Ref No:

Sri Krishna Institute of Technology,
Bangalore

COURSE PLAN

Academic Year 2019-2020

Program:	INFORMATION SCIENCE AND ENGINEERING
Semester :	VI
Course Code:	17CS61
Course Title:	CRYPTOGRAPHY AND NETWORK SECURITY
Credit / L-T-P:	2-2-0
Total Contact Hours:	50
Course Plan Author:	Shruti B P

Academic Evaluation and Monitoring Cell

Sri Krishna Institute of Technology
#29,Chimney hills,Hesaraghata Main road, Chikkabanavara Post
Bangalore – 560090, Karnataka, INDIA
Phone / Fax :08023721477/28392221/23721315
Web: www.skit.org.in , e-mail: skitprinci@gmail.com

Table of Contents

A. COURSE INFORMATION

1. Course Overview

Degree:	B E	Program:	IS
Semester:	6	Academic Year:	2019-20
Course Title:	Cryptography and Network Security	Course Code:	17CS61
Credit / L-T-P:	4/4-0-0	SEE Duration:	180 Min
Total Contact Hours:	50	SEE Marks:	60
CIA Marks:	40	Assignment	10
Course Plan Author:	Shruti B P	Sign ..	
Checked By:		Sign ..	
CO Targets	CIA Target :92	SEE Target:	58.4

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.

Module	Content	Teaching Hours	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	L3
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	L3
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, IPSec- 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	L4
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	L4
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	10	L2

	adjudication, The cyberregulations appellate tribunal, Offences, Network service providers not to be liable in certain cases, Miscellaneous Provisions.		
-	**Total**		

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	Cryptography, Network Security and Cyber Laws – Bernard Menezes, Cengage Learning, 2010 edition		In Lib
B	**Reference books (Title, Authors, Edition, Publisher, Year.)**	**-**	**-**
1	Cryptography and Network Security- Behrouz A Forouz an, Debdeep Mukhopadhyay, Mc-GrawHill, 3rd Edition, 2015		In Dept
2	Cryptography and Network Security- William Stalling s, Pearson Education, 7 th Edition		In Dept
3	Cyber Law simplified- Vivek Sood, Mc-GrawHill, 11 th reprint , 2013		In Dept
4	Cyber security and Cyber Laws, Alfred Basta, Nadine Basta, Mary brown, ravindra kumar, Cengage learning		In Dept
C	**Concept Videos or Simulation for Understanding**	**-**	**-**
C1	https://www.youtube.com/watch?v=SCvtxjpVQms&list=PL71FE85723FD414D7&index=3		
C2	https://www.youtube.com/watch?v=UliGdYl-nzI		
C3	https://www.youtube.com/watch?v=H1GS99J2fvs		
C4	https://www.youtube.com/watch?v=gyCj3Psau-g		
C5	https://www.youtube.com/watch?v=F7mH5vz1qEI		
D	**Software Tools for Design**	**-**	**-**
E	**Recent Developments for Research**	**-**	**-**
F	**Others (Web, Video, Simulation, Notes etc.)**	**-**	**-**
	http://www.diginotes.in/notescsesem6.html		
	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	15CS52	Computer Networks	Connection-Oriented Transport TCP, IPv6,A Brief foray into IP Security, Network Support for Multimedia	5		L2,L3

2	15CS43	Design and Analysis of Algorithm	Basic knowledge of algorithms	4		L2
3	15CS41	Maths	To know the importance of learning theories and strategies in Mathematic	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

B. OBE PARAMETERS

1. Course Outcomes

Expected learning outcomes of the course, which will be mapped to POs.

