**Actividad 1.1**

**Análisis del crecimiento exponencial en la seguridad de claves RSA y su relación con la capacidad computacional**

**Objetivo**

El objetivo de esta actividad es que razones sobre cómo cambia la cantidad de operaciones necesarias para romper una clave según el algoritmo RSA, en función de la longitud de la clave (número de dígitos). Utilizando el código proporcionado, debes realizar experimentos y responder preguntas para comprender mejor la relación entre la longitud de la clave y el número de operaciones necesarias, así como la capacidad computacional requerida para romper la clave.

**Introducción**

El algoritmo RSA es uno de los sistemas de cifrado más utilizados en la actualidad para la seguridad en la transmisión de información digital. Su seguridad se basa en la dificultad de factorizar números muy grandes. A medida que aumenta el número de dígitos de la clave, también aumenta exponencialmente el número de operaciones necesarias para "romper" la clave (es decir, encontrar los factores primos).

**Conceptos clave**

* **RSA (Rivest-Shamir-Adleman)**: algoritmo de cifrado asimétrico basado en la dificultad de factorizar números grandes.
* **Número de operaciones**: cantidad de pasos que un ordenador debe realizar para encontrar los factores primos de una clave RSA.
* **Velocidad computacional**: número de operaciones que un superordenador puede realizar por segundo.
* **Crecimiento exponencial**: la cantidad de operaciones crece exponencialmente con el número de dígitos en la clave.

**EJERCICIO 1:** Analiza el [siguiente código](https://drive.google.com/file/d/1swvRAEahiNWIPkQkPsaIQ_qNXpNEa_tC/view?usp=sharing) y entiéndelo.

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

VelocidadCPU representa el número de operaciones por segundo que puede realizar el superordenador. Es un valor ya establecido por el mismo límite de roadrunner.

Es importante porque es el número de cálculos que va ha ser capaz de resolver para romper la clave RSA. Cuanto mayor sea la capacidad del ordenador, más rápido podrá probar posibles combinaciones y, por tanto, más probable es que pueda romper claves RSA más grandes.

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

Cuanto mayor sea el número de digitos de la clave, más operaciones necesitara realizar roadrunner para romper la clave RSA. Por ello, necesitara más tiempo.

* ¿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.

Porque el aumento de números de dígitos es exponencial, por lo tanto cada vez que aumenten los dígitos va aumentando mucho más la longitud de números de la clave.

El logaritmo ayuda a moderar el crecimiento de n antes de que se apliquen los pasos posteriores de la fórmula.

Raíz cuadrada: Suaviza aún más el crecimiento, pero no lo reduce lo suficiente para evitar el crecimiento general.

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

Antes de que existieran este tipo de superordenadores era muy dificil romper este tipo de clave. A día de hoy, son claves bastantes vulnerables pues el ordenador a sido capaz de resolverlo 222 veces en un año antes de que la clave cambie.

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

Si la velocidad de computo aumentara a su vez, aumentaría el número de resoluciones que podria realizar el superordenador. A su vez, si disminuye, también disminuye el número de operaciones.