educación IT
CODE YOUR FUTURE

# Criptografía y Blockchain

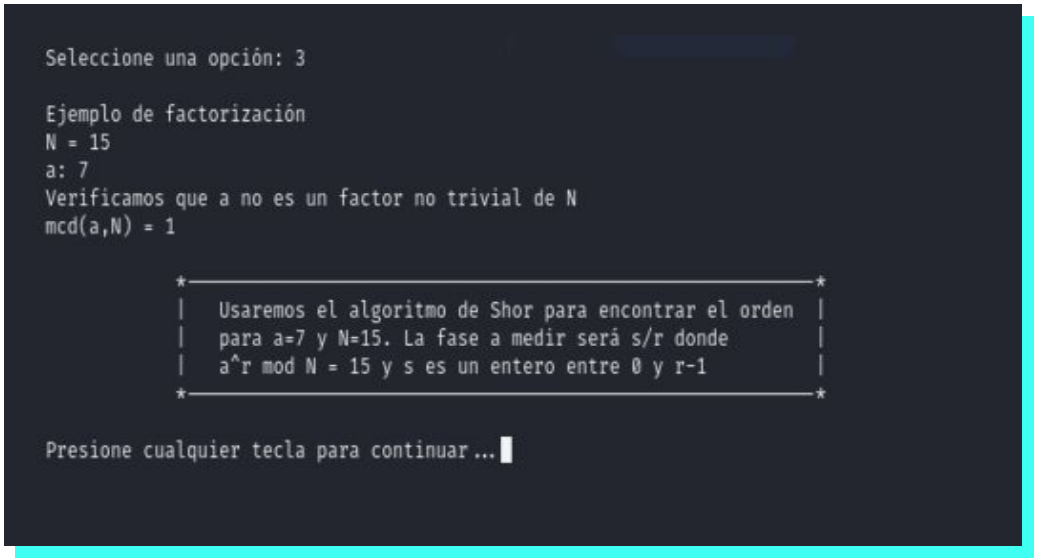
## Módulo 4 - Resolución del laboratorio

# Resolución del ejercicio

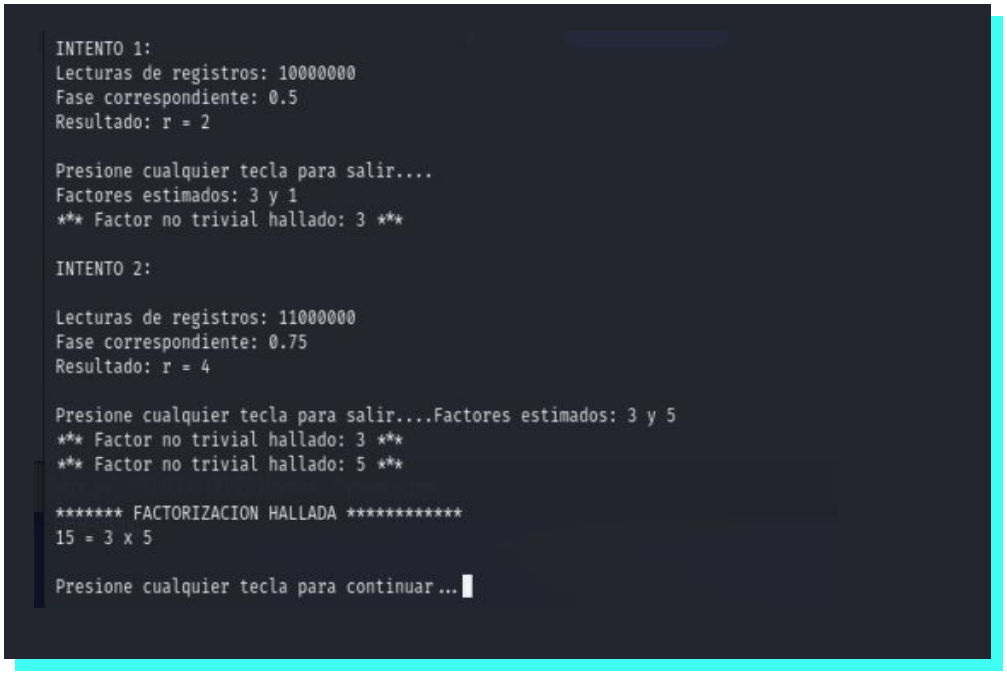
2b.

```
Seleccione una opción: 2

Fases medidas:
{'10000000': 25024, '01000000': 24913, '00000000': 25073, '11000000': 24990}

      Total medido           Fase Fracción  r estimado
0  10000000 = 128  128/256 = 0.50      1/2          2
1  01000000 =  64   64/256 = 0.25      1/4          4
2  00000000 =   0    0/256 = 0.00      0/1          1
3  11000000 = 192  192/256 = 0.75      3/4          4

Presione cualquier tecla para continuar...
```

2c.


Seleccione una opción: 3
Ejemplo de factorización
N = 15
a: 7
Verificamos que a no es un factor no trivial de N
mcd(a,N) = 1
Usaremos el algoritmo de Shor para encontrar el orden
para a=7 y N=15. La fase a medir será s/r donde
a^r mod N = 15 y s es un entero entre 0 y r-1
Presione cualquier tecla para continuar...

2c.


INTENTO 1:
Lecturas de registros: 10000000
Fase correspondiente: 0.5
Resultado: r = 2
Presione cualquier tecla para salir....
Factores estimados: 3 y 1
** Factor no trivial hallado: 3 **
INTENTO 2:
Lecturas de registros: 11000000
Fase correspondiente: 0.75
Resultado: r = 4
Presione cualquier tecla para salir....Factores estimados: 3 y 5
** Factor no trivial hallado: 3 **
** Factor no trivial hallado: 5 **
******* FACTORIZACION HALLADA ***********
15 = 3 x 5
Presione cualquier tecla para continuar...

educación IT
CODE YOUR FUTURE

# ¡Sigamos trabajando!