

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**CRYPTOGRAPHY AND NETWORK SECURITY**

**Class &Sem: III & II Academic Year: 2024-2025**

**Question Bank**

**UNIT-I**

**Basic Principles:**

**Security Goals:**

1. Illustrate a brief note on security goals.**[7M] [R20, SET-2, July -2023] [Understand]**
2. Write a short note on authentication and data integrity. **[7M] [R20, SET-4, July -2023] [Evaluate]**
3. What is Network Security? What are the Four Goals of Network Security? Explain with examples. **[7M] [R20, SET-3, May/June-2024]**
4. Elaborate on the security goals to be achieved. **[7M] [R20, SET-4, May/June-2024]**
5. Explain the operational security model with a block diagram. **[7M] [R20, SET-4, May/June-2024]**
6. What are the elements of information security? Explain each in brief. **[7M] [R20, SET-4, May/June-2024]**

**Cryptographic Attacks:**

1. Explain the categories of security threats. **[7M] [R20, SET-1, July -2023] [Understand]**
2. Explain active and passive attacks in detail. **[7M] [R20, SET-1, July -2023] [Understand]**
3. Write a brief note on integrity and non-repudiation with an example. **[7M] [R20, SET-2, July -2023] [Evaluate]**
4. What is the need of security? Explain about various security threats. **[7M] [R20, SET-1, May/June-2024]**
5. What is Cryptography? What are the main challenges and risks? **[7M] [R20, SET-1, May/June-2024]**
6. What is a Cryptographic Attack? What are the different types of attacks? **[7M] [R20, SET-2, May/June-2024]**
7. Which Tools are used by attackers to attack web sites? Explain. **[7M] [R20, SET-2, May/June-2024]**
8. What tricks attackers use to hack online banking accounts? How to prevent them? **[7M] [R20, SET-3, May/June-2024]**
9. Elaborate on attacks threatening confidentiality. **[7M] [R20, SET-3, May/June-2024]**
10. What is timing Attack? What are the possible defenses against timing attack? **[7M] [R20, SET-4, May/June-2024]**

**Services and Mechanisms:**

1. Differentiate policies, mechanisms and services in network security. **[7M] [R20, SET-1, July -2023] [Evaluate]**
2. Differentiate between symmetric and asymmetric encryption. **[7M] [R20, SET-1, July -2023][Evaluate]**
3. Define security attack, security mechanism and security services. **[7M] [R20, SET-2, July -2023] [Evaluate]**
4. Explain different types of security services. **[7M] [R20, SET-3,July -2023][Understand]**
5. What is steganography? explain the techniques in it, it from cryptography. **[7M] [R20, SET-, 3July -2023][Analyze]**
6. What kinds of services are provided for data security? Discuss in detail. **[7M] [R20, SET-4, July -2023] [Analyze]**
7. Explain the aspects required for network security model. **[7M] [R20, SET-4, July -2023][Understand]**
8. Explain the network security model with neat sketch. **[7M] [R20, SET-2, July -2023][Understand]**

**Mathematics of Cryptography:**

1. What are the basic mathematical concepts used in cryptography? Explain with examples. **[7M] [R20, SET-3, July -2023] [Analyze]**
2. Define plain text, cipher text, enciphering, deciphering with an example. **[7M] [R20, SET-4, July -2023] [Evaluate]**
3. What are the mathematical methods used in cryptography? Give their significance. **[7M] [R20, SET-2, May/June-2024]**
4. What is Fermat's theorem? Explain how it is used in security? **[7M] [R20, SET-2, May/June-2024]**

