Started on	Tuesday, 30 April 2024, 9:21 AM
State	Finished
Completed on	Tuesday, 30 April 2024, 9:38 AM
Time taken	16 mins 57 secs
Grade	**7.00** out of 7.00 (**100**%)

Question **1**

Correct

Mark 0.50 out of 0.50

If g is a generator of the group Z_m^* where

$Z_m^* = \{x \mid \gcd(x, m) = 1\}$ (m is not a prime) then what is the

order of g?

a. $(m-1)(m-2)$

b. $\phi(m)$ ✔

c. $m-1$

Your answer is correct.

Question **2**

Correct

Mark 0.50 out of 0.50

Let n=pq where p,q are primes. Consider e such that

$gcd(e, \phi(n)) = 1$ [here ϕ is the Euler's totient function].

The function defined by $f(x) = x^e \mod n$ is

a. not a bijection on $\mathbb{Z}_n^*$

b. a bijection on $\mathbb{Z}_n^*$ ✔

Your answer is correct.

Question **3**

Correct

Mark 0.50 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 one. Which of the

following statement is true?

a. f is not preimage resistant function

b. f is preimage resistant function ✔

Your answer is correct.

Question **4**

Correct

Mark 0.50 out of 0.50

CBC-MAC constructed using AES-512 will have MAC size

a. Depends on the message size

b. 128 bit ✔

c. 512 bit

d. 256 bit

Your answer is correct.

Question **5**

Correct

Mark 0.50 out of 0.50

We define the following two problems Computational Diffie-Hellman (CDH) problem and Discrete Log (DL) problem :

CDH: Given $p, g,\ g^a$ and g^b compute g^{ab}

DL: Given p, g and g^a, find a.

Here p is a large prime number and g is a generator of the cyclic group $\mathbb{Z}_p^*$ with multiplication modulo p operation. Which of the following statement is most accurate?

a. If CDH is solved then DL is also solved

b. If DL is solved then CDH is also solved ✔

c. DL and CDH both are equivalent

Your answer is correct.

Question **6**

Correct

Mark 0.50 out of 0.50

Consider the prime number p = 311 and the group $\mathbb{Z}_p^*$ with multiplication modulo p operation. Let g=17 be a generator of the group $\mathbb{Z}_p^*$. Alice and Bob now would like to establish a common secret key using Diffie-Hellman key exchange protocol on the above mentioned group. The secret key of Alice and Bob are 119 and 62 respectively. Which of the following statement is correct.

a. Alice's public key = 215, Bob's public key = 36, Common secret key = 216 ✔

b. Alice's public key = 215, Bob's public key = 36, Common secret key = 213

c. Alice's public key = 40, Bob's public key = 128, Common secret key = 210

d. none of these

Your answer is correct.

Question **7**

Correct

Mark 0.50 out of 0.50

Suppose that K = (5, 21) is a key in an Affine Cipher over $\mathbb{Z}_{31}$. The decryption function $d_K(y)$ can be expressed as $d_K(y) = a'y + b'$, where $a', b' \in \mathbb{Z}_{31}$.

a. $a' = 2, b' = 25$

b. a'=25,b'=2 ✔

c. none of these

d. a'=23,b'=3

Your answer is correct.

Question **8**

Correct

Mark 0.50 out of 0.50

Let F be a preimage resistant function from S to S. Consider a new function G = F o F (i.e., F compose F).

Which of the following statement is true?

a. G need not be a preimage resistant function ✔

b. G is a preimage resistant function

Your answer is correct.

Question **9**

Correct

Mark 0.50 out of 0.50

Expanded key size of AES-256 is

a. 56 words

b. 60 words ✔

c. 44 words

d. none of these

e. 48 words

Your answer is correct.

Question **10**

Correct

Mark 0.50 out of 0.50

Let n = 19 * 23 and the encryption key of RSA be e = 7.

For the message M = 88 which of the following statement is true.

a. the decryption key d = 113, ciphertext C = 211

b. the decryption key d = 283, ciphertext C = 107 ✔

c. none of these

d. the decryption key d = 23, ciphertext C = 111

Your answer is correct.

Question **11**

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 AES-128 encryption algorithm and F_k, P_k each is of 128-bit. The initial F_0 is a 128-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 not a collision resistant hash function

b. The above iterated hash function is a collision resistant hash function ✔

Your answer is correct.

Question **12**

Correct

Mark 0.50 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 $x\in\{0,1\}^n$, otherwise $h'(x)=1||h(x)$. Which of the following statement is true.

a. h' is not a preimage resistant but collision resistant ✔

b. h' is a preimage resistant as well as collision resistant

c. h' is neither preimage resistant nor collision resistant

Your answer is correct.

Question **13**

Correct

Mark 0.50 out of 0.50

Which of the following is true for forward secrecy?

a. if the security of present message is compromised still the security of previous messages remain unaffected ✔

b. if Pr[m0|c0] is known then Pr[m1|c1] will also be known

c. if Pr[m1|c1] is known then Pr[m0|c0] will also be known

d. forward secrecy implies perfect secrecy

Your answer is correct.

Question **14**

Correct

Mark 0.50 out of 0.50

Consider AES-256 bit encryption algorithm and CBC modes of operation.

Using AES-256 in CBC mode we define a CBC-MAC. Let M1 be a message of

256 bit and CBC-MAC corresponding to M1 be T1. Let M1=m1 || m2 where

each m1 and m2 is of 128 bits. The MAC corresponding

to M2=M1 || (m2 $\oplus$ T1) will be,

a. C=AES-256(m2 $\oplus$ T1)

b. T1 || C where C=AES-256(m2 $\oplus$ T1)

c. None of these

d. C=AES-256(m2) ✔

e. T1

Your answer is correct.

◄ Midterm

Jump to...