| | |
|---|---|
| **Started on** | Tuesday, 18 April 2023, 2:36 PM |
| **State** | Finished |
| **Completed on** | Tuesday, 18 April 2023, 3:06 PM |
| **Time taken** | 30 mins 1 sec |
| **Grade** | **8.00** out of 10.00 (**80**%) |

Question **1**

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 legitimate, d = 43141, ciphertext = 48006
- b. e is legitimate, d = 44141, ciphertext = 48006
- c. e is legitimate, d = 47141, ciphertext = 48006 ✔
- d. e is not legitimate, thus none of these
- e. e is legitimate, d = 4741, ciphertext = 48006

Your answer is correct.

The correct answer is:
e is legitimate, d = 47141, ciphertext = 48006

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 = 1758, Bob's public key = 1582, Shared secret key = 1891
- c. Alice's public key = 1658, Bob's public key = 1582, Shared secret key = 1890
- d. Alice's public key = 1582, Bob's public key = 1758, Shared secret key = 1890
- e. none of these

Your answer is correct.

The correct answer is:
Alice's public key = 1758, Bob's public key = 1582, Shared secret key = 1890

Question **3**

Correct

Mark 1.00 out of 1.00

Consider the Elliptic curver 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. (7, 14)

c. (8, 28)

d. None of these

e. (16, 21)

Your answer is correct.

The correct answer is:

(24, 6)

Question **4**

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. (31, 38)
- c. (38, 31)
- d. (41, 6) ✔
- e. (6, 41)

Your answer is correct.

The correct answer is:
(41, 6)

Question **5**

Incorrect

Mark 0.00 out of 1.00

AES-MIXCOLUMN (234, 56, 118, 221,)

a. (54, 221, 63, 202)

b. (44, 221, 66, 202)

c. (44, 220, 66, 202)

d. none of these

e. (44, 221, 66, 201)

Your answer is incorrect.

The correct answer is:
(44, 221, 66, 202)

Question **6**

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 = 2573 , Bob's public key = 1631 , Common secret key = 2409

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

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

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

e. none of these

Your answer is correct.

The correct answer is:
Alice's public key = 2573 , Bob's public key = 1631 , Common secret key = 2409

Question **7**

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. none of these
- c. (8,19) ✔
- d. (133, 73)
- e. (138, 10)

Your answer is correct.

The correct answer is:
(8,19)

Question **8**

Correct

Mark 1.00 out of 1.00

AES-INV-MIXCOLUMN (123, 202, 87, 77)

- a. (114, 54, 143, 96)
- b. (52, 215, 139, 72)
- c. none of these
- d. (157, 132, 225, 110)

e. (54, 69, 87, 143)

Your answer is correct.

The correct answer is:
(54, 69, 87, 143)

Question **9**

Incorrect

Mark 0.00 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 legitimate, d = 62617, ciphertext = 315318 ✖
- b. e is legitimate, d = 62727, ciphertext = 315318
- c. e is legitimate, d = 61627, ciphertext = 315318
- d. e is legitimate, d = 62627, ciphertext = 315318
- e. e is not legitimate, thus none of these

Your answer is incorrect.

The correct answer is:
e is legitimate, d = 62627, ciphertext = 315318

Question **10**

Correct

Mark 1.00 out of 1.00

AES-INV-MIXCOLUMN (123, 212, 88, 77) [inputs are in decimal]

- a. (175, 152, 227, 110) ✔
- b. (175, 15, 227, 110)
- c. none of these
- d. (75, 152, 227, 110)
- e. (175, 152, 27, 110)

Your answer is correct.

The correct answer is:
(175, 152, 227, 110)

◄ Announcements

Jump to...

| | |
|---|---|
| **Started on** | Wednesday, 15 September 2021, 9:09 AM |
| **State** | Finished |
| **Completed on** | Wednesday, 15 September 2021, 9:49 AM |
| **Time taken** | 39 mins 59 secs |
| **Grade** | **5.50** out of 10.00 (**55**%) |

Question **1**

Incorrect

Mark 0.00 out of 0.50

Let $g:\{0,1\}^{256} \rightarrow \{0,1\}^{256}$ be any preimage resistant function. Define $f:\{0,1\}^{512} \rightarrow \{0,1\}^{512}$ by using the following rule:

$f(x[0], \ldots, x[511]) = 1^{512}$ if $x[0] = x[1] = \cdots = x[255] = 1$
$f(x[0], \ldots, x[511]) = 1^{256} \,||\, g(x[256], \ldots, x[511])$ otherwise

Here $1^d$ denotes a d-bits string whose all bits are 1. Which of the following statement is true?

