Dashboard / My courses / CS304_2024 / General / Classtest

Started on	Friday, 1 March 2024, 11:03 AM
State	Finished
Completed on	Friday, 1 March 2024, 11:22 AM
Time taken	19 mins 40 secs
Grade	**5.00** out of 6.00 (**83**%)

Question **1**

Incorrect

Mark 0.00 out of 0.50

Which is the correct multiplicative inverse of the polynomial $g(x)=x^3+x^2$ in $Z_2[x]/x^8+x^4+x^3+x+1$.

○ a. x^3+x+1

○ b. $x^7+x^5+x^4$

● c. x^6+x^3+x ✖

Your answer is incorrect.

The correct answer is:

$x^7+x^5+x^4$

Question **2**

Correct

Mark 1.00 out of 1.00

```
If AES-Mixcolumn(23, 67, 45, 89) = (x,y,z,w) then y =
```

```
[here input and output are in integer]
```

○ a. 121

○ b. 159

● c. 191 ✓

○ d. 229

Your answer is correct.

The correct answer is:

191

Question **3**

Correct

Mark 1.00 out of 1.00

```
If AES-Mixcolumn(23, 67, 89, 45) = (x,y,z,w) then w =
```

```
[here input and output are in integer]
```

○ a. `159`

○ b. `87`

○ c. `145`

● d. `121` ✓

○ e. `none of these`

Your answer is correct.

The correct answer is:

```
121
```

Question **4**

Correct

Mark 0.50 out of 0.50

What is the period of the 5-bit LFSR whose connection polynomial is $x^5 + x^4 + x^2 + x + 1$

○ a. 15

○ b. none of these

○ c. 16

● d. 31 ✓

○ e. 32

Your answer is correct.

The correct answer is:
31

Question **5**

Correct

Mark 0.50 out of 0.50

We define a new encryption algorithm TEnc using AES-128 encryption

technique.

TEnc : $\{0,1\}^{384} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ where

C = TEnc(K||K1||K2, M) = K2 ⊕ AES-128-Enc(K, K1 ⊕ M).

Here K, K1, K2 each is of 128 bit. What will be the decryption algorithm

(TDec) corresponding to TEnc.

○ a. None of these

○ b. M = TDec(K||K1||K2, C) = K ⊕ AES-128-Dec(K1, K2 ⊕ C)

○ c. M = TDec(K||K1||K2, C) = K2 ⊕ AES-128-Dec(K, K1 ⊕ C)

● d. M = TDec(K||K1||K2, C) = K1 ⊕ AES-128-Dec(K, K2 ⊕ C) ✓

Your answer is correct.

The correct answer is:
M = TDec(K||K1||K2, C) = K1 ⊕ AES-128-Dec(K, K2 ⊕ C)

Question **6**

Correct

Mark 0.50 out of 0.50

Consider one-bit encryption $C = P \oplus K$. If $Pr[K=0] = 0.5$ and $Pr[P=1] = 0.3$

then $Pr[P=0|C=1]$ is

○ a. none of these

● b. 0.7 ✓

○ c. 0.4

○ d. 0.5

○ e. 0.3

Your answer is correct.

The correct answer is:

0.7

Question **7**

Correct

Mark 0.50 out of 0.50

Select the correct answer where S_1: $\{0,1\}^6 \rightarrow \{0,1\}^4$ and S_2:$\{0,1\}^6 \rightarrow \{0,1\}^4$ are the first two

defined S-boxes for the round function of DES. (For the description of these S-boxes please

see Handbook of Applied Cryptography book.)

○ a. $S_1(59) = 4$, $S_2(23) = 8$

● b. $S_1(59) = 0$, $S_2(23) = 10$. ✓

○ c. $S_1(59) = 1$, S2(23) = 10.

○ d. $S_1(59) = 0$, $S_2(23) = 14$.

Your answer is correct.

The correct answer is:
$S_1(59) = 0$, $S_2(23) = 10$.

Question **8**

Incorrect

Mark 0.00 out of 0.50

Which is the correct multiplicative inverse of the polynomial $g(x) = x^3 + x^2$ in $\mathbb{Z}_2[x]/x^5 + x^4 + x^2 + x + 1$.

● a. $x^4 + x^2 + x + 1$ ✖

○ b. $x^4 + x^3 + x$

○ c. $x^4 + x^3 + x^2 + x + 1$

Your answer is incorrect.

The correct answer is:

$x^4 + x^3 + x^2 + x + 1$

Question **9**

Correct

Mark 0.50 out of 0.50

A sequence of plaintext blocks x1,...,xn are encrypted by

using AES-128 in CBC 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. none of these

○ b. n

○ c. 1

● d. 2 ✓

○ e. 3

Your answer is correct.

The correct answer is:

2

Question **10**

Correct

Mark 0.50 out of 0.50

```
Consider AES-256 bit encryption algorithm and a 512 bit key K=K1||K2 where K1 and K2 are of 256 bit.
```

```
The encryption algorithm C=AES-256(AES-256(M,K1),K2) provides
```

● a. `256-bit security` ✓

○ b. `512-bit security`

Your answer is correct.

The correct answer is:

```
256-bit security
```

◄ Announcements

Jump to...

Dashboard / My courses / CS304 2024 / General / Classtest-Pre-Endterm

Started on	Tuesday, 30 April 2024, 9:20 AM
State	Finished
Completed on	Tuesday, 30 April 2024, 9:36 AM
Time taken	16 mins 26 secs
Grade	**6.50** out of 7.00 (**93**%)

Question **1**

Incorrect

Mark 0.00 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 is a preimage resistant function` ✗

○ b. `G need not be a preimage resistant function`

Your answer is incorrect.

Question **2**

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. DL and CDH both are equivalent

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

● c. If DL is solved then CDH is also solved ✓

Your answer is correct.

Question **3**

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 ⊕ T1) will be,

○ a. None of these

○ b. T1 || C where C=AES-256(m2 ⊕ T1)

● c. C=AES-256(m2) ✓

○ d. C=AES-256(m2 ⊕ T1)

○ e. T1

Your answer is correct.

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

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 a collision resistant hash function ✓

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

Your answer is correct.

Question **5**

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 **6**

Correct

Mark 0.50 out of 0.50

```
Which of the following is true for forward secrecy?
```

○ a. `forward secrecy implies perfect secrecy`

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

● c. `if the security of present message is compromised still the security of previous messages remain unaffected` ✓

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

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. $a'=25,b'=2$ ✓

○ b. $a'=23,b'=3$

○ c. $a'=2,b'=25$

○ d. `none of these`

Your answer is correct.

Question **8**

Correct

Mark 0.50 out of 0.50

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

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

order of g?

● a. $\phi(m)$ ✓

○ b. $(m-1)(m-2)$

○ c. $m-1$

Your answer is correct.

