UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 1

Quiz relates to Lectures 3, 5 and 6. Questions might have been seen in a different order on LEARN.

QUESTION 1

The inverse of 3 modulo 17 is:

(a) 4

(b) 1

(c) 3

(d) 6

6

QUESTION 2

Which of the following integers does not have an inverse modulo 21?

(a) 1

(b) 2

(c) 3

(d) 4

3

---

cont/. . .

QUESTION 3

Which of the following integers is a generator for $\mathbb{Z}_7^*$, the non-zero integers modulo 7?

(a) 1

(b) 2

(c) 3

(d) 6

3

QUESTION 4

What is $8^{-1} \mod 21$?

(a) 1

(b) 2

(c) 4

(d) 8

8

QUESTION 5

A generator for $\mathbb{Z}_{15}^*$ has order:

(a) 1

(b) 3

(c) 8

(d) 14

8

---

cont/...

QUESTION 6

Which of the following is a fundamental weakness of the Hill cipher for any size of encryption matrix?

(a) The number of possible keys is too small

(b) Encryption is a linear function

(c) The encryption function is computationally expensive

(d) Decryption is not always possible

Encryption is a linear function

QUESTION 7

Following Kerckhoff's principle, we usually assume that an attacker of an encryption scheme has access to:

(a) unbounded computational power

(b) the encryption and decryption keys

(c) the description of the encryption and decryption algorithms

(d) all of the above

---

the description of the encryption and decryption algorithms

QUESTION 8

If a plaintext comes from a natural language, such as English, which of the following encryption algorithms can be expected to have the most uniform ("flattest") frequency distribution of ciphertext characters?

(a) The Caesar cipher

(b) The random simple substitution cipher

(c) A transposition cipher on blocks of size 12

(d) The Vigenere cipher with a key of length 8

The Vigenere cipher with a key of length 8

---

cont/...

QUESTION 9

If a plaintext comes from a natural language, such as English, for which of the following ciphers is the frequency of any particular character equal in both plaintext and ciphertext?

(a) The Caesar cipher

(b) The random simple substitution cipher

(c) A transposition cipher on blocks of size 12

(d) The Vigenere cipher with a key of length 8

A transposition cipher on blocks of size 12

QUESTION 10

Which is the smallest of the following key sizes that would be acceptable to prevent exhaustive key search today?

(a) 256 bits

(b) 512 bits

(c) 1024 bits

(d) 2048 bits

---

256 bits
