UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 4

Quiz relates to Lectures 11 and 12. Questions might have been seen in a different order on LEARN.

QUESTION 1

The Merkle-Damgård construction for hash functions makes use of a compression function, h, which acts on successive message blocks. A benefit of this construction is:

(a) computation of a hash value requires a fixed number of calls to h, independent of the length of the input message

(b) if h is collision-resistant then the whole hash function is collision-resistant

(c) no padding is required for the input message, no matter what is the output size of h

(d) the length of the input message does not need to be included

if h is collision-resistant then the whole hash function is collision-resistant

QUESTION 2

Due to the birthday paradox, we can expect to find a collision in the SHA-256 hash function after around:

(a) 2^7 trials

(b) 2^8 trials

(c) 2^{128} trials

(d) 2^{255} trials

2^{128} trials

cont/...

QUESTION 3

Suppose that an attacker has the ability to compute the output of a certain hash function for 2^{128} input values. In order to prevent the attacker from finding a collision in the hash function, the output of the hash function should be of length at least:

(a) 128 bits

(b) 256 bits

(c) 384 bits

(d) 512 bits

---

384 bits

QUESTION 4

A message authentication code (MAC) takes as input a message and a key and outputs a tag. To be considered secure a MAC should have the property:

(a) the correct tag for a new message cannot be computed without the key

(b) the message used to compute the tag cannot be distinguished from a random message

(c) different tags are computed if a message is repeated

(d) any output tag cannot be distinguished from a random string

---

the correct tag for a new message cannot be computed without the key

---

QUESTION 5

Which of the following block cipher modes of operation is not designed to provide data confidentiality?

(a) Counter mode (CTR)

(b) Cipher block chaining (CBC)

(c) Cipher-based MAC (CMAC)

(d) Counter with CBC-MAC (CCM)

Cipher-based MAC (CMAC)

---

cont/...

QUESTION 6

Which of the following block cipher modes of operation is not designed to provide data integrity?

(a) Galois counter mode (GCM)

(b) Cipher block chaining (CBC)

(c) Cipher-based MAC (CMAC)

(d) Counter with CBC-MAC (CCM)

Cipher block chaining (CBC)

QUESTION 7

When public key cryptography is used for encryption:

(a) the public key of the sender is required in order to decrypt the ciphertext

(b) the public key of the receiver is required in order to decrypt the ciphertext

(c) the private key of the sender is required in order to decrypt the ciphertext

(d) the private key of the receiver is required in order to decrypt the ciphertext

the private key of the receiver is required in order to decrypt the ciphertext

QUESTION 8

The keys for the RSA encryption algorithm include a public exponent e, a private exponent d, and a public modulus n. It is common to choose:

(a) $d = 2^{16} + 1$

(b) $e = 2^{16} + 1$

(c) $e = n - 1$

(d) $d = n - 1$

$e = 2^{16} + 1$

QUESTION 9

For the RSA encryption scheme a large modulus n is chosen, typically around 2048 bits in practice. To improve efficiency, this is often used together with:

(a) a small value for e

(b) a small value for d

(c) a small value for one of the factors of n

(d) a small value for the Euler function $\phi(n)$

---

a small value for e

QUESTION 10

For any given values x and m, the square-and-multiply algorithm when used to compute $x^{66} \mod m$ requires:

(a) 5 squarings and 3 multiplications modulo m

(b) 6 squarings and 1 multiplication modulo m

(c) 8 squarings and 1 multiplication modulo m

(d) 63 squarings and 3 multiplication modulo m

---

6 squarings and 1 multiplication modulo m
