Code No: 157CC **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, January/February - 2023
INFORMATION SECURITY
(Information Technology)

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

Note: i) Question paper consists of Part A, Part B.
ii) Part A is compulsory, which carries 25 marks. In Part A, answer all questions.
iii) In Part B, Answer any one question from each unit. Each question carries 10 marks and may have a, b as sub questions.

PART – A

(25 Marks)

1.a)	What do you mean by security service?	[2]
b)	What is Cryptanalysis?	[3]
c)	Describe the use of public key Cryptography.	[2]
d)	What are the requirements of MAC function?	[3]
e)	What is Digital Signature?	[2]
f)	What are the authentication applications?	[3]
g)	What is TLS?	[2]
h)	Write about Security Association.	[3]
i)	What do you mean by Worms?	[2]
j)	What is the function of firewall?	[3]

PART-B

(50 Marks)

2.	Explain in detail about the Blowfish Algorithm.	[10]
	OR	
3.a)	Explain about Random number generation.	
b)	What is traffic confidentiality?	[5+5]
4.	Explain the Diffie –Hellman key exchange algorithm.	[10]
	OR	
5.	Explain the SHA 512 algorithm. Illustrate with an example.	[10]
6.	Explain in detail about Kerberos.	[10]
	OR	
7.	What do you mean by PGP? Explain the working of PGP.	[10]
8.	What is IP Security? Discuss in detail about IP Security Architecture.	[10]
	OR	
9.	Explain in detail Secure Electronic Transaction.	[10]
10.	Discuss about: a) Intruders b) Trusted system.	[5+5]
	OR	
11.	Explain in detail about Intrusion Detection System.	[10]

--ooOoo--

Code No: 157CC **R18**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech IV Year I Semester Examinations, July/August - 2022
INFORMATION SECURITY
(Information Technology)

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

Answer any five questions
All questions carry equal marks
- - -

1.a) Draw a matrix that shows the relationship between security mechanisms and attacks.
b) List and explain the Strength of DES. [7+8]

2.a) 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.

b) With the help of a neat diagram, explain the model for Internetwork security. [8+7]

3.a) Consider a Diffie- Hellman key with a common prime q=11 and primitive root $\alpha = 2$, If the user has a public key $Y_a = 9$ what is A's private key X_A.
b) Briefly explain the Public key Cryptography Principles in detail. [5+10]

4. Discuss about Message authentication and Hash Functions. [15]

5.a) List and explain the PGP services and explain how PGP message generation is done with a neat diagram.
b) Mention three variations of digital signatures and briefly state the purpose of each. [8+7]

6.a) Explain the X.509V3 certificate format.
b) In PGP, what is the probability that a user with N public keys will have at least one, duplicate key ID? [8+7]

7.a) Discuss the steps involved in Secure Electronic Transaction.
b) Draw and explain the IP security architecture. [8+7]

8.a) Select any antivirus of your choice and explain it in detail.
b) Where would you place a web server in an organization assuming that you can use a network firewall and why? [8+7]

--ooOoo--

Code No: 126AQ **R13**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, May - 2016
INFORMATION 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 carries 10 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 root

α=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 biometric 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]

Code No: 126AQ **R13**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, October/November - 2016
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)	Explain the network security model.	[2]
b)	What are the two basic functions used in encryption algorithms?	[3]
c)	What are the advantages of Key Distribution?	[2]
d)	What are the principles of public key cryptosystems?	[3]
e)	List three approaches to Message Authentication.	[2]
f)	Explain the importance of knapsack algorithm.	[3]
g)	What are different approaches to Public-key Management?	[2]
h)	How does PGP provides public key management?	[3]
i)	What is Secure Socket Layer?	[2]
j)	What are different alert codes of TLS protocol?	[3]

PART - B

(50 Marks)

2.a)	Explain the terminologies used in Encryption.	
b)	Describe in detail about Conventional Encryption Model.	[5+5]
	OR	
3.a)	Compare symmetric and asymmetric key cryptography.	
b)	What is Steganography? Explain its features.	[5+5]
4.a)	Differentiate linear and differential crypto-analysis.	
b)	Explain Block Cipher design principles.	[5+5]
	OR	
5.	Briefly explain the characteristics and operations of RC4 Encryption algorithm.	[10]
6.a)	What are the requirements of Authentication?	
b)	Discuss about Secure Hash algorithm.	[5+5]
	OR	
7.a)	Explain the approaches for Digital Signatures based on Public Key Encryption.	
b)	Discuss about Biometric Authentication.	[5+5]

8. Briefly discuss about different services provided by Pretty Good Privacy (PGP). [10]

OR

9. What are different cryptographic algorithms used in S/MIME? Explain how S/MIME is better than MIME.

10.a) List and briefly define the parameters that define an SSL session state.

b) What are different services provided by the SSL Record Protocol? [5+5]

OR

11.a) What is a Firewall? Explain its design principles and types with example.

b) Discuss about Password Management. [5+5]

---ooOoo---

R13

Code No: 126AQ

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, May - 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)	Give various security services.	[2]
b)	What are the principles of security?	[3]
c)	Define Stream ciphers?	[2]
d)	Discuss about Blowfish.	[3]
e)	What is Biometric authentication?	[2]
f)	Discuss various Digital signatures.	[3]
g)	Give features of Authentication Header.	[2]
h)	Explain IP Security.	[3]
i)	How to manage the password?	[2]
j)	Discuss cross site scripting vulnerability.	[3]

PART - B

(50 Marks)

2.a) Discuss in detail about various types of Security attacks with neat diagrams.
b) Give a model for Network Security with neat diagram. [5+5]

OR

3.a) What is symmetric key cryptography? Discuss its advantages and limitations.
b) Explain various substitution techniques with suitable examples. [5+5]

4.a) Explain DES algorithm with suitable examples. Discuss its advantages and limitations.
b) What is Elliptic Curve Cryptography (ECC)? Discuss ECC algorithm with neat diagram. [5+5]

OR

5.a) Explain RSA algorithm with suitable examples.
b) Write a short note on RC4. [5+5]

6.a) Write a short note on knapsack algorithm.
b) Give various Hash Functions. Discuss secure hash algorithm with suitable examples. [5+5]

OR

7.a) Discuss HMAC and CMAC.
b) Write short notes on Kerberos. [5+5]

8.a) Write a short note on Pretty Good Privacy.
b) Give IP Security architecture with neat diagram. [5+5]

OR

9.a) Write a short note on S/MIME.
b) Discuss in detail encapsulating security payload. [5+5]

10.a) What is Intrusion? Discuss Intrusion detection system with neat diagram.
b) Discuss the need of Secure Socket Layer. [5+5]

OR

11.a) Write a short note on firewall design principles and types of firewalls.
b) Discuss in detail about secure electronic transaction. [5+5]

---ooOoo---

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---