Final Exam
Graded Quiz • 26 min

Due Dec 16, 1:29 PM IST

Congratulations! You passed!

TO PASS 80% or higher

Keep Learning

GRADE
100%

Final Exam

LATEST SUBMISSION GRADE
100%

1. **Let (E,D) be an authenticated encryption system built by combining a CPA-secure symmetric cipher and a MAC. The system is combined with an error-correction code to correct random transmission errors. In what order should encryption and error correction be applied?**

1 / 1 point

- (selected) Encrypt and then apply the error correction code.
- The order does not matter -- neither one can correct errors.
- Apply the error correction code and then encrypt the result.
- The order does not matter -- either one is fine.

Correct
That is correct. The error correction code will do its best to correct random errors after which the MAC in the ciphertext will be checked to ensure no other errors remains.

2. **Let X be a uniform random variable over the set $\{0,1\}^n$. Let Y be an arbitrary random variable over the set $\{0,1\}^n$ (not necessarily uniform) that is independent of X. Define the random variable $Z = X \oplus Y$. What is the probability that Z equals 0^n?**

1 / 1 point

- 0.5
- $2/2^n$
- (selected) $1/2^n$
- 0

Correct
The probability is $1/2^n$. To see why, observe that whatever Y is, the probability that $Z = X \oplus Y = 0^n$ is the same as the probability that $X = Y$ which is exactly $1/2^n$ because X is uniform.

3. **Suppose (E_1, D_1) is a symmetric cipher that uses 128 bit keys to encrypt 1024 bit messages. Suppose (E_2, D_2) is a symmetric cipher that uses 128 bit keys to encrypt 128 bit messages. The encryption algorithms E_1 and E_2 are deterministic and do not use nonces. Which of the following statements is true?**

1 / 1 point

- [x] (E_1, D_1) can be one-time semantically secure.

Correct
Yes, for example (E_1, D_1) can be a secure stream cipher.

- [x] (E_1, D_1) can be one-time semantically secure, but cannot be perfectly secure.

Correct
Yes, for example (E_1, D_1) can be a secure stream cipher.

Yes, for example (E_1, D_1) can be a secure stream cipher.

☐ (E_2, D_2) can be semantically secure under a chosen plaintext attack.

☐ (E_1, D_1) can be perfectly secure.

4. **Which of the following statements regarding CBC and counter mode is correct?**

1 / 1 point

○ counter mode encryption requires a block

cipher (PRP), but CBC mode encryption only needs a PRF.

○ Both counter mode and CBC mode require a block

cipher (PRP).

○ Both counter mode and CBC mode can operate

just using a PRF.

◉ CBC mode encryption requires a block

cipher (PRP), but counter mode encryption only needs a PRF.

✓ **Correct**
Yes, CBC needs to invert the PRP for decryption, while

counter mode only needs to evaluate the PRF in the forward direction

for both encryption and decryption. Therefore, a PRF is

sufficient for counter mode.

5. **Let $G : X \to X^2$ be a secure PRG where $X = \{0,1\}^{256}$.**

1 / 1 point

We let $G(k)[0]$ denote

the left half of the output and $G(k)[1]$ denote the right half.

Which of the following statements is true?

○ $F(k,m) = m \oplus k$ is a secure PRF with key space and message space X.

◉ $F(k,m) = G(k)[m]$ is a secure PRF with key space X and message

space $m \in \{0,1\}$.

○ $F(k,m) = G(m)[0] \oplus k$ is a secure PRF with key space and message

space X.

○ $F(k,m) = G(k)[0] \oplus m$ is a secure PRF with key space and message

space X.

✓ **Correct**
Yes, since the output of $G(k)$ is indistinguishable from

random, the left and right halves are indistinguishable from random

independent values.

6. **Let (E, D) be a nonce-based symmetric encryption system (i.e. algorithm**

1 / 1 point

E takes as input a key, a message, and a nonce, and similarly the

decryption algorithm takes a nonce as one of its inputs). The system

provides chosen plaintext security (CPA-security) as long as the nonce

never repeats. Suppose a single encryption key is used to encrypt

2^{32} messages and the nonces are generated independently at random for each

encryption, how long should the nonce be to ensure that it never repeats

with high probability?

○ 16 bits

◉ 128 bits

○ 48 bits

○ 64 bits

✓ **Correct**
Yes, the probability of repetition after 2^{32} samples

is negligible

is negligible.

7. **Same as question 6 except that now the nonce is generated using a counter. The counter resets to 0 when a new key is chosen and is incremented by 1 after every encryption. What is the shortest nonce possible to ensure that the nonce does not repeat when encrypting 2^{32} messages using a single key?**

1 / 1 point

- 48 bits
- the nonce must be chosen at random, otherwise the system

  cannot be CPA secure.
- 128 bits
- 32 bits

Correct
Yes, with 32 bits there are 2^{32} nonces and each

message will use a different nonce.

