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:

Cadena : santiagocabra					
# ceros	tiempo (ms)	hash generado	tipo hash	Numero Threads	Valor V
20	931	0000095cc1624f8eb92be8e03e2bf93abf138c1b70a1d07cbcfc718e94d677a441592bb40b87b049c5fa891b694eb0f9ffefd101529cb34709013b05f025e4f6	SHA-512	1	499337
24	1900	000000245c813ad1fc0d2bbea1088450cb4c1dda957a6cd4449100b3afc3fcc3e9d7bfe6eff4ebe08a40815cffb51aafaf4f2cdb1caca2f5d15e03ca2638c0d8	SHA-512	1	1608594
28	82690	00000003dc3384c77968f8235342c48f3c6f2f7e4060537df07ceabed28d89dd1814ad1014c989f836d533c5386994ed022f5e02102025578912 6e890c5d5d28	SHA-512	1	78241810
32	2158627	No se encontró una solución.	SHA-512	1	N/A
36	2458313	No se encontró una solución.	SHA-512	1	N/A
20	828	0000095cc1624f8eb92be8e03e2bf93abf138c1b70a1d07cbcfc718e94d677a441592bb40b87b049c5fa891b694eb0f9ffefd101529cb34709013b05f025e4f6	SHA-512	2	499337
24	2019	000000245c813ad1fc0d2bbea1088450cb4c1dda957a6cd4449100b3afc3fcc3e9d7bfe6eff4ebe08a40815cffb51aafaf4f2cdb1caca2f5d15e03ca2638c0d8	SHA-512	2	1608594
28	103254	00000003dc3384c77968f8235342c48f3c6f2f7e4060537df07ceabed28d89dd1814ad1014c989f836d533c5386994ed022f5e02102025578912 6e890c5d5d28	SHA-512	2	78241810
32	1256074	No se encontró una solución.	SHA-512	2	N/A
36	1213654	No se encontró una solución.	SHA-512	2	N/A

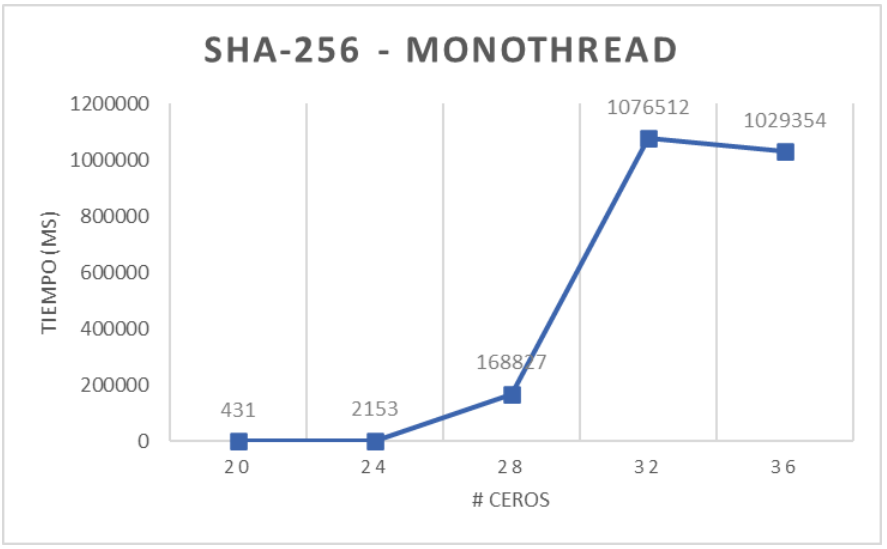
Cadena : santiagocabra					
# ceros	tiempo (ms)	hash generado	tipo hash	Numero Threads	Valor V
20	431	000004c0c994b71dc7ae5a27b4ad5376ab0301f89f01ba927a7ffff82a6c774c	SHA 256	1	512916
24	2153	0000004df5d7d9b8ca6a36ce8151e518a95b5ea97a539807d53b8a825eaa7769	SHA 256	1	3315100
28	168827	0000000f72740f98980d2546d62ae157722fb341e6f4bd4ab09611bf1c90952b	SHA 256	1	300018654
32	1076512	No se encontró una solución.	SHA 256	1	
36	1029354	No se encontró una solución.	SHA 256	1	
20	452	000004c0c994b71dc7ae5a27b4ad5376ab0301f89f01ba927a7ffff82a6c774c	SHA 256	2	512916
24	2102	0000004df5d7d9b8ca6a36ce8151e518a95b5ea97a539807d53b8a825eaa7769	SHA 256	2	3315100
28	174724	0000000f72740f98980d2546d62ae157722fb341e6f4bd4ab09611bf1c90952b	SHA 256	2	300018654
32	545620	No se encontró una solución.	SHA 256	2	
36	533330	No se encontró una solución.	SHA 256	2	

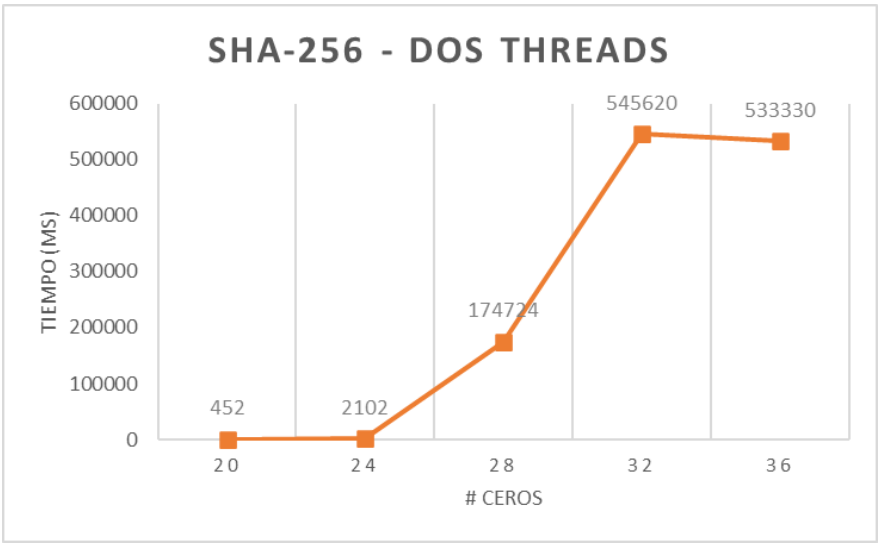
Cadena : infracomputacional					
# ceros	tiempo (ms)	hash generado	tipo hash	Numero Threads	Valor v
20	641	00000cbd4a25b989d45e076a31d88c4f3df616e726679d801121f3d4bd4154e79e67268f1a8ab05f4071803306b3674d01017c109da1b322b09126a7bd52774c	SHA-512	1	432541
24	12911	00000077cb896fc626d6a9857db4c1e0eee46dc9c11f19c29aaed2ed74794563cd6074d1997c64aafff99696c9f2b29c5a1be0340b1684ac1ab19cd313308345	SHA-512	1	11826900
28	146368	000000063d43e2f6cc8c48835bbd9fdd41435086b181d2a41c2f4c5bbf4feed16fd0788fc8908874f3182a20b25c862f2d49581a1e8eb4e0e7e229398805baac	SHA-512	1	139968072
32	2138749	No se encontró una solución.	SHA-512	1	N/A
36	18683221	No se encontró una solución.	SHA-512	1	N/A
20	684	00000092cf9cd8718c8ab4ae80e8bd720ebf6adc8c0fd1c9a81255fb5574191a3f576c2a0990ac365af5633f05df46fc1345df4f469524e5807d5b44fc0b69aa	SHA-512	2	1,074E+09
24	702	00000092cf9cd8718c8ab4ae80e8bd720ebf6adc8c0fd1c9a81255fb5574191a3f576c2a0990ac365af5633f05df46fc1345df4f469524e5807d5b44fc0b69aa	SHA-512	2	1,074E+09
28	173566	000000063d43e2f6cc8c48835bbd9fdd41435086b181d2a41c2f4c5bbf4feed16fd0788fc8908874f3182a20b25c862f2d49581a1e8eb4e0e7e229398805baac	SHA-512	2	139968072
32	1682592	No se encontró una solución.	SHA-512	2	N/A
36	2632573	No se encontró una solución.	SHA-512	2	N/A

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:

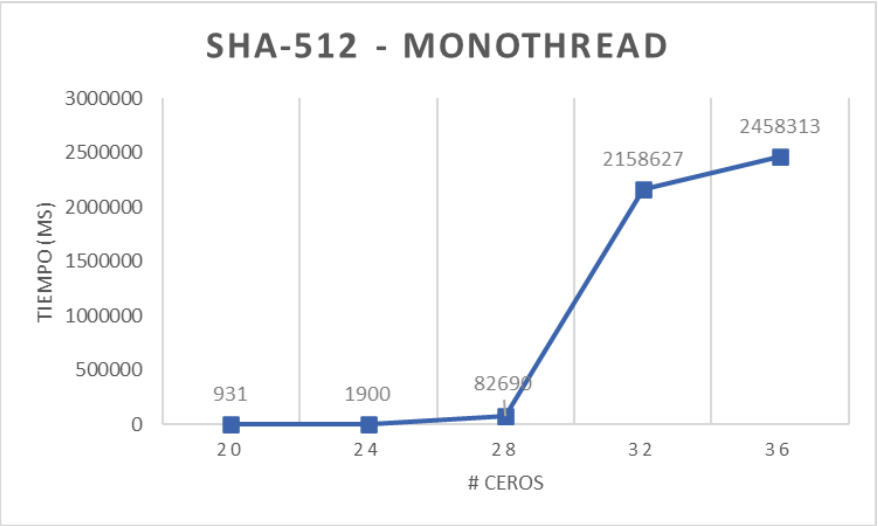
Gráficas Cadena #1 : santiagocabra

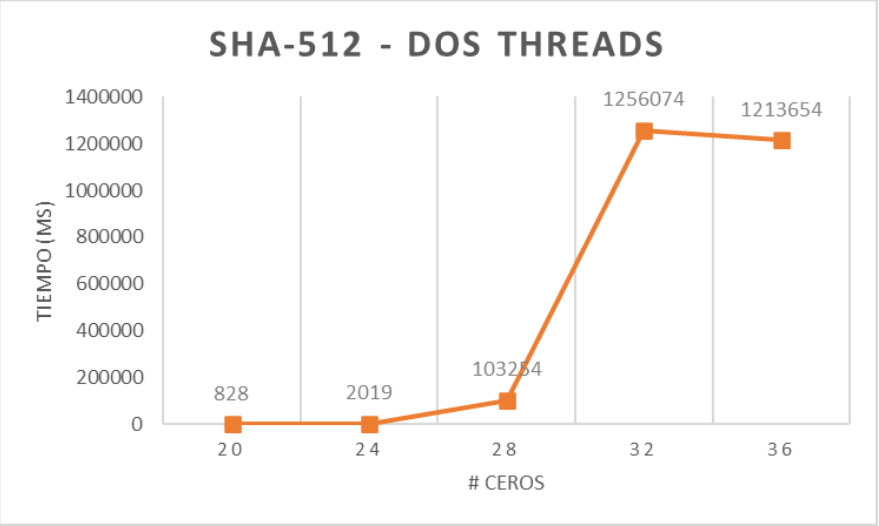
Utilizando algoritmo SHA-256:





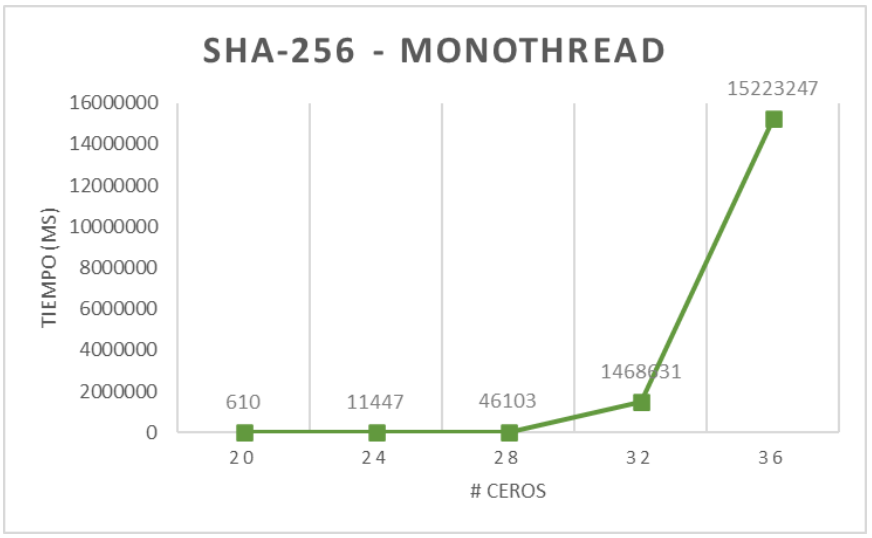
Utilizando algoritmo SHA-512:

