CSS322 – Quiz 3

Name: _____   ID: _____   Marks: _____ (10)

Question 1   [5 marks]

Calculate the following. A calculator is *not allowed*. Show calculations/explanations.

(a) $\phi(27)$ Answer: _____ [1.5 marks]

(b) $\phi(31)$ Answer: _____ [1.5 marks]

(c) $(16 \div 17) \bmod 42$ [2 marks]

(d) $5^{30} \bmod 124$ [Bonus: 2 marks]

Question 2   [2 marks]

Circle one or more of the following 5 algorithms that can be used in or as part of a PRNG:

Blum-Blum-Shub   Triple DES   RC4

Linear Congruential Generator   AES in Counter Mode

Question 3 [3 marks]

Assume when encrypting 3-bit plaintext with a block cipher with key K, the following ciphertext is obtained:

```
 P   C        P   C
000 110      100 000
001 001      101 011
010 111      110 101
011 010      111 100
```

The following ciphertext was encrypted with the above cipher with key K in counter mode (initial value 0): 101111010 What is the plaintext?

Answer: ⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯⎯