*Infraestructura Computacional*

*2023-02*

*Caso 3*

*Integrantes:*

Santiago Cabra Chavez - 202110929

Jhostin Aleck - 202214064

Pablo Martinez - 202122937

Para la realización de las pruebas del caso, se eligieron dos cadenas C:

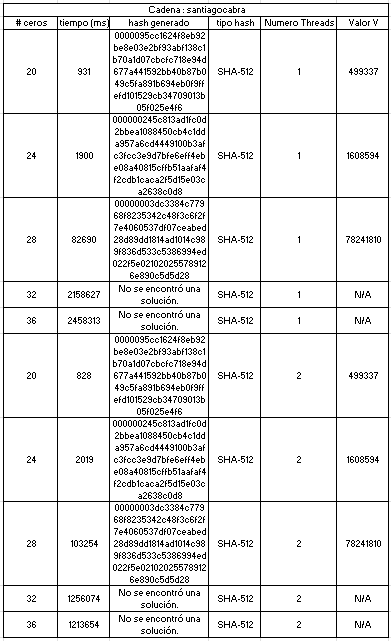
1. santiagocabra
2. infracomputacional

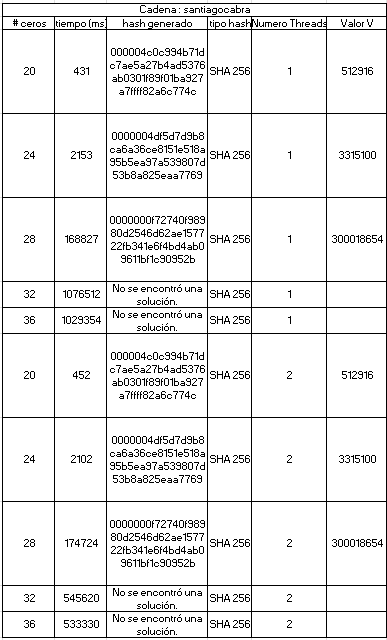
Ambas cadenas cumplen con poseer entre 16 a 20 caracteres

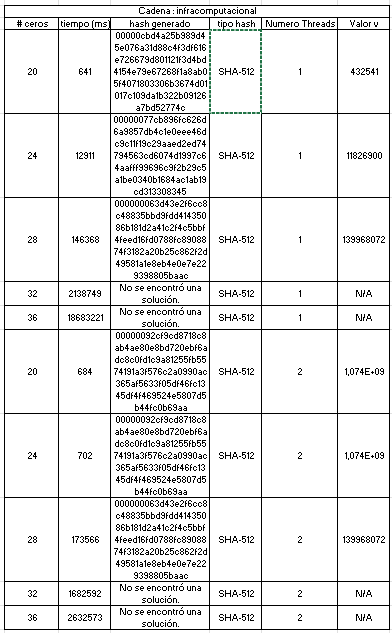
Se realizaron múltiples pruebas para las dos cadenas escogidas en las cuales se realizaron las siguientes variaciones:

* Alternancia entre algoritmo hash (SHA-256 o SHA-512)
* Alternancia entre el número de ceros al comienzo del hash (20, 24, 28 , 32 , 36)
* Alternancia entre el número de threads (1 o 2)

Los resultados de las pruebas quedaron consignados en las siguientes tablas:



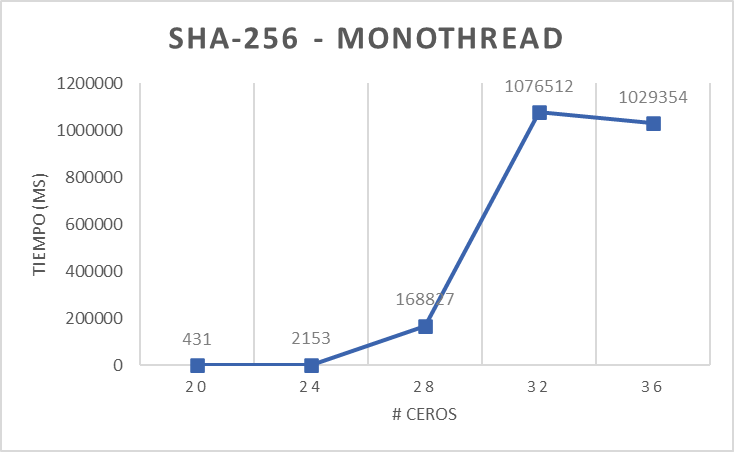


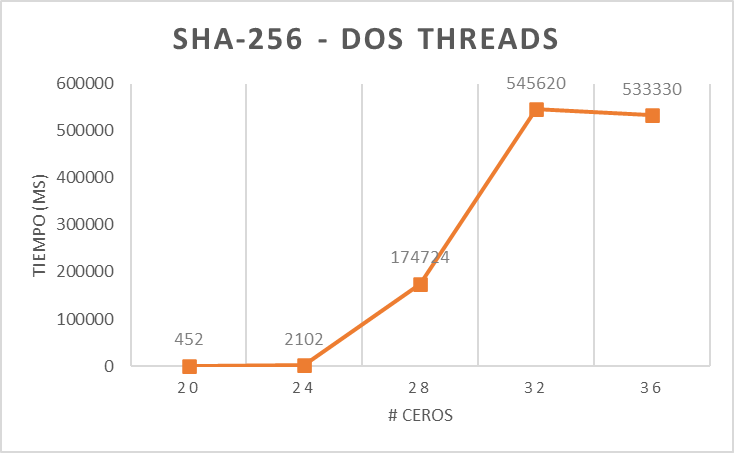


Haciendo uso de los datos obtenidos y consignados en las respectivas tablas se construyeron las siguientes gráficas de Tiempo (ms) vs # de Ceros, con variación en el algoritmo hash y en el número de Threads para cada una de las cadenas escogidas:

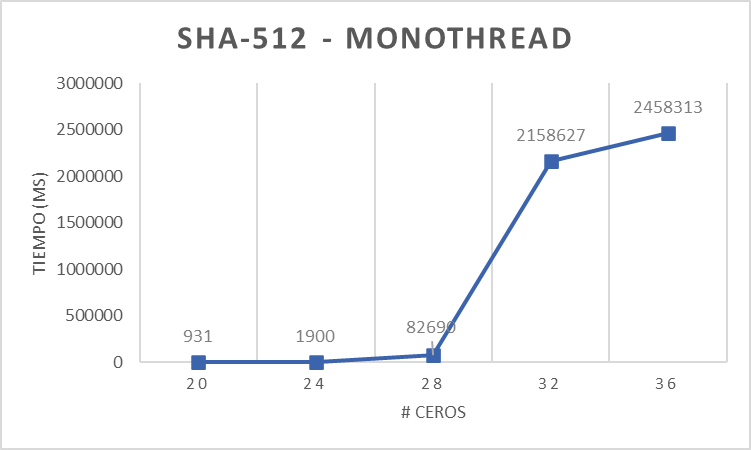
*Gráficas Cadena #1 : santiagocabra*

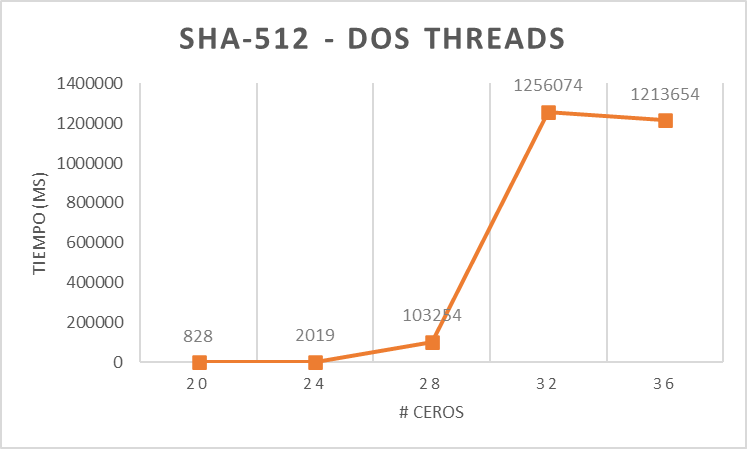
*Utilizando algoritmo SHA-256:*





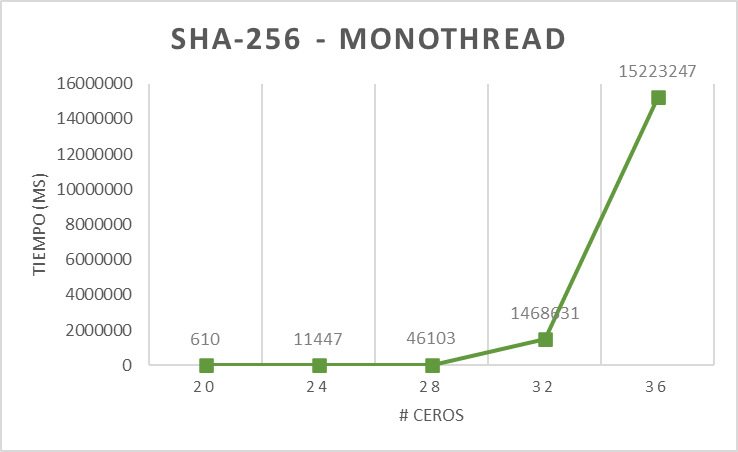
*Utilizando algoritmo SHA-512:*

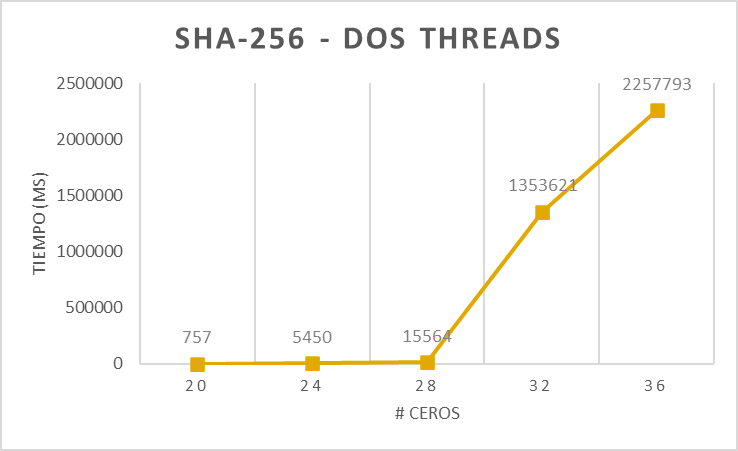




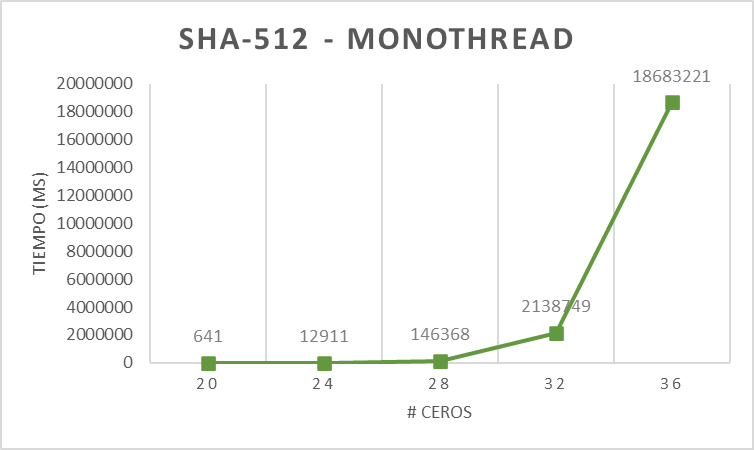
*Gráficas Cadena #2 : infracomputacional*

