SIDDHARTH GROUP OF INSTITUTIONS :: PUTTUR
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code : (16EC5509) CRYPTOGRAPHY AND NETWORK SECURITY

Course & Branch: M.Tech - ES **Year & Sem:** I-M.Tech & II-Sem

Regulation: R16

UNIT –I

SYMMETRIC CIPHERS, PUBLIC-KEY ENCRYPTION AND HASH FUNCTIONS

1.(a)What is steganography? What is its purpose? (6M)
(b)Explain various modes of operations of block ciphers. (6M)

2.(a)How the hash function value is generated in simple hash functions. (6M)
(b)Discuss about classical encryption techniques (6M)

3.(a)Explain active and passive security attacks. (6M)
(b)Explain the steganography technique with a block diagram. (6M)

4.(a)Explain DES encryption algorithm (6M)
(b)Describe Blowfish symmetric block cipher algorithm. (6M)

5.(a)Discuss the key distribution scenario with flow diagram. (6M)
(b)Explain the RSA algorithm with an example (6M)

6.(a)Explain basic requirements for public-key cryptography. (6M)
(b)Write short notes on digital signature and authentication protocols. (6M)

7.(a)What are symmetric key algorithms? Explain in brief. (6M)
(b)What is secure hash algorithm? Explain. (6M)

8.(a)Explain about authentication protocols (6M)
(b)State the requirements for the design of an elliptic curve cryptosystem. Using that, discuss how secret keys are exchanged and messages are encrypted. (6M)

9.(a)What are cryptanalytic attacks? How do they differ from brute force attack? (6M)
(b)Explain Diffie-Hellman key exchange scheme in detail. (6M)

10.(a)In AES, explain how the encryption is expanded to produce keys for 10 rounds. (6M)
(b)Discuss about different conventional encryption techniques (6M)

SIDDHARTH GROUP OF INSTITUTIONS :: PUTTUR
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code : (16EC5509) CRYPTOGRAPHY AND NETWORK SECURITY

Course & Branch: M.Tech - ES **Year & Sem:** I-M.Tech & II-Sem

Regulation: R16

UNIT –II

NETWORK SECURITY PRACTICE

1.(a)What are the approaches of message authentication? (6M)
(b)Discuss about Euler's theorem. (6M)

2.(a)Differentiate between Kerbors version 4 and version 5. (6M)
(b)Explain how both confidentiality and authentication are achieved by using PGP. (6M)

3.(a)Discuss about X509 authentication service in detail. (6M)
(b)Explain about S/MIME in detail. (6M)

4.(a)Describe the different cryptographic functions provided by PGP. (6M)
(b)Explain in detail about Kerberos. (6M)

5.(a)Describe the authentication dialogue used by Kerberos for obtaining services from another realm. (6M)
(b)List and explain three approaches to secure user authentication over a network or internet. (6M)

6.(a)Explain X.509 authentication service and its certificates. (6M)
(b)Explain the services of Pretty Good Privacy (PGP). (6M)

7.(a)What is biometric authentication? Explain. (6M)
(b)Explain about the authentication tokens. (6M)

8.(a)What are the approaches of message authentication? (6M)
(b)Explain the concept of PGP in electronic mail security. (6M)

9.(a)Explain with the help of an example, how a user's certificate is obtained from another certification authority in X.509 scheme. (6M)
(b)Why does PGP maintain key rings with every user? Explain how the messages are generated and received by PGP. (6M)

10.(a)Explain encapsulating security payload. (6M)
(b)write short notes on key management. (6M)

SIDDHARTH GROUP OF INSTITUTIONS :: PUTTUR
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code : (16EC5509) CRYPTOGRAPHY AND NETWORK SECURITY

Course & Branch: M.Tech – ES **Year & Sem:** I-M.Tech & II-Sem

Regulation: R16

UNIT –III

SYSTEM SECURITY, WIRELESS SECURITY

1.Discuss in detail the different classes of intruders and the intrusion techniques. (12M)

2.(a)Explain any two approaches for intrusion detection. (6M)
(b)Explain wireless LAN security factors and issues in detail. (6M)

3(a)Elaborate the characteristics of a good firewall implementation. (6M)
(b)Explain about wireless LAN security standards. (6M)

4.(a)Explain in detail about firewalls. (6M)
(b)Explain briefly about trusted systems. (6M)

5.(a)What are the different types of attacks? Explain. (6M)
(b)Write a short note on data security. (6M)

6.(a)Discuss about different types of intrusion detection techniques. (6M)
(b)Explain the basic principles of firewall design. (6M)

7.(a)What are firewall design principles? Explain. (6M)
(b)Explain about trusted systems. (6M)

8.(a)Explain rule based intrusion detection schemes. (6M)
(b)Explain any two types of firewalls. (6M)

9.(a)Explain in detail about password management schemes with neat diagram. (6M)
(b)Write short notes on firewall design principles. (6M)

10.(a)Elaborate the characteristics of a good firewall implementation. (6M)
(b)Write short notes on Malicious Software. (6M)

SIDDHARTH GROUP OF INSTITUTIONS :: PUTTUR
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code : (16EC5509) CRYPTOGRAPHY AND NETWORK SECURITY

Course & Branch: M.Tech - ES **Year & Sem:** I-M.Tech & II-Sem

Regulation: R16

UNIT –IV

SECURE NETWORKING THREATS, ENCRYPTION TECHNIQUES

1.List and explain the following:
(a)Security attacks. (4M)
(b)Security services. (4M)
(c)Security mechanisms. (4M)

2.(a)Write short notes on random number generation. (6M)
(b)In a public-key system using RSA, you intercept the ciphertext C=10 sent to a user whose public key is e=5, n=35. What is the plaintext M? (6M)

3.(a)Discuss about secure socket layer and transport layer security. (6M)
(b)What is digital certificate? Explain its role in network security. What is the process of obtaining a digital certificate? (6M)

4.(a)Is it necessary to recover the secret key in order to attack a MAC algorithm? Explain.(6M)
(b)What characteristics are needed in a secure hash function? Discuss. (6M)

5.Explain the following:
(a)Data security. (4M)
(b)Detection system. (4M)
(c)Attacker types. (4M)

6.(a)Write down the triple DES algorithm and explain with neat diagram. (6M)
(b)Explain about RSA algorithm with example as p = 11, q = 5, e = 3 and PT = 9. (6M)

7(a)Explain RSA algorithm with an example. (6M)
(b)Discuss about different functions of secure hash algorithm. (6M)

8.(a)What is biometric authentication? Explain. (6M)
(b)Explain about the authentication tokens. (6M)

9.(a)Explain DES encryption algorithm. (6M)
(b)Describe Blowfish symmetric block cipher algorithm. (6M)

10.Write short notes on (a) Message digest algorithm. (6M)
(b) Hash Algorithm. (6M)

SIDDHARTH GROUP OF INSTITUTIONS :: PUTTUR
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code : (16EC5509) CRYPTOGRAPHY AND NETWORK SECURITY

Course & Branch: M.Tech – ES **Year & Sem:** I-M.Tech & II-Sem

Regulation: R16

UNIT –V

DESIGNING SECURE NETWORKS

1.Discuss about secure socket layer and transport layer security. (12M)

2.What is virus? Explain different types of viruses and their counter measures. (12M)

3.(a)Explain the internet control message protocol design considerations. (6M)

(b)Explain the layer 2 security considerations. (6M)

4.(a)Explain about IP addressing design considerations. (6M)

(b)Write a short notes on transport protocol design considerations. (6M)

5.(a)Discuss about components of hardening strategy. (6M)

(b)Explain the importance of IP addressing design considerations (6M)

6. (a)Explain the features of IPSec architecture. (6M)

(b)Discuss SSL protocol stack. (6M)

7. (a) Mention the difficulties of Secure Networking. (6M)

(b)Write short notes on Security Technologies. (6M)

8. (a) Explain briefly about Host Operating Systems. (6M)

(b) Write short notes on Rogue Device Detection. (6M)

9. List and explain three approaches to secure user authentication over a network or internet. (12M)

10.(a)Describe the Network Security Technologies. (6M)

(b)Explain about the Difficulties of Secure Networking. (6M)