**UNIT-II**

**Symmetric Encryption: Mathematics of Symmetric Key Cryptography:**

1. Explain about the essential ingredients of symmetric cipher. **[7M] [R20, SET-1, July -2023] [Understand]**
2. Compare and contrast between stream cipher with block cipher. **[7M] [R20, SET-1, July -2023] [Analyze]**
3. List and explain block cipher modes of operation. **[7M] [R20, SET-1, July -2023] [Analyze]**
4. Differentiate between cryptanalysis and brute force attack. **[7M] [R20, SET-2, July -2023] [Evaluate]**
5. Describe various mathematics used for symmetric key encryption algorithm. **[7M] [R20, SET-4, July -2023][Understand]**
6. Describe about RC4 and RC5 algorithm. **[7M] [R20, SET-4, July -2023][Understand]**

**Introduction to ModernSymmetric Key Ciphers:**

1. Explain about symmetric key cryptography and public key cryptography. **[7M] [R20, SET-2, July -2023] [Understand]**
2. Write about different symmetric key ciphers.**[7M] [R20, SET-3, July -2023] [Evaluate]**

**Data Encryption Standard:**

1. Explain DES and different modes of operation in DES state its advantages and disadvantages. **[7M] [R20, SET-1, July -2023] [Understand]**
2. Explain the techniques involved for each round in DES with neat sketch **[7M] [R20, SET-2, July -2023] [Understand]**
3. Draw the general structure of DES and explain encryption and decryption process. **[7M] [R20, SET-3, July -2023] [Create]**
4. Explain the block structures and S-Box design used in DES algorithm. **[7M] [R20, SET-4, July -2023] [Evaluate]**
5. Explain the strength and weakness of DES algorithm. **[7M] [R20, SET-4, July -2023] [Understand]**

**Advanced Encryption Standard:**

1. Explain AES and various operations used in its round function. **[7M] [R20, SET-2, July -2023] [Evaluate]**
2. Briefly explain AES with neat sketch. **[7M] [R20, SET-3, July -2023] [ Understand]**
3. Explain the transformation functions and key expansion for each round in AES. **[7M] [R20, SET-3, July -2023] [Understand]**

**UNIT-III**

**Asymmetric Encryption: Mathematics of Asymmetric Key Cryptography:**

1. Explain various mathematics used for asymmetric key cryptography. **[7M] [R20, SET-1, July -2023] [Understand]**
2. Differentiate between private key and public key encryption. **[7M] [R20, SET-3, July -2023] [Analyse]**

**Asymmetric Key Cryptography**

1. State the differences between diffusion and confusion. **[7M] [R20, SET-1,July -2023][Knowledge]**
2. Brief the strength of RSA algorithm and analyse its performance. **[7M] [R20, SET-1, July -2023] [Understand]**
3. Perform encryption and decryption using RSA for p=17, q=11, e=7, M=88 **[7M] [R20, SET-2, July -2023] [Create]**
4. Write about elliptic curve cryptography. **[7M] [R20, SET-2, July -2023] [Analyse]**
5. Explain substitute byte transformation in AES. **[7M] [R20, SET-2, July -2023] [Understand]**
6. Explain the primitive operations of RC5. **[7M] [R20, SET-2,3, July -2023] [Understand]**
7. Differentiate between private key and public key encryption. **[7M] [R20, SET-3, July -2023] [Analyze]**
8. Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7, N=5 **[7M] [R20, SET-3,July -2023][Create]**
9. Justify your answer whether Diffie Hellman key exchange protocol is vulnerable. **[7M] [R20, SET-3, July -2023] [Evaluate]**
10. User A&B exchange the key using Diffie Hellman algorithm assume A=5, q=11, XA=2, XB=3 find YA, YB,K.**[7M] [R20, SET-4,July -2023][Understand]**
11. Explain the approaches to attack the RSA algorithm. **[7M] [R20, SET-4, July -2023] [Understand]**
12. State the difference between AES decryption algorithm and the equivalent inverse cipher. **[7M] [R20, SET-4, July -2023][Analyze]**
13. Explain RSA algorithm in detail. Identify the possible threats for RSA algorithm and list their counter measures. **[7M] [R20, SET-4,July -2023][Evaluate]**

**UNIT IV**

**Data Integrity, Digital Signature Schemes & Key Management:**

**Message Integrity and Message Authentication:**

1. Explain the classes of message authentication function. **[7M] [R20, SET-1, July -2023] [Understand]**
2. Briefly explain the requirements of message authentication. **[7M] [R20, SET-4,July -2023][Understand]**
3. Differentiate between message authentication and one-way hash function. **[7M] [R20, SET-3, July -2023] [Analyze]**
4. Explain different types of attacks that are addressed by message authentication. **[7M] [R20, SET-3, July -2023][Understand]**

**Cryptographic Hash Functions:**

1. Explain HASH function and its properties in cryptography. **[7M] [R20, SET-1, July -2023] [Evaluate]**
2. Differentiate between MAC and Hash function...**[7M] [R20, SET-1, July -2023] [Analyze]**
3. Explain the role of compression function in hash function. **[7M] [R20, SET-2, July -2023][Evaluate]**
4. Explain any one Hash algorithm. **[7M] [R20, SET-4, July -2023] [Understand]**
5. Write the difference between MD5 and SHA. **[7M] [R20, SET-3,July -2023][Apply]**
6. Explain secure hash algorithm in detail. **[7M] [R20, SET-4, July -2023] [Understand]**
7. Explain in detail about hash function. **[7M] [R20, SET-4, July -2023] [Understand]**
8. Discuss about the objectives of HMAC and its security features. **[7M] [R20, SET-4, July -2023] [Create]**
9. Explain MD5 with neat sketch. **[7M] [R20, SET-4, July -2023] [Understand]**

**Digital Signature:**

1. Explain the requirements of digital signature scheme. **[7M] [R20, SET-4, July -2023] [Understand]**
2. Give a brief note on digital signature algorithm. **[7M] [R20, SET-4,July -2023][Knowledge]**

**Key Management**

1. Differentiate between internal and external error control. **[7M] [R20, SET-4, July -2023] [Analyze]**

**UNIT V:**

**Network Security-I:**

**Security at application layer: PGP and S/MIME:**

1. Explain the operational description of PGP. **[7M] [R20, SET-1,2, July -2023] [Understand]**
2. Write a short note on S/MIME. **[7M] [R20, SET-1, July -2023] [Analyze]**
3. Write a short note on E-mail security. **[7M] [R20, SET-2, July -2023] [Analyze]**
4. Explain the services provided by PGP. **[7M] [R20, SET-2, July -2023] [Understand]**
5. Why is the segmentation and reassembly function in PGP needed explain? **[7M] [R20, SET-4, July -2023] [Understand]**

**Security at the Transport Layer: SSL and TLS:**

1. Explain in detail the operation of SSL. **[7M] [R20, SET-2, July -2023] [Understand]**
2. Differentiate between SSL version 3 and TLS. **[7M] [R20, SET-2, July -2023] [Analyze]**
3. Write a short note on web security. **[7M] [R20, SET-4, July -2023] [Create]**
4. Differentiate between SSL connection and SSL session. **[7M] [R20, SET-4, July -2023] [Analyze]**

**Network Security-II:**

**Security at the Network Layer: IPSec, System Security**

1. Explain the architecture of IP security. **[7M] [R20, SET-4,July -2023][Evaluate]**
2. Write a short note on Authentication header and ESP. **[7M] [R20, SET-4, July -2023] [Analyze]**
3. Give a brief note on IP security. **[7M] [R20, SET-3, July -2023] [Knowledge]**
4. Explain internet key management in IPSEC. **[7M] [R20, SET-3, July -2023] [Understand]**
5. Explain SET with neat sketch. **[7M] [R20, SET-3,July -2023][Understand]**
6. Explain the features of SET. **[7M] [R20, SET-3,July -2023][Evaluate]**
7. Explain the steps involved in SET. **[7M] [R20, SET-4, July -2023][Understand]**