Define Information Security and its importance.

What are the three principles of Information Security?

Differentiate between Active and Passive Attacks.

Explain the significance of Confidentiality in security.

What is Malware? Give two examples.

Define Data Breach and mention one real-world example.

What is the role of Cryptography in Information Security?

Explain the key differences between Information Security and Cybersecurity.

Describe the Network Security Model and its components.

Discuss the importance of Information Security Policies in organizations.

Explain the GDPR regulation and its impact on data privacy.

Differentiate between Data Security and Data Privacy with suitable examples.

Illustrate the various types of Security Attacks with examples.

Explain the Elements of Information Security Policies in detail.

Explain the various areas of security and their importance in modern computing.

Discuss the Security and Privacy challenges in the context of Cloud Computing and IoT.

Analyze the major threats to Information Security and suggest countermeasures.

Discuss the US Data Privacy Laws and compare them with GDPR regulations.

Explain the Security Design Process, including algorithms, secret key distribution, and secure communication protocols.

Evaluate Kerberos Authentication System and its role in secure identity management.

Case Study: A financial company suffered a ransomware attack. Analyze the security policies they should implement to prevent future attacks.

Explain the role of MAC (Message Authentication Code) in ensuring data integrity.

Why is key management crucial in public key cryptography? Explain with an example of PKI.

How does Elliptic Curve Digital Signature Algorithm (ECDSA) improve security over traditional RSA signatures?

Compute the digital signature using SHA-256 and RSA where document hash is given and private key d=13,n=3233d = 13, n = 3233d=13,n=3233.

Explain the role of public and private keys in asymmetric cryptography. How does it enhance security over symmetric cryptography?

Describe the Kerberos authentication process with step-by-step message flow between the client, KDC, and service.

What are the properties of a cryptographic hash function? Explain how SHA-256 ensures integrity and collision resistance.

If a system uses SHA-3 instead of SHA-256 for password hashing, analyze the performance and security trade-offs.

In an AES encryption system, if the key length increases from 128-bit to 256-bit, what is the impact on security?

If an attacker tries a brute-force attack on an RSA key of size 4096 bits, estimate the computational feasibility.

Given a system using both symmetric and asymmetric encryption, compare their performance and security impact.

Given two prime numbers p=17p = 17p=17, q=23q = 23q=23, calculate nnn, ϕ(n)\phi(n)ϕ(n), public key eee, and private key ddd using RSA.

If Alice and Bob agree on a public prime p=23p = 23p=23 and base g=5g = 5g=5, compute their public keys and shared secret using Diffie-Hellman.

Given the elliptic curve y2=x3+4x+20mod 29y^2 = x^3 + 4x + 20 \mod 29y2=x3+4x+20mod29, verify if P(5,22)P(5,22)P(5,22) lies on the curve and compute 2P2P2P.

Discuss the structure of an X.509 certificate. How does it facilitate authentication in TLS/SSL?

Compare the security and efficiency of ECC and RSA. Why is ECC considered more secure with shorter key lengths?

Explain the role of digital signatures in blockchain transactions and their impact on security.

Calculate the time complexity of RSA key generation for a 2048-bit key using modular exponentiation principles.

Derive the key length required for an ECC-based cryptosystem to match the security of a 2048-bit RSA system.

What is the impact of key distribution in public key cryptography? Discuss with examples.

Given an encrypted message using RSA with e=7,n=3233e = 7, n = 3233e=7,n=3233, decrypt it if the ciphertext is 2790.

Define Public Key Cryptography and its importance in security.

What is the role of Key Distribution in cryptography?

Define Digital Signature and its purpose in authentication.

What are the two main components of RSA Algorithm?

List the advantages of Elliptic Curve Cryptography (ECC) over RSA.

Given an Elliptic Curve equation y2=x3+4x+7mod 23y^2 = x^3 + 4x + 7 \mod 23y2=x3+4x+7mod23, verify if the point P(3,10)P(3,10)P(3,10) lies on the curve.

Given an RSA encryption system, if p=5p = 5p=5 and q=11q = 11q=11, compute nnn.

Explain the working of the RSA Algorithm with a simple example.

Differentiate between Public Key Cryptography and Symmetric Cryptography.

Illustrate the steps of the Diffie-Hellman Key Exchange Protocol.

How does Elliptic Curve Cryptography (ECC) work? Explain with an example.

Describe the Message Digest function and its role in integrity verification.

Given p=23p = 23p=23, g=5g = 5g=5, Alice selects a=6a = 6a=6 and Bob selects b=15b = 15b=15, compute their public keys and the shared Diffie-Hellman key.

Compute the digital signature for a given message hash H=20H = 20H=20 using RSA, where d=7d = 7d=7, n=143n = 143n=143.

Analyze the security strengths and weaknesses of RSA and Diffie-Hellman algorithms.

Compare Elliptic Curve Cryptography (ECC) and RSA, and justify which is better for modern cryptography.

Evaluate the role of Digital Signatures in Blockchain and Cryptocurrency Security.

Explain the architecture and working of the Kerberos Authentication System.

Discuss the role of X.509 certificates in SSL/TLS protocols.

Design a secure key exchange mechanism for a cloud-based system.

Propose an enhanced authentication model using a combination of biometric security and public key cryptography.