Modules	Course Code.#	Course Outcome **At the end of the course, student should be able to . . .**	Teach. Hours	Instr Method	Assessment Method	Blooms' Level
1	15CS61.1	Understand the fundamental concepts of Cyber security	10	Lecture / PPT,	Lecture / PPT,	L2,L3
2	15CS61.2	Students will be able to solve and relate mathematical concepts behind the cryptographic algorithms	10	Lecture / PPT, problem solving	Lecture / PPT, problem solving	L3
3	15CS61.3	Apply different Key management techniques in cryptographic applications	10	Discussion, lecture, ppt	Discussion, lecture, ppt	L4
4	15CS61.4	Classify various Algorithms and analyze protocols to be used at various TCP/IP Layers & to operate Digital Signature in Real World Situation	10	Lecture, discussion	Lecture, discussion	L4
5	15CS61.5	Awareness about the existing Cyber Laws and Ethics in security issues	10	Discussion, lecture , PPT	Discussion, lecture , PPT	L3
-	**-**	**Total**	**40**	**-**	**-**	**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
2	Manage the security of applications and systems in depth so that you can detect vulnerabilities as early as possible	CO2	L2
3	securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures.	CO3	L3
4	Blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.	CO3	L2
5	Digital signatures can be used to authenticate the source of messages.	CO3	L4
6	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.	CO3	L4
7	Wireless LAN provides a solutions complete network visibility to help successfully manage a network's wireless life cycle.	CO4	L2
8	Some standard provides a framework for encrypting and decrypting entire XML documents or just portions of an XML document.	CO4	L4
9	The goal of E-commerce technology is to give a secure, convenient and immediate payment facility to the users over the Internet.	CO4	L3

3. 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	15CS61.1	Understand the fundamental concepts of Cyber security	**3**	**3**	2	**1**	**1**							**1**	**3**	**2**	1	L2,L3
2	15CS61.2	Students will be able to solve and relate mathematical concepts behind the cryptographic algorithms	**3**	**3**	**2**	-	-	-	-	-	-	-	-	**1**	**3**	**2**	1	L3
3	15CS61.3	Apply different Key management techniques in cryptographic applications	**3**	**3**	-	**2**	-	-	-	-	-	-	-	**1**	**3**	**2**	-	L4
4	15CS61.4	Classify various Algorithms and analyze protocols to be used at various TCP/IP Layers & to operate Digital Signature in Real World Situation	**3**	**3**	-	**2**	-	-	-	-	-	-	-	**1**	**3**	**3**	-	L4
5	15CS61.5	Awareness about the existing Cyber Laws and Ethics in security issues	**3**	3	-	-	-	**1**	**2**	**2**	**1**	**1**	-	**1**	**3**	-	-	L3
-	**17CS61**	Average	**3**	**3**	**2**	**2**	**1**	**1**	**2**	**2**	**1**	**1**		**1**	**3**	**2**	**1**	**-**
-	*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*															

4. Curricular Gap and Content

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

Mod	Gap Topic	Actions Planned	Schedule Planned	Resources Person	PO Mapping

ules					
1		Seminar	2nd week / date	Dr XYZ, Inst	List from B4 above
2		Seminar	3rd Week		

C. COURSE ASSESSMENT

1. Course Coverage

Assessment of learning outcomes for Internal and end semester evaluation.

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	L3
3	Key Management	10	-	2	-	1	1	2	CO3	L4
4	IEEE 802.11 Wireless LAN Security	10	-	2	2	1	1	2	CO4	L4
5	IT act	10	-	-	2	1	1	2	CO5	L2
-	**Total**	**50**	**4**	**4**	**4**	**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	L2, L3,
3, 4	CIA Exam – 2	30	CO2,CO3	L4, L2
5	CIA Exam – 3	30	CO4,CO5	L2, L3
1, 2	Assignment - 1	10	CO1, CO2	L2, L3,
3, 4	Assignment - 2	10	CO2,CO3	L4, L2
5	Assignment - 3	10	CO4,CO5	L2, L3
1, 2	Seminar - 1	-	-	-
3, 4	Seminar - 2	-	-	-
5	Seminar - 3	-	-	-
1, 2	Quiz - 1	-	-	-
3, 4	Quiz - 2	**40**	**-**	**-**
5	Quiz - 3		-	-
1 - 5	Other Activities – Mini Project	-		
	Final CIA Marks		**-**	**-**

D1. TEACHING PLAN - 1

Module - 1

Title:		Appr Time:	10 Hrs
a	***Course Outcomes***	**CO**	**Blooms**
	The student should be able to:		
1	Understand the fundamental concepts of Cyber security	CO1	L2,L3
b	***Course Schedule***	-	-

Class No	Portion covered per hour	-	-
1	**Introduction** - Cyber Attacks, Defence Strategies and Techniques,	CO1	L2
2	Guiding Principles, Mathematical Background for Cryptography -	CO1	L2
3	Modulo Arithmetic's, The Greatest Comma Divisor,	CO1	L2
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**		
-	Students should be able employ / apply the Module learnings to . . .		
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	CO2	L2
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	CO1	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	L2
e	**Experiences**	-	-
1			
2			

