Midterm #1 Results for Khuong Huynh

Score for this quiz: **15.67** out of 26

Submitted Jun 28 at 7:58pm

This attempt took 75 minutes.

Question 1

0 / 2 pts

Given the data X = (X_1,X_2,X_3,…,X_n), where each X_i is a byte and n is the total number of bytes, and a hash function defined as:

$h(X) = (2n*X_1 + n+X_2 + 2n*X_3 + n+X_4 +...+ 2n*X_{n-1} + n+X_n) \bmod 256$ [if n is even]

$h(X) = (2n*X_1 + n+X_2 + 2n*X_3 + n+X_4 +...+ n+X_{n-1} + 2n*X_n) \bmod 256$ [if n is odd]

Please, propose an example of collision adding the necessary proof.

Your Answer:

h(4)*2=8

h(2,2)

0,2 = 2(0 * 2) + 2(2*2) = 0 +8 = 8

h(2,2) is not 8 but 12 h(0,2) is 4

Question 2

2 / 2 pts

In the context of Diffie-Hellman key exchange algorithm, using the values: $p=23, g=12$

and: $a=4$, $b=2$

Show how Alice and Bob are able to exchange the same key. Show all the necessary steps.

Your Answer:

Alice send g^a mod P to Bob and Bob received and send g^b mod P back to Alice.

Then Alice computes [g^a mod p]^b = g^ab mod p

Bob computes the same [g^b mod p]^a = g^ab mod p

Shared key:

g^ab mod P = 12^(4*2) mod 23 = 12^(2*4) mod 23

= 429,981,696 mod 23 = 8

Question 3

0 / 1 pts

Given the Diffie-Hellman scheme from the previous question, show how Trudy can perform a Man-in-the-Middle attack by using the private value $t = 5$.

Note that the two values are sent in plaintext.

Your Answer:

Trudy knows g^a, g^b, g^t

She will elevated to g^at with Alice and g^bt with Bob then computes, g^(a*b*t)

12^(4*2*5) mod 23 = 16

Question 4

3 / 4 pts

These set of questions deals with the A5/1 cipher. Justify your answers to get full credits.

A. On average, how often does the Z register step?
B. On average, how often do all three registers step?
C. On average, how often do al least two registers step?
D. On average, how often does exactly one register step?

Your Answer:

A. Each register based on maj (X8, Y10,Z10).

There are 6/8 register often shift = 0.75

3	0	0	0	0
2	0	0	1	0
2	0	1	0	0
2	0	1	1	1
2	1	0	0	0
2	1	0	1	1
2	1	1	0	1
3	1	1	1	1

B. All 3 registers shift 2/8

C. 2 registers shift 6/8

D. Zero.

Question 5

3 / 3 pts

Suppose that Bob receives Alice’s digital certificate from someone claiming to be Alice.

A. Before Bob verifies the signature on the certificate, what does he know about the identity of the sender of the certificate?

B. How can Bob recognize that the following certificate is not to be trusted:

$$\left(M,\ [M]_{Trudy}\right),\ where\ M\ =\ (Alice,\ Trudy's\ Public\ Key)$$

C. After Bob verifies the signature on the certificate, what does he know about the identity of the sender of the certificate?

Your Answer:

A.

Bob knows nothing about the sender. Because it is public, and anyone can access the certificate.

B.

To verify the signature on Certificate. Bob needs to use Certificate Authority public key. Bob can verify if the signature belongs to Alice or not. Signature is used private key so no one could access to it. Bob need to receive CA by asking Alice.

C.

Nothing. Even the CA verified doesn't means it's Alice because the CA is public anyone can access it.

Question 6

0 / 2 pts

Trudy wants to share the same key with both Alice and Bob using Diffie-Hellman. Thus, she tries to attack their key-exchange protocol in this way:

She changes (g^a mod p) with (g^{ap} mod p) and sends it to Bob

She changes (g^b mod p) with (g^p mod p) and sends it to Alice

What will she able to achieve in this case?

Remember: 'a' is Alice's private value and 'b' is Bob's private value.

