3 makr questions

**1. Show that 21 = -9 (mod 10).**  
In modulo 10 arithmetic, we subtract multiples of 10 from 21 until we get a value between 0 and 9. So, 21 mod 10 is 1 because 21 - 2(10) = 1. On the other hand, -9 mod 10 means finding the positive equivalent of -9, which is 1 because -9 + 10 = 1. Therefore, 21 ≡ -9 (mod 10).

**2. What is Euler’s totient function?**  
Euler's totient function, denoted as φ(n), is the count of numbers less than or equal to n that are coprime with n. For example, if n is a prime number, φ(n) = n - 1, because every number less than a prime is relatively prime to it.

**3. Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees".**  
Using the Playfair cipher, we first create a 5x5 matrix using the letters in "occurrence" (no repeating letters), followed by the remaining alphabet (omitting 'j'). The cipher text is generated by pairing the letters of the plaintext and encrypting them according to the rules of the Playfair cipher.

**4. What is a zero point of an elliptic curve?**  
The zero point, or the point at infinity, on an elliptic curve is a conceptual point that acts as the identity element for the group of points on the curve. It behaves like a neutral element in elliptic curve addition.

**5. Differentiate between weak and strong hash function.**  
A weak hash function is susceptible to finding two inputs that produce the same hash output (collision). A strong hash function resists such collisions and ensures that small changes in input produce a vastly different hash, making it ideal for cryptographic applications.

**6. Find the GCD(1970, 1066) using Euclid’s Algorithm.**  
Euclid’s Algorithm is used to find the greatest common divisor (GCD) of two numbers. By repeatedly applying the division algorithm, GCD(1970, 1066) is calculated as 2.

**7. Using the Vigenere cipher, encrypt the word "explanation" using the key 'leg'.**  
The Vigenere cipher uses a repeating key to encrypt plaintext. For "explanation" and the key "leg," the encryption is done by shifting each letter of the plaintext according to the corresponding letter in the key, resulting in the cipher text "ofpebnlvzsb".

**8. Explain rail fence cipher technique (d=2) by encoding the message "ALL THAT GLITTERS ARE NOT GOLD".**  
In a rail fence cipher with depth 2, the message is written in a zigzag pattern across two rows. The encoded message is obtained by reading off the rows one by one. For "ALL THAT GLITTERS ARE NOT GOLD", the cipher text would be "ALTATLTESARNOGLTTIRGOLD".

**9. What are the principal elements of a public key cryptosystem?**  
The principal elements of a public key cryptosystem are the public key, the private key, and the encryption/decryption algorithms. The public key is distributed openly, while the private key remains secret. The system relies on the computational difficulty of deriving the private key from the public key.

**10. What is a message authentication code?**  
A message authentication code (MAC) is a cryptographic code that verifies the integrity and authenticity of a message. It is generated by applying a secret key to the message, ensuring that only parties with the key can authenticate the message.

**11. Why is it important to study the Feistel cipher?**  
The Feistel cipher structure is significant because it forms the basis of many block ciphers, including DES. Its design allows for encryption and decryption to be very similar operations, improving efficiency and security.

**12. What requirements must a public key cryptosystem fulfill to be a secure algorithm?**  
For a public key cryptosystem to be secure, it must ensure confidentiality, integrity, and non-repudiation. Additionally, it must be computationally infeasible to derive the private key from the public key or forge messages

**1. What are the various attacks on MAC?**  
The various attacks on Message Authentication Codes (MACs) include brute force attacks, where an attacker attempts to guess the MAC by trying different combinations, and forgery attacks, where the attacker tries to generate a valid MAC for a fraudulent message. Replay attacks are also possible, where a previously authenticated message is reused.

**2. Demonstrate that the set of polynomials whose coefficients form a field is a ring.**  
A set of polynomials with coefficients from a field forms a ring because it satisfies the ring properties: closure under addition and multiplication, associativity, distributivity, and the presence of an additive identity. For example, polynomials with real coefficients form a ring under polynomial addition and multiplication.

**3. Discuss the advantages of elliptic curve cryptography.**  
Elliptic Curve Cryptography (ECC) offers advantages like smaller key sizes compared to RSA while maintaining equivalent security levels, making it more efficient in terms of computation and memory usage. ECC is also well-suited for mobile and IoT devices due to its low resource requirements and high security.

**4. Verify Euler’s theorem for a=3 and n=10.**  
Euler's theorem states that if aaa and nnn are coprime, then aϕ(n)≡1mod  na^{\phi(n)} \equiv 1 \mod naϕ(n)≡1modn, where ϕ(n)\phi(n)ϕ(n) is Euler's totient function. For n=10n=10n=10, ϕ(10)=4\phi(10) = 4ϕ(10)=4, so we compute 34mod  10=81mod  10=13^4 \mod 10 = 81 \mod 10 = 134mod10=81mod10=1, verifying Euler's theorem.

**5. What is the difference between link and end-to-end encryption?**  
Link encryption encrypts data at each hop between devices in a communication path, meaning that the data is decrypted and re-encrypted at each node. End-to-end encryption ensures that data is encrypted at the sender and remains encrypted until it reaches the final recipient, with no intermediate decryption.

**6. Discuss the concept of a polynomial ring.**  
A polynomial ring is a set of polynomials with coefficients from a particular ring, typically a field, that supports addition and multiplication. The concept extends algebraic structures by allowing operations between polynomials similarly to numbers, while maintaining closure, associativity, and distributive properties.

**7. How to check whether two numbers are relatively prime?**  
Two numbers are relatively prime if their greatest common divisor (GCD) is 1. To check this, you can use Euclid's algorithm. For example, if you want to check whether 8 and 15 are relatively prime, you find that GCD(8, 15) = 1, so they are relatively prime.

**8. What is the avalanche effect?**  
The avalanche effect in cryptography refers to a small change in input (such as flipping one bit) causing significant and unpredictable changes in the output (the cipher text). This property is crucial for strong encryption algorithms, ensuring that small modifications to the input do not produce patterns in the output.

**9. Explain whether the Diffie-Hellman key exchange protocol is vulnerable?**  
The Diffie-Hellman key exchange protocol is vulnerable to man-in-the-middle attacks if the communication channel is not authenticated. An attacker can intercept the exchange and generate separate keys with each party, allowing them to decrypt and alter messages undetected. Secure implementations use additional authentication mechanisms.

**10. What two levels of functionality comprise a message authentication?**  
Message authentication typically involves two functionalities: integrity verification, ensuring that the message has not been altered, and authenticity verification, confirming that the message came from the claimed sender. This can be achieved through mechanisms like MAC or digital signatures.

**11. Verify Fermat’s theorem for a=7 and p=19.**  
Fermat's Little Theorem states that if ppp is a prime and aaa is not divisible by ppp, then ap−1≡1mod  pa^{p-1} \equiv 1 \mod pap−1≡1modp. For a=7a=7a=7 and p=19p=19p=19, we compute 718mod  197^{18} \mod 19718mod19. By calculation, 718≡1mod  197^{18} \equiv 1 \mod 19718≡1mod19, verifying Fermat's theorem.

**12. What requirements should a digital signature scheme satisfy?**  
A digital signature scheme must satisfy authenticity (the signature must verify the signer), integrity (the message cannot be altered without detection), and non-repudiation (the signer cannot deny having signed the message). The scheme must also be computationally infeasible for an attacker to forge a signature.