Treasure Hunt Event Questions

1. RSA Encryption: In an RSA system, the public key is (n=91,e=5)(n = 91, e = 5) (n=91,e=5) and the ciphertext is c=27 c = 27 c=27. If the prime factors of nnn are p=7 p = 7 p=7 and q=13 q = 13 q=13, what is the private key ddd?
A) 29
B) 17
C) 23
D) 19
Answer: C) 23

2. Elliptic Curve Cryptography (ECC): Over F7F_7F7 , the elliptic curve y2=x3+2x+4y^2 = x^3 + 2x + 4y2 = x3+2x+4 includes the point P=(2,5)P = (2,5)P=(2,5). What is 2P2P2P on this curve?
A) (6,1)(6, 1)(6,1)
B) (5,0)(5, 0)(5,0)
C) (3,4)(3, 4)(3,4)
D) (2,6)(2, 6)(2,6)
Answer: A) (6,1)(6, 1)(6,1)

3. AES Encryption: In AES-GCM mode, which of the following must be known to both the sender and the receiver to successfully decrypt a message?
A) Initialization vector (IV) and hash key
B) The public key
C) Ciphertext length
D) The block size
Answer: A) Initialization vector (IV) and hash key

4. Diffie-Hellman: Alice and Bob use p=37p = 37p=37 and g=2g = 2g=2 for the Diffie-Hellman key exchange. Alice sends A=9A = 9A=9, and Bob sends B=27B = 27B=27. What is their shared secret sss?
A) 5
B) 15
C) 22
D) 33
Answer: D) 33

5. Cryptographic Hash Functions: Which of the following best describes a property of a cryptographic hash function?
A) It is a public-key encryption algorithm

B) It can be reversed to retrieve the original data
C) It generates a fixed-size output for any input
D) It relies on symmetric encryption
Answer: C) It generates a fixed-size output for any input

6. Padding Oracle Attack: What is the most important piece of information that an attacker gains when performing a padding oracle attack on a CBC-encrypted message?
A) The correct padding
B) The encryption key
C) A portion of the plaintext
D) The block size used in the encryption
Answer: C) A portion of the plaintext

7. RSA Decryption: For an RSA public key with n=77n = 77n=77 and e=7e = 7e=7, if the ciphertext is c=43c = 43c=43 and p=7p = 7p=7 and q=11q = 11q=11, what is the private key ddd?
A) 55
B) 23
C) 37
D) 19
Answer: D) 19

8. Elliptic Curve Discrete Logarithm: In elliptic curve cryptography, solving the elliptic curve discrete logarithm problem means finding which of the following?
A) The point addition formula for the curve
B) The secret scalar kkk given PPP and Q=kPQ = kPQ=kP
C) The public key from the private key
D) The curve's equation
Answer: B) The secret scalar kkk given PPP and Q=kPQ = kPQ=kP

9. AES ECB Mode: In AES-ECB (Electronic Codebook) mode, which of the following vulnerabilities can occur?
A) Key reuse
B) Predictable ciphertext patterns
C) Reduced key length
D) Padding scheme exploitation
Answer: B) Predictable ciphertext patterns

10. Diffie-Hellman Man-in-the-Middle Attack: In a Diffie-Hellman key exchange, how can a man-in-the-middle attack be prevented?
A) Using elliptic curves
B) By exchanging public keys directly
C) By using digital signatures or certificates
D) Changing the prime number in every session
Answer: C) By using digital signatures or certificates

11. RSA Key Size: What is the minimum recommended key size for RSA encryption to ensure security against modern attacks?
A) 512 bits
B) 1024 bits
C) 2048 bits
D) 4096 bits
Answer: C) 2048 bits

12. Elliptic Curve Point Doubling: For an elliptic curve y2=x3+ax+by^2 = x^3 + ax + by2=x3+ax+b over a prime field, what is the operation of point doubling used for?
A) Adding two distinct points
B) Generating the curve's equation
C) Calculating a secret key
D) Adding a point to itself
Answer: D) Adding a point to itself

13. AES Key Expansion: In AES-128, how many rounds of key expansion are performed to generate round keys?
A) 10 rounds
B) 12 rounds
C) 14 rounds
D) 16 rounds
Answer: A) 10 rounds

14. Diffie-Hellman Prime: In Diffie-Hellman key exchange, what is the role of the prime number ppp?
A) It ensures that all keys are symmetric
B) It helps in the generation of public keys
C) It is used as the shared secret
D) It forms the modulus for exponentiation
Answer: D) It forms the modulus for exponentiation

15. Padding Scheme: Which of the following is commonly used as a padding scheme for block ciphers?
A) PKCS#7
B) RSA-PSS
C) SHA-256
D) XOR
Answer: A) PKCS#7

16. RSA Decryption:
For an RSA public key with n=77n = 77n=77 and e=13e = 13e=13, if the ciphertext is c=17c = 17c=17 and the prime factors of nnn are p=7p = 7p=7 and q=11q = 11q=11, what is the private key ddd?
A) 37
B) 29
C) 27
D) 19
Answer: B) 29

17. Elliptic Curve Cryptography (ECC):
Given the elliptic curve y2=x3+x+1y^2 = x^3 + x + 1y2=x3+x+1 over F7F_7F7, and the point P=(3,6)P = (3, 6)P=(3,6), what is 2P2P2P?
A) (0,3)(0, 3)(0,3)
B) (5,6)(5, 6)(5,6)
C) (1,2)(1, 2)(1,2)
D) (4,0)(4, 0)(4,0)
Answer: A) (0,3)(0, 3)(0,3)

18. AES Encryption:
In AES-256 encryption using GCM mode, what additional piece of data is necessary to verify the integrity of the ciphertext?
A) The padding method
B) The key length
C) The authentication tag
D) The hash function
Answer: C) The authentication tag

19. Diffie-Hellman Key Exchange:
In a Diffie-Hellman key exchange, Alice and Bob use p=31p = 31p=31 and g=3g = 3g=3. Alice sends A=27A = 27A=27, and Bob sends B=10B = 10B=10. What is their shared secret sss?
A) 7
B) 15
C) 22
D) 24
Answer: D) 24

20. Padding Oracle Attack:
In a padding oracle attack, what part of the encryption scheme allows an attacker to reveal plaintext without knowing the decryption key?
A) The symmetric key
B) The encryption algorithm used
C) The error messages generated when incorrect padding is detected
D) The length of the ciphertext
Answer: C) The error messages generated when incorrect padding is detected