Module – 2

Title:		Appr Time:	10 Hrs
a	***Course Outcomes***	**CO**	**Blooms**
-		-	**Level**
	The student should be able to:		
1	Students will be able to solve and relate mathematical concepts behind the cryptographic algorithms	CO2	L3
b	***Course Schedule***	-	-
Class No	**Portion covered per hour**	**-**	**-**
1	Public Key Cryptography and RSA – RSA Operations,	CO2	L3
2	Why Does RSA Work?, Performance,	CO2	L3

3	Applications, Practical Issues,	CO2	L3
4	Public Key Cryptography Standard (PKCS),	CO2	L3
5	Cryptographic Hash - Introduction, Properties	CO2	L3
6	Construction, Applications and Performance,	CO2	L3
7	The Birthday Attack	CO2	L2
8	Discrete Logarithm and its Applications	CO2	L2
c	**Application Areas**	**-**	**-**
-	Students should be able employ / apply the Module learnings to . . .	-	-
1	securing cryptographic techniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures.	CO2	L3
2	Blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.	CO2	L2
d	**Review Questions**	-	-
-			
1	Explain the RSA operations with example.	CO3	L3
2	Why does RSA works.	CO3	L3
3	List and explain the performance parameters of RSA	CO3	L3
4	Explain the side channel and other attacks.	CO3	L2
5	Explain Public Key Cryptography Standard (PKCS).	Co3	L2
6	Explain Generic Cryptographic hash construction	CO3	L3
7	Explain the applications of Hash	CO3	L2
8	Explain Birthday Attack	CO3	L2
9	Solve using RSA algorithm p=11, q=5,e=3 PT=9	CO3	L3
10	Explain Diffe- Hellman Key exchange	CO3	L2
e	**Experiences**	-	-
1		CO3	L2
2			

E1. CIA EXAM – 1

a. Model Question Paper - 1

Crs Code:	18CS43	Sem:	6	Marks:	40	Time:	90 mins
Course:	Operating System						

-	-	**Note: Answer all questions, each carry equal marks. Module : 1, 2**	**Marks**	**CO**	**Level**

b. Assignment -1

Model Assignment Questions							
Crs Code:	18CS43	Sem:	4	Marks:	10	Time:	
Course:	Operating System						

SNo	Assignment Description	Marks	CO	Level
1	Define vulnerability. Explain the types of vulnerabilities in the domain of Security.		CO1	L2
2	Explain access control,authentication and authorization.		CO1	L2
3	Define a)cryptography b) ciphertext c) encryption d)decryption e)kerchoffs principle.		CO1	L2
4	Explain Three Round SPN Network /		CO1	L2
5	Consider the group <Z 13,*13>, is it a cyclic group. check whether 2 is a generator of Z 13.		CO2	L3
6	Bring out the difference between secret key cryptography and public key cryptography.		CO2	L2
7	Perform encryption and decryption using RSA algorithms for prime numbers p=3,q=11,e=3,and message = 011101011.		CO2	L3
8	Explain the computation of hash using SHA-1 OR SECURE HASH ALGORITHM -1.		CO2	L2
9	Explain Digital signature .		CO2	L2
10	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 .		CO2	L3
11	Explain MAC / message authentication code. // (refer notes :explain the introduction part of HMAC)		CO2	L4
12	Explain birthday analogy and attack.		CO2	L2
13	Explain the extended euclids algorithm pseudocode along with illustration of this example b=79 and c= 12		CO2	L3
14	Define lagranges theorem,eulers, fermats little theorem.		CO2	L3

D2. TEACHING PLAN - 2

Module – 3

Title:	Deadlocks and Memory management	Appr Time:	10 Hrs
a	***Course Outcomes***	**CO**	**Blooms**
-	At the end of the topic the student should be able to . . .	-	**Level**
1	Apply different Key management techniques in cryptographic applications	CO3	L4
b	***Course Schedule***		
Class No	**Portion covered per hour**	**-**	**-**
1	**Key Management** - Introduction, Digital Certificates,	CO3	L2,L4
2	Public Key Infrastructure, Identity–based Encryption,	CO3	L4
3	Authentication–I - One way Authentication, Mutual Authentication	CO3	L4
4	Dictionary Attacks, Authentication – II – Centalised Authentication,	CO3	L4
5	The Needham-Schroeder Protocol, Kerberos, Biometrics,	CO3	L4

6	PSec- Security at the Network Layer – Security at Different layers	CO3	L2,L4
7	I: Pros and Cons, IPSec in Action, Internet Key Exchange (IKE) Protocol,	CO3	L4
8	Security Policy and IPSEC, Virtual Private Networks,	CO3	L4
9	Security at the Transport Layer - Introduction, SSL Handshake Protocol	CO3	L4
10	SSL Record Layer Protocol, OpenSSL.	CO3	L4
c	**Application Areas**	**-**	**-**
-	Students should be able employ / apply the Module learnings to . . .	-	-
1	Classify various Algorithms and protocols to be used at various TCP/IP Layers & to operate Digital Signature in Real World Situation	CO3	L4
2	Students will be able analyze protocols for various security objectives with cryptographic tools	CO3	L4
d	**Review Questions**	-	-
-	The attainment of the module learning assessed through following questions		
1	Explain the types of PKI Architecture.	CO3	L2
2	Explain the identity-based encryption.	CO3	L2
3	explain mutual authentication methods(	CO3	L4
4	Demonstrate the working of a Kerberos protocol with a neat figure.	CO3	L4
5	Explain Needham Schroeder protocol version 1 and 2 along with the attacks launched on these versions.	CO3	L4
6	Explain IPSec protocols in transport mode with a neat diagram.	CO3	L4
7	Explain IKE phase 1 main mode protocol with description of messages exchanged between the entities.	CO3	L2
8	Explain SSL handshake protocol. /how a client and a server communicate using SSL handshake protocol	CO3	L2
9	Explain SSL record layer protocol with a neat figure.	CO3	L3
e	**Experiences**	-	-
1			
2			

Module – 4

Title:	Virtual Memory Management:	Appr Time:	10 Hrs
a	***Course Outcomes***	**CO**	**Blooms**
-	At the end of the topic the student should be able to . . .	-	**Level**
1	Classify various Algorithms and analyze protocols to be used at various TCP/IP Layers & to operate Digital Signature in Real World Situation	CO4	L2
b	***Course Schedule***		
Class No	**Portion covered per hour**	**-**	**-**
1	**IEEE 802.11 Wireless LAN Security** - Background, Authentication,	CO4	L2
2	Confidentiality and Integrity, Viruses, Worms, and Other Malware,	CO4	L2
3	Firewalls – Basics, Practical Issues,	CO4	L2
4	Intrusion Prevention and Detection - Introduction,	CO4	L4
5	Prevention Versus Detection,	CO4	L4
6	Types of Instruction Detection Systems,	CO4	L4
7	DDoS Attacks Prevention/Detection,	CO4	L4
8	Web Service Security – Motivation,	CO4	L4
9	Technologies for Web Services,	CO4	L4

10	WS- Security, SAML, Other Standards.	CO4	L4
c	**Application Areas**	**-**	**-**
-	Students should be able employ / apply the Module learnings to . . .	-	-
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	L4
d	**Review Questions**	-	-
-	The attainment of the module learning assessed through following questions	-	-
1	Explain the infrastructure of WLAN/wireless LAN .	CO4	L2
2	Explain key hierarchy and four way handshake protocol in 802.11i	CO4	L2
3	Explain the classification /types of firewalls based on the processing modes.	CO4	L2
4	Explain IP traceback using Probablistic Packet marking and packet logging with an example.	CO4	L4
5	Explain entities involved in web services	CO4	L4
6	Explain XML signature elements and sub elements with an example code	CO4	L4
e	**Experiences**	-	-
1			
2			

E2. CIA EXAM – 2

a. Model Question Paper - 2

Crs Code:	18CS43	Sem:	4	Marks:	40	Time:	90 mins
Course:	Operating System						

-	-	**Note: Answer all questions, each carry equal marks. Module : 3, 4**	**Marks**	**CO**	**Level**

b. Assignment – 2

Model Assignment Questions							
Crs Code:	18CS43	Sem:	6	Marks:	10	Time:	
Course:	Operating System						

