NARSIMHA REDDY ENGINEERING COLLEGE
UGC-AUTONOMOUS INSTITUTION
NRCM
Your roots to success...

An Autonomous Institute
NAAC Accreditation 'A' Grade
Accredited by NBA
Approved by AICTE, Affiliated to JNTUH

Previous Question Papers:

Q.P Code: AM4101PC Hall Ticket NO □□□□□□□□□

NARSIMHA REDDY ENGINEERING

MODEL QUESTION PAPER

COLLEGE(UGC AUTONOMOUS)

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

Information security

(Common to AIML,DS)

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

Previous Question Papers

R13

Code No: 126AQ

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech III Year II Semester Examinations, May - 2016INFORMATION SECURITY

(Computer Science and Engineering)

Time: 3hours **Max.Marks:75**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries10 marks and may have a, b, c as sub questions.

PART- A

(25 Marks)

1.a) What are the types of security attacks? [2
]

b) Compare substitution ciphers with transposition ciphers. [3]

c) Compare block ciphers with stream ciphers. [2]

d) Write about strength of DES algorithm. [3]

e) What is a digital signature? [2]

f) What properties must a hash function have to be useful for message authentication?[3]

g) What are the various PGP services? [2]

h) What parameters identify an SA and what parameters characterize the nature of a particular SA?
[
3]

i) What is cross site scripting vulnerability? [2]

j) What are the limitations of firewalls? [3]

PART-B

(50 Marks)

2.a) Consider the following:
Plaintext:
“PROTOCOL” Secret
key: “NETWORK”
What is the corresponding cipher text using play fair cipher method?

b) What is the need for security? [5+5]

OR

3.a) Explain the model of network security.

b) Write about steganography. [5+5]

4. Explain the AES algorithm. [10]

OR

5. Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive rootα=2.
   a) If user „A‟ has public key Y_A=9, what is A‟s private key X_A.
   b) If user „B‟ has public key Y_B=3, what is shared secret key K. [5+5]

6. Explain HMAC algorithm. [10]

OR

7.a) Explain the DSA algorithm.
   b) What is bio-metric authentication? [5+5]

8.a) Explain PGP trust model.
   b) What are the key components of internet mail architecture? [5+5]

OR

9.a) Explain MIME context types.
   b) What are the five principal services provided by PGP? [5+5]

10. Explain secure electronic transaction. [10]

OR

11.a) Explain password management.
   b) What are the types of firewalls? [5+5]

R13

Code No: 126AQ

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech III Year II Semester Examinations, December - 2017

INFORMATION SECURITY

(Computer Science and Engineering)

Time: 3 hours **Max. Marks: 75**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 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, c as sub questions.

PART - A

(25 Marks)

1. a) Define Non Repudiation. [2]
b) Write a short notes on steganography. [3]
c) Define linear cryptanalysis. [2]
d) Discuss about Electronic code book mode? [3]
e) Define Message Authentication Code. [2]
f) Illustrate about biometric authentication. [3]
g) What is IP Security? [2]
h) Discuss about the concept of combining security associations. [3]
i) What is Firewall? [2]
j) Write short notes on virtual elections. [3]

PART - B

(50 Marks)

2. Compare and Contrast between Symmetric and Asymmetric key cryptography. [10]

OR

3. Give an example to explain the concept of transposition ciphers in detail. [10]

4. With a neat diagram explain how encryption and decryption are done using Blowfish algorithm? [10]

OR

5. 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. [10]

6. Give a neat sketch to explain the concept of Secured Hash Algorithm (SHA). [10]

OR

7. Client machine C wants to communicate with server S. Explain how it can be achieved through Kerberos protocol? [10]

8. How the messages are generated and transmitted in pretty good privacy (PGP) protocol? Explain with clear diagrams. [10]

OR

9. Draw the IP security authentication header and explain the functions of each field. [10]

10. Explain the steps involved in performing Secure Inter-branch Payment Transactions. [10]

OR

11. List the characteristics of a good firewall implementation? How is circuit gateway different from application gateway? [10]

---ooOoo---