16 من إجمالي 24 نقطة

Select the most accurate answer

0/2 The key space (i.e. number of possible keys) in a shift cipher (i.e. Caser _____ Cipher) to encrypt plain text is ✗

Assume that you are encrypting plaintext in a language that has 32 different letters

✗

- 32 ◉
- 26 ○
- 25 ○
- 31 ○

الإجابة الصحيحة

31 ◉

2/2 In stream ciphers where the keystream generator produces keystream [K_1, K_2, ..., K_n] to encrypt plaintext [P_1, P_2, ... P_n], the ciphertext will _____ = be C_i ✓

- K_i + P_i
- ✓ K_i ⊕ P_i
- Enc_K_i (P_i)
- P_i mod K_i

2/2 Among the 3 encryption modes (ECB, CBC & CTR) for block ciphers, _____ offer(s) randomized encryption ✓

Check the box of all that applies (more than on option is allowed)

- ✓ CBC
- ECB
- ✓ CTR

2/2 Among the 3 encryption modes (ECB, CBC & CTR) for block ciphers, ✓
_____ can use parallelism to speed up encryption

Check the box of all that applies (more than on option is allowed)

✓ CTR ☑

✓ ECB ☑

CBC ☐

2/2 In the RSA encryption algorithm, assume that public encryption key is (x, e), and the private decryption key is (d), where (x) is the product of two large prime numbers (p, q). To encrypt a message (M), one computes the

_____ = ciphertext C

"X^(Y*W) -> this read "X to the power (Y*W)

- C = M^(e) mod x ◉
- C = M^(d) mod x ○
- C = M^(e*d) mod x ○

2/2 Following on the question above, to decrypt C, one computes

_____

- M = C^(d) mod x ◉
- M = C^(e) mod x ○
- M = C^(e*d) mod x ○

0/2Following on the question above, knowing (x=p*q), the decryption key (d) ✗ _____ can be computed from (p,q,e) by solving

- e * d mod x = 1
- e * d mod (p-1)(q-1) = 1
- ✗ e * d mod (p-1) (q-1) = x ◉
- e * d mod p * q = 1

الإجابة الصحيحة

- e * d mod (p-1)(q-1) = 1 ◉

0/2 In the Diffie-Hellman protocol, Alice and Bob want to agree on a shared secret. They have two public numbers: a generator (x) and a large prime number (w). Alice chooses (m) at random and sends _____ to Bob. ✗

- x^w mod m
- ✗ m^x mod w ◉
- w^x mod m
- x^m mod w

الإجابة الصحيحة

- x^m mod w ◉

0/2 Following on the question above, Bob chooses (n) at random and send _____ to Alice ✗

- x^w mod n
- x^n mod w
- ✗ n^x mod w ◉
- w^x mod n
- الإجابة الصحيحة
- x^n mod w ◉

2/2

Following on the question above, the shared secret is ✓

x^w mod (m*n)

w^(m+n) mod x

✓ x^(m*n) mod w

x^(m+n) mod w

2/2 Because of birthday attacks the length of hash function outputs should ✓ _____ the key length of block ciphers to achieve equivalent :security

be the same as ○

half of ○

triple ○

✓ double ◉

2/2 Identify which of the following protection mechanisms is not helpful in addressing the problem of buffer overflow. ✓

StackGuard ○

✓ TrustedPath ◉

Non-executable Stack ○

Address space randomization ○

6 من إجمالي 10 نقطة

Please select (Yes/No)

2/2 .The substitution cipher is insecure even in a ciphertext only attack ✓

✓ True ◉

False ○

2/2 The main vulnerability is the subsituation cipher is that they key space is too small. ✓

Yes ○

✓ No ◉

2/2 A Pseudo Random Number Generator is actually a deterministic function such that the same input (seed) will always result in the same output stream. ✓

✓ True ◉

False ○

0/2 Public salting passwords increases the difficulty to launch a dictionary attack against a single user account. ✗

✗ True ◉

False ○

الإجابة الصحيحة

False ◉

0/2

.A hash function that have collisions in it is insecure ✗

✗ True ◉

False ○

الإجابة الصحيحة

False ◉