SNo	**Assignment Description**	**Marks**	**CO**	**Level**

1	Demonstrate the working of a Kerberos protocol with a neat figure.		CO3	L4
2	What are dictionary attacks and how an attacker would implement this attack.		CO3	L4
3	Explain key hierarchy and four way handshake protocol in 802.11i		CO3	L2
4	Explain the characteristics /features of virus and worms.		CO3	L2
5	Explain Email And P2p Worms or explain topological worms.		CO3	L2
6	Explain the types of Intrusion detection system .		CO3	L2
	Explain IKE phase 1 main modeprotocol with description of messages exchanged between the entities.		CO3	L4
7	Explain SSL handshake protocol. /how a client and a server communicate using SSL handshake protocol		CO3	LL4
8	Explain IP traceback using Probablistic Packet marking and packet logging with an example.		CO4	L4
9	Explain XML signature elements and sub elements with an example code		CO4	L4
10	Explain SAML and assertion types.		CO4	L2
11	Write a note on XML with an example.		CO4	L4
12	Demonstrate the working of a Kerberos protocol with a neat figure.		CO4	L4

D3. TEACHING PLAN - 3

Module – 5

Title:	Secondary Storage Structures, Protection	Appr Time:	10 Hrs
a	***Course Outcomes***	**CO**	**Blooms**
-	At the end of the topic the student should be able to . . .	-	**Level**
1	Awareness about the existing Cyber Laws and Ethics in security issues	CO5	L3
b	***Course Schedule***	-	-
Class No	**Portion covered per hour**	**-**	**-**
1	**IT act aim and objectives**, Scope of the act, Major Concepts,	CO5	L2
2	Important provisions, Attribution, acknowledgement,	CO5	L2
3	and dispatch of electronic records,	CO5	L2
4	Secure electronic records and secure digital signatures,	CO5	L3
5	Regulation of certifying authorities: Appointment of Controller and Other officers,	CO5	L3
6	Digital Signature certificates, Duties of Subscribers,	CO5	L3
7	Penalties and adjudication,	CO5	L2
8	The cyberregulations appellate tribunal,	CO5	L2
9	Offences, Network service providers not to be liable in certain case	CO5	L3
10	Miscellaneous Provisions	CO5	L2
c	**Application Areas**	**-**	**-**
-	Students should be able employ / apply the Module learnings to . . .	-	-
1	The goal of E-commerce technology is to give a secure, convenient and immediate payment facility to the users over the Internet.	CO5	L3
d	**Review Questions**	-	-
-	The attainment of the module learning assessed through following questions	-	-
1	Explain any four important provisions of IT act 2000	CO5	L2
2	Discuss the penalties and adjudication under section 43 IT act 2000 for a) Damage to computer, computer system	CO5	L2

	b) Failure to protect data. c) Failure to furnish information return		
3	Define the following terms: 1. Certifying Authority b)Addressee c) Digital signature d)Public key	CO5	L2
4	Explain offense ,punsishments ,penalties under IT act 2000.	CO5	L2
5	Explain aim and objectives of IT act 2000.	CO5	L2
e	**Experiences**	-	-
1			
2			

E3. CIA EXAM – 3

a. Model Question Paper - 3

Crs Code	18CS43	Sem:	4	Marks:	40	Time:	90 mins
Course:	Operating System						

-	-	**Note: Answer all questions, each carry equal marks. Module : 5**	**Marks**	**CO**	**Level**

b. Assignment – 3

Model Assignment Questions							
Crs Code:		Sem:		Marks:		Time:	
Course:							

SNo	**Assignment Description**	**Marks**	**CO**	**Level2**
1	Explain any four important provisions of IT act 2000		CO5	L2
2	What is IT ACT? Discuss its aim		CO5	L2
3	Describe the duties of subscribers		CO5	L2
4	Describe the role of certifying authority with regard to issuing digital certificate and Representation upon issuance,suspension .		CO5	L2
5	Who is a controller? Outline his functions as a controller		CO5	L2
6	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
7	Describe the duties of subscriber under the section 40, 41, and 42 of IT act 2000		CO5	L2

8	Define the following terms: 1. Certifying Authority b)Addressee c) Digital signature d)Public key		CO5	L2
9	Explain offense ,punsishments ,penalties under IT act 2000.		CO5	L2
10	Explain aim and objectives of IT act 2000.		CO5	L2