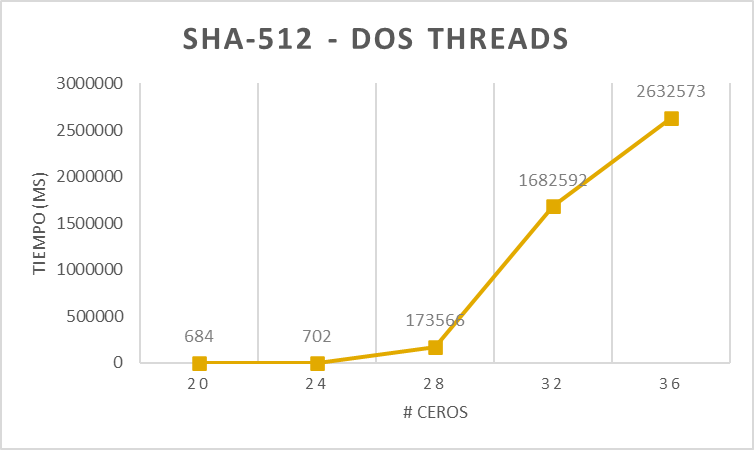
*Utilizando algoritmo SHA-256:*

**

**

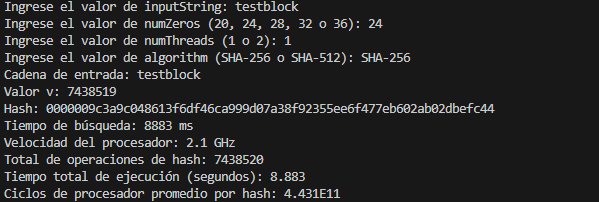
*Utilizando algoritmo SHA-512:*

**

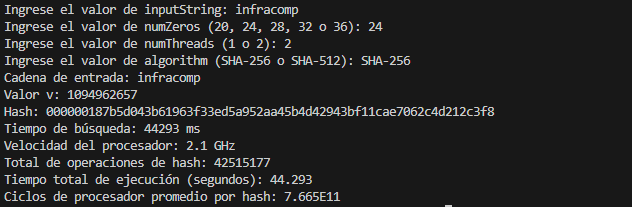
**

3. Identifique la velocidad de su procesador, y estime cuántos ciclos de procesador toma, en promedio, generar y evaluar un valor para determinar si cumple o no con la condición buscada. Escriba todos sus cálculos.

