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 ►

Dashboard / My courses / CS304 / Topic 1 / 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...