Question **9**

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:

$f(x_0,\ldots,x_{511})=1^{512} \text{ if } x_0=x_1=\cdots =x_{255}=1$

$f(x_0,\ldots,x_{511})=1^{256}||g(x_{256},\ldots ,x_{511}) \text{ otherwise}$

Here 1^d denotes a d-bits string whose all bits are one. Which of the

following statement is true?

● a. f is preimage resistant function ✓

○ b. f is not preimage resistant function

Your answer is correct.

Question **10**

Correct

Mark 0.50 out of 0.50

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

● a. 128 bit ✓

○ b. 256 bit

○ c. 512 bit

○ d. Depends on the message size

Your answer is correct.

Question **11**

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 neither preimage resistant nor collision resistant

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

● c. h' is not a preimage resistant but collision resistant ✓

Your answer is correct.

Question **12**

Correct

Mark 0.50 out of 0.50

```
Expanded key size of AES-256 is
```

○ a. `44 words`

○ b. `48 words`

○ c. none of these

● d. `60 words` ✓

○ e. `56 words`

Your answer is correct.

Question **13**

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

○ d. none of these

Your answer is correct.

Question **14**

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 = 40, Bob's public key = 128, Common secret key = 210`

○ c. none of these

○ d. `Alice's public key = 215, Bob's public key = 36, Common secret key = 213`

Your answer is correct.

◄ Midterm

Jump to...

Dashboard / My courses / CS304 / Topic 1 / Midterm

Started on	Thursday, 10 March 2022, 2:34 PM
State	Finished
Completed on	Thursday, 10 March 2022, 3:53 PM
Time taken	1 hour 18 mins
Grade	**20.00** out of 40.00 (**50**%)

Question **1**

Incorrect

Mark 0.00 out of 1.00

`The expansion function of DES is`

● a. `not invertible` ✖

○ b. `invertible`

Your answer is incorrect.

The correct answer is:

`invertible`

Question **2**

Incorrect

Mark 0.00 out of 1.00

```
Assume that in a classroom there are 250 students. Form a group by taking x many
```

```
students randomly from the classroom. For which value of x there will be atleast
```

```
two students with same date of birth with probability 0.9.
```

● a. none of these ✖

○ b. `35`

○ c. `41`

○ d. `30`

Your answer is incorrect.

The correct answer is:

```
41
```

Question **3**

Incorrect

Mark 0.00 out of 1.00

Expanded key size of AES-256 is

● a. 44 words ✖

○ b. 56 words

○ c. 48 words

○ d. 60 words

○ e. none of these

Your answer is incorrect.

The correct answer is:

60 words

Question **4**

Correct

Mark 1.00 out of 1.00

```
If AES-Mixcolumn(23, 67, 45, 89) = (x,y,z,w) then y =
```

```
[here input and output are in integer]
```

● a. 191 ✓

○ b. 159

○ c. 229

○ d. 121

Your answer is correct.

The correct answer is:

191

Question **5**

Correct

Mark 1.00 out of 1.00

What are the correct values of x,y such that 23x+43y=gcd(23,43)?

○ a. x=13,y=7

● b. x=15,y=-8 ✓

○ c. x=25,y=-18

○ d. none of these

○ e. x=-24,y=16

Your answer is correct.

The correct answer is:

x=15,y=-8

Question **6**

Incorrect

Mark 0.00 out of 1.00

Let P, C, K be the plaintext space, ciphertext space and key space respectively.

Consider an encryption algorithm E with the following conditions:

1. $|P| = |C| = |K|$

2. every key is equiprobable

3. for every $p \in P$, $c \in C$ there is an unique key k such that $E(p, k) = c$,

Select the most appropriate option

○ a. E provides perfect secrecy

○ b. E will provide perfect secrecy if $|K| > |P|$

● c. E can not provide perfect secrecy as it differs from OTP ✖

Your answer is incorrect.

The correct answer is:

E provides perfect secrecy

Question **7**

Incorrect

Mark 0.00 out of 1.00

What is meant by the security of an Encryption Scheme?

○ a. An attacker who gets hold of a ciphertext should not be able to get any function of the bits of the plaintext

○ b. An attacker who gets hold of a ciphertext should not be able to get any bit of the plaintext

○ c. An attacker who gets hold of a ciphertext should not be able to know the plaintext

● d. An attacker who gets hold of a ciphertext should not be able to get the secret key used for the encryption ✖

Your answer is incorrect.

The correct answer is:

An attacker who gets hold of a ciphertext should not be able to get any bit of the plaintext

Question **8**

Incorrect

Mark 0.00 out of 1.00

The number of valid keys in the Affine Cipher over \mathbb{Z}_{46} is

● a. none of these ✖

○ b. 1012

○ c. 46

○ d. 2116

Your answer is incorrect.

The correct answer is:

1012

Question **9**

Incorrect

Mark 0.00 out of 1.00

Let F denotes the AES-128 bit encryption algorithm.

Define a function $f:\{0,1\}^{128}\rightarrow \{0,1\}^{128}$ as

$f(x)=F(x,K)\oplus x$, here x,K are of 128-bits and K is a fixed secret key.

Which of the following statement is correct?

● a. f is not an one-way function ✖

○ b. f is an one-way function

Your answer is incorrect.

The correct answer is:

f is an one-way function

Question **10**

Correct

Mark 1.00 out of 1.00

Which is the multiplicative inverse of (x^3+x^2+1) in

(\mathbb{F}_2[x]/<x^8+x^4+x^3+x+1>,+,*). Here + and * are

the polynomial addition and polynomial multiplication under

modulo x^8+x^4+x^3+x+1.

○ a. x^7+x^6+x+1

○ b. none of these

○ c. x^7+x^6+x^2+1

○ d. x^7 + x^6 + x^3 + x^2

● e. x^7 + x^6 + x^5 + 1 ✓

Your answer is correct.

The correct answer is:

x^7 + x^6 + x^5 + 1

Question **11**

Correct

Mark 1.00 out of 1.00

For a fixed key any symmetric key encryption algorithm should

○ a. not necessary to be surjective

○ b. none of these

○ c. not necessary to be injective

○ d. be surjective function

● e. be injective function ✓

Your answer is correct.

The correct answer is:

be injective function

Question **12**

Incorrect

Mark 0.00 out of 1.00

Select the correct answer where $S_1:\{0,1\}^6\rightarrow\{0,1\}^4$

and $S_2:\{0,1\}^6\rightarrow\{0,1\}^4$ are the pre-defined S-boxes

for the round function of DES.

○ a. $S_1(55)=14$, $S_2(43)=15$

○ b. $S_1(55)=6$, $S_2(43)=7$

○ c. $S_1(55)=15$, $S_2(43)=14$

○ d. $S_1(55)=7$, $S_2(43)=6$

● e. none of these ✖

Your answer is incorrect.

The correct answer is:

$S_1(55)=14$, $S_2(43)=15$

Question **13**

Correct

Mark 1.00 out of 1.00

Let $n=p\times q$ where p,q are two large primes.

