Q1 True or False: Cryptography

7 Points

Q1.1

1 Point

If the daily lottery numbers are truly random, then they can be used as the entropy for a one-time-pad since a one-time-pad needs to be random.

○ True

● False

Q1.2

1 Point

Suppose there is a transmission error in a block B of ciphertext using CBC mode. This error propagates to every subsequent block in decryption, which means that the block B and every block after B cannot be decrypted correctly.

○ True

● False

Q1.3

1 Point

The IV for CBC mode must be kept secret.

○ True

● False

Q1.4

1 Point

Alice and Bob share a symmetric key k. Alice sends Bob a message encrypted with k stating, "I owe you $100", using AES-CBC encryption. Assuming AES is secure, we can be confident that an active attacker cannot tamper with this message; its integrity is protected.

○ True

● False

Q1.5

1 Point

Alice and Bob share a secret symmetric key k which they use for calculating MACs. Alice sends the message $M =$ "I, Alice, owe you, Bob, $100" to Bob along with its message authentication code $\mathrm{MAC}_k(M)$. Bob can present $(M, \mathrm{MAC}_k(M))$ to a judge as proof that Alice owes him $100 since a MAC provides integrity.

○ True

● False

Q1.6

1 Point

The random number r in El Gamal can be made public.

○ True

● False

Q1.7
1 Point

It is okay if multiple people use the same modulus p for their El Gamal public key.

● True

○ False

Q2 Hashing Functions

4 Points

Recall the definition of "one-way functions" and "collision-resistance" from lecture.

- We say a function f is one-way if given $f(x)$ it is hard to find x' such that $f(x') = f(x)$.
- We say a function f is “collision-resistant” if it is hard to find two inputs x, y such that $f(x) = f(y)$ but $x \neq y$.

For each of the given functions H below, determine if it is one-way or not, and if it is collision-resistant or not.

Q2.1

1 Point

Select if $H(x) = x$ is:

○ One way

● Collision resistant

○ Both

○ None

Q2.2

1 Point

Select if $H(x) = x \bmod 2$ is:

○ One way

○ Collision resistant

○ Both

● None

Q2.3
1 Point

Let E_k be an ideally secure block cipher with a known and published key k.

Select if $H(x) = E_k(x)$ is:

○ One way

● Collision resistant

○ Both

○ None

Q2.4
1 Point

Select if $H(x) = 0$ is:

○ One way

○ Collision resistant

○ Both

● None

Q3 El Gamal Encryption

3 Points

Recall the definition of El Gamal encryption from lecture:

- Everyone knows a large prime p, and an integer g.
- Bob chooses a private key b, and computes a public key $B = g^b \pmod{p}$.
- To encrypt a message m, Alice generates a random r, and creates the ciphertext $(c_1, c_2) = (g^r,\ m \cdot B^r) \pmod{p}$.
- To decrypt the ciphertext, Bob calculates $c_1^{-b} c_2 \equiv m \pmod{p}$.

(Note: Since everything is $\mathrm{mod}\ p$, we need $2 \leq g \leq p-2,\ 0 \leq b \leq p-2$, and $0 \leq r \leq p-2$.)

As mentioned in the textbook, this simplified El Gamal scheme is actually not IND-CPA secure. In this question, we'll explore some attacks on this scheme.

Q3.1
1 Point

Alice encrypts m and sends the ciphertext (c_1, c_2) to Bob. Construct a ciphertext (c_1', c_2') which is the encryption of $2m$. All computations are mod p.

$c_1' =$

● c_1

○ $2 + c_1$

○ $2 \oplus c_1$

○ $2c_1$

○ c_1^2

$c_2' =$

○ c_2

○ $2 + c_2$

○ $2 \oplus c_2$

● $2c_2$

○ c_2^2

Q3.2
1 Point

Suppose you intercept two ciphertexts $(g^{r_1}, m_1 B^{r_1})$ and $(g^{r_2}, m_2 B^{r_2})$ that Alice has encrypted for Bob. Assume they are encryptions of some unknown messages m_1 and m_2.

Construct a ciphertext (c_1, c_2) which is a valid El Gamal encryption of the message
$m_1 m_2$. All computations are mod p.

$c_1 =$

○ $g^{r_1} B^{r_1}$

○ $g^{r_1} m_1$

● $g^{r_1+r_2}$

○ $g^{r_1 * r_2}$

$c_2 =$

○ $m_1 m_2$

○ $B^{r_1+r_2}$

○ $g^{r_1+r_2} B^{r_1+r_2}$

● $m_1 m_2 B^{r_1+r_2}$

Q3.3
1 Point

Consider a new scheme where the value r is not generated randomly every time. Instead, Alice randomly generates an initial value r_0, and then increments r_0 by 1 every time she needs to encrypt another message. Is this encryption scheme IND-CPA secure?

○ Yes

● No

Suppose Alice encrypts m_0 and then encrypts m_1 immediately after, both using the scheme above. Which of the following values can an adversary obtain, given knowledge of these two ciphertexts?

