat figure.	8	CO3	
3	43	Explain SSL handshake protocol. /how a client and a server communicate using SSL handshake protocol	8	CO3	
4	44	Explain authentication in WEP and 802.11i.	8	CO4	
4	45	Explain MAC generation and encryption in CCMP protocol with a neat schematic diagram.	8	CO4	
4	46	Explain Email And P2p Worms or explain topological worms.	5	CO4	
4	47	Explain IP traceback using Probablistic Packet marking and packet logging with an example.	7	CO4	
4	48	Explain the types of Intrusion detection system .	8	CO4	
4	49	Explain DDos attack detection and prevention methods.	8	CO4	
4	50	Explain XML signature elements and sub elements with an example code	8	CO4	
5	51	Describe the role of certifying authority with regard to issuing digital certificate and Representation upon issuance,suspension	8	CO5	
5	52	Who is a controller? Outline his functions as a controller.	8	CO5	
5	53	Discuss the penalties and adjudication under section 43 IT act 2000 for a) Damage to computer, computer system b) Failure to protect data. c) Failure to furnish information return	6	CO5	
5	54	Describe the duties of subscriber under the section 40, 41, and 42 of IT act 2000	8	CO5	
5	55	Define the following terms: 1. Certifying Authority b)Addressee c) Digital signature d)Public key	8	CO5	
5	56	Explain offense ,punsishments ,penalties under IT act 2000.	8	CO5	
5	57	Explain aim and objectives of IT act 2000.	5	CO5	