CSS 322 – Quiz 4 Answers

First name: ______________________________ Last name: ___________________________

ID: _____________________________ Total Marks: ____________
out of 10

Question 1 [3 marks]

In the following, Ø(n) is Eulers Totient function. Give the answers to the following functions (show calculations where necessary):

a) Ø(27)

b) Ø(29)

c) (8 × 7) mod 17

d) (9 – 12) mod 13

e) (7 ÷ 8) mod 23

f) (9 ÷ 3) mod 12

Answers

a. Ø(27) = 18

Factors of 27 are: 1, 3, 9, 27. Therefore the numbers relatively prime with 27 are: 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26.

b. Ø(29) = 28 since 29 is prime (factors are 1 and 29).

c. 8 x 7 = 56. 56 mod 17 = 5.

d. The additive inverse of 12 is 1. Therefore 9 + 1 = 10. 10 mod 13 = 10.

e. 3 does not have a multiplicative inverse in mod 12 (since 3 is a factor of 12). Therefore, an answer does not exist.

f. The multiplicative inverse of 8 is 3 (8 x 3 = 24, 24 mod 23 = 1). Therefore 7 x 3 = 21. 21 Mod 23 = 21.

Question 2 [2 marks]

Give an advantage and disadvantage of using link-level encryption (as opposed to end-to-end encryption) in the Internet.

Advantage:

Can make traffic analysis harder

Easier to be implemented in hardware

Disadvantage:

Requires more keys to be exchanged between end-points

Has vulnerabilities at network devices where decrypt/encrypt operations must be performed (the plaintext becomes available)

Question 3 [3 marks]

Assume you are using a centralised Key Distribution Centre (KDC) in your symmetric key cryptosystem.

a) List the keys that are used if A wants to communicate with B. Give each key a meaningful name or short description.

b) For each key from part (a), list which of the three hosts (A, B, KDC) have access to the key.

Master key of A: A and KDC have access

Master key of B: B and KDC have access

Shared key: A, B and KDC have access

Question 4 [2 marks]

Assume you are using the linear congruential generator (see equation below) to generate random numbers.

$$X_{n+1} = (aX_n + c) \bmod m$$

a) If the input is X_0=1, c=0 and m=9, and the first three output numbers are X_1 to X_3 = {7, 4, 1}, then what is X_4?

b) A desirable property of a random number sequence is a long period. What parameter can be modified to potentially produce a sequence of more than 10 different random numbers?

Answers:

a) 7. Since the initial value is 1 and the last value (X_3) is 1, then the sequence has wrapped (repeated). So X_4 will be the same as the value after X_0, that is 7.

b) *m*. Since the value is mod *m*, with *m*=9, there are a maximum of 9 possible outputs: 0 to 8. Hence increase *m* to get more possible values.