- a. f is not preimage resistant function ✖
- b. f is preimage resistant function

Your answer is incorrect.

The correct answer is:
f is preimage resistant function

Question **2**

Incorrect

Mark 0.00 out of 0.50

How many distinct constants are used in the construction of

SHA-1 hash function ?

- a. 4
- b. 79
- c. 80
- d. None of these ✖

Your answer is incorrect.

The correct answer is:
4

Question **3**

Incorrect

Mark 0.00 out of 0.50

A sequence of plaintext blocks x1,...,xn are encrypted by using DES in CFB mode.

The corresponding ciphertext blocks are y1,...,yn. During transmission y1 is transmitted incorrectly

(i.e., some 1's are changed to 0's and vice verse). The number of plaintext blocks that will be decrypted

incorrectly is

- a. 3
- b. 2
- c. None of these ✖
- d. 1
- e. 0

Your answer is incorrect.

The correct answer is:
2

Question **4**

Correct

Mark 0.50 out of 0.50

Let $F_k = F_{k-1} \oplus Enc\ (P_k , F_{k-1})$ be an iterated hash function where Enc is the DES encryption algorithm and $F_k$ , $P_k$ each is of 64-bit. The initial $F_0$ is a 64-bit public data, $P_k$ is the k-th message block. Which of the following statement is correct?

- a. The above iterated hash function is a collision resistant hash function.
- b. The above iterated hash function is not a collision resistant hash function. ✔

Your answer is correct.

The correct answer is:
The above iterated hash function is not a collision resistant hash function.

Question **5**

Correct

Mark 0.50 out of 0.50

Let H be the MERKLE -DAMGARD based hash function.

Let h be the Message Authentication Code (MAC) of M and h = H(K || M).

Here K is the secret key which is unknown to the attacker.

From M and h is it possible for an attacker to produce a valid MAC on

a different message M1 without knowing the secret key K.

- a. Yes ✔
- b. No

Your answer is correct.

The correct answer is:
Yes

Question **6**

Correct

Mark 0.50 out of 0.50

Let $M = x_1 || x_2 || x_3 || x_4 .... || x_n$ be a message with $len(x_i)=128$ bit

Let $y_0$ be an 128-bit public parameter and K be the 128-bit secret key.

E denotes the AES-128 bit encryption

algorithm. We use the following procedure to generate $y_i = E( y_{i-1} \oplus x_i , K)$ for i = 1 to n.

Which of the following is true?

- a. $y_n$ is the encryption of M
- b. $y_n$ is the neither MAC nor the encryption of M
- c. $y_n$ is the MAC of M ✔

Your answer is correct.

The correct answer is:
$y_n$ is the MAC of M

Question **7**

Incorrect

Mark 0.00 out of 0.50

SUBBYTES(C7)=

- a. None of these ✖
- b. 10
- c. F0
- d. C6
- e. F4

Your answer is incorrect.

The correct answer is:

C6

Question **8**

Correct

Mark 0.50 out of 0.50

How many fixed pre-defined functions are involved in SHA-1

- a. 79
- b. 69
- c. 80 ✔
- d. None of these

Your answer is correct.

The correct answer is:
80

Question **9**

Correct

Mark 0.50 out of 0.50

AES-192 requires how many round keys?

- a. 12
- b. None of these
- c. 10
- d. 13 ✔
- e. 11
- f. 14

Your answer is correct.

The correct answer is:
13

Question **10**

Correct

Mark 0.50 out of 0.50

Suppose two different plaintexts X=(x1,x2,...,xn) and Y=(y1,y2,...,yn) are encrypted using same key and IV in OFB mode. Then which of the following is true?

- a. Two ciphertexts will be completely independent
- b. It will depend on the encryption algorithm used in OFB mode
- c. Ciphertexts will reveal an information regarding the plaintexts ✔
- d. Nothing can be said about the plaintexts from ciphertexts

Your answer is correct.

The correct answer is:
Ciphertexts will reveal an information regarding the plaintexts

Question **11**

Correct

Mark 0.50 out of 0.50

Consider the AES-128 encryption algorithm. AES-128 encryption algorithm takes an 128-bit key and an 128-bit message block and generates 128-bit ciphertext block (AES-128(M,K)=C)

i.e., AES-128: $\{0, 1\}^{128} \times \{0, 1\}^{128} \rightarrow \{0, 1\}^{128}$ .