Here n is known to everyone and p,q are hidden.

Consider the hash function $h(x)=x^2\mod n$.

○ a. h is not an one-way function

● b. h is an one-way function ✓

Your answer is correct.

The correct answer is:

h is an one-way function

Question **14**

Incorrect

Mark 0.00 out of 1.00

If AES-Mixcolumn(23, 67, 89, 45) = (x,y,z,w) then w =

[here input and output are in integer]

○ a. 121

○ b. 87

● c. 159 ✗

○ d. 145

○ e. none of these

Your answer is incorrect.

The correct answer is:

121

Question **15**

Correct

Mark 1.00 out of 1.00

Let h:\mathbb{Z}_{2^{512}}\rightarrow \mathbb{Z}_{2^{256}} be a hash function

defined as h(x)=(155x^4+201x^3+2x^2+101x+1)\mod 2^{256}.

Is h second preimage resistant?

○ a. yes

● b. no ✓

Your answer is correct.

The correct answer is:

no

Question **16**

Correct

Mark 1.00 out of 1.00

Consider AES-128 in CFB mode of operation. One message of length 1024 bits

has been encrypted using AES-128 in CFB mode of operation.

Now to decrypt the ciphertext which of the following process needs to be followed

● a. encryption of AES-128 needs to fit in CFB mode ✓

○ b. decryption of AES-128 needs to fit in CFB mode

Your answer is correct.

The correct answer is:

encryption of AES-128 needs to fit in CFB mode

Question **17**

Correct

Mark 1.00 out of 1.00

```
Consider playfair cipher with the key KEYWORD. Which is the correct
ciphertext of the plaintext COMMUNICATION when the plaintext is
encrypted using playfair cipher with the mentioned key.
```

○ a. none of these

○ b. `LCQTNTQGBRXFES`

● c. `LCQTNTQGRBXFES` ✓

○ d. `LCQTNQTGRBXFES`

○ e. `LCQTNTQRGBXFES`

Your answer is correct.

The correct answer is:

`LCQTNTQGRBXFES`

Question **18**

Correct

Mark 1.00 out of 1.00

`Decryption of CBC mode of operation can be implemented in parallel`

○ a. `no`

● b. `yes` ✓

Your answer is correct.

The correct answer is:

`yes`

Question **19**

Incorrect

Mark 0.00 out of 1.00

Which is the multiplicative inverse of (x^4+x^3+x+1) in $(\mathbb{F}_2[x]/<x^8+x^4+x^3+x+1>,+,*)$.

Here + and * are the polynomial addition and polynomial multiplication under modulo $x^8+x^4+x^3+x+1$.

○ a. $x^7 + x^6 + x^3 + x^2$

○ b. $x^7 + x^6 + x^5 + 1$

○ c. $x^7 + x^6 + x^2 + x + 1$

○ d. $x^7 + x^6 + x^3 + x^2+1$

● e. none of these ✖

Your answer is incorrect.

The correct answer is:

$x^7 + x^6 + x^3 + x^2$

Question **20**

Incorrect

Mark 0.00 out of 1.00

```
SUBBYTES(6A) =
```

● a. none of these ✖

○ b. `34`

○ c. 20

○ d. `24`

○ e. `02`

Your answer is incorrect.

The correct answer is:

```
02
```

Question **21**

Incorrect

Mark 0.00 out of 1.00

```
How many distinct predefined functions are used in SHA-1
```

● a. `none of these` ✖

○ b. `4`

○ c. `3`

○ d. `80`

Your answer is incorrect.

The correct answer is:

```
3
```

Question **22**

Incorrect

Mark 0.00 out of 1.00

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 a collision resistant hash function

● b. The above iterated hash function is not a collision resistant hash function ✗

Your answer is incorrect.

The correct answer is:

The above iterated hash function is a collision resistant hash function

Question **23**

Correct

Mark 1.00 out of 1.00

```
Consider Affine cipher with the key K=(11, 16). Which is the correct ciphertext
```

```
of the plaintext MIDSEM when the plaintext is encrypted using Affine cipher
```

```
with the mentioned key.
```

● a. SAXGIS ✓

○ b. SAGXIS

○ c. SAXIGS

○ d. none of these

○ e. SAXGSI

Your answer is correct.

The correct answer is:

SAXGIS

Question **24**

Incorrect

Mark 0.00 out of 1.00

```
Which of the following statement is correct?
```

○ a. `if encryption function is oneway then decryption is not possible`

○ b. `encryption function is oneway if the private key is unknown`

● c. `only hash functions are oneway functions` ✗

Your answer is incorrect.

The correct answer is:

```
encryption function is oneway if the private key is unknown
```

Question **25**

Correct

Mark 1.00 out of 1.00

```
Consider playfair cipher with the key MIDSEM. Which is the correct
```

```
ciphertext of the plaintext VADODARA when the plaintext is
```

```
encrypted using playfair cipher with the mentioned key.
```

● a. `MHELMCPC` ✓

○ b. `MHEMLCPC`

○ c. none of these

○ d. `MHLEMCPC`

○ e. `MHELCMPC`

Your answer is correct.

The correct answer is:

```
MHELMCPC
```

Question **26**

Correct

Mark 1.00 out of 1.00

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 neither preimage resistant nor collision resistant

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

● c. h' is not a preimage resistant but collision resistant ✓

Your answer is correct.

The correct answer is:

h' is not a preimage resistant but collision resistant

Question **27**

Correct

Mark 1.00 out of 1.00

`If all the 16 round keys of DES are identical then`

○ a. `only the last round and first round of DES will be identical`

○ b. `DES encryption and decryption functions will not be identical due to the IP`

● c. `DES encryption and decryption functions will be exactly equal` ✓

○ d. `none of these`

Your answer is correct.

The correct answer is:

`DES encryption and decryption functions will be exactly equal`

Question **28**

Incorrect

Mark 0.00 out of 1.00

Consider AES-128 in OFB mode of operation. One message M of length 1024 bits

has been encrypted using AES-128 in OFB mode of operation. During transmission 256-th bit

and 512-th bit of the ciphertext are altered. Now the receiver performs the

decryption on the received ciphertext and obtained the decrypted text M'.

Which of the following statement is true?

○ a. M and M' will differ from 256-th bit to 512-th bit

● b. M and M' will differ at 256-th bit to 1024-th bit ✗

○ c. none of these

○ d. M and M' will differ at 256-th bit and 512-th bit

Your answer is incorrect.

The correct answer is:

M and M' will differ at 256-th bit and 512-th bit

Question **29**

Correct

Mark 1.00 out of 1.00

S-boxes in DES map

○ a. 4 bits to 6 bits

○ b. 2 bits to 4 bits

○ c. 4 bits to 4 bits

● d. 6 bits to 4 bits ✓

○ e. none of these

Your answer is correct.

The correct answer is:

6 bits to 4 bits

Question **30**

Correct

Mark 1.00 out of 1.00

```
Consider Affine cipher with the key K=(9, 19). Which is the correct
ciphertext of the plaintext INDIA when the plaintext is encrypted
using Affine cipher with the mentioned key.
```

○ a. NGUNM

○ b. none of these

○ c. NGTNU

○ d. NUGNT

● e. NGUNT ✓

Your answer is correct.

The correct answer is:

NGUNT

Question **31**

Correct

Mark 1.00 out of 1.00

Let h:\mathbb{Z}_{512}\times Z_{512}\rightarrow \mathbb{Z}_{512} be a hash

function defined as h(x,y)=(ax+by)\mod 512, a,b\in\mathbb{Z}_{512}.

Which of the following is correct?

○ a. h is an ideal hash function

● b. h is not an ideal hash function ✓

Your answer is correct.

The correct answer is:

h is not an ideal hash function

Question **32**

Incorrect

Mark 0.00 out of 1.00

A sequence of plaintext blocks x1,...,xn are encrypted by

using AES-128 in CBC 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. none of these

○ b. 1

○ c. 2

○ d. 3

● e. n ✖

Your answer is incorrect.

The correct answer is:

2

Question **33**

Incorrect

Mark 0.00 out of 1.00

`Consider one-bit encryption` C=P\oplus K`. If` Pr[K=0]=0.5 `and` Pr[P=1]=0.3

`then` Pr[P=0|C=1] `is`

○ a. `0.7`

● b. `0.5` ✖

○ c. none of these

○ d. `0.4`

○ e. `0.3`

Your answer is incorrect.

The correct answer is:

`0.7`

Question **34**

Incorrect

Mark 0.00 out of 1.00

```
Select the most appropriate one. Hash function has the following property
```

● a. `Preimage finding is hard` ✖

○ b. `Finding preimage, collision, second preimage all are hard`

○ c. `Finding preimage or collision or second preimage may not be hard`

○ d. `Second preimage finding is hard`

○ e. `Collision finding is hard`

Your answer is incorrect.

The correct answer is:

```
Finding preimage or collision or second preimage may not be hard
```

Question **35**

Correct

Mark 1.00 out of 1.00

Let C_1=DES(M,K) and C_2=DES(\bar{M},K). Which of the following relation is true?

● a. none of these ✓

○ b. C_1=\bar{C_2}

○ c. C_1=C_2

Your answer is correct.

The correct answer is:

none of these

Question **36**

Incorrect

Mark 0.00 out of 1.00

Consider AES-128 in OFB mode of operation. One message of length 1024 bits

has been encrypted using AES-128 in OFB mode of operation. Now to decrypt the

ciphertext which of the following process needs to be followed

● a. decryption of AES-128 needs to fit in OFB mode ✗

○ b. encryption of AES-128 needs to fit in OFB mode

Your answer is incorrect.

The correct answer is:

encryption of AES-128 needs to fit in OFB mode

Question **37**

Correct

Mark 1.00 out of 1.00

Consider one round of Feistel network with the block size 64-bit and

the secret key K of size 32-bit. The round function is defined by

f(R_0,K)=S(R_0\oplus K) where S(X)=(X+1)\mod 2^{32}.

Find the ciphertext for the plaintext = 1 and key K = 1.

○ a. 2147483648

● b. 4294967297 ✓

○ c. none of these

○ d. 2147483649

○ e. 4294967296

Your answer is correct.

The correct answer is:

4294967297

Question **38**

Correct

Mark 1.00 out of 1.00

```
Assume that in a classroom there are 220 students. Form a group by
taking x many students randomly from the classroom. For which value
of x there will be atleast two students with same date of birth
with probability 0.7.
```

● a. `30` ✓

○ b. `35`

○ c. none of these

○ d. `28`

Your answer is correct.

The correct answer is:

`30`

Question **39**

Correct

Mark 1.00 out of 1.00

```
Encryption of CBC mode of operation can be implemented in parallel
```

● a. `no` ✓

○ b. `yes`

Your answer is correct.

The correct answer is:

`no`

Question **40**

Incorrect

Mark 0.00 out of 1.00

For each key DES is basically a permutation i.e., we can have 2^{56} such

permutations. With all these permutations consider the set G.

Now G with the operation composition of permutations

○ a. is not closed

● b. is closed ✖

Your answer is incorrect.

The correct answer is:

is not closed

◄ Announcements

Jump to...

Endterm ►

Started on	Thursday, 12 May 2022, 2:05 PM
State	Finished
Completed on	Thursday, 12 May 2022, 3:25 PM
Time taken	1 hour 20 mins
Grade	**20.00** out of 40.00 (**50**%)

Question **1**

Correct

Mark 1.00 out of 1.00

Let n = 53 * 73 and the encryption key of RSA be e = 679.

For the message M = 1234 which of the following statement is true.

○ a. none of these

○ b. the decryption key d = 2160, ciphertext C = 3693

○ c. the decryption key d = 787, ciphertext C = 760

● d. the decryption key d = 2167, ciphertext C = 3693 ✓

Your answer is correct.

The correct answer is:

the decryption key d = 2167, ciphertext C = 3693

Question **2**

Correct

Mark 1.00 out of 1.00

$p = 2^{255} - 19$ is a

○ a. pseudo-prime number

● b. prime number ✓

○ c. composite number

Your answer is correct.

The correct answer is:

prime number

Question **3**

Correct

Mark 1.00 out of 1.00

`Consider the Elliptic curve EL:` $y^2 = x^3 + 5x + 3$ `under modulo 11.`

$\boxplus$ `denotes the addition operation between two points on EL.`

`If` $P = (3, 1)$`,` $Q = (0, 5)$ `are two points on this curve then` $P \boxplus Q$

`will be`

● a. `(0,6)` ✓

○ b. `(1,8)`

○ c. none of these

○ d. `(0,5)`

○ e. `(1,3)`

Your answer is correct.

The correct answer is:

`(0,6)`

Question **4**

Correct

Mark 1.00 out of 1.00

Let H be a collision resistant hash function. Define a new hash

function H1 based on H in the following way.

H1(X) = H(X) if X \neq X0, H1(X) = H(X1) if X = X0 where X0 and X1 are

not equal. Is H1 collision resistant?

○ a. Yes

● b. No ✓

Your answer is correct.

The correct answer is:

No

Question **5**

Incorrect

Mark 0.00 out of 1.00

Consider the RSA encryption algorithm with N=pq, here p,q are

large primes. Let the encryption key be e=3.

The encryption of the message m is c1 and encryption of the

message m+1 is c2. Is it possible to find m from c1 and c2 with out

performing decryption?

● a. No ✗

○ b. Yes

Your answer is incorrect.

The correct answer is:

Yes

Question **6**

Incorrect

Mark 0.00 out of 1.00

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)

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

○ c. T1

○ d. None of these

● e. C=AES-256(m2 \oplus T1) ✖

Your answer is incorrect.

The correct answer is:

C=AES-256(m2)

Question **7**

Correct

Mark 1.00 out of 1.00

Consider the prime number p=2267 and the group \mathbb{Z}_p^* with

multiplication modulo p operation. Let g=2 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 1197 and 62 respectively. Which of the

following statement is correct.

● a. Alice's public key = 1965, Bob's public key = 1209, Common secret key = 1459 ✓

○ b. none of these

○ c. Alice's public key = 1758, Bob's public key = 1528, Common secret key = 1980

○ d. Alice's public key = 1284, Bob's public key = 1975, Common secret key = 1890

Your answer is correct.

The correct answer is:

Alice's public key = 1965, Bob's public key = 1209, Common secret key = 1459

Question **8**

Correct

Mark 1.00 out of 1.00

Forward secrecy implies end to end encryption

○ a. True

● b. False ✓

Your answer is correct.

The correct answer is:

False

Question **9**

Correct

Mark 1.00 out of 1.00

```
In Signal protocol the initial secret key that will be established
```

```
between two users is
```

● a. `SHA-256(concatenation of Diffie-Hellman shared keys)` ✓

○ b. `SHA-256(concatenation of Diffie-Hellman shared keys and 1)`

○ c. `Concatenation of SHA-256(Diffie-Hellman shared keys)`

○ d. `Diffie-Hellman shared key`

Your answer is correct.

The correct answer is:

```
SHA-256(concatenation of Diffie-Hellman shared keys)
```

Question **10**

Incorrect

Mark 0.00 out of 1.00

```
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 DL is solved then CDH is also solved`

○ b. `If CDH is solved then DL is also solved`

● c. `DL and CDH both are equivalent` ✖

Your answer is incorrect.

The correct answer is:

```
If DL is solved then CDH is also solved
```

Question **11**

Incorrect

Mark 0.00 out of 1.00

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

○ a. `Depends on the message size`

○ b. `128 bit`

○ c. `256 bit`

● d. `512 bit` ✖

Your answer is incorrect.

The correct answer is:

```
128 bit
```

Question **12**

Incorrect

Mark 0.00 out of 1.00

Select the most appropriate option. During the registration phase

in Signal protocol the user

○ a. uploads public key of identity key, signed prekey, and signature on public key of signed prekey

○ b. uploads public key of identity key, signed prekey

● c. uploads public key of identity key, signed prekey, ephemeral key and signature on public key of signed prekey ✗

○ d. uploads public key of identity key, signed prekey, and signature on public key of identity key

Your answer is incorrect.

The correct answer is:

uploads public key of identity key, signed prekey, and signature on public key of signed prekey

Question **13**

Incorrect

Mark 0.00 out of 1.00

Consider the RSA encryption RSA-Enc algorithm and construct the

bit-generator G defined as follows.

G(K)= z = j-th bit of c. Here c = RSA-Enc(K) = K^e\mod n and j is fixed.

Which of following statement is correct?

● a. G is not Pseudorandom ✗

○ b. G is Pseudorandom

Your answer is incorrect.

The correct answer is:

G is Pseudorandom

Question **14**

Correct

Mark 1.00 out of 1.00

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:

$f(x_0,\ldots,x_{511})=1^{512} \text{ if } x_0=x_1=\cdots =x_{255}=1$

$f(x_0,\ldots,x_{511})=1^{256}||g(x_{256},\ldots ,x_{511}) \text{ otherwise}$

Here 1^d denotes a d-bits string whose all bits are one. Which of the

following statement is true?

● a. f is preimage resistant function ✓

○ b. f is not preimage resistant function

Your answer is correct.

The correct answer is:

f is preimage resistant function

Question **15**

Correct

Mark 1.00 out of 1.00

A trapdoor function is a function that is easy to compute in one

direction, yet difficult to compute in the opposite direction (finding

its inverse) without special information, called the "trapdoor".

Which of the following statement is correct?

○ a. RSA encryption is a trapdoor function with public key is the trapdoor

● b. RSA encryption is a trapdoor function with private key is the trapdoor ✓

○ c. Public key encryption function can not be a trapdoor function

Your answer is correct.

The correct answer is:

RSA encryption is a trapdoor function with private key is the trapdoor

Question **16**

Incorrect

Mark 0.00 out of 1.00

Consider the Elliptic curve EL: y^2=x^3+6x+3 under modulo 17.

\boxplus denotes the addition operation between two points on EL.

If P=(16,8), Q=(15,0) are two points on this curve then P\boxplus Q

will be

● a. (8,11) ✖

○ b. (16,9)

○ c. none of these

○ d. (9,2)

○ e. (6,0)

Your answer is incorrect.

The correct answer is:

(16,9)

Question **17**

Correct

Mark 1.00 out of 1.00

```
AES-Mixcolumn(160, 189, 63, 98) [all are in decimal]
```

○ a. `165, 179, 213, 25`

○ b. `211, 100, 225, 123`

○ c. `18, 23, 16, 21`

○ d. none of these

● e. `218, 226, 197, 189` ✓

Your answer is correct.

The correct answer is:

```
218, 226, 197, 189
```

Question **18**

Correct

Mark 1.00 out of 1.00

Consider the prime number p=353 and the group \mathbb{Z}_p^* with

multiplication modulo p operation. Let g=3 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 97 and 233 respectively. Which of the

following statement is correct.

○ a. Alice's public key = 340, Bob's public key = 28, Common secret key = 210

○ b. None of these

○ c. Alice's public key = 240, Bob's public key = 48, Common secret key = 130

● d. Alice's public key = 40, Bob's public key = 248, Common secret key = 160 ✓

Your answer is correct.

The correct answer is:

Alice's public key = 40, Bob's public key = 248, Common secret key = 160

Question **19**

Correct

Mark 1.00 out of 1.00

Consider the Elliptic curve EL: y^2=x^3+5x+3 under modulo 13.

\boxplus denotes the addition operation between two points on EL.

If P=(9,7), Q=(4,3) are two points on this curve then P\boxplus Q

will be

○ a. (8,3)

○ b. (8,10)

○ c. (13,10)

○ d. none of these

● e. (10,0) ✓

Your answer is correct.

The correct answer is:

(10,0)

Question **20**

Incorrect

Mark 0.00 out of 1.00

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

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

order of g?

● a. m-1 ✖

○ b. \phi(m)

○ c. (m-1)(m-2)

Your answer is incorrect.

The correct answer is:

\phi(m)

Question **21**

Correct

Mark 1.00 out of 1.00

Which of the following is true for forward secrecy?

○ a. forward secrecy implies perfect secrecy

○ 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. if the security of present message is compromised still the security of previous messages remain unaffected ✓

Your answer is correct.

The correct answer is:

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

Question **22**

Incorrect

Mark 0.00 out of 1.00

```
If n = pq, where p, q are large primes. We state the following problems P1 and P2:
```

```
P1: Find p, q from n.
```

```
P2: Compute \phi(n) without knowing p, q.
```

```
Which of the following statement is true?
```

○ a. Solving P2 is harder than P1.

○ b. Problems P1 and P2 are equivalent.

● c. Solving P1 is harder than P2. ✗

Your answer is incorrect.

The correct answer is:

Problems P1 and P2 are equivalent.

Question **23**

Correct

Mark 1.00 out of 1.00

Consider the prime number p=3319 and the group \mathbb{Z}_p^* with

multiplication modulo p operation. Let g = 6 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 1197 and 62 respectively. Which of the

following statement is correct.

○ a. Alice's public key = 1582, Bob's public key = 1758, Common secret key = 1890

● b. Alice's public key = 1758, Bob's public key = 1582, Common secret key = 1890 ✓

○ c. none of these

○ d. Alice's public key = 1658, Bob's public key = 1528, Common secret key = 1980

Your answer is correct.

The correct answer is:

Alice's public key = 1758, Bob's public key = 1582, Common secret key = 1890

Question **24**

Correct

Mark 1.00 out of 1.00

`Let n = 43 * 73 and the encryption key of RSA be e = 1195.`

`For the message M = 1234 which of the following statement is true.`

● a. `the decryption key d = 787, ciphertext C = 760` ✓

○ b. `the decryption key d = 760, ciphertext C = 787`

○ c. none of these

○ d. `the decryption key d = 777, ciphertext C = 760`

Your answer is correct.

The correct answer is:

`the decryption key d = 787, ciphertext C = 760`

Question **25**

Correct

Mark 1.00 out of 1.00

`The key derivation function of the Signal protocol is`

○ a. `an invertible function`

○ b. `an one to one function`

● c. `an one way function` ✓

Your answer is correct.

The correct answer is:

`an one way function`

Question **26**

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

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

○ d. none of these

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

Your answer is correct.

The correct answer is:

c0 39 34 78 84 6c 52 0f 0c f5 f8 b4 c0 28 16 4b

Question **27**

Incorrect

Mark 0.00 out of 1.00

```
Which of the following technique is followed in the SSL record protocol
to achieve confidentiality as well as integrity?
```

○ a. `None of these`

● b. `Encryption((MAC(compressed data)) || Encryption(compressed data)` ✖

○ c. `Encryption (compressed data || MAC(compressed data))`

○ d. `Encryption(compressed data) || MAC(compressed data)`

Your answer is incorrect.

The correct answer is:

`Encryption (compressed data || MAC(compressed data))`

Question **28**

Incorrect

Mark 0.00 out of 1.00

```
Let n be a product of two large primes i.e., n = p*q. We know that
finding p, q from n is a computationally hard problem. If I give you n
along with \phi(n) then will you be able to find p, q in polynomial time?
```

● a. `No` ✖

○ b. `Yes`

Your answer is incorrect.

The correct answer is:

`Yes`

Question **29**

Correct

Mark 1.00 out of 1.00

Let n = 17 * 11 = 187 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 = 13, ciphertext C = 21

○ b. the decryption key d = 21, ciphertext C = 11

● c. the decryption key d = 23, ciphertext C = 11 ✓

Your answer is correct.

The correct answer is:

the decryption key d = 23, ciphertext C = 11

Question **30**

Incorrect

Mark 0.00 out of 1.00

Select the most appropriate option.

In Signal protocol perfect secrecy is achieved

○ a. by deleting previous root key and using SHA-256

● b. by deleting previous root key, previous chain key and using SHA-256 ✗

○ c. by deleting previous root key, previous chain key, previous message key and by using SHA-256

Your answer is incorrect.

The correct answer is:

by deleting previous root key, previous chain key, previous message key and by using SHA-256

Question **31**

Incorrect

Mark 0.00 out of 1.00

The initial message in Signal protocol is encrypted using

● a. AES-256 in CBC mode on (Message || MAC on the message) ✖

○ b. AES-256 in CTR mode with signature based encryption

○ c. authenticated encryption with associated data using AES-256

Your answer is incorrect.

The correct answer is:

authenticated encryption with associated data using AES-256

Question **32**

Incorrect

Mark 0.00 out of 1.00

In SSL the sequence number of the sending data and receiving

data is a part of

● a. session state ✖

○ b. connection state

Your answer is incorrect.

The correct answer is:

connection state

Question **33**

Correct

Mark 1.00 out of 1.00

`We define a new encryption algorithm TEnc using AES-128 encryption`

`technique.`

`TEnc :` $\{0,1\}^{384}\times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ `where`

`C = TEnc(K||K1||K2, M) = K2` $\oplus$ `AES-128-Enc(K, K1` $\oplus$ `M).`

`Here K, K1, K2 each is of 128 bit. What will be the decryption algorithm`

`(TDec) corresponding to TEnc.`

○ a. None of these

● b. `M = TDec(K||K1||K2, C) = K1` $\oplus$ `AES-128-Dec(K, K2` $\oplus$ `C)` ✓

○ c. `M = TDec(K||K1||K2, C) = K2` $\oplus$ `AES-128-Dec(K, K1` $\oplus$ `C)`

○ d. `M = TDec(K||K1||K2, C) = K` $\oplus$ `AES-128-Dec(K1, K2` $\oplus$ `C)`

Your answer is correct.

The correct answer is:

`M = TDec(K||K1||K2, C) = K1` $\oplus$ `AES-128-Dec(K, K2` $\oplus$ `C)`

Question **34**

Incorrect

Mark 0.00 out of 1.00

```
In which message of the SSL protocol, server sends its random number?
```

○ a. `in server's hello message`

○ b. `in change cipher message`

● c. `in handshake message` ✗

○ d. `inside record header`

Your answer is incorrect.

The correct answer is:

```
in server's hello message
```

Question **35**

Correct

Mark 1.00 out of 1.00

```
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 is a preimage resistant function`

● b. `G need not be a preimage resistant function` ✓

Your answer is correct.

The correct answer is:

```
G need not be a preimage resistant function
```

Question **36**

Not answered

Marked out of 1.00

Select the most appropriate option. Signal protocol provides

○ a. end to end encryption, forward secrecy only

○ b. end to end encryption, forward secrecy and handles out of order messages

○ c. end to end encryption only

Your answer is incorrect.

The correct answer is:

end to end encryption, forward secrecy and handles out of order messages

Question **37**

Not answered

Marked out of 1.00

A 5-bit LFSR is constructed using the connection polynomial

f(x)=x^5+x^4+x^2+x+1. The period of this LFSR will be

○ a. 31

○ b. none of these

○ c. 63

○ d. 30

○ e. 15

Your answer is incorrect.

The correct answer is:

31

Question **38**

Not answered

Marked out of 1.00

If the two fragmented data are identical in SSL Record protocol, then

which of the following statement is correct?

○ a. the corresponding encrypted data will be identical as the compressed data will be the same

○ b. the corresponding encrypted data will be different

○ c. nothing can be said

Your answer is incorrect.