○ Trudy can only share a key with Bob

orrect Answer ○ Trudy can only share a key with Alice

ou Answered ● Trudy cannot share any key with Alice and Bob

○ Trudy can share a key with both Alice and Bob

Question 7

0 / 2 pts

Given the following Diffie-Hellman scheme, which of the sentences below is/are correct?

Select all that apply.

Alice to Bob - “I’m Alice”, g^a mod p
Bob to Alice - $\{[g^b \text{ mod } p]_{Bob}\}_{Alice}$

[...] is encryption with specified PRIVATE key.

{...} is encryption with specified PUBLIC key.

Correct! ☑ Alice generates the key g^{ab} mod p

☐ Trudy can share g^{at} with Bob

□ Bob generates the key g^t mod p

□ Trudy can share g^{bt} with Alice

orrect Answer

□ Trudy cannot share any key

ou Answered

☑ Trudy can share g^{at} mod p with Alice

ou Answered

☑ Trudy can share g^{bt} mod p with Bob

Question 8

0 / 2 pts

Given the following Diffie-Hellman scheme, which of the sentences below is/are correct?

Select all that apply.

Alice to Bob - [“I’m Alice”]$_{Alice}$, g^a mod p
Bob to Alice - [g^b mod p]$_{Bob}$

[...] is encryption with specified PRIVATE key.

{...} is encryption with specified PUBLIC key.

orrect Answer

○ Trudy can share g^{bt} with Bob

○ Trudy can share g^{at} with Bob

○ Trudy can share g^{at} with Alice

○ Trudy can share g^{bt} with Alice

ou Answered

● Trudy cannot share any key

Question 9

1 / 1 pts

In the context of the DES cipher, what is the output of the "S-box" showed below if the bits in input are:

001001

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

○ 0110

Correct!

● 1110

○ 1001

○ 0101

○ 1100

Question 10

1 / 1 pts

Is AES a Feistel Cipher?

Correct!

● No

○ Yes

Question 11

2 / 2 pts

Which of these sentences are TRUE (select all that apply).

NOTE: MAC is Message Authentication Code

□ Private key encryption can be used to achieve repudiation

□ Private key encryption can be used to achieve confidentiality

□ Public key encryption can be used to achieve non-repudiation

□ HMAC can be used to achieve non-repudiation

Correct! ☑ HMAC can be used to achieve repudiation

Correct! ☑ Symmetric key encryption can be used to achieve repudiation

Question 12

1 / 1 pts

How many unique keys are needed to encrypt and decrypt a message using Public key crypto?

○ 0

○ 1

○ π (pi)

Correct! ● 2

○ 299,792,458

○ 1,6180339887

○ 6.0221415×10^{23}

Question 13

0 / 2 pts

Alice needs to exchange a critical information M with Bob. She wants to ensure confidentiality using AES (CBC mode), and she shares with Bob the key K1 for this purpose. Furthermore, she also wants to ensure integrity using Message Authentication Code (MAC), and she shares with Bob the key K2 for this purpose.

What does Alice need to send to Bob to achieve both confidentiality and integrity in this case?

Select all that apply.

ou Answered

☑ The key K1

Correct!

☑ The Initialization Vector (IV)

□ The output of h(M, K), where h() is SHA-2

□ The plaintext blocks

orrect Answer

□ The last encrypted block using K2

□ The key K2

□ The last encrypted block using K1

orrect Answer

□ All the encrypted blocks using K1

ou Answered

☑ The output of h(K, M), where h() is SHA-2

Question 14

Original Score: 0 / 1 pts Regraded Score: 0.67 / 1 pts

ⓘ **This question has been regraded.**

Ignoring the ipad and opad values, which of these HMAC outputs are not subject to attack? Select all that apply.

Correct! ☑ The output of h(K, M, M'), where h() is SHA-3

□ The output of h(K, M, M'), where h() is SHA-2

Correct! ☑ The output of h(M, M', K), where h() is SHA-3

ou Answered ☑ The output of h(M, K, M'), where h() is SHA-2

Correct! ☑ The output of h(M, K, M'), where h() is SHA-3

Quiz Score: **15.67** out of 26

This quiz score has been manually adjusted by +2.0 points.