○ m_0

○ m_1

○ r_0

○ $m_0 m_1$

○ $m_0 + m_1$

○ $m_0 - m_1$

● m_0 / m_1

○ None of the above

Q4 Length Extension

4 Points

One subtle crypto fail you've heard about in lecture is SHA-2's susceptibility to *length extension attacks*. In this question, we'll walk you through a simplified version of the SHA-2 algorithm and show how that algorithm is fundamentally vulnerable.

Q4.1

1 Point

Hashes are functions that map a string of arbitrary length to a string of constant length. However, it turns out the SHA-2 algorithm actually only works if the input is a multiple of 64 bytes. So the first step of the SHA-2 algorithm is to pad the input by appending `0` repeatedly to the input until its length is a multiple of 64.

In problem 4, we reasoned that padding with zeros isn't a valid padding to use for encryption. Why is it acceptable for hashing?

○ We always know the input's length before running the hashing algorithm

● There is no need to recover a hash function's input

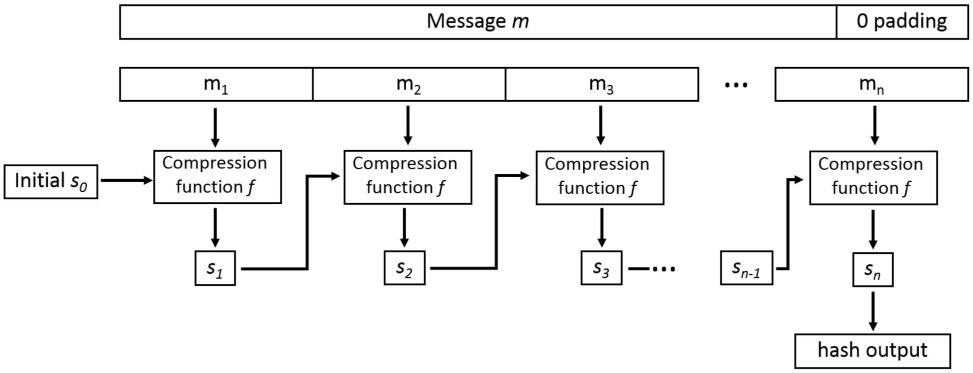
○ Cryptographic hash functions map zeros to random bits

Q4.2
1 Point

Given a padded input (i.e. the input length is a multiple of 64), the SHA-2 algorithm first divides the message into 64-byte blocks. Then, it initializes its *internal state* to a constant, publicly known value s_0.

For each block, SHA-2 updates the internal state by calculating $s_i = f(s_{i-1}, m_i)$, where s_i is the new internal state after processing the current block, s_{i-1} is the previous internal state, m_i is the current block, and f is some complicated *one-way compression function*.

The final hash output is the internal state after all n blocks have been processed.



Suppose that an attacker observes an internal state s_i before the algorithm completes $(i < n)$. Can they compute the hash output $\text{SHA-2}(m)$ without knowing m?

○ Yes

● No

Q4.3
1 Point

Again, suppose the attacker observes an internal state s_i. Let m' be an arbitrary one-block-long message of the attacker's choosing.

Can the attacker compute $\text{SHA-2}(m_1 \mid\mid m_2 \mid\mid \ldots \mid\mid m_i \mid\mid m')$?

● Yes

○ No

Q4.4
1 Point

Suppose that SHA-2 used 8-byte blocks instead of 64-byte blocks. Given SHA-2(`EvanBot`), which of the following could an attacker calculate?

□ SHA-2(EvanBot-is-real)

☑ SHA-2(EvanBot001)

□ SHA-2(Evan-is-a-Bot)

□ None of the above

Q5 Feedback

0 Points

What's something we could do to make the class better? Or, what did you find most difficult or confusing from lectures or the rest of class, and what would you like to see explained better?

Homework 3

● Graded

Select each question to review feedback and grading details.

Student

Yiyun Chen

Total Points

18 / 18 pts

Question 1

	True or False: Cryptography	**7** / 7 pts
1.1	(no title)	**1** / 1 pt
1.2	(no title)	**1** / 1 pt
1.3	(no title)	**1** / 1 pt
1.4	(no title)	**1** / 1 pt
1.5	(no title)	**1** / 1 pt
1.6	(no title)	**1** / 1 pt
1.7	(no title)	**1** / 1 pt

Question 2

Hashing Functions		**4** / 4 pts
2.1	(no title)	**1** / 1 pt
2.2	(no title)	**1** / 1 pt
2.3	(no title)	**1** / 1 pt
2.4	(no title)	**1** / 1 pt

Question 3

El Gamal Encryption		**3** / 3 pts
3.1	(no title)	**1** / 1 pt
3.2	(no title)	**1** / 1 pt
3.3	(no title)	**1** / 1 pt

Question 4

Length Extension		**4** / 4 pts
4.1	(no title)	**1** / 1 pt
4.2	(no title)	**1** / 1 pt
4.3	(no title)	**1** / 1 pt
4.4	(no title)	**1** / 1 pt

Question 5

Feedback	**0** / 0 pts