

Cálculo de Operaciones de Cifrado por Segundo

Introducción

En este documento, explicaremos el cálculo para estimar la cantidad de operaciones de cifrado por segundo que una máquina puede realizar. Este cálculo se basa en los tiempos promedio de cifrado simétrico y asimétrico medidos en nanosegundos. Los pasos incluyen el cálculo del tiempo promedio, la conversión de unidades y la estimación de operaciones por segundo.

Cálculo del Tiempo Promedio

Para cada tipo de operación (cifrado simétrico y cifrado asimétrico), primero calculamos el tiempo promedio en nanosegundos (ns) sumando todos los tiempos individuales de las operaciones y dividiendo por la cantidad de operaciones:

$$\text{Tiempo Promedio (ns)} = \frac{\sum_{i=1}^n t_i}{n} \quad (1)$$

donde:

- t_i es el tiempo individual de la operación i en nanosegundos.
- n es el número total de operaciones.

Conversión de Nanosegundos a Segundos

Para obtener el tiempo promedio en segundos, convertimos el resultado dividiendo entre 10^9 , ya que $1 \text{ segundo} = 10^9 \text{ ns}$:

$$\text{Tiempo Promedio (s)} = \frac{\text{Tiempo Promedio (ns)}}{10^9} \quad (2)$$

Estimación de Operaciones por Segundo

Una vez que tenemos el tiempo promedio en segundos para una operación, podemos estimar el número de operaciones de cifrado que la máquina puede realizar por segundo. Esto se calcula tomando el inverso del tiempo promedio en segundos:

$$\text{Operaciones por Segundo} = \frac{1}{\text{Tiempo Promedio (s)}} \quad (3)$$

Aplicación al Cifrado Simétrico y Asimétrico

Aplicamos los pasos anteriores tanto para el cifrado simétrico como para el cifrado asimétrico:

- **Cifrado Simétrico:**

$$\text{Tiempo Promedio Simétrico (ns)} = \frac{\sum_{i=1}^n t_{s,i}}{n} \quad (4)$$

$$\text{Tiempo Promedio Simétrico (s)} = \frac{\text{Tiempo Promedio Simétrico (ns)}}{10^9} \quad (5)$$

$$\text{Operaciones Simétricas por Segundo} = \frac{1}{\text{Tiempo Promedio Simétrico (s)}} \quad (6)$$

- **Cifrado Asimétrico:**

$$\text{Tiempo Promedio Asimétrico (ns)} = \frac{\sum_{i=1}^m t_{a,i}}{m} \quad (7)$$

$$\text{Tiempo Promedio Asimétrico (s)} = \frac{\text{Tiempo Promedio Asimétrico (ns)}}{10^9} \quad (8)$$

$$\text{Operaciones Asimétricas por Segundo} = \frac{1}{\text{Tiempo Promedio Asimétrico (s)}} \quad (9)$$

donde:

- $t_{s,i}$ es el tiempo individual de una operación de cifrado simétrico i .
- $t_{a,i}$ es el tiempo individual de una operación de cifrado asimétrico i .
- n y m son las cantidades de muestras para el cifrado simétrico y asimétrico, respectivamente.

Uso

Estos cálculos nos permiten estimar cuántas operaciones de cifrado por segundo puede realizar la máquina. Los resultados de estos cálculos se calculan a partir del archivo CSV y se guardan en el proyecto en un archivo llamado processor performance txt