

Laboratorio B de Seguridad en la Computación, Informe Práctica 00

ESTUDIANTE: García Cáceres Uberto

GRUPO: B

ACTIVIDADES

1) Hallar la congruencia demostrada de:

- a) $-18 \bmod 20 = 2$
- b) $25 \bmod 31 = 6$
- c) $33 \bmod 10 = 4$
- d) $-9 \bmod 6 = 2$

Respuesta/s:

- a) $-18 \bmod 20 = 2$, hay congruencia
- b) $25 \bmod 31 = 25$, no hay congruencia
- c) $33 \bmod 10 = 3$, no hay congruencia
- d) $-9 \bmod 6 = 3$, no hay congruencia

2) Hallar el inverso multiplicativo de 5 mod 27:

- a) 10
- b) 2
- c) 7
- d) 4
- e) 11

Respuesta:

- e) 11

3) El valor de x en la expresión $2^x \bmod 19 = 7$ es:

- a) 6
- b) 5
- c) 4
- d) 3

Respuesta:

- f) 6

4) Luego de investigar el concepto de raíz primitiva de un número primo, responda: Si α es una raíz primitiva del primo p, es porque cumple que:

- a) Es número impar y genera todos los restos del primo p
- b) Es número par y genera todos los restos del primo p
- c) Es número par o impar y genera todos los restos del primo p
- d) Es un número que no genera todos los restos del primo p

Respuesta:

- c) Es número par o impar y genera todos los restos del primo p

Repositorio de Github usado:

<https://github.com/UbertoGC/Laboratorio-B-Seguridad-en-la-Computacion>