F. EXAM PREPARATION

1. University Model Question Paper

Course:		Cryptography and Network Security And Cyber Law					Month / Year	2015	
Crs Code:		15CS61	Sem:	VI	Marks:	80	Time:	180 minutes	
Module		Answer all FIVE full questions. All questions carry equal marks.					**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	CO2	L3
		OR							
2	a	Distinguish between: a)[confusion and diffusion ciphers. b)?Block cipher and stream cipher					8	CO2	L2
	b	With neat diagram schematic explain single round of DES encryption model.					8	CO2	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	CO3	L3
	b	Define Hash Function. Explain the construction of generic cryptography Hash					8	CO3	L2
		OR							
4	a	With a neat diagram explain the proccess of computing Hash function using SHA-1 algorithm					8	CO3	L2
	b	Explain the working of Diffie-Hellman key exchange protocol					8	CO3	L2
5	a	What is digital certificate? Explain the X.509 digital certificate format					8	CO4	L2
	b	Distinguish working of Diffie-Hellman key exchange protocol					8	CO4	L4
		OR							
6	a	Assume a client ‘C’ wants to communicate with server ‘S’ using kerberos protocol. How can it be achived					8	CO4	L4
	b	What is secure socket layer? Explain SSL handshake protocols					8	CO4	L2
7	a	What is intrusion detection system(IDS)? Explain different types of IDS.					6	CO5	L2
	b	Explain how 802.11i provides message confidentiality and integrity.					5	CO5	L4
		OR							
	c	Explain the characteristics of virus and worm					5	CO5	L2
8	a	What is WS-security? Explain the various types of WS-security					5	CO5	L2
	b	Explain the prevention and detection methods on DDOS attack.					6	CO5	L4
	c	List and explain any two technologies used for web services.					5	CO5	L3

9	a	List and explain the objectives and scope of IT Act	8	CO6	L2
	b	Explain the process of issuing digital signature certificate and revocation of digital certificate by certifying authority	8	CO6	L2
		OR			
10	a	Explain he various offences and punishment on cyber crime	8	CO6	L2
	b	Explain the process of attribution, acknowledgement and dispatch of electronic record	8	CO6	L2

2. SEE Important Questions

Course:		Cryptography and Network Security And Cyber Law					Month / Year		
Crs Code:		15CS61	Sem:	VI	Crs Code:	15CS61	Sem:	VI	
	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	
	2	Explain the types of attacks/common attacks launched /high profile attacks.					8	CO1	
	3	Define vulnerability. Explain the types of vulnerabilities in the domain of Security.					8	CO1	
		Briefly explain the defence strategies and techniques deployed to overcome network attacks.					8	CO1	
	4	Explain access control,authentication and authorization.					8	CO1	
	5	Explain the guiding principles in security practice.					8	CO1	
	6	Explain the properties of modulo arithmetic.					7	CO1	
		Solve using euclids algorithm for gcd(161,112)					8	CO1	
	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	
	8	Define group and explain the properties of group.					8	CO1	
	9	Define lagranges theorem,eulers, fermats little theorem.					8	CO1	
	10	Consider the group <Z 13,*13>, is it a cyclic group. check whether 2 is a generator of Z 13.					7	CO1	
	11	Explain Chinese remainder theorem.					5	CO1	
	12	Define a)cryptography b) ciphertext c) encryption d)decryption e)kerchoffs principle.					10	CO1	
	13	Bring out the difference between secret key cryptography and public key cryptography.					6	CO1	
	14	Explain known ciphertext attack with a pseudocode.					6	CO1	
	15	Explain the types of elementary substitution ciphers with example.					8	CO1	
	16	Explain monoalphabetic ciphers with example.					6	CO1	
	17	Explain all polyalphabetic ciphers methods with an example.					8	CO1	
	18	Explain hill cipher ,vigenere cipher and one time pad cipher methods with example.					8	CO1	
	19	What are transposition ciphers. explain the working of it with an example					8	CO1	
	20	Differentiate between confusion and diffusion.					6	CO1	
	21	Write a note on stream and block cipher.					5	CO1	
	22	Demonstrate the working of a product cipher with a neat figure. OR Explain Three Round SPN Network					8	CO1	
	23	Explain DES algorithm(along with round function)./ orExplain Fiestel cipher structure.					7	CO1	