8. **Let (S, V) be a deterministic MAC system with message space M and key**

space K. Which of the following properties is implied by the

standard MAC security definition?

1 / 1 point

- For any two distinct messages m_0 and m_1,

  given m_0, m_1 and $S(k, m_0)$ it is difficult to compute $S(k, m_1)$.
- $S(k, m)$ preserves semantic security of m.

  That is, the adversary learns nothing about m given $S(k, m)$.
- Given a key k in K it is difficult to find

  distinct messages m_0 and m_1 such that $S(k, m_0) = S(k, m_1)$.
- The function $S(k, m)$ is a secure PRF.

Correct
yes, this is implied by existential unforgeability under

a chosen message attack.

9. **Let $H : M \to T$ be a collision resistant hash function where $|T|$ is smaller than $|M|$.**

Which of the following properties is implied by collision resistance?

1 / 1 point

- it is difficult to find m_0 and m_1 such

  that $H(m_0) = H(m_1) + 1$. (here we treat the outputs of H as integers)
- Given a tag $t \in T$ it is difficult to construct

  $m \in M$ such that $H(m) = t$.
- $H(m)$ preserves semantic security of m

  (that is, given $H(m)$ the attacker learns nothing about m).
- For all m in M, $H(m)$ must be shorter than m.

Correct
yes, if these were easy then the attacker could easily

find collisions.

10. **Recall that when encrypting data you should typically use**

a symmetric encryption system that provides authenticated encryption.

Let (E, D) be a symmetric encryption system providing authenticated

encryption. Which of the following statements is implied by

authenticated encryption?

1 / 1 point

- [x] Given m and $E(k, m)$ it is difficult to find k.

Correct
yes, otherwise the system would not even be chosen plaintext

secure.

- [ ] Given $c = E(k, m)$ for some secret k, m,

  the attacker cannot find k', m' such that $c = E(k', m')$.

- [ ] Given k, m and $E(k, m)$ the attacker

  cannot create a valid encryption of $m + 1$ under key k.

  (here we treat plaintexts as integers)

- [x] (E, D) provides chosen-ciphertext security.

> ✓ **Correct**
> yes, we showed this in class.

11. Which of the following statements is true about the basic Diffie-Hellman

key-exchange protocol.

1 / 1 point

- [ ] The basic protocol provides key exchange secure against

  active adversaries that can inject and modify messages.

- [ ] As with RSA, the protocol only provides

  eavesdropping security in the group $\mathbb{Z}_N^*$ where N is an

  RSA modulus.

- [x] The protocol can be converted to a public-key

  encryption system called the ElGamal public-key system.

> ✓ **Correct**
> yes, that is correct.

- [x] The protocol provides security against eavesdropping

  in any finite group in which the Hash Diffie-Hellman (HDH) assumption holds.

> ✓ **Correct**
> yes, in any such group the hash of the Diffie-Hellman
>
> secret g^{ab} can be used as a shared secret.

12. Suppose $n + 1$ parties, call them $B, A_1, \ldots, A_n$, wish to setup

a shared group key. They want a protocol so that at the end

of the protocol they all have a common secret key k, but an eavesdropper

who sees the entire conversation cannot determine k. The parties

agree on the following protocol that runs in a group G of prime order q

with generator g:

1 / 1 point

- **for $i = 1, \ldots, n$ party A_i chooses a random a_i in $\{1, \ldots, q\}$ and sends to Party B the quantity $X_i \leftarrow g^{a_i}$.**
- **Party B generates a random b in $\{1, \ldots, q\}$ and for $i = 1, \ldots, n$ responds to Party A_i with the messages $Y_i \leftarrow X_i^b$.**

The final group key should be g^b. Clearly Party B can compute

this group key. How would each Party A_i compute this group key?

- ( ) Party A_i computes g^b as $Y_i^{-a_i}$
- ( ) Party A_i computes g^b as $Y_i^{a_i}$
- ( ) Party A_i computes g^b as Y_i^{-1/a_i}
- (•) Party A_i computes g^b as Y_i^{1/a_i}

> ✓ **Correct**
> Yes, $Y_i^{1/a_i} = g^{(ba_i)/a_i} = g^b$.

13. Recall that the RSA trapdoor permutation is defined in the group

$\mathbb{Z}_N^*$ where N is a product of two large

primes. The public key is (N, e) and the private key is (N, d)

1 / 1 point

where d is the inverse of e in $\mathbb{Z}^*_{\varphi(N)}$.

Suppose RSA was defined modulo a prime p instead of an RSA

composite N. Show that in that case anyone can compute the private

key (N, d) from the public key (N, e) by computing:

- $d \leftarrow e^{-1} \pmod{p-1}$.
- $d \leftarrow -e \pmod{p}$.
- $d \leftarrow e^{-1} \pmod{p^2}$.
- $d \leftarrow e^{-1} \pmod{p+1}$.

Correct

yes, that is correct.