COURSE INSTRUCTOR NAME: Dr. Praveen chouksey ACADEMIC YEAR: 2024-25

SUBJECT NAME: INFORMATION SECURITY AND RISK MANAGEMENT

EMAIL-ID: praveenchouksey@cmrec.ac.in CLASS ROOM NO: D401

CONTACT NO: 9302009302

SEM START DATE AND END DATE: 01-8-24 T0 -11-24

CONTENTS OF COURSE FILE

1. **Department vision & mission**
2. **List of PEOs, POs, PSOs**
3. **List of Cos (Action verbs as per blooms with BTL)**
4. **Syllabus copy and suggested or reference books**
5. **Individual Time Table**
6. **Session plan/ lesson plan**
7. **Session execution log**
8. **Lecture notes(handwritten or softcopy printout-5 units)**
9. **Assignment Questions with (original or Xerox of mid 1 and mid 2 assignment samples)**
10. **Mid exam question papers with (Xerox of mid 1 and mid 2 script samples)**
11. **Scheme of evaluation**
12. **Mapping of Cos with Pos and PSOs**
13. **COs, POs, PSOs Justification**
14. **Attainment of Cos, Pos and PSOs (Excel sheet)**
15. **Previous year question papers**
16. **Power point presentations (PPTs)**
17. **Innovative Teaching method**
18. **References (Textbook/Websites/Journals)**

HOD

1. DEPARTMENT VISION & MISSION

Vision:

To produce globally competent and industry-ready graduates in Computer Science & Engineering by imparting quality education with the know-how of cutting-edge technology and holistic personality.

Mission:

1. To offer high-quality education in Computer Science & Engineering in order to build core competence for the graduates by laying a solid foundation in Applied Mathematics and program framework with a focus on concept building.
2. The department promotes excellence in teaching, research, and collaborative activities to prepare graduates for a professional career or higher studies.
3. Creating an intellectual environment for developing logical skills and problem-solving strategies, thus developing, an able and proficient computer engineer to compete in the current global scenario.

2. LIST OF PEOs, POs AND PSOs

2.1 Program Educational Objectives (PEO):

PEO 1: Excel in professional career and higher education by acquiring knowledge of mathematical computing and engineering principles.
PEO 2: To provide an intellectual environment for analyzing and designing computing systems for technical needs.
PEO 3: Exhibit professionalism to adapt current trends using lifelong learning with legal and ethical responsibilities.
PEO 4: To produce responsible graduates with effective communication skills and multidisciplinary practices to serve society and preserve the environment.

2.2. Program Outcomes (POs):

Engineering Graduates will be able to satisfy these NBA graduate attributes:

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **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
11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **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 of technological change.
13. **2.3 Program Specific Outcomes (PSOs):**

PSO1: Professional Skills and Foundations of Software development: Ability to analyze, design and develop applications by adopting the dynamic nature of Software developments.
PSO2: Applications of Computing and Research Ability: Ability to use knowledge in cutting edge technologies in identifying research gaps and to render solutions with innovative ideas.

3. COURSE OUTCOMES

CO1: Students will be able to **Classify** information security concepts and applications. [Understanding]
CO2 : Students will be able to **Apply** Public Key Cryptography . [Applying]
CO3 : Students will be able to **Explain** digital signatures and data leakages. [Analyzing]
CO4 : Students will be able to **Compare** IP security and WEB security. [Evaluating]
CO5: Students will be able to **Elaborate** information security management- roles and responsibilities. [Creating]

REVISED Bloom's Taxonomy Action Verbs

Definitions	I. Remembering	II. Understanding	III. Applying	IV. Analyzing	V. Evaluating	VI. Creating
Bloom's Definition	Exhibit memory of previously learned material by recalling facts, terms, basic concepts, and answers.	Demonstrate understanding of facts and ideas by organizing, comparing, translating, interpreting, giving descriptions, and stating main ideas.	Solve problems to new situations by applying acquired knowledge, facts, techniques and rules in a different way.	Examine and break information into parts by identifying motives or causes. Make inferences and find evidence to support generalizations.	Present and defend opinions by making judgments about information, validity of ideas, or quality of work based on a set of criteria.	Compile information together in a different way by combining elements in a new pattern or proposing alternative solutions.
Verbs	• Choose • Define • Find • How • Label • List • Match • Name • Omit • Recall • Relate • Select • Show • Spell • Tell • What • When • Where • Which • Who • Why	• Classify • Compare • Contrast • Demonstrate • Explain • Extend • Illustrate • Infer • Interpret • Outline • Relate • Rephrase • Show • Summarize • Translate	• Apply • Build • Choose • Construct • Develop • Experiment with • Identify • Interview • Make use of • Model • Organize • Plan • Select • Solve • Utilize	• Analyze • Assume • Categorize • Classify • Compare • Conclusion • Contrast • Discover • Dissect • Distinguish • Divide • Examine • Function • Inference • Inspect • List • Motive • Relationships • Simplify • Survey • Take part in • Test for • Theme	• Agree • Appraise • Assess • Award • Choose • Compare • Conclude • Criteria • Criticize • Decide • Deduct • Defend • Determine • Disprove • Estimate • Evaluate • Explain • Importance • Influence • Interpret • Judge • Justify • Mark • Measure • Opinion • Perceive • Prioritize • Prove • Rate • Recommend • Rule on • Select • Support • Value	• Adapt • Build • Change • Choose • Combine • Compile • Compose • Construct • Create • Delete • Design • Develop • Discuss • Elaborate • Estimate • Formulate • Happen • Imagine • Improve • Invent • Make up • Maximize • Minimize • Modify • Original • Originate • Plan • Predict • Propose • Solution • Solve • Suppose • Test • Theory