Define the compression function h : $\{0, 1\}^{256} \rightarrow \{0, 1\}^{128}$ by using the following rule

h(m1 || m2 ) = AES-128(m1 , m2 ).

Which of the following statement is true

- a. h is not collision resistant. ✔
- b. h is collision resistant.

Your answer is correct.

The correct answer is:
h is not collision resistant.

Question **12**

Incorrect

Mark 0.00 out of 0.50

Let H be a hash function from $\{0,1\}^*$ to $\{0,1\}^{128}$ . Given $X_1$ from $\{0,1\}^*$ finding $X_2$ from $\{0,1\}^*$ not equal to $X_1$ such that $H(X_1)=H(X_2)$ is known as

- a. Collision finding problem ✖
- b. Preimage finding problem
- c. Second preimage finding problem
- d. None of these

Your answer is incorrect.

The correct answer is:
Second preimage finding problem

Question **13**

Incorrect

Mark 0.00 out of 0.50

Let $h:\{0,1\}^* \rightarrow \{0,1\}^n$ be a preimage resistant and collision resistant hash function.

Define a new hash function $h':\{0,1\}^* \rightarrow \{0,1\}^{n+1}$ by using following rule

$h'(x)=0||x$ if x belongs to $\{0,1\}^n$,

otherwise $h'(x)=1||h(x)$.

Which of the following statement is true.

- a. h' is a preimage resistant as well as collision resistant. ✖
- b. h ' is neither preimage resistant nor collision resistant.
- c. h' is not a preimage resistant but collision resistant.

Your answer is incorrect.

The correct answer is:
h' is not a preimage resistant but collision resistant.

Question **14**

Correct

Mark 0.50 out of 0.50

Suppose you have an encrypted ciphertext C=C1||C2||....||Cn which is encrypted using AES-128 in CBC mode of operation. Is it possible to decrypt the ciphertext blocks in parallel?

- a. Yes it is possible ✔
- b. No it is not possible

Your answer is correct.

The correct answer is:
Yes it is possible

Question **15**

Incorrect

Mark 0.00 out of 0.50

Let H be a compression function from A to B where |A| = N and |B| = M and N > M.

For a given H(X) from B the worst case complexity of finding X from A is

- a. None of these
- b. O(M)
- c. $O(M^{1/2})$
- d. $O(N^{1/2})$
- e. O(N) ✖

Your answer is incorrect.

The correct answer is:
O(M)

Question **16**

Correct

Mark 0.50 out of 0.50

Select the most appropriate statement:

(1) Hash function can be used for encryption

(2) Hash function can be used for authentication and can not be used for correctness checking of the message

(3) Hash function can be used for authentication and for checking of correctness of message

- a. (2)
- b. (3) ✔
- c. None of these are correct
- d. (1)

Your answer is correct.

The correct answer is:
(3)

Question **17**

Incorrect

Mark 0.00 out of 0.50

Let F be a bijection from $\{0,1\}^m$ to $\{0,1\}^m$ and F is also preimage resistant.

Define a new function H from $\{0,1\}^{2m}$ to $\{0,1\}^m$ in the following way

for any X from $\{0,1\}^{2m}$ , X = X1 || X2, where X1, X2 both are of m bits and

H(X) = F(X1 ⊕ X2)

Which of the following statement is correct?

- a. H is not second preimage resistant
- b. H is second preimage resistant function ✖

Your answer is incorrect.

The correct answer is:
H is not second preimage resistant

Question **18**

Correct

Mark 0.50 out of 0.50

What is the size of Y = SHA-1(X) for any X ?

- a. None of these
- b. 256 bits
- c. 128 bits
- d. 64 bits
- e. 160 bits ✔

Your answer is correct.

The correct answer is:
160 bits

Question **19**

Incorrect

Mark 0.00 out of 0.50

AES-128(M,K)=C1 and AES(M',K')=C2, where X' is bitwise complement of X.

a. C1=C2 ✖

b. None of these

c. C1=C2'

Your answer is incorrect.

The correct answer is:

None of these

Question **20**

Correct

Mark 0.50 out of 0.50

What is the biggest advantage of CBC mode of operation

a. It does not need IV.

b. It does not propagate error in the ciphertext.

c. It can encrypt in parallel different parts of the message.

d. The IV is secret, so the length of the key is doubled.

e. Ciphertext block depends on all the ciphertext blocks before it. ✔

Your answer is correct.

The correct answer is:

Ciphertext block depends on all the ciphertext blocks before it.

◄ Pre Midterm

Jump to...