The correct answer is:

the corresponding encrypted data will be different

Question **39**

Not answered

Marked out of 1.00

Certificate is a

○ a. signed public key of an user signed by some trusted party

○ b. MAC of an user's public key generated by some trusted party

○ c. signed private key of an user signed by some trusted party

○ d. signed public key of user signed by the same user

Your answer is incorrect.

The correct answer is:

signed public key of an user signed by some trusted party

Question **40**

Not answered

Marked out of 1.00

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

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

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

○ a. not a permutation on \mathbb{Z}_n^*

○ b. none of these

○ c. a permutation on \mathbb{Z}_n^*

Your answer is incorrect.

The correct answer is:

a permutation on \mathbb{Z}_n^*

◄ Midterm

Jump to...

Dashboard / My courses / CS364_2024 / General / LAB test

Started on	Friday, 1 March 2024, 11:33 AM
State	Finished
Completed on	Friday, 1 March 2024, 11:53 AM
Time taken	20 mins
Grade	**5.00** out of 9.00 (**56**%)

Question **1**

Not answered

Not graded

Consider a modified Playfair cipher on

{ A, B, C, D,..., Z, \ , /, [,] } . Note that the set has 30 elements.

Consider the key = AETIMPSB and select the encryption of

plaintext = CRYPTO\N

☐ a. QDUDWBEV

☐ b. QDDUBWEV

☐ c. QDUDBWEV

☐ d. none of these

☐ e. QDUDBWVE

Your answer is incorrect.

The correct answers are:
QDUDBWEV,

none of these

Question **2**

Incorrect

Mark 0.00 out of 1.00

Consider AES-Subbyte table Sub().

We define a new S-box from Sub as follows:

S(x) = Sub((2*x)+1), here a*x and y+b are done in

$\mathbb{F}_2[x]/ < x^8 + x^6 + x^5 + x^4 + x^2 + x + 1 >$.

What is value of S(212)? Here input, output are in decimal.

● a. 28 ✖

○ b. none of these

○ c. 92

○ d. 29

○ e. 113

Your answer is incorrect.

The correct answer is:
29

Question **3**

Incorrect

Mark 0.00 out of 1.00

```
MIXCOLUMN (32, 198, 201, 35) = ?
```

`when we work on` $\mathbb{F}_2[x]/ < x^8 + x^6 + x^5 + x^4 + x^2 + x + 1 >$.

```
Input, output are in decimal.
```

● a. (151, 202, 102, 41) ✖

○ b. (151, 102, 212, 41)

○ c. (151, 212, 102, 11)

○ d. (151, 212, 102, 41)

○ e. none of these

Your answer is incorrect.

The correct answer is:
(151, 212, 102, 41)

Question **4**

Correct

Mark 1.00 out of 1.00

Consider Shift cipher and find the encryption of

the plaintext = aeqwg

where key = 5

● a. fjvbl ✓

○ b. fvjbl

○ c. fjvbp

○ d. none of these

○ e. fjvlb

Your answer is correct.

The correct answer is:
fjvbl

Question **5**

Correct

Mark 1.00 out of 1.00

Let p = 2147483647. If a = 13 then the multiplicative inverse

of a under mod p is =

○ a. none of these

○ b. 1486729448

○ c. 1486719447

○ d. 1486619448

● e. 1486719448 ✓

Your answer is correct.

The correct answer is:

1486719448

Question **6**

Incorrect

Mark 0.00 out of 1.00

Consider a Playfair cipher with key = aedoqmw

What is the correct ciphertext of the plaintext = iamd

○ a. ehew

● b. hewe ✗

○ c. dgab

○ d. none of these

○ e. gdba

Your answer is incorrect.

The correct answer is:
gdba

Question **7**

Correct

Mark 1.00 out of 1.00

CAESAR-Encryption (aeqwg) = ?

● a. dhtzj ✓

○ b. dthjz

○ c. dhtzq

○ d. ahtzj

○ e. none of these

Your answer is correct.

The correct answer is:
dhtzj

Question **8**

Correct

Mark 1.00 out of 1.00

Consider Affine encryption algorithm.

If the secret key is K = (11,5), the ciphertext of the

plaintext = aeswq is = ?

○ a. none of these

○ b. fxvny

● c. fxvnz ✓

○ d. fxnvz

○ e. fzvnx

Your answer is correct.

The correct answer is:
fxvnz

Question **9**

Incorrect

Mark 0.00 out of 1.00

```
MIXCOLUMN (32, 198, 201, 35) = ?
```

when we work on $\mathbb{F}_2[x]/<x^8+x^4+x^3+x^2+1>$.

```
Input, output are in decimal.
```

○ a. `(253, 212, 12, 41)`

○ b. `(251, 212, 10, 41)`

○ c. `(231, 18, 101, 55)`

○ d. `(211, 213, 17, 37)`

● e. none of these ✗

Your answer is incorrect.

The correct answer is:

```
(253, 212, 12, 41)
```

Question **10**

Correct

Mark 1.00 out of 1.00

Consider AES-Subbyte table Sub().

We define a new S-box from Sub as follows:

S(x) = Sub((2*x)+1), here a*x and y+b are done in

$\mathbb{F}_2[x]/ < x^8 + x^4 + x^3 + x + 1 >.$

What is value of S(126)? Here input, output are in decimal.

○ a. 48

● b. 84 ✓

○ c. 88

○ d. none of these

○ e. 83

Your answer is correct.

The correct answer is:
84

◄ Announcements

Jump to...

Dashboard / My courses / IT301_IT / Topic 1 / Midterm (2nd Online)

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} → {0,1}^{256} be any preimage resistant function. Define f:{0,1}^{512} → {0,1}^{512} by using the following rule:

f (x[0] , ... , x[511]) = 1^{512} if x[0] = x[1] = · · · · = x[255] = 1
f (x[0] , ... , x[511]) = 1^{256} ||g(x[256] , ... , 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 $F_k = F_{k-1} \oplus \text{Enc}(P_k, F_{k-1})$ 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

$H(X) = F(X1 \oplus X2)$

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...

Dashboard / My courses / IT301_IT / Topic 1 / Pre Midterm

Started on	Monday, 23 August 2021, 11:49 AM
State	Finished
Completed on	Monday, 23 August 2021, 12:33 PM
Time taken	44 mins 41 secs
Grade	**7.50** out of 10.00 (**75**%)

Question **1**

Incorrect

Mark 0.00 out of 0.50

Select the correct answer where S_1: $\{0,1\}^6 \rightarrow \{0,1\}^4$ and S_2:$\{0,1\}^6 \rightarrow \{0,1\}^4$ are the first two

defined S-boxes for the round function of DES. (For the description of these S-boxes please

see page 260 of Handbook of Applied Cryptography book.)

○ a. $S_1(59) = 0$, $S_2(23) = 14$.