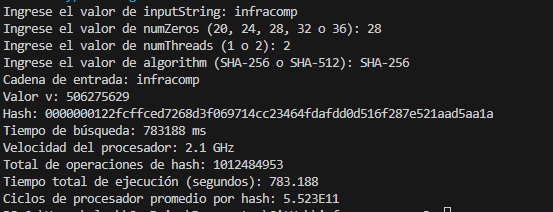
**Cálculo 1**

****

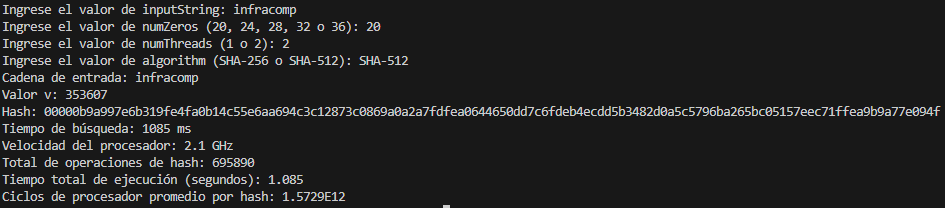
**Cálculo 2**

****

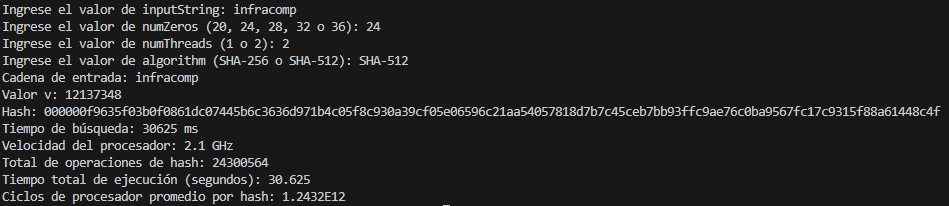
**Cálculo 3**

****

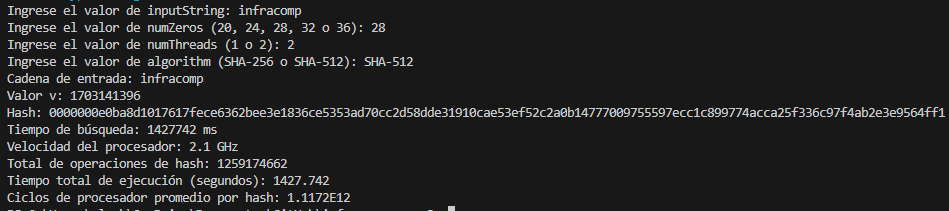
**Cálculo 4**

****

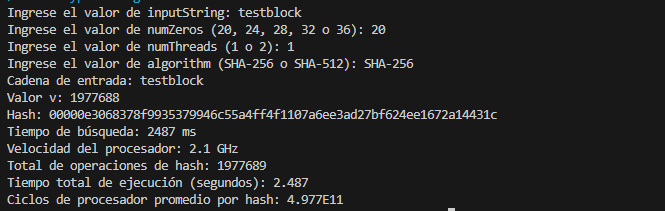
**Cálculo 5**

****

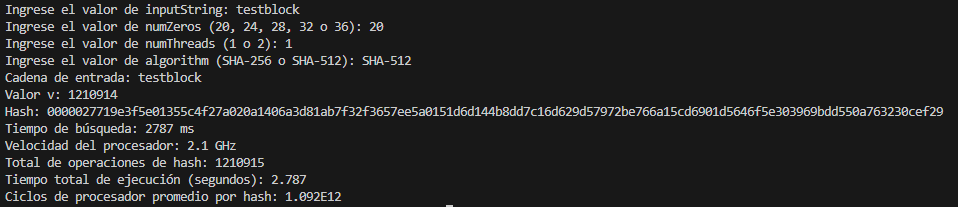
**Cálculo 6**

****

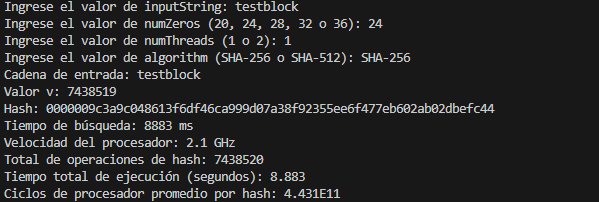
**Cálculo 7**

****

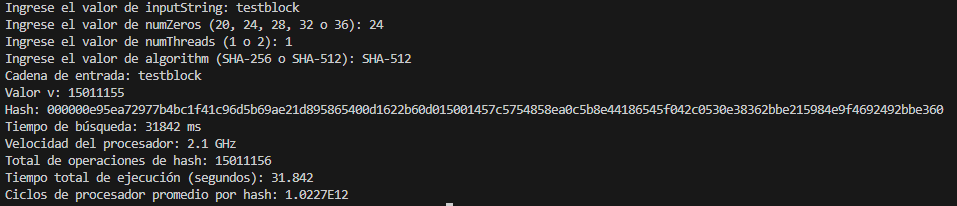
**Cálculo 8**

****

**Cálculo 9**

****

**Cálculo 10**



4. Con base en los cálculos del punto anterior, calcule cuánto tiempo tomaría un programa monothread, en el peor caso (explorar todo el espacio de búsqueda).

