Ejercicio 1 – Daniel Marín López
Sistemas de Big Data

Ejercicio 1

Analiza el siguiente código y analizalo:

```
#================================================================================
# IMPORTACIÓN DE LIBRERÍA
#================================================================================
from math import *                # Carga de la libreria math para calcular log10
VelocidadCPU = 2* 1.105 * 10 ** 15  # Operaciones/segundo realizadas por Roadrunner
n=1                               # número de dígitos de la clave
fA=1                              # número de operaciones para romper la clave
# ¿ nº operaciones requeridas  <  nº operaciones en un  año?
while  fA <= (VelocidadCPU *24 * 60 * 60 *365):
    n = n+1
    fA = 10 ** ( pow( n * log(n,10) , 0.5 ) )
print('Número máximo de cifras  =' , n-1)
```

Figura 1: Código del Roadrunner.ipynb

a) ¿Qué significa el valor "VelocidadCPU" en el código y por qué es relevante para romper una clave RSA?

El valor de *VelocidadCPU* representa el n.º de operaciones que tiene el *Roadrunner*, es bastante importante porque es el número de operaciones máximas que puede ejecutar el superordenador.

b) ¿Cómo afecta el valor de n (el número de dígitos de la clave) a la cantidad de operaciones necesarias para romper la clave?

El valor de n afecta a que cuando incrementa el n.º de dígitos de la clave, el n.º de operaciones incrementará de manera exponencial. Esto puede llegar a un punto que el superordenador llegará a su máximo de n.º de operaciones y no podrá continuar descifrando la clave.

c) ¿Por qué el número de operaciones aumenta exponencialmente a medida que aumenta el número de dígitos? Explica el papel del logaritmo y la raíz cuadrada en la fórmula.

El n.º de operaciones aumenta de manera exponencial ya que ayuda a modelar el crecimiento del n.º de posibles combinaciones.

- El **logaritmo** se usa para moderar el crecimiento exponencial, ya que el aumento de complejidad de las claves no es una simple función lineal de n.
- La **raíz cuadrada** se aplica para representar el crecimiento exponencial moderado que caracteriza el aumento de combinaciones posibles en una clave de mayor longitud.

d) Ejecuta el código y analiza el valor final de n. ¿Qué significa este valor en términos prácticos para la seguridad de las claves RSA?

Tras ejecutar el código, el valor de n es de 222. Esto significa que el Roadrunner podría romper claves de 222 dígitos. Actualmente estas claves son muchos más grandes como las de 2048 bits que equivalen aproximadamente 617 dígitos, lo que hace que estas claves muchos más seguras contra un ataque realizado por el Roadrunner.

e) ¿Cómo cambiaría el resultado si la potencia computacional del ordenador (VelocidadCPU) aumentara o disminuyera? Haz una suposición, muestra y explica tu razonamiento.

Si se cambiara la potencia computacional, aumentaría el n.º de dígitos máximo que se pueden romper en un año. Por ejemplo, si VelocidadCPU aumenta el doble aumentaría el n.º de dígitos máximo que pueden ser vulnerados.

Esto es porque existe una relación exponencial entre n y el n.º de combinaciones posibles, lo que implica que cualquier alteración mínima en esta variable (VelocidadCPU) afecta notablemente el n.º de dígitos que pueden romperse en el plazo dado.