NARASIMHA REDDY ENGINEERING COLLEGE

(Autonomous)

Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad

Accredited by NAAC with A Grade, Accredited by NBA

COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

Course Title : **INFORMATION SECURITY**

Course Code : **CY3101PC(CS)**

Regulation :**NR20**

Course Objectives

- Explain the objectives of information security
- Explain the importance and application of each of confidentiality, integrity, authentication and availability
- Understand various cryptographic algorithms.
- Understand the basic categories of threats to computers and networks
- Describe public-key cryptosystem.
- Describe the enhancements made to IPv4 by IPSec
- Understand Intrusions and intrusion detection
- Discuss the fundamental ideas of public-key cryptography.
- Generate and distribute a PGP key pair and use the PGP package to send an encrypted e-mail message.
- Discuss Web security and Firewalls

CourseOutcomes(CO's)

CO1	To identify how to protect network from network attacks.
CO2	To analyze the Design of new security approaches
CO3	To discover the appropriate security algorithm based on requirement
CO4	To understand the current legal issues towards information security.
CO5	Able to develop file security software,PGP,and efficiently use the code to encrypt and sign messages.

UNIT–I

Security concepts, Cryptography and concepts

S.No		Questions	BT	CO	PO
Part –A(Short Answer Questions)					
1		Define cryptanalysis and cryptology.	L1	CO1	PO1,PO6
2		What is masquerade?	L1	CO1	PO1,PO6
3		Define passive attack and active attack.	L1	CO1	PO1,PO6
4		Define Denial of service.	L1	CO1	PO1,PO6
5		What is steganography? Mention few techniques in it.	L1	CO1	PO1,PO6
6		Mention few mono-alphabetic and poly-alphabetic ciphers.	L1	CO1	PO1,PO6
7		Define Threat and attack. List out what are the attacks that canbe performed in network.	L1	CO1	PO1,PO6
8		Convert the Given Text “CRYPTOGRAPHY” into cipher text using Rail fence Technique.	L3	CO1	PO1,PO6
9		Define security attack, security mechanism and security services.	L1	CO1	PO1,PO6
10		Define the two basic building blocks of encryption techniques	L1	CO1	PO1,PO6
Part– B(Long Answer Questions)					
11	a)	Explain in detail about OSI security architecture.	L2	CO1	PO1,PO6
	b)	Explain classical encryption techniques (Steps involved in each encryption technique like Caesar cipher, playfair cipher, hill cipher, vigenere cipher, one time pad cipher, rail fence, etc)	L2	CO1	PO1,PO6
12	a)	Explain about steganography, transposition cipher.	L2	CO1	PO1,PO6
	b)	Write short notes on security mechanisms	L6	CO1	PO1,PO6
13	a)	Explain about substitution ciphers in detail with an example.	L2	CO1	PO1,PO6
	b)	What are the goals of security? Explain in detail about security Services?	L1	CO1	PO1,PO6
14	a)	what is meant by security attack? Explain various types of security attacks.	L1	CO1	PO1,PO6
	b)	Draw a matrix that shows the relationship between security mechanisms and attacks.	L2	CO1	PO1,PO6
15	a)	Explain various transposition ciphers with an example	L2	CO1	PO1,PO6
	b)	Explain any three substitution ciphers with an example.	L2	CO1	PO1,PO6

16	a)	Define Cryptography.What is the need of CIA Triad.	L1	CO1	PO1,PO6
	b)	What are the different levels of losses that occur without CIA Triad.	L1	CO1	PO1,PO6