Anderson, L. W., & Krathwohl, D. R. (2001). A taxonomy for learning, teaching, and assessing, Abridged Edition. Boston, MA: Allyn and Bacon.

Action Words for Bloom's Taxonomy					
Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Create**
define	explain	solve	analyze	reframe	design
identify	describe	apply	compare	criticize	compose
describe	interpret	illustrate	classify	evaluate	create
label	paraphrase	modify	contrast	order	plan
list	summarize	use	distinguish	appraise	combine
name	classify	calculate	infer	judge	formulate
state	compare	change	separate	support	invent
match	differentiate	choose	explain	compare	hypothesize
recognize	discuss	demonstrate	select	decide	substitute
select	distinguish	discover	categorize	discriminate	write
examine	extend	experiment	connect	recommend	compile
locate	predict	relate	differentiate	summarize	construct
memorize	associate	show	discriminate	assess	develop
quote	contrast	sketch	divide	choose	generalize
recall	convert	complete	order	convince	integrate
reproduce	demonstrate	construct	point out	defend	modify
tabulate	estimate	dramatize	prioritize	estimate	organize
tell	express	interpret	subdivide	find errors	prepare
copy	identify	manipulate	survey	grade	produce
discover	indicate	paint	advertise	measure	rearrange
duplicate	infer	prepare	appraise	predict	rewrite
enumerate	relate	produce	break down	rank	role-play
listen	restate	report	calculate	score	adapt
observe	select	teach	conclude	select	anticipate
omit	translate	act	correlate	test	arrange
read	ask	administer	criticize	argue	assemble
recite	cite	articulate	deduce	conclude	choose
record	discover	chart	devise	consider	collaborate
repeat	generalize	collect	diagram	critique	collect
retell	give examples	compute	dissect	debate	devise
visualize	group	determine	estimate	distinguish	express
	illustrate	develop	evaluate	editorialize	facilitate
	judge	employ	experiment	justify	imagine
	observe	establish	focus	persuade	infer
	order	examine	illustrate	rate	intervene
	report	explain	organize	weigh	justify
	represent	interview	outline		make
	research	judge	plan		manage
	review	list	question		negotiate
	rewrite	operate	test		originate
	show	practice			propose
	trace	predict			reorganize
	transform	record			report
		schedule			revise
		simulate			schematize
		transfer			simulate
		write			solve
					speculate
					structure
					support
					test
					validate

4. SYLLABUS COPY

UNIT - I

Information Security Management:

Information Security Overview, Threat and Attack Vectors, Types of Attacks, Common Vulnerabilities and Exposure(CVE), Security Attacks, Fundamentals of Information Security, Computer Security Concerns, Information Security Measures etc.

A model for Internetwork security. Classical Encryption Techniques, DES, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operation, Blowfish, Placement of Encryption Function, Traffic Confidentiality, key Distribution, Random Number Generation.

UNIT - II

Public key Cryptography: Principles, RSA algorithm, Key Management, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography. Message authentication and Hash Functions, Authentication Requirements and Functions, Message Authentication, Hash Functions and MACs Hash and MAC Algorithms SHA-512, HMAC.

UNIT - III

Digital Signatures: Authentication Protocols, Digital signature Standard, Authentication Applications, Kerberos, X.509 Directory Authentication Service.

Email Security: Pretty Good Privacy (PGP) and SIMIME.

Data Leakage: What is Data Leakage and Statistics, Data Leakage Threats, Reducing the Risk of Data Loss, Key Performance Indicators (KPI), Database Security etc.

UNIT - IV

IP Security: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

Web Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET). Intruders, Viruses and Worms Intruders, Viruses and related threats Firewalls: Firewall Design Principles, Trusted Systems, Intrusion Detection Systems.