● b. $S_1(59) = 4$, $S_2(23) = 8$ ✖

○ c. $S_1(59) = 1$, S2$(23) = 10$.

○ d. $S_1(59) = 0$, $S_2(23) = 10$.

Your answer is incorrect.

The correct answer is:
$S_1(59) = 0$, $S_2(23) = 10$.

Question **2**

Correct

Mark 0.50 out of 0.50

Consider Playfair cipher encrypt the plaintext MIDSEM using the key MAYANK.

Which is the correct ciphertext?

○ a. GYQENB

● b. None of the other ✓

○ c. GYEQBN

○ d. YGEQNB

○ e. YGQEBN

○ f. YGEQBN

Your answer is correct.

The correct answer is:
None of the other

Question **3**

Correct

Mark 0.50 out of 0.50

Round function of every block cipher has to be invertible.

● a. The above statement is not always true ✓

○ b. It is never true

○ c. It is always true

Your answer is correct.

The correct answer is:
The above statement is not always true

Question **4**

Correct

Mark 0.50 out of 0.50

The S-boxes of any SPN based block cipher

○ a. may not be invertible

● b. has to be invertible ✓

Your answer is correct.

The correct answer is:
has to be invertible

Question **5**

Correct

Mark 0.50 out of 0.50

Which of the following property is true for the expansion function of DES ?

○ a. it is bijective

○ b. none of the other

● c. it is one to one ✓

○ d. it is onto

Your answer is correct.

The correct answer is:
it is one to one

Question **6**

Correct

Mark 0.50 out of 0.50

Round key size of DES is

○ a. 64 bit

● b. 48 bit ✓

○ c. 56 bit

Your answer is correct.

The correct answer is:
48 bit

Question **7**

Incorrect

Mark 0.00 out of 0.50

Total memory required to store an S-box $S:\{0,1\}^m \to \{0,1\}^m$ is

○ a. 2^m bits

● b. m ✗

○ c. $m2^m$ bits

Your answer is incorrect.

The correct answer is:
$m2^m$ bits

Question **8**

Correct

Mark 0.50 out of 0.50

AES-512 has 16 rounds.

● a. Flase ✓

○ b. True

Your answer is correct.

The correct answer is:
Flase

Question **9**

Correct

Mark 0.50 out of 0.50

Total number of possible valid keys of affine cipher is

● a. 312 ✓

○ b. 676

○ c. 338

○ d. 26

Your answer is correct.

The correct answer is:
312

Question **10**

Incorrect

Mark 0.00 out of 0.50

Exhausitve search complexity of substitution cipher is

● a. None of the other ✗

○ b. `403291461126605635584000001`

○ c. `403291461126605635584000000`

○ d. `403291461126605635584000003`

Your answer is incorrect.

The correct answer is:

`403291461126605635584000000`

Question **11**

Correct

Mark 0.50 out of 0.50

S-boxes in DES map

○ a. 4 bits to 6 bits

○ b. 2 bits to 4 bits

● c. 6 bits to 4 bits ✓

○ d. 4 bits to 4 bits

Your answer is correct.

The correct answer is:

6 bits to 4 bits

Question **12**

Correct

Mark 0.50 out of 0.50

Consider one-bit encryption $C = P \oplus K$. If $Pr[K=0]=0.5$ and $Pr[P=1]=0.2$ then $Pr[P=0|C=1]$ is

○ a. 0.5

○ b. 0.4

○ c. 0.2

● d. 0.8 ✓

Your answer is correct.

The correct answer is:
0.8

Question **13**

Incorrect

Mark 0.00 out of 0.50

How many distinct keys are required for a successful bi-directional encrypted communication using DES in a group of 6 people.

● a. None of the other ✖

○ b. 15

○ c. 46656

○ d. 720

○ e. 120

Your answer is incorrect.

The correct answer is:
15

Question **14**

Correct

Mark 0.50 out of 0.50

Suppose we have used (4,5) as a key corresponding to affine cipher. Which of the following is true?

○ a. None of the above

○ b. Encryption function can be used to decrypt the ciphertext

○ c. Output from the encryption function will be wrong

● d. It is not a valid key ✔

Your answer is correct.

The correct answer is:
It is not a valid key

Question **15**

Correct

Mark 0.50 out of 0.50

The original name of AES is

○ a. Advanced Encryption System

○ b. Advanced Encryption Standard

● c. Rijndael ✓

Your answer is correct.

The correct answer is:
Rijndael

Question **16**

Correct

Mark 0.50 out of 0.50

Consider one round of Feistel Network with the block size 64 bit and secret key K of size 32 bit.

The round function is defined by $f(R, K) = S(R \oplus K)$ where $S(X) = (1 + X) \mod 2^{32}$.

The ciphertext corresponding to the plaintext = 1 is

○ a. 4294967296

○ b. 4294967297

● c. None of the other ✓

○ d. 458129844

○ e. 1

Your answer is correct.

The correct answers are:
4294967297,

458129844,

4294967296,

1,

None of the other

Question **17**

Incorrect

Mark 0.00 out of 0.50

Let E be encryption algorithm of DES with 3 rounds. Let M be a message and K be a secret key.

Let $C_1 = E(M, K)$ and $C_2 = E(\bar{M}, \bar{K})$.

Here $\bar{X}$ denotes the bitwise complement of X.

Which of the following relation is correct?

○ a. $\bar{C_1} = C_2$

● b. None of the other ✗

○ c. $C_1 = C_2$

Your answer is incorrect.

The correct answer is:
$\bar{C_1} = C_2$

Question **18**

Correct

Mark 0.50 out of 0.50

Which is the correct statement for DES among the following statements:

● a. Block size = 64, Key size = 56, Number of rounds = 16. ✓

○ b. Block size = 56, Key size = 48, Number of rounds = 16.

○ c. Block size = 64, Key size = 48, Number of rounds = 10.

Your answer is correct.

The correct answer is:

Block size = 64, Key size = 56, Number of rounds = 16.

Question **19**

Correct

Mark 0.50 out of 0.50

Let us consider Feistel Network encryption with 16 rounds. The 16 round keys are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,

11, 12, 13, 14, 15, 16. Consider the message = 32.

Find the ciphertext C corresponding to the message = 32 generated using above

Feistel Network and the above mentioned round keys.

We further apply same encryption on the ciphertext C using the round keys

in reverse order (i.e., 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1) and generate C1.

What will be the value of C1?

○ a. 23

○ b. 2147

● c. 32 ✓

○ d. None of the other

Your answer is correct.

The correct answer is:
32

Question **20**

Correct

Mark 0.50 out of 0.50

Shift cipher provides perfect secrecy or not.

○ a. It will never provide perfect secrecy as it differs from OTP.

● b. Yes if we use an independent key for each plaintext character. ✓

Your answer is correct.

The correct answer is:

Yes if we use an independent key for each plaintext character.

◄ Announcements

Jump to...

Midterm (2nd Online) ►