uc3m | Universidad Carlos III de Madrid

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

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

"Fundamentos matemáticos"

Test de autoevaluación

Seleccione la respuesta correcta.

- 1. Dado un conjunto Z de números al que pertenecen los valores a, b y c:
 - o Si Z es un Grupo, el valor "a" no tiene por qué tener inverso.
 - O Si Z es un anillo $(Z, +, \cdot)$, se cumplirá que $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
 - o Si Z es un cuerpo, el valor "a" no tiene por qué tener inverso.
 - o Si Z es un cuerpo, entonces a \cdot b = b \cdot a no tiene por qué cumplirse.
- 2. ¿Qué significa que dos números a y b sean congruentes módulo "n"?
 - o Que ambos son divisibles por n.
 - o Que ambos son múltiplos de n.
 - O Que a-b es un múltiplo de n.
 - O Que a+b y a-b dejan el mismo resto al dividirlos por "n".
- 3. ¿Cuál es el resultado de 2343 mod 10?
 - 0 43
 - 0 23,4
 - 0 234
 - o **3**
- 4. Dos miembros de la clase de congruencia [9]₁₅ son:
 - o -6 y 39
 - o 0 y 9
 - o 15 y 24
 - o -21 y 33
- 5. ¿Cuántos resultados distintos puede generar una reducción módulo 7?
 - o **7.**
 - 0 6.
 - o Infinitos.
 - o Depende del valor del número que se reduzca.

- 6. Suponga que a mod 9 = 3, y b mod 9 = 7. ¿Cuál de los siguientes resultados es correcto, aplicando los principios fundamentales de la aritmética modular?
 - o $a*b \mod 9 = 21$.
 - o Siendo c=2, entonces a \cdot (b+c) mod 9 = 6.
 - o Depende del valor del número que se reduzca.
 - o a+b mod 9 = 1.
- 7. El inverso de 3 módulo 7 es...
 - 0 1/3.
 - o -1/3.
 - o **5.**
 - 0 4
- 8. Acerca de los teoremas de Fermat y Euler, aplicados a la ecuación ax=1 mod n:
 - o Ambos exigen que "n" sea primo.
 - o Fermat es un caso particular de Euler.
 - o Euler necesita que "a" y "n-1" sean coprimos.
 - o Si n=0, se pueden aplicar ambos indistintamente.
- 9. ¿Cuál de los siguientes indicadores de Euler es correcto?
 - \circ $\Phi(12) = 3.$
 - \circ $\Phi(35) = 24.$
 - Φ(11) = 11.
 - \circ $\Phi(34) = 33.$
- 10. El orden de 4 respecto de 7 es...
 - o 7, y por eso es generador.
 - o 6, y por eso es generador.
 - o 3, y por eso no es generador.
 - o 6, y por eso no es generador.