UNIT - V

Information Security Management- Roles and Responsibilities:

Security Roles and Responsibilities, Accountability, Roles and Responsibilities of Information Security Management, Team Responding to Emergency Situation- Risk Analysis Process etc.

TEXT BOOK:

1. Cryptography and Network Security (principles and approaches) by William Stallings
Pearson Education, 4th Edition,
2. Management of Information Security by Michael E.Whiman and Herbert J Mattord

REFERENCE BOOKS:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education,
2. Principles of Information Security, Whitman, Thomson.

5. INDIVIDUAL TIME TABLE (Dr. Praveen chouksey)

	I	II	III	IV	V	VI	VII
MON							
TUE	ISRM-D					ISRM-D	
WED							
THU			ISRM-D			ISRM-D	
FRI							
SAT	ISRM-D		ISRM-D				

6. SESSION PLAN/LESSON PLAN

S.NO]\	Topic (Autonomous Syllabus)	Sub-Topic	NO. Of Lectures Required	Planed Date	Conducted Date	Remark
UNIT-I						
1	**Information Security Management**	Introduction to ISRM	**L1**	**08-07-24**	**08-07-24**	**M1,M4**
		Information security overview	**L2**	**09-07-24**	**09-07-24**	**M1,M4**
2		Threats and attacks vectors, Types of attacks	**L3**	**11-07-24**	**11-07-24**	**M1,M4**
3		Common Vulnerabilities and exposure CVE	**L4**	**12-07-24**	**12-07-24**	**M1,M4**
4		Security Attacks	**L5**	**13-07-23**	**13-07-24**	**M1,M4**
		Fundamentals of information security	**L6**	**15-07-23**	**15-07-24**	**M1,M4**
5		Computer Security Concerns	**L7**	**19-07-24**	**19-07-24**	**M1,M4**
		Information Security Measures	**L8**	**20-07-24**	**20-07-24**	**M1,M4**
6		A model for internetwork security	**L9**	**23-07-24**	**23-07-24**	**M1,M4**
7		Classical Encryption Techniques	**L10**	**24-07-24**	**24-07-24**	**M1,M4**
		Data Encryption Standard, strengths	**L11**	**25-07-24**	**25-07-24**	**M1**
8		Differential and	**L12**	**26-07-24**	**26-07-24**	**M1,M4**

		Linear Cryptanalysis Block Cipher Design Principles	**L13**	**30-07-24**	**30-07-24**	**M1,M4**
9		Modes of operation, Blowfish Placement of Encryption Function	**L14**	**03-08-24**	**03-08-24**	**M1,M4**
			L15	**04-08-24**	**04-08-24**	**M1,M4**
10		Traffic Confidentiality, key Distribution Random Number Generation	**L16**	**05-08-24**	**05-08-24**	**M1,M4**
			L17, L18	**06-08-24**	**06-08-24**	**M1,M4**
		UNIT-II				
11	**Public key Cryptography**	Public key Cryptography Principles	**L21**	**07-08-24**	**07-08-24**	**M1,M4**
12		RSA algorithm, Key Management	**L22**	**08-08-24**	**08-08-24**	**M1**
13		Diffie-Hellman Key Exchange	**L23**	**15-08-24**	**15-08-24**	**M1,M4**
14		Elliptic Curve Cryptography	**L23**	**20-08-24**	**20-08-24**	**M1,M4**
15		Message authentication and Hash Functions	**L24**	**21-08-24**	**21-08-24**	**M1,M4**
16		Authentication Requirements and Functions	**L25**	**21-08-24**	**21-08-24**	**M1,M4**
17 **18**		Message Authentication, Hash Functions and MACs	**L26**	**27-08-24**	**27-08-24**	**M1,M4**

19 **20**		Hash and MAC Algorithms SHA-512, HMAC	**L27**	**28-08-23**	**28-08-23**	**M1**
		UNIT-III				
21 **22**		Authentication Protocols, Digital signature Standard	**L30**	**30-08-23**	**30-08-23**	**M1,M4**
23 **24**		Authentication Applications, Kerberos	**L31**	**04-09-24**	**04-09-24**	**M1,M4**
25		X.509 Directory Authentication Service	**L33**	**19-09-24**	**19-09-24**	**M1,M4**
26	**Digital Signatures**	Email Security: Pretty Good Privacy (PGP) and SIMIME	**L34**	**20-09-24**	**20-09-24**	**M1**
27		Data Leakage: What is Data Leakage and Statistics	**L35**	**20-09-24**	**20-09-24**	**M1,M4**
28 29		Data Leakage Threats, Reducing the Risk of Data Loss	**L36**	**23-09-24**	**23-09-24**	**M1,M4**
30		Key Performance Indicators (KPI), Database Security etc	**L37**	**24-09-24**	**24-09-24**	**M1,M4**
		UNIT-IV				
31	**IP Security**	Overview: IP Security Architecture	**L38**	**25-09-24**	**25-09-24**	**M1,M4**
32		Authentication Header, Encapsulating	**L39**	**26-09-24**	**26-09-24**	**M1,M4**

