Dashboard / Courses / Winter 2023-24 / B.Tech Semester 6 / CS364_2024 / General / Endterm Test

Started on	Tuesday, 30 April 2024, 9:50 AM
State	Finished
Completed on	Tuesday, 30 April 2024, 10:06 AM
Time taken	16 mins 25 secs
Grade	**11.00** out of 11.00 (**100**%)

Question **1**

Correct

Mark 1.00 out of 1.00

AES-MIXCOLUMN (234, 56, 118, 221) [Input/Output are in Decimal]

● a. (44, 221, 66, 202) ✓

○ b. (44, 221, 66, 201)

○ c. (44, 220, 66, 202)

○ d. (54, 221, 63, 202)

○ e. none of these

Your answer is correct.

Question **2**

Correct

Mark 1.00 out of 1.00

Consider the Diffie-Hellman key exchange on the Group $\mathbb{Z}_p^*$ with multiplication mod p operation.

Let p = 3319 and generator of the group g = 6.

Alice's secret key = 1197, Bob's secret key = 62.

Select the most appropriate option.

● a. Alice's public key = 1758, Bob's public key = 1582, Shared secret key = 1890 ✓

○ b. Alice's public key = 1582, Bob's public key = 1758, Shared secret key = 1890

○ c. none of these

○ d. Alice's public key = 1658, Bob's public key = 1582, Shared secret key = 1890

○ e. Alice's public key = 1758, Bob's public key = 1582, Shared secret key = 1891

Your answer is correct.

Question **3**

Correct

Mark 1.00 out of 1.00

Consider RSA cryptosystem with p = 691, q = 701 and e = 563.

Here public key = (n, e), private key = (p,q,d)

Consider the message m = 600.

Select the appropriate option.

○ a. e is not legitimate, thus none of these

○ b. e is legitimate, d = 62727, ciphertext = 315318

● c. e is legitimate, d = 62627, ciphertext = 315318 ✓

○ d. e is legitimate, d = 61627, ciphertext = 315318

○ e. e is legitimate, d = 62617, ciphertext = 315318

Your answer is correct.

Question **4**

Correct

Mark 1.00 out of 1.00

AES-INVERSE-MIXCOLUMN (123, 202, 87, 77) [Input/Output are in Decimal]

○ a. (114, 54, 143, 96)

○ b. (157, 132, 225, 110)

○ c. none of these

○ d. (52, 215, 139, 72)

● e. (54, 69, 87, 143) ✓

Your answer is correct.

Question **5**

Correct

Mark 1.00 out of 1.00

Consider RSA cryptosystem with p = 761, q = 769 and e = 941.

Here public key = (n, e), private key = (p, q, d)

Consider the message m = 600.

Select the appropriate option.

○ a. e is not legitimate, thus none of these

● b. e is legitimate, d = 47141, ciphertext = 48006 ✓

○ c. e is legitimate, d = 4741, ciphertext = 48006

○ d. e is legitimate, d = 44141, ciphertext = 48006

○ e. e is legitimate, d = 43141, ciphertext = 48006

Your answer is correct.

Question **6**

Correct

Mark 1.00 out of 1.00

Consider the Elliptic curve E: $y^2 = x^3 + 11x + 23$ defined over $\mathbb{Z}_{43} \times \mathbb{Z}_{43}$.

What is the addition of two points (11, 23) and (26, 30)?

○ a. (7, 20)

○ b. (38, 31)

○ c. (31, 38)

○ d. (6, 41)

● e. (41, 6) ✓

Your answer is correct.

Question **7**

Correct

Mark 1.00 out of 1.00

AES-INVERSE-MIXCOLUMN (123, 212, 88, 77) [Input/Output are in Decimal]

○ a. (75, 152, 227, 110)

● b. (175, 152, 227, 110) ✓

○ c. (175, 152, 27, 110)

○ d. none of these

○ e. (175, 15, 227, 110)

Your answer is correct.

Question **8**

Correct

Mark 1.00 out of 1.00

Consider the Diffie-Hellman key exchange on the Group $\mathbb{Z}_p^*$ with multiplication mod p operation.

Let p = 2689 and generator of the group g = 19.

Alice's secret key = 119, Bob's secret key = 62.

Select the most appropriate option.

○ a. Alice's public key = 1630 , Bob's public key = 2563 , Common secret key = 2409

○ b. Alice's public key = 2573 , Bob's public key = 1631 , Common secret key = 2309

● c. Alice's public key = 2573 , Bob's public key = 1631 , Common secret key = 2409 ✓

○ d. Alice's public key = 1631 , Bob's public key = 2573 , Common secret key = 2409

○ e. none of these

Your answer is correct.

Question **9**

Correct

Mark 1.00 out of 1.00

```
Consider the AES-128 key-scheduling algorithm.
```

```
If K0, K1, ... , K10 denotes the 11 round keys corresponding to the
```

```
secret key K (in hexadecimal),
```

```
K = 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
```

```
Then K1 (in hexadecimal) is
```

● a. `c0 39 34 78 84 6c 52 0f 0c f5 f8 b4 c0 28 16 4b` ✓

○ b. `none of these`

○ c. `c1 84 21 af ed 10 c0 2a 45 fb 89 de 5d a3 52 a5`

○ d. `d6 aa 74 fd d2 af 72 fa da a6 78 f1 d6 ab 76 fe`

○ e. `00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff`

Your answer is correct.

Question **10**

Correct

Mark 1.00 out of 1.00

Consider the Elliptic curve E: $y^2 = x^3 + 23x + 11$ defined over $\mathbb{Z}_{173} \times \mathbb{Z}_{173}$.

What is the addition of two points (28 ,109) and (88, 147)?

○ a. (112, 92)

● b. (8,19) ✓

○ c. (138, 10)

○ d. (133, 73)

○ e. none of these

Your answer is correct.

Question **11**

Correct

Mark 1.00 out of 1.00

Consider the Elliptic curve E: $y^2 = x^3 + 13x + 23$ defined over $\mathbb{Z}_{29} \times \mathbb{Z}_{29}$.

What is the addition of two points (16 , 21) and (9, 12)?

● a. (24, 6) ✓

○ b. (16, 21)

○ c. (7, 14)

○ d. None of these

○ e. (8, 28)

Your answer is correct.

◄ LAB Assignment 3

Jump to...