SRINIVAS UNIVERSITY
INSTITUTE OF ENGINEERING AND TECHNOLOGY
MUKKA, MANGALURU

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

Cryptography and Network Security

SUBJECT CODE: 19SEC641

COMPILED BY:

Mr.Veeranna Kotagi, Assistant Professor

MODULE 1

INTRODUCTION

1.What are the 3 impacts of cyber security attacks?

2.What are 3 different types of cyber attacks?

3.What is the main cause of cyber attacks?

4.What methods are used to defend against cyber attacks?

5.Which technique is used in cyber attack?

6.Which technique is used in cyber attack?

7.What is the best Defence against the cyber threat?

8.What is the best defense against injection attacks?

9.What are the consequences of cyber attacks?

10.How modular arithmetic is used for encryption?

11.How is mod in information security calculated?

12.What is modular arithmetic GCD?

13.What is modulo arithmetic and discuss its properties in cryptography?

14.What are the properties of modular arithmetic?

15.What is Chinese remainder theorem give an example?

16.How do you solve Chinese remainder theorem problems?

17.How is Chinese remainder calculated?

18.What is an example of a substitution cipher?

19.What is the weakness of substitution cipher?

20.In which cipher more than one alphabet is used for substitution?

21.What makes a product cipher secure?

22.What are the examples of product cipher?

23.What is the strength of DES in CNS?

24.How many rounds is implemented in DES?

25.Which mode of operation is used in DES?

MODULE 2

PUBLIC KEY CRYPROGRAPHY AND RSA

1.What is RSA in CNS?

2.How do you perform an RSA encryption?

3.Explain Steps in RSA Algorithm.

4.How the cryptographic algorithms RSA works?

5.Why RSA algorithm works in cryptography?

6.What are the possible attacks on RSA?

7.On what problem is the RSA algorithm based on?

8.Why RSA algorithm is slow?

9.Why is RSA difficult to break?

10.What applications use RSA encryption?

11.How do you generate a key using RSA algorithm?

12.How is RSA used for encryption in practice?

13.Why is RSA not used to encrypt application messages?

14.What is PKCS encoding?

15.Where is PKCS 11 used?

16.Is PKCS key exchange secure?

17.What are some common uses of cryptographic hashes?

18.What are properties of cryptographic hash function?

19.What is the output of a cryptographic hash function?

20.Which are the applications of cryptographic hash function?

21.What makes a good cryptographic hash function?

22.What is Diffie-Hellman key exchange in cryptography?

23.What type of key is generated or exchanged by using Diffie-Hellman key exchange algorithm?

24.How do you set the Diffie-Hellman key exchange?

25.What are the features of Diffie-Hellman key exchange?

MODULE 3

KEY MANAGEMENT

1.How are cryptographic keys managed?

2.Why cryptographic key management is important for security?

3.What is an example of key management?

4.How is hashing used in digital certificates?

5.What is digital certificate? What it contains?

6.What are differences between digital certificate and digital signature?

7.What type of key technology is used with public-key cryptography?

8.What type of certificate is most often used in modern PKI?

9.What are the specific components of the public key infrastructure PKI?

10.Which certificate are used as the base of the public key infrastructure?

11.How does identity-based encryption work?

12.What is the motivation for proposing the identity-based encryption?

13.What is a one-way cryptographic hash?

14.Explain the process of mutual authenticity.

15.What is dictionary attack in cryptography?

16.How does a dictionary attack break a cipher?

17.How does a dictionary attack work?

18.How long does a dictionary attack take?

19.Explain centralized authenticity.

20.What is Needham Schroeder proposed for secret key distribution?

21.Which two cryptographic algorithms are used with IPSec?

22.How does IPSec hash work?

23.What are the three protocols used in IPsec?

24.What are the 2 modes of IPsec operation?

25.How cryptography is used in network security?

26.What are pros and cons of security at different layers?

MODULE 4

IEEE 802.11

1.What standard does IEEE 802.11i use for confidentiality integrity and authentication?

2.What security protocol does 802.11 use?

3.What encryption ciphers does 802.11 use?

4.What vulnerabilities do worms exploit?

5.How a worm can disrupt a computer or a network?

6.What is the difference between a virus and a worm?

7.What is firewall and explain?

8.What is firewall and explain?

9.What is firewall and its application?

10.What is the purpose of IPS?

11.What is the best intrusion prevention system?

12.What is an example of an intrusion prevention system?

13.What are two types of intrusion prevention systems?

14.What are the different types of intrusion detection system?

15.Explain differences between IDS and IPS.

16.How can DDoS attacks be detected and prevented?

17.How do you detect a DDoS attack?

18.What is DDoS prevention system?

19.What is the best defense against a DDoS attack?

20.What id DDoS?

MODULE 5

IT ACTS

1.What are the aims of IT act 2000?

2.Explain the objectives of IT act 2000.

3. What is the scope of IT act 2000?

4.Explain the provisions of IT act.

5.What is attribution of electronic records?

6.What is the procedure for authentication of electronic records?

7.Which sections of IT Act, 2000 deals with Acknowledgement of receipt?

8.HOW IT Act deals with secure digital signatures?

9.What is secure digital signature?

10.What is electronic signature as per IT Act, 2000?

11.Explain the procedure of appointment of controllers in IT act.

12.What are digital signature certificates?. Explain