33		Web Security: Web Security Requirements	**L40**	**28-09-24**	**01-10-24**	**M1,M4**
34		Secure Socket Layer (SSL) and Transport Layer Security (TLS)	**L41**	**01-10-24**	**01-10-24**	**M1,M4**
35		Secure Electronic Transaction (SET)	**L39**	**03-10-24**	**03-10-24**	**M1,M4**
36		Intruders, Viruses and Worms Intruders,	**L40**	**04-10-24**	**04-10-24**	**M1,M4**
37		Viruses and related threats	**L41**	**05-10-24**	**05-10-24**	**M1,M4**
38		Firewalls: Firewall Design Principles	**L39**	**17-10-24**	**17-10-24**	**M1,M4**
39		Trusted Systems	**L40**	**18-10-24**	**18-10-24**	**M1,M4**
40		Intrusion Detection Systems	**L41**	**22-10-24**	**22-10-24**	**M1,M4**
		UNIT -V				
41	**Information Security Management**	Introduction ISM	**L43**	**24-10-24**	**24-10-24**	**M1,M4**
42		Roles and Responsibilities	**L44**	**26-10-24**	**26-10-24**	**M1,M4**
43 **44**		Security Roles and Responsibilities Accountability	**L45**	**29-10-24**	**29-10-24**	**M1,M4**
45 **46**		Roles and Responsibilities of Information Security Management	**L46**	**04-11-24**	**04-11-24**	**M1,M4**
47 **48**		Team Responding to Emergency Situation- Risk Analysis Process etc	**L47**	**05-11-24** 06-11-24	**05-11-24** **06-11-24**	**M1,M4**

49		Prevention Risk Management	**L-48**	**08-11-24**	**08-11-24**	**M1**

METHODS OF TEACHING:

M1 : Lecture Method	**M4 : Presentation /PPT**	**M7 : Assignment**
M2 : Demo Method	**M5 : Lab/Practical**	**M8 : Industry Visit**
M3 : Guest Lecture	**M6 : Tutorial**	**M9 : Project Based**

NOTE:

1. Any Subject in a Semester is suppose to be completed in 55 to 65 periods.
2. Each Period is of 50 minutes.
3. Each unit duration & completion should be mentioned in the Remarks Column.
4. List of Suggested books can be marked with Codes like T1, T2, R1, R2 etc.

7. Session Execution Log:

S no	Units	Scheduled started date	Completed date	Remarks
1	**I**	**8-7-24**	**24-7-24**	**COMPLETED**
2	**II**	**25-7-24**	**15-8-24**	**COMPLETED**
3	**III**	**20-8-24**	**22-9-24**	**COMPLETED**
4	**IV**	**23-9-24**	**17-10-24**	**COMPLETED**
5	**V**	**18-10-24**	**8-11-24**	**COMPLETED**

8. Lecture Notes – (hand written)

9. ASSIGNMENT QUESTIONS ALONG SAMPLE ASSIGNMENT SCRIPTS

CMR ENGINEERING COLLEGE

UGC AUTONOMOUS

(Approved by AICTE - New Delhi. Affiliated to JNTUH and Accredited by NAAC & NBA)

MID-1 ASSIGNMENT QUESTIONS

ACADEMIC YEAR 2024-25

SUBJECT NAME: INFORMATION SECURITY AND RISK MANAGEMENT

1. Discuss in detail about various types of Security attacks with neat diagrams (CO1)

2. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption? Also, state some differences between Block & Stream ciphers. (CO1)

3. What is symmetric key cryptography? Discuss its advantages and limitations. (CO2)

4. Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive root α=2.

a) If user „A“ has public key YA=9, what is A“s private key XA.

b) If user „B“ has public key YB=3, what is shared secret key K. (CO2)

5. Client machine C wants to communicate with server S. Explain how it can be achieved through Kerberos protocol? (CO3)

CMR ENGINEERING COLLEGE
UGC AUTONOMOUS
(Approved by AICTE - New Delhi. Affiliated to JNTUH and Accredited by NAAC & NBA)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MID-II Assignment Questions 2024-25

