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 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]

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]

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---

Code No: 126AQ **R13**

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 a short note on Verberos. [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---

Code No: 126AQ **R13**

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---

R13

Code No: 126AQ

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, December - 2018
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)	Compare transposition ciphers with substitution cipher.	[2]
b)	Explain the principles of security.	[3]
c)	What are the advantages of public key cryptography algorithm comparing ryman encryption algorithm.	[2]
d)	List the advantages of elliptic-curve cryptography.	[3]
e)	List three approaches to message authentication.	[2]
f)	What is the function of TGS server in Kerberoes.	[3]
g)	What are S/MIME message?	[2]
h)	List the different encryption and authentication algorithms used for AH and ESP protocols.	[3]
i)	What are the limitations of firewalls?	[2]
j)	What is intruder?	[3]

PART-B

(50 Marks)

2.a) Consider the following:
Plaintext: “KEY”
Secret key: “CRYPTOGRAPHY”
Compute the cipher text from given plain text and key using hill cipher method.
b) Explain the model for network security. [5+5]

OR

3.a) Explain the transposition techniques.
b) What are the advantages of steganography comparing with cryptography? [5+5]

4. Explain the AES algorithm. [10]

OR

5.a) Write short notes on key distribution.
b) In an RSA system, the public key of a given user is e=31, n=3599. What is the private key of this user? [5+5]

6. Explain whirlpool algorithm. [10]

OR

7. Explain X.509 authentication service. [10]

8. Explain the operation PGP message generation and message reception. [10]

OR

9.a) What are the cryptographic algorithms used in S/MIME?

b) Draw and explain fields in AH header. [5+5]

10. Explain secure inter branch payment transactions. [10]

OR

11.a) What is password management?

b) What are the various virus counter measures? [5+5]

---ooOoo—