1. What are the various attack on MAC? The main attacks on Message Authentication Codes (MAC) include:

* Length extension attacks: Attacker can append additional data to an existing message
* Key recovery attacks: Attempts to discover the secret key through cryptanalysis
* Forgery attacks: Creating valid MAC without knowing the key
* Replay attacks: Capturing and reusing legitimate MAC values
* Collision attacks: Finding two different messages that produce the same MAC
* Birthday attacks: Exploiting probability theory to find collisions

1. Demonstrate that the set of polynomials whose coefficients form a field is a ring. To prove this, we need to show the following ring properties: a) Closure under addition and multiplication b) Associativity of addition and multiplication c) Commutativity of addition and multiplication d) Existence of additive and multiplicative identities e) Existence of additive inverses f) Distributive property

For polynomials with coefficients from a field:

* Addition is closed as sum of polynomials yields another polynomial
* Multiplication is closed as product of polynomials yields another polynomial
* Zero polynomial serves as additive identity
* Constant polynomial 1 serves as multiplicative identity
* Each polynomial has an additive inverse (negative coefficients)
* Associative and commutative properties inherit from the field properties
* Distributive property holds as per standard polynomial arithmetic

1. Discuss the advantages of elliptic curve cryptography. Key advantages of ECC include:

* Smaller key sizes for equivalent security level compared to RSA
* Lower computational requirements
* Reduced storage and transmission requirements
* Better power efficiency (important for mobile devices)
* Strong security basis (discrete logarithm problem is harder in elliptic curves)
* Faster key generation
* More efficient implementation in hardware

1. Verify Euler's theorem for a=3 and n=10. Let's solve this step by step:
2. Euler's theorem states: aφ(n) ≡ 1 (mod n) where a and n are coprime
3. First, find φ(10):
   * φ(10) = φ(2 × 5) = φ(2) × φ(5) = 1 × 4 = 4
4. Now compute 34:
   * 34 = 81
5. 81 ≡ 1 (mod 10) Therefore, Euler's theorem is verified for a=3 and n=10
6. What is the difference between link and end-to-end encryption? Link encryption:

* Encrypts data between each network node
* Decryption/re-encryption at each intermediate node
* Protects communication links
* Headers and routing information are encrypted
* Used mainly in lower network layers

End-to-end encryption:

* Encrypts data only at source and destination
* Data remains encrypted through intermediate nodes
* Protects actual message content
* Headers and routing information remain visible
* Used mainly in application layer
* Provides better security for actual message content

1. Discuss the concept of polynomial ring. A polynomial ring is an algebraic structure that consists of:

* Set of all polynomials with coefficients from a ring
* Two operations: addition and multiplication
* Properties:
  + Closed under addition and multiplication
  + Associative and commutative
  + Has identity elements
  + Has distributive property
* Notation: R[x] where R is the coefficient ring
* Examples include: Z[x], Q[x], R[x]

1. How to check whether two numbers are relatively prime? To check if two numbers are relatively prime:
2. Calculate their Greatest Common Divisor (GCD)
3. If GCD = 1, they are relatively prime
4. Use Euclidean algorithm to find GCD:
   * Divide larger number by smaller
   * Replace larger with smaller
   * Replace smaller with remainder
   * Repeat until remainder is 0
   * Last non-zero remainder is GCD
5. What is avalanche effect? The avalanche effect is a crucial property in cryptography where:

* A small change in input (plaintext or key) results in significant changes in output
* Ideally, changing one bit should change about 50% of output bits
* Important for:
  + Diffusion in block ciphers
  + Hash function security
  + Making cryptanalysis more difficult
* Indicates the cryptographic algorithm's strength

1. Explain whether the Diffie Hellman key exchange protocol is vulnerable? Diffie-Hellman protocol has several vulnerabilities:

* Man-in-the-Middle (MITM) attacks
* No authentication by default
* Vulnerable to weak group parameters
* Subject to computational attacks if small prime numbers used
* Small subgroup attacks possible
* Implementation vulnerabilities Mitigations include:
* Using authenticated DH
* Proper parameter selection
* Implementation security measures

1. What two levels of functionality comprise a message authentication? Message authentication comprises:
2. Message Integrity
   * Ensures message hasn't been modified
   * Detects any changes during transmission
   * Uses hash functions or MAC
3. Origin Authentication
   * Verifies the source of message
   * Confirms sender's identity
   * Usually implemented using digital signatures or MAC
4. Verify Fermat's theorem for a=7 and p=19. Fermat's Little Theorem states: ap-1 ≡ 1 (mod p) for prime p Let's verify for a=7, p=19:
5. Calculate 718:
   * 718 = 7 × 717
   * Using modular exponentiation...
6. Result: 718 ≡ 1 (mod 19) Therefore, Fermat's theorem is verified
7. What requirements should a digital signature scheme satisfy? A digital signature scheme should satisfy:
8. Authentication: Verify signer's identity
9. Non-repudiation: Signer cannot deny signing
10. Integrity: Detect message modifications
11. Unforgeability: Cannot be created by others
12. Non-reusability: Signature cannot be used on other documents
13. Efficiency: Reasonable computational requirements
14. Time-independence: Valid regardless of when verified
15. Hardware/software independence: Implementation flexible