Subject: INFORMATION SECURITY & RISK MANAGEMENT

1. Explain about Key Performance Indicators (KPI)? (CO3)

2. Explain brief about Database Security? (CO3)

3. What is SSL Record Protocol? Explain two services provided for SSL connections by this protocol. (CO4)

4. Explain Encapsulation Security Payload of IPSec. (CO4)

5. What are the roles and responsibilities of Information Security Management? (CO5)

10. MID EXAM QUESTION PAPER ALONG SAMPLE ANSWER SCRIPTS

CMR ENGINEERING COLLEGE
UGC AUTONOMOUS
(Approved by AICTE - New Delhi. Affiliated to JNTUH and Accredited by NAAC & NBA)

IV.B.TECH-I-SEM I-MID EXAMINATION

Date: 29/08/2023 Time: 10:00-11:30 AM
Subject: INFORMATION SECURITY & RISK MANAGEMENT (CS743PE)
Branch: CSE Section: A & C Marks: 25 M
Note: Question paper contains two parts, Part – A and Part - B.
Part-A is compulsory which carries 10 marks. Answer all questions in part-A.
Part-B consists of (21/2) units. Answer any one full question from each unit.
Each question carries 5 marks and may have a, b, c sub questions.

PART-A 5X2=10

1. What are the types of security attacks? (CO1)
2. Compare transposition ciphers with substitution cipher. (CO1)
3. Discuss about Electronic code book mode? (CO2)
4. What properties must a hash function have to be useful for message authentication? (CO2)
5. What is a digital signature? (CO3)

PART-B 3X5=15

6. Consider the following:
Plaintext: “PROTOCOL”
Secret key: “NETWORK”
What is the corresponding cipher text using play fair cipher method? (CO1)
(OR)
7. Explain DES algorithm with suitable examples. Discuss its advantages and limitations. (CO1)
8. Given two prime numbers p=5 and q=11, and encryption key e=7 derive the decryption key d. Let the message be x=24. Perform the encryption and decryption using R.S.A algorithm. (CO2)
(OR)
9. Explain the SHA 512 algorithm. Illustrate with an example. (CO2)
10. Explain X.509 authentication service (CO3)
(OR)
11. Explain in detail about Kerberos. (CO3)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
IV.B.TECH- I-SEM MID-II EXAMINATION Date: 07/11/2023 Time: 10:00-11:30 AM
Subject: INFORMATION SECURITY & RISK MANAGEMENT (CS743PE)
Branch: CSE Section: A&C Marks: 25 M

Note: Question paper contains two parts, Part - A and Part - B.
Part-A is compulsory which carries 10 marks. Answer all questions in part-A.
Part-B consists of (21/2) units. Answer any one full question from each unit. Each question carries 5 marks and may have a, b, c sub questions.

PART-A 5X2=10

1. What are Data Leakage Threats? (CO3)
2. Write about Reducing the Risk of Data Loss? (CO3)
3. What is IPSec? Draw the architecture of it? (CO4)
4. What protocols comprise SSL? (CO4)
5. Define Risk Analysis Process? (CO5)

PART-B 3X5=15

6. Explain brief about Database Security? (CO3)

(OR)

7. What are the five principal services provided by PGP? Explain. (CO4)
8. Explain authentication header of IPSec. (CO4)

(OR)

9. Compare TLS and SSL. (CO4)
10. a) Discuss the purpose of SA selectors? (CO4)
    b) Define payload? And discuss about encapsulating security payload?

(OR)

11. What are the roles and responsibilities of Information Security Management? (CO5)

11. SCHEME OF EVALUATION:

MID 1

S.NO	THEORY	MARKS	TOTAL MARKS
	PART-A		
1	What are the types of security attacks	2	2
2	Compare transposition ciphers with	2	2
3	Discuss about Electronic code book mode	2	2
4	What properties must a hash function have to be useful for message	2	2
5	What is a digital signature	2	2
	PART-B		
1	Consider the following: Plaintext: "PROTOCOL" Secret key: "NETWORK" What is the corresponding cipher text using play fair cipher method?	5	5
2	Explain DES algorithm with suitable examples. Discuss its advantages and limitations.	5	5
3	Given two prime numbers p=5 and q=11, and encryption key e=7 derive the decryption key d. Let the message be x=24. Perform the encryption and decryption using R.S.A algorithm.	5	5
4	Explain the SHA 512 algorithm. Illustrate with an example.	5	5
5	Explain X.509 authentication service	5	5
6	Explain in detail about Kerberos	5	5