UNIT–II

Symmetric key cipher, Assysmmetric cipher

S.No		Questions	BT	CO	PO
Part –A(Short Answer Questions)					
1		Define symmetric key cryptography and public key cryptography.	L1	CO2	PO3
2		Define Euler's totient function (used in RSA algorithm).	L1	CO2	PO3
3		Why do we need Diffie Hellman algorithm?	L2	CO2	PO3
4		Mention the various types of cryptanalytic attack.	L1	CO2	PO3
5		What are the operations used in AES?	L1	CO2	PO3
6		What are the various approaches to attacks the RSA algorithm?	L1	CO2	PO3
7		How to find primitive root with an example.	L3	CO2	PO3
8		What primitive operations are used in RC4	L1	CO2	PO3
9		Compare stream cipher with block cipher with example	L3	CO2	PO3
10		Define Euler's theorem and its application.	L1	CO2	PO3
Part– B(Long Answer Questions)					
11	a)	Discuss various steps of IDEA algorithm.	L3	CO2	PO3
	b)	Explain Diffie-Hellman key exchange algorithm in detail.	L2	CO2	PO3
12	a)	Explain the steps involved in knapsack algorithm with an example.	L2	CO2	PO3
	b)	Explain in detail about the steps involved in DES.	L2	CO2	PO3
13	a)	Explain Elgamal algorithm in detail.	L2	CO2	PO3
	b)	Discuss different block cipher modes of operation	L3	CO2	PO3
14	a)	Explain in detail about the steps involved in Blowfish.	L2	CO2	PO3
	b)	AES consists of four functions in three layers. Which of the functions are primarily for confusion and which are primarily for diffusion? Which of the layers are for confusion and which are for diffusion? Justify your answers.	L3	CO2	PO3
15	a)	Explain the steps involved in RC4.	L2	CO2	PO3

	b)	Explain RSA algorithm. And perform Encryption and Decryption using RSA p=3 q=11 e=7 M=5	L2	CO2	PO3
16	a)	Explain RC5 algorithm	L2	CO2	PO3
	b)	Differentiate Block cipher and Stream Cipher	L4	CO2	PO3

UNIT–
III
Cryptographic hash functions

S.No		Questions	BT	CO	PO
Part –A(Short Answer Questions)					
1		What is meant by Message Authentication?	L1	CO3	PO2,PO3
2		List out the attack on MAC	L1	CO3	PO2,PO3
3		Define Digital signature	L1	CO3	PO2,PO3
4		What you meant by MAC	L1	CO3	PO2,PO3
5		Differentiate Message Authentication Code and Hash function.	L4	CO3	PO2,PO3
6		What are the two approaches of Digital Signature?	L1	CO3	PO2,PO3
7		Define Hash function .	L1	CO3	PO2,PO3
8		List out the different techniques of distributing the public key	L1	CO3	PO2,PO3
9		Define one way property, weak collision resistance and strong collision resistance of hash function.	L1	CO3	PO2,PO3
10		Define the classes of message authentication function.	L1	CO3	PO2,PO3
Part– B(Long Answer Questions)					
11	a)	With the example, explain in detail about Secure Hash Algorithm	L2	CO3	PO2,PO3
	b)	Explain in detail about HMAC and Digital Signature Standard	L2	CO3	PO2,PO3
12	a)	Give a brief note on basic uses of message authentication code.	L3	CO3	PO2,PO3
	b)	Explain the process involved in message digest generation and processing of single block in SHA512.	L2	CO3	PO2,PO3
13	a)	What is the purpose of digital signature? Explain its properties and requirements.	L1	CO3	PO2,PO3
	b)	Explain the requirements of digital signatures and also discuss how problems related to digital signature are taken care by an arbiter?	L2	CO3	PO2,PO3

14	a)	State and explain the different approaches to message authentication	L3	CO3	PO2,PO3
	b)	Explain the format of X.509v3 certificate and certificate revocation list. Explain each in detail.	L2	CO3	PO2,PO3
15	a)	Explain about characteristics of hash functions	L2	CO3	PO2,PO3
	b)	Explain briefly about Kerberos and give its requirements.	L2	CO3	PO2,PO3
16	a)	Explain in detail about Elgamal Digital signature scheme.	L2	L2	PO2,PO3
	b)	Verify the signature with the Elgamal Digital signature of values q=19,α=10,XA=16,m=14,k=5.	L3	L5	PO2,PO3

UNIT–
IV
Transport level security

S.No		Questions	BT	CO	PO
Part –A(Short Answer Questions)					
1		Define transport and tunnel mode.	L1	CO4	PO1,PO3
2		What are the benefits of mobile device security.	L1	CO4	PO1,PO3
3		Mention the phases of the Handshake protocol.	L1	CO4	PO1,PO3
4		Why do we need an anti replay service?	L2	CO4	PO1,PO3
5		What is the use of the change cipher spec protocol?	L1	CO4	PO1,PO3
6		What are the two characteristic of wired LAN that are not inherent in wireless	L1	CO4	PO1,PO3
7		What is the need pf padding in Encapsulating Security Payload (ESP)?	L1	CO4	PO1,PO3
8		What is security association?	L1	CO4	PO1,PO3
9		Define the terms: connection and session.	L1	CO4	PO1,PO3
10		How the security associations be combined?	L3	CO4	PO1,PO3
Part– B(Long Answer Questions)					
11	a)	Briefly explain about transport layer security and Padding.	L2	CO4	PO1,PO3
	b)	With a neat diagram, explain the operation of SSL and SSH Record Protocol.	L2	CO4	PO1,PO3
12	a)	Differentiate SSL & TLS	L4	CO4	PO1,PO3
	b)	Write a short notes on IEEE 802.11 i services.	L6	CO4	PO1,PO3

