UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 2

Quiz relates to Lectures 7 and 8. Questions might have been seen in a different order on LEARN.

QUESTION 1

In an iterative block cipher, the purpose of the key schedule is to:

(a) define how to derive the round keys from the master key

(b) generate different keys for every block encrypted

(c) choose between different master keys

(d) define how the master key is generated

---

define how to derive the round keys from the master key

QUESTION 2

The Data Encryption Standard (DES) is an iterated block cipher. In each round the DES algorithm:

(a) performs a substitution on a complete block

(b) operates on multiple blocks at the same time

(c) performs a non-linear operation

(d) uses the same key bits

---

performs a non-linear operation

---

cont/. . .

QUESTION 3

Which of the following encryption algorithms has the largest number of possible keys?

(a) DES (the Data Encryption Standard algorithm)

(b) The random simple substitution cipher on an alphabet of 26 characters

(c) A transposition cipher on blocks of size 10

(d) The Vigenere cipher with a key of length 5 and an alphabet of 26 characters

---

The random simple substitution cipher on an alphabet of 26 characters

---

QUESTION 4

Double encryption with DES (double DES) with two independent keys:

(a) has twice as many possible key values as ordinary DES

(b) uses half as much computation as ordinary DES

(c) runs twice as fast as ordinary DES

(d) is vulnerable to a meet-in-the-middle attack

---

is vulnerable to a meet-in-the-middle attack

QUESTION 5

Triple DES is a variant of the original Data Encryption Standard (DES) algorithm. In Triple DES:

(a) the original DES algorithm is run three times for each input block

(b) the block size is three times longer than original DES

(c) the algorithm runs three times faster than original DES

(d) there are three times as many possible keys as original DES

---

the original DES algorithm is run three times for each input block

---

cont/...

QUESTION 6

AES, the Advanced Encryption Standard, algorithm:

(a) has a 128 bit block size

(b) has a 192 bit block size

(c) has a 256 bit block size

(d) allows any of the other block sizes

---

has a 128 bit block size

QUESTION 7

Each round of the AES algorithm:

(a) performs a substitution on a complete block

(b) operates on multiple blocks at the same time

(c) performs a non-linear operation

(d) uses the same key bits

---

performs a non-linear operation

QUESTION 8

Which of the following modes of operation for block ciphers does not introduce randomness?

(a) CBC mode

(b) CTR mode

(c) ECB mode

(d) OFB mode

ECB mode

---

cont/...

QUESTION 9

Counter mode (CTR) is a mode of operation for block ciphers. Which of the following statements about CTR mode is true?

(a) Messages to be encrypted must be padded to be a complete number of blocks

(b) One bit in error in the ciphertext leads to a whole random block in the decrypted plaintext

(c) Equal plaintext blocks encrypt to equal ciphertext blocks

(d) Decryption of a sequence of blocks can be conducted in parallel

---

Decryption of a sequence of blocks can be conducted in parallel

---

QUESTION 10

The main disadvantage of basic Electronic Code Book (ECB) mode of operation for block ciphers, in comparison with counter mode (CTR) and cipher block chaining (CBC) mode, is:

(a) ECB mode encryption is less efficient

(b) ECB mode has large error propagation

(c) equal plaintext blocks in ECB mode give equal ciphertext blocks

(d) ECB mode requires longer keys

---

equal plaintext blocks in ECB mode give equal ciphertext blocks

---