MID 2

S.NO	THEORY	MARKS	TOTAL MARKS
	PART-A		
1	What are Data Leakage Threats?	2	2
2	Write about Reducing the Risk of	2	2
3	What is IPSec? Draw the architecture of it?	2	2
4	What protocols comprise SSL?	2	2
5	Define Risk Analysis Process?	2	2
	PART-B		
1	Explain brief about Database Security?	5	5
2	What are the five principal services provided by PGP? Explain.	5	5
3	Explain authentication header of IPSec.	5	5
4	Compare TLS and SSL.	5	5
5	Discuss the purpose of SA selectors?	5	5
	Define payload? And discuss about encapsulating security payload	5	5
6	What are the roles and responsibilities of Information Security Management?	5	5

COURSE	Relationship of Course Outcomes to Program Outcomes (PO AVG)													
CO-PO&PSO MATRIX	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	-	2	2	-	1	-	-	-	-	1	-	-	-	-
CO2	2	-	-	-	-	1	-	-	-	-	-	-	-	-
CO3	-	2	-	-	1	-	-	-	-	-	-	-	-	-
CO4	-	-	-	-	-	2	-	-	-	-	-	1	-	-
CO5	-	-	-	-	-	1	-	-	-	-	-	1	-	-

12. **Mapping of COs and Pos with PSOs**

Mapping of COs and Pos with PEOs

	Program Outcome(PO):												
PEOS		1	2	3	4	5	6	7	8	9	10	11	12
	I	X	X										
	II	X	X										
	III		X			X							
	IV			X					X				

13. COs, POs, PSOs JUSTIFICATION

COURSE	Relationship of Course outcomes to Program Outcomes (PO AVG)													
CO-PO&PSO MATRIX	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	1	-	-	-	-	-	-	-	-	-	-	-	-
CO2	2	-	1	-	-	-	-	-	-	1	-	-	-	-
CO3	1	-	1	-	2	-	-	-	-	-	-	-	-	-
CO4	-	-	-	-	-	1	1	-	2	-	2	-	-	-
CO5	2	1	-	-	-	-	1	-	1	-	2	-	-	-

COURSE OUTCOMES

CO1: Students will be able to **Classify** information security concepts and applications. [Understanding]
CO2 : Students will be able to **Apply** Public Key Cryptography . [Applying]
CO3 : Students will be able to **Explain** digital signatures and data leakages. [Analyzing]
CO4 : Students will be able to **Compare** IP security and WEB security. [Evaluating]
CO5: Students will be able to **Elaborate** information security management- roles and responsibilities. [Creating]

Justification:

CO1: Students will be able to **Classify** information security concepts and applications. [Understanding]
Correlated with PO1 moderately: Because it contributes the knowledge on Information Security and types of threats and encryption techniques, student can categorize different utilities. So, overall the correlation of CO1 to PO1 is good.
Correlated with PO2 low: Because it provides information Security by encryption techniques, student can . know how to apply it. So, overall the correlation of CO1 to PO2 is low.

CO2 : Students will be able to **Apply** Public Key Cryptography . [Applying]
Correlated with PO1 moderately: Because it provides cryptography principles for key management. So,

correlation is good.
Correlated with PO3 low: Because it provides message authentication and hash functions in information security. So Correlation of Co2 with PO3 is low.
Correlated with PO10 low: Because it provides different hash algorithms. So Correlation of Co2 with PO10 is low.

CO3: Students will be able to **Explain** digital signatures and data leakages. [Analyzing]
Correlated with PO1 low: it provides authentication protocols and digital signature applications. So CO3 Correlation is low with PO1.
Correlated with PO3 low: it **provides** student to identify Authentication services like PGP and S/MIME with python languages and packages. So Correlation CO3 is low with PO3.
Correlated with PO5 moderately: it provides student to identify Data Leakage problems, risks and security for database. So Correlation CO3 is moderate with PO5.

CO4 : Students will be able to **Compare** IP security and WEB security. [Evaluating]
Correlated with PO6 low: Because it provides IP security and Web security concepts. So, correlation is low.
Correlated with PO7 low: it provides IP security architecture and protocols for security associations, So,correlation is low.
Correlated with PO9 moderately: it provides Web security and different layers importance in security. So, correlation is good.
Correlated with PO11 moderately: Because it conducts intrusion detection systems with firewalls. So, correlation is good.

CO5: Students will be able to **Elaborate** information security management- roles and responsibilities. [Creating]
Correlated with PO1 moderately: it provides information security management .So, overall correlation of CO5 is good.
Correlated with PO2 low: it provides students to identify different roles in Information security management. So, overall the correlation of CO5 is low.
Correlated with PO7 low: it gives brief about roles and responsibility of employee in an organization. So, that the students know roles and responsibilities in the risk. So the correlation is low.
Correlated with PO9 low: outcome contributes better for identification of different aspects as a team

work. So that the students can apply to build some applications. So the correlation is low.
Correlated with PO11 moderately: it provides students to identify different Problems like risk analysis process that occur when dealing with information and response in emergency situations So, overall the correlation of CO5 is good.

14.Attainment of COs,POs AND PSOs (Excel sheet)

AFTER RESULT

15. Previous Question Papers

Roll No. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐ Total No. of Pages : 02

Total No. of Questions : 09

B.Tech.(IT) (2011 Onwards) (Sem.–6)

INFORMATION SECURITY AND RISK MANAGEMENT

Subject Code : BTIT-602

M.Code : 71172

Time : 3 Hrs. Max. Marks : 60

INSTRUCTION TO CANDIDATES :

1. SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.
2. SECTION-B contains FIVE questions carrying FIVE marks each and students have to attempt any FOUR questions.
3. SECTION-C contains THREE questions carrying TEN marks each and students have to attempt any TWO questions.

SECTION-A

Q1 Answer briefly :

a) What are Intruders in Information Security?

b) What do you mean by vulnerability?

c) Discuss SHA 1 hash function.

d) What are digital signature standards?

e) Give the role of Key management in cryptography.

f) Define message confidentiality.

g) What is *DoS* attack in information security?

h) Write the purpose of DMZs?

i) What is risk assessment process?

j) Discuss risk value analysis.

SECTION-B

Q2 List the steps to develop a corporate information security process life cycle.

Q3 Explain the principle of RSA algorithm by taking an example.

Q4 What are the message authentication functions? What are its requirements?

Q5 What is cyber crime and security? Give the examples of cyber crime.

Q6 Discuss the role of effective risk analysis in risk management.

SECTION-C

Q7 Explain the importance of DES algorithm using the block diagram. Discuss the modified AES.

Q8 How Pretty Good Privacy is used for sending secure encrypted messages in network?

Q9 Show how risk management is used to identifying, monitoring and managing potential risks?

Total No. of Questions: 09

B.Tech. (IT) (2011 Onwards) (Sem. – 6)

INFORMATION SECURITY AND RISK MANAGEMENT

M Code: 71172

Subject Code: BTIT-602

Paper ID: [A2352]

Time: 3 Hrs. Max. Marks: 60

INSTRUCTIONS TO CANDIDATES:

1. SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.
2. SECTION-B contains FIVE questions carrying FIVE marks each and students have to attempt any FOUR questions.
3. SECTION-C contains THREE questions carrying TEN marks each and students have to attempt any TWO questions.

SECTION A

1. Write in brief:
   a) Explain ethical hacking.
   b) What is a Worm?
   c) What is Cyber Crime?
   d) What is a message digest?
   e) What is Confidentiality?
   f) Explain Triple DES Algorithm.
   g) What do you mean by term "risk management"?
   h) What is DDoS?
   i) Explain use of digital signature.
   j) What is risk assessment?

SECTION B

2. Explain various Cyber Crimes. What are the various ways to make yourself secure?
3. Differentiate between 'penetration testing' and 'threat assessment'.
4. Explain use of firewall in any organization.
5. What is Email Security?
6. Explain various modes of risk analysis.

SECTION C

7. Explain Information Security Life Cycle in detail.
8. What is difference between 'MD5' and 'SHA-1 Algorithm'.
9. Explain RSA Algorithm mathematically.

16. Power point presentations (PPTs)

PPTs AND PRESENTATION

Information Security

- **Information Security** is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.
- IT security performs four important functions for an organization:
  - Protects the organization's ability to function
  - Enables the safe operation of applications implemented on the organization's IT systems
  - Protects the data the organization collects and uses
  - Safeguards the technology assets in use at the organization

Information Security: Features

Confidentiality:-

- Assurance that information is shared only among authorized persons or organizations.

Integrity:-

- Assurance that the information is authentic and complete.
- Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Availability:-

- Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Vulnerabilities

- A **vulnerability** is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system.
- Vulnerabilities are classified according to the asset class they are related to:-
  - **Hardware:-** Susceptibility to humidity/dust ; Unprotected storage; Over-heating.
  - **Software:-** Insufficient testing; insecure coding; lack of audit trail; Design flaw.
  - **Network:-** Unprotected communication lines; Insecure network architecture.
  - **Personnel:-** Inadequate recruiting process; Inadequate security awareness; insider threat
  - **Physical site:-** Area subject to natural disasters (e.g. flood, earthquake); interruption to power source
  - **Organizational:-** Lack of regular audits; lack of continuity plans;

Threats

- **A threat** is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.
- *Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.*
- A countermeasure is any step you take to ward off a threat to protect user, data, or computer from harm.
- Various Security threats:-
  - **Users:-** Identity Theft; Loss of Privacy; Exposure to Spam; Physical Injuries.
  - **Hardware:-** Power-related problems; theft; vandalism; and natural disasters.
  - **Data:- M**alwares; Hacking; Cybercrime; and Cyber-terrorism.

Attack Descriptions

- **Denial-of-service (DoS)** –
  - attacker sends a large number of connection or information requests to a target
  - so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
  - may result in a system crash, or merely an inability to perform ordinary functions
- **Distributed Denial-of-service (DDoS)** - an attack in which a coordinated stream of requests is launched against a target from many locations at the same time

Threats to Information Security

TABLE 2-1 Threats to Information Security[4]

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Threats(Keywords)

- Spam:-Unsolicited commercial e-mail/Junk e-mail
- Cookie:- Small text file that a Web server put on computer
- Web Bugs:-a small gif embedded in webpage/email
- **Mal**wares:-**Mal**icious Soft**ware**
  - Virus(require Some executables), Worms(Self executables), Spyware, Trojan Horses, Botnet (**Robot Net**work)
- Shoulder Surfing
- Hacking:-
  - Sniffing:- finding user's password(Password Sharing, Password Guessing or Password Capture
  - Social Engineering:- Dumpster Diving, Phishing(Email) & Vishing(Phone Calls)
  - Spoofing
- DDoS:-Distributed Denial of Services.
- Cybercrime; and Cyber-terrorism.

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.

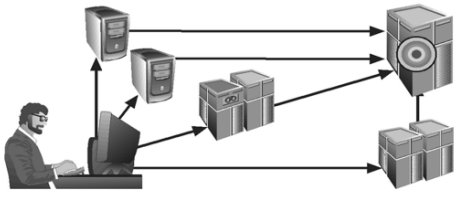

FIGURE 2-9 Denial-of-Service Attacks

Attack Descriptions

- **Spoofing** - technique used to gain unauthorized access whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host
- **Man-in-the-Middle** - an attacker sniffs packets from the network, modifies them, and inserts them back into the network

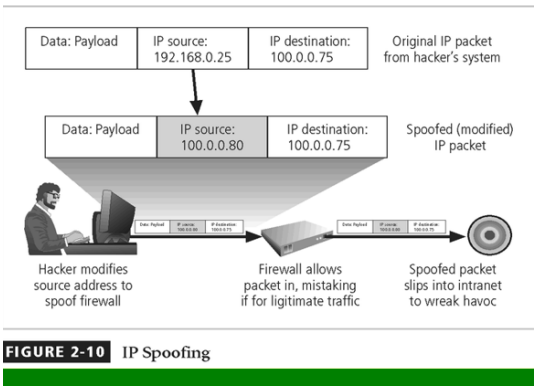

FIGURE 2-10 IP Spoofing

A Model For Network Security

A Generic Model For Network Security

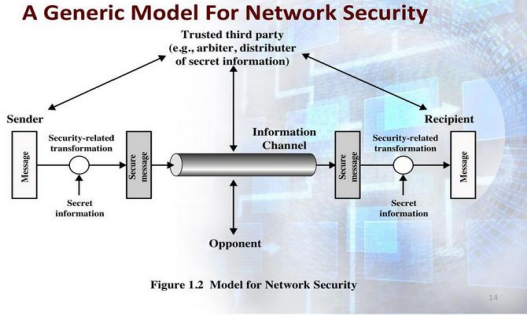

Figure 1.2 Model for Network Security

Basic Terminology

- Plaintext
  - The original message
- Ciphertext
  - The coded message
- Enciphering or Encryption
  - Process of converting from plaintext to ciphertext
- Deciphering or Decryption
  - Restoring the plaintext from the ciphertext
- Cryptography
  - Study of encryption
- Cryptanalysis (breaking the code)
  - Techniques used for deciphering a message without any knowledge of the enciphering details
- Cryptology
  - Areas of cryptography and cryptanalysis together

17. Innovative Teaching method if any (Attached Innovative Assignment)

1. What role does blockchain technology play in enhancing information security and managing risks?

2.How can artificial intelligence AI revolutionize risk management in information security?

18. References (Textbook/Websites/Journals)

Textbook

1.Information Security and IT Risk Management

Manish Agrawal,Alex Campoe,Eric Pierce

Websites or URLs e- Resources

https://www.geeksforgeeks.org/risk-management-for-information-security-

https://hyperproof.io/resource/cybersecurity-risk-management-process

https://www.sapphire.net/blogs-press-releases/information-security-risk-management

Journals:-

1.Chapter in Encyclopedia of Multimedia Technology and Networking, 2nd ed., M. Pagani (ed.), Idea Group Publishing, to appear 2009. Information Security and Risk Management Thomas M. Chen Dept. of Electrical Engineering SMU, Dallas, Texas

2. https://www.sciencedirect.com/science/article/pii/S1877050922007633