	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	
	26	Perform encryption and decryption using RSA algorithms for prime numbers p=3,q=11,e=3,and message = 011101011.	8	CO2	
	27	Explain RSA applications and performance.	5	CO2	
	28	Explain weak and strong collision attack.	5	CO2	
	29	Define hashing.Illustrate the properties of cryptographic hash with a neat figure.	8	CO2	
	30	Explain attack complexity OR weak collision and strong collision resistance with a pseudocose/program	6	CO2	
	31	Explain the computation of generic cryptographic hash with a neat figure	7	CO2	
	32	Explain MAC / message authentication code. // (refer notes :explain the introduction part of HMAC)	5	CO2	
	33	Explain HMAC OR (Hash Based Message Authentication Code).	6	CO2	
	34	Explain the computation of hash using SHA-1 OR SECURE HASH ALGORITHM -1.	7	CO2	
	35	Explain birthday analogy and attack.	5	CO2	
	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	
	37	Explain man in the middle attack on Diffie hellman key exchange algorithm.	6	CO2	
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	
	40	Explain authentication and key agreement using session key.	6	CO3	
	41	Explain Needham Schroeder protocol version 1 and 2 along with the attacks launched on these versions.	8	CO3	
	42	Demonstrate the working of a Kerberos protocol with a neat figure.	8	CO3	
	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	
	45	Explain MAC generation and encryption in CCMP protocol with a neat schematic diagram.	8	CO4	
	46	Explain Email And P2p Worms or explain topological worms.	5	CO4	
	47	Explain IP traceback using Probablistic Packet marking and packet logging with an example.	7	CO4	
	48	Explain the types of Intrusion detection system .	8	CO4	
	49	Explain DDos attack detection and prevention methods.	8	CO4	
	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	
	52	Who is a controller? Outline his functions as a controller.	8	CO5	
	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	
	54	Describe the duties of subscriber under the section 40, 41, and 42 of IT act 2000	8	CO5	
	55	Define the following terms: 1. Certifying Authority b)Addressee c) Digital signature d)Public key	8	CO5	
	56	Explain offense ,punsishments ,penalties under IT act 2000.	8	CO5	

	57	Explain aim and objectives of IT act 2000.	5	CO5	

Course Outcome Computation

Academic Year:

Odd / Even semester

INTERNAL TEST			**T1**						**T2**				
Course Outcome	**CO1**		**CO2**		**CO3**		**CO4**		**CO5**		**CO6**		
QUESTION NO	**Q1**	**LV**	**Q2**	**LV**	**Q3**	**LV**	**Q1**	**LV**	**Q2**	**LV**	**Q3**	**LV**
MAX MARKS	10	-	10	-	10	-	10	-	10	-	10	-
USN-1	5	2	10				10	3	9	3	4	1
USN-2	5	2	8	3								
USN-3	7	3	7	3	10	3	8	3	8	3	5	2
USN-4					4	1	10	3	8	3	6	2
USN-5	8	3	6	2	9	3	10	3	8	3		
USN-6							10	3	9	3	4	1
Average CO Attainment		2.5		2.75		2.33		3		3		1.5

LV Threshold : 3:>60%, 2:>=50% and <=60%, 1: <=49%
CO1 Computation :(2+2+2+3)/4 = 10/4=2.5

PO Computation

Program Outcome	PO1		PO3		PO3		PO1		PO12		PO12	
Weight of CO - PO	3		1		3		2		2		3	
Course Outcome	CO1		CO2		CO3		CO4		CO5		CO6	
Test/Quiz/Lab	T1						T2					
QUESTION NO	Q1	LV	Q2	LV	Q3	LV	Q1	LV	Q2	LV	Q3	LV
MAX MARKS	10	-	10	-	10	-	10	-	10	-	10	-
USN-1	5	2	10	3			10	3	9	3	4	1
USN-2	5	2	8	3								
USN-3	7	3	7	3	10	3	8	3	8	3	5	2

USN-4						4	1	10	3	8	3	6	2	
USN-5		8	3	6	2	9	3	10	3	8	3			1
USN-6								10	3	9	3	4	1	
Average Attainment	CO		2.5		2.75		2.33		3		3		1.5	