UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 3

Quiz relates to Lectures 9 and 10. Questions might have been seen in a different order on LEARN.

QUESTION 1

Which of the following is not a binary synchronous stream cipher?

(a) the one time pad

(b) RC4

(c) SHA-1

(d) A5/1

SHA-1

QUESTION 2

In a binary synchronous stream cipher:

(a) the keystreams generated by the sender and receiver are the same

(b) the keystreams generated by the sender and receiver are complementary (every bit is different)

(c) the keystream generated by the receiver is the XOR sum of the plaintext and the keystream generated by the sender

(d) the keystream generated by the receiver is the XOR sum of the ciphertext and the keystream generated by the sender

---

the keystreams generated by the sender and receiver are the same

---

cont/. . .

QUESTION 3

The one time pad:

(a) provides data integrity

(b) provides perfect secrecy

(c) produces ciphertext which is twice the length of the plaintext

(d) requires much more computation for encryption than for decryption

---

provides perfect secrecy

QUESTION 4

Which of these statements about the keystream used in the one time pad is true?

(a) The keystream has a large, but finite, period

(b) The keystream starts with an initialisation vector (IV)

(c) The keystream is generated by a linear feedback shift register (LFSR)

(d) Each keystream bit is only used once

Each keystream bit is only used once

QUESTION 5

In typical usage, a true random number generator (TRNG) and a pseudo-random number generator (PRNG) are often combined in practice so that:

(a) the PRNG provides the seed for the TRNG

(b) the TRNG provides the seed for the PRNG

(c) the TRNG and the PRNG output alternate bits

(d) the TRNG and PRNG output is combined using exclusive-OR (XOR)

---

the TRNG provides the seed for the PRNG

---

cont/...

QUESTION 6

The Fermat test can be used to decide whether or not a number n is prime. The test can sometimes fail with the result that:

(a) a prime number is labelled as a composite number

(b) a composite number is labelled as a prime number

(c) the test halts without producing any output

(d) the test continues computing without producing a result

---

a composite number is labelled as a prime number

QUESTION 7

By Euler's theorem, if $\gcd(a, n) = 1$ then it is always true that:

(a) $a^{n-1} \mod \phi(n) = 1$

(b) $a^{n-1} \mod n = 1$

(c) $a^{\phi(n)} \mod \phi(n) = 1$

(d) $a^{\phi(n)} \mod n = 1$

$a^{\phi(n)} \mod n = 1$

QUESTION 8

Which of the following pairs of equations cannot be solved using the Chinese Remainder Theorem?

(a) $x \equiv 3 \mod 5$ and $x \equiv 3 \mod 11$

(b) $x \equiv 3 \mod 6$ and $x \equiv 4 \mod 11$

(c) $x \equiv 3 \mod 5$ and $x \equiv 3 \mod 12$

(d) $x \equiv 3 \mod 6$ and $x \equiv 4 \mod 12$

$x \equiv 3 \mod 6$ and $x \equiv 4 \mod 12$

---

cont/...

QUESTION 9

Suppose $n = 77 = 7 \times 11$. According to Euler's theorem:

(a) $2^7 \mod n = 1$

(b) $2^{11} \mod n = 1$

(c) $2^{60} \mod n = 1$

(d) $2^{76} \mod n = 1$

$2^{60} \mod n = 1$

QUESTION 10

Let g be a generator for the integers modulo p. The discrete logarithm problem is:

(a) given y, find x with $y = x^g \mod p$

(b) given x, find y with $y = x^g \mod p$

(c) given y, find x with $y = g^x \mod p$

(d) given x, find y with $y = g^x \mod p$

---

given y, find x with $y = g^x \mod p$
