uc3m | Universidad **Carlos III** de Madrid

CRYPTOGRAPHY AND COMPUTER SECURITY COURSE

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Sergio Pastrana Portillo
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

cc BY NC SA

Mathematical background

Self-assessment test

Select the correct answer.

1. Given a, b and c, which belongs to Z number set:

   ○ If Z is a Group, “a” value does not have to have inverse.
   ○ **If Z is a ring (Z, +, ·), a · (b + c) = (a · b) + (a · c) will be met**
   ○ If Z is a field, “a” value does not have to have inverse.
   ○ If Z is a field, then a · b = b · a does not have to be met.

2. What does it mean that a pair of numbers a and b are congruent modulo n?

   ○ Both are divisible by n.
   ○ Both are multiples of n.
   ○ **That a-b is a multiple of n.**
   ○ That a+b and a-b leave the same remainder after being divided by n.

3. What is the result of 2343 mod 10?

   ○ 43
   ○ 23,4
   ○ 234
   ○ **3**

4. Choose a pair of numbers within the congruence $[9]_{15}$:

   ○ **-6 y 39**
   ○ 0 y 9
   ○ 15 y 24
   ○ -21 y 33

5. How many different results could generate a reduction module 7?

   ○ **7**
   ○ 6
   ○ Endless.
   ○ It depends on the value of the number to reduce.

6. Assume that a mod 9 = 3, and b mod 9 = 7. Choose the correct result from the following ones, applying modular arithmetic principles:

   ○ a*b mod 9 = 21
   ○ Given c=2, then a · (b+c) mod 9 = 6
   ○ It depends on the value of the number to reduce.
   ○ **a+b mod 9 = 1**

7. The inverse of 3 module 7 is…

   ○ 1/3
   ○ -1/3
   ○ **5**
   ○ 4

8. According to Fermat and Euler theorems, once applied to equation ax=1 mod n:

   ○ Both demand “n” to be a prime number.
   ○ **Fermat is an instance of Euler.**
   ○ Euler needs “a” and “n-1” to be coprime numbers.
   ○ If n=0, both can be applied interchangeably.

9. What of the following Euler totient function is the right one?

   ○ Φ(12) = 3.
   ○ **Φ(35) = 24.**
   ○ Φ(11) = 11.
   ○ Φ(34) = 33.

10. The order of 4 regarding 7 is…

   ○ 7, and this is the reason why it is generator.
   ○ 6, and this is the reason why it is generator.
   ○ **3, and this is the reason why it is not generator.**
   ○ 6, and this is the reason why it is not generator.