**Exercise 3**

**Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Multiple Choice Questions**

1. The key size of the affine cipher is

A. 25

B. 1226

C. 1325

D. 2526

2. The simplified AES uses a \_\_\_\_\_\_\_ bit block size and a key size of \_\_\_\_\_\_\_ bits.

A. 16; 16

B. 32; 32

C. 64; 56

D. 128; 128

3. In the substitution of the simplified AES, \_\_\_\_\_\_\_ bits are substituted by \_\_\_\_\_\_\_bits.

A. 4; 4

B. 6; 4

C. 8; 8

D. 16; 16

4. In the simplified AES, columns of a state matrix are mixed over the Galois Field

A. GF(2)

B. GF(22)

C. GF(24)

D. GF(28)

5. In the simplified AES, \_\_\_\_\_ round keys are needed.

A. 2

B. 3

C. 4

D. 5

6. AES uses a \_\_\_\_\_\_\_\_\_\_\_\_ bit block size and a key size of \_\_\_\_\_\_\_\_\_\_ bits.

A. 128; 128 or 256

B. 64; 128 or 192

C. 256; 128, 192, or 256

D. 128; 128, 192, or 256

7. The 4×4 byte matrices in the AES algorithm are called

A. States

B. Words

C. Transitions

D. Permutations

8. For the AES-128 algorithm there are \_\_\_\_\_\_ similar rounds and \_\_\_\_\_\_\_\_\_ round is different.

A. 8; the first

B. 9; the last

C. 10; the first

D. 16; no

9. In AES, columns of a state matrix are mixed over the Galois Field

A. GF(2)

B. GF(22)

C. GF(24)

D. GF(28)

10. In the AES-128, \_\_\_\_\_ round keys are needed.

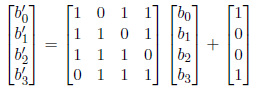
A. 10

B. 11

C. 12

D. 13

11. In the simplified AES, the substitution is determined as follows.



Based on the above equation, determine the substitution of the nibble 1101.

12. In the simplified AES, verify that

Note: The additions and multiplications are over the Galois field GF(24).