Tiempo promedio hashing = 2635

Número de combinaciones =

Número de combinaciones = 8,353,082,582

Tiempo total = Tiempo promedio hashing \* Número de combinaciones  
  
Tiempo total = 5.88 horas

*Parte B.*

*1. Algoritmos de Generación de Códigos Criptográficos de Hash:*

(i) Los algoritmos de generación de códigos criptográficos de hash utilizados en la actualidad incluyen:

a. SHA-256 (Secure Hash Algorithm 256-bit): Este es uno de los algoritmos más ampliamente utilizados y forma parte de la familia de algoritmos SHA-2. Es el algoritmo subyacente en la minería de Bitcoin y se emplea en muchos otros sistemas criptográficos debido a su seguridad y resistencia a colisiones.

b. SHA-3 (Secure Hash Algorithm 3): SHA-3 es el último miembro de la familia de algoritmos Secure Hash Algorithm, diseñado para ser una alternativa segura y eficiente a los anteriores. Aunque no es tan ampliamente adoptado como SHA-256, se utiliza en aplicaciones de seguridad.

(ii) Los algoritmos de hash se vuelven obsoletos debido a avances en la capacidad de procesamiento de hardware y técnicas de criptoanálisis. Cuando un algoritmo ya no puede garantizar la seguridad necesaria frente a las amenazas actuales, se considera obsoleto y debe ser reemplazado.

(iii) Las referencias bibliográficas consultadas para responder esta pregunta fueron:

a. "Federal Information Processing Standards (FIPS) Publication 180-4" del Instituto Nacional de Estándares y Tecnología (NIST). Esta referencia es autoritaria ya que el NIST es una organización de confianza en la definición de estándares criptográficos en los Estados Unidos.

2. Caso de Uso de la Tecnología Blockchain en la Universidad de los Andes:

En el contexto de la Universidad de los Andes, la tecnología blockchain puede ser útil para abordar el problema de la verificación de credenciales académicas, como títulos, certificados y diplomas. Esto resolvería el problema de la autenticación y la integridad de los registros académicos, y podría involucrar la resolución de los siguientes problemas de seguridad estudiados en clase:

(i) Problema de Autenticación: Blockchain puede resolver el problema de la autenticación al proporcionar un sistema de registro inmutable y seguro para las credenciales académicas. Los estudiantes y empleadores pueden verificar la autenticidad de los diplomas y certificados sin depender de intermediarios de confianza, lo que reduce el riesgo de falsificación.

(ii) Problema de Integridad de Datos: La integridad de los datos académicos es crucial. La tecnología blockchain garantiza la integridad de los registros al hacer que los datos sean inmutables y resistentes a la manipulación. Los registros almacenados en bloques enlazados criptográficamente no pueden ser modificados sin dejar un rastro evidente.

Cómo se Resuelve:

La tecnología blockchain consta de varios componentes clave para resolver estos problemas:

a. Registros Inmutables: Cada registro académico se almacena en un bloque, que se vincula de manera segura a bloques anteriores, formando una cadena inmutable. Esto garantiza la integridad y autenticidad de los registros.

b. Criptografía: Los registros se almacenan de manera segura mediante técnicas criptográficas. Las credenciales pueden ser firmadas digitalmente para verificar su autenticidad.

c. Descentralización: La información académica se almacena en una red descentralizada de nodos, lo que reduce el riesgo de manipulación de datos centralizada.

d. Transparencia: La información es transparente y accesible para todas las partes interesadas, lo que aumenta la confianza en la autenticidad de las credenciales.

e. Acceso Controlado: Se pueden establecer permisos para garantizar que solo las partes autorizadas tengan acceso a los registros, lo que protege la privacidad y la seguridad de los datos.

En resumen, la tecnología blockchain en la Universidad de los Andes resolvería los problemas de autenticación y la integridad de los registros académicos al proporcionar una plataforma segura y confiable para el almacenamiento y verificación de credenciales.