13	a)	Write a short notes on IEEE 802.11 i Phases of operation.	L6	CO4	PO1,PO3
	b)	Explain in detail, the Handshake protocol in secure socket layer	L2	CO4	PO1,PO3
14	a)	Write a short note on Wireless LAN Security.	L6	CO4	PO1,PO3
	b)	Write a short note on HTTPS.	L6	CO4	PO1,PO3
15	a)	What are the different types of mobile device security. Explain each.	L1	CO4	PO1,PO3
	b)	How does mobile device security work?	L3	CO4	PO1,PO3
16	a)	Explain in detail about SSL	L2	CO4	PO1,PO3
	b)	What is the importance of providing Security for wireless LAN	L1	CO4	PO1,PO3

UNIT–V

Email security

S.No	Questions	BT	CO	PO
Part –A(Short Answer Questions)				
1	Mention the services provided by the Pretty Good Privacy (PGP).	L1	CO5	PO5,PO6 ,PO7
2	What are the notations of PGP?	L1	CO5	PO5,PO6 ,PO7
3	What do you mean by IKE.	L1	CO5	PO5,PO6 ,PO7
4	Classify the intruders.	L3	CO5	PO5,PO6 ,PO7
5	How E-mail compatibility is performed?	L3	CO5	PO5,PO6 ,PO7
6	How the password files be protected?	L3	CO5	PO5,PO6 ,PO7
7	List out the limitations of secure multiparty computation.	L1	CO5	PO5,PO6 ,PO7
8	Mention the benefits of IPSec.	L1	CO5	PO5,PO6 ,PO7
9	Define cross site scripting vulnerability.	L1	CO5	PO5,PO6 ,PO7
10	Define different types of voting systems in virtual elections.	L1	CO5	PO5,PO6 ,PO7
Part– B(Long Answer Questions)				

11	a)	Name the protocols that provide security in IPSec.	L2	CO5	PO5,PO6 ,PO7
	b)	Write short notes on PGP.	L6	CO5	PO5,PO6 ,PO7
12	a)	Explain in detail about IP Security Policy	L2	CO5	PO5,PO6 ,PO7
	b)	Explain how S/MIME differs form MIME	L2	CO5	PO5,PO6 ,PO7
13	a)	What are the design goals for a firewall? Also mention its Limitations	L1	CO5	PO5,PO6 ,PO7
	b)	List the five important features of IKE key determination algorithm	L1	CO5	PO5,PO6 ,PO7
14	a)	Write a short note on cross site scripting vulnerability.	L6	CO5	PO5,PO6 ,PO7
	b)	Explain secure inter branch payment transactions.	L2	CO5	PO5,PO6 ,PO7
15	a)	Explain the secure multiparty calculation..	L2	CO5	PO5,PO6 ,PO7
	b)	Write a short note on Single sign on.	L6	CO5	PO5,PO6 ,PO7
16	a)	What are the features of IKE Key algorithm.	L1	CO5	PO5,PO6 ,PO7
	b)	Explain the voting systems in virtual elections.	L2	CO5	PO5,PO6 ,PO7

***BloomsTaxonomyLevel(BT)**(L1–Remembering;L2–Understanding;L3–Applying;L4–Analyzing;L5–Evaluating;L6–Creating)

Course Outcomes

(CO)ProgramOutcomes

(PO)

PreparedBy: ANUSHA.K
Assistant Professor
CSE

HOD,CSE

Sample Question paper

Q.P Code: CY3101PC **Hall Ticket No:** | | | | | | | | | | |

NARSIMHA REDDY ENGINEERING

MODEL QUESTION PAPER

COLLEGE(UGC AUTONOMOUS)

III B.Tech I Semester (NR20) Regular Examination, January 2023

Information security

(CSE / CS)

Time :3 hours **Maximum marks:** 75

Note:
- This question paper contains two parts A and B
- Part A is compulsory which carries 25 marks (1st 5 sub questions are one from each unit carry 2 Marks each & Next 5 sub questions are one from each unit carry 3 Marks). Answer all questions in Part A
- Part B Consists of 5 Units. Answer any one full question from each unit. Each question carries 10 Marks and may have a, b sub questions

Part-A (25 Marks)

Answer all questions

Q.No		Question	M	BL	CO	PO
1)	a.	Define passive attack and active attack	2	L1	CO1	PO1,PO6
	b.	Define Denial of service.	2	L1	CO1	PO1,PO6
	c.	Mention the various types of cryptanalytic attack.	2	L2	CO2	PO3
	d.	What are the operations used in AES?	2	L1	CO2	PO3
	e.	Define Digital signature	2	L1	CO3	PO2,PO3
	f.	What you meant by MAC	3	L1	CO3	PO2,PO3
	g.	What are the benefits of mobile device security.	3	L1	CO4	PO1,PO3
	h.	Mention the phases of the Handshake protocol.	3	L2	CO4	PO1,PO3
	i.	What are the notations of PGP?	3	L1	CO5	PO5,PO6, PO7
	j.	What do you mean by IKE.	3	L1	CO5	PO5,PO6, PO7

Part-B (50 Marks)

Answer any five questions

All Questions carry equal Marks

Q.No		Question	M	BL	CO	PO
UNIT–I						
2)	a.	Explain in detail about OSI security architecture.	5	L2	CO1	PO1,PO6
	b.	Explain classical encryption techniques (Steps involved in each encryption technique like Caesar cipher, playfair cipher, hill cipher, vigenere cipher, one time pad cipher, rail fence, etc)	5	L3	CO1	PO1,PO6
OR						
3)	a.	what is meant by security attack? Explain various types of security attacks.	5	L2	CO1	PO1,PO6
	b.	Draw a matrix that shows the relationship between security mechanisms and attacks.	5	L2	CO1	PO1,PO6
UNIT–II						
4)	a.	Explain the steps involved in knapsack algorithm with an example	5	L2	CO2	PO3
	b.	Explain in detail about the steps involved in DES.	5	L3	CO2	PO3
OR						
5)	a.	Explain the steps involved in RC4.	5	L3	CO2	PO3
	b.	Explain RSA algorithm. And perform Encryption and Decryption using RSA p=3 q=11 e=7 M=5	5	L3	CO2	PO3
UNIT–III						
6)	a.	With the example, explain in detail about Secure Hash Algorithm	5	L2	CO3	PO2,PO3
	b.	Explain in detail about HMAC and Digital Signature Standard	5	L3	CO3	PO2,PO3
OR						
7)	a.	Explain in detail about Elgamal Digital signature scheme.	5	L2	CO3	PO2,PO3
	b.	Verify the signature with the Elgamal Digital signature of values q=19,α=10,XA=16,m=14,k=5.	5	L3	CO3	PO2,PO3
UNIT–IV						
8)	a.	Briefly explain about transport layer security and Padding.	5	L3	CO4	PO1,PO3
	b.	With a neat diagram, explain the operation of SSL and SSH Record Protocol.	5	L4	CO4	PO1,PO3
OR						

9)	a.	Write a short note on HTTPS.	5	L3	CO4	PO1,PO3
	b.	What are the different types of mobile device security. Explain each.	5	L2	CO4	PO1,PO3
UNIT–V						
10)	a.	Name the protocols that provide security in IPSec.	5	L2	CO5	PO5,PO6 ,PO7
	b.	Write short notes on PGP.	5	L4	CO5	PO5,PO6 ,PO7
OR						
11)	a.	Explain in detail about IP Security Policy	5	L2	CO5	PO5,PO6 ,PO7
	b.	Explain how S/MIME differsform MIME	5	L2	CO5	PO5,PO6 ,PO7

M – Marks **CO –** Course Outcomes **PO –** Program Outcomes

BL – Bloom's Taxonomy Levels (**L1–**Remembering, **L2–**Understanding, **L3–** Applying,**L4–**Analyzing, **L5–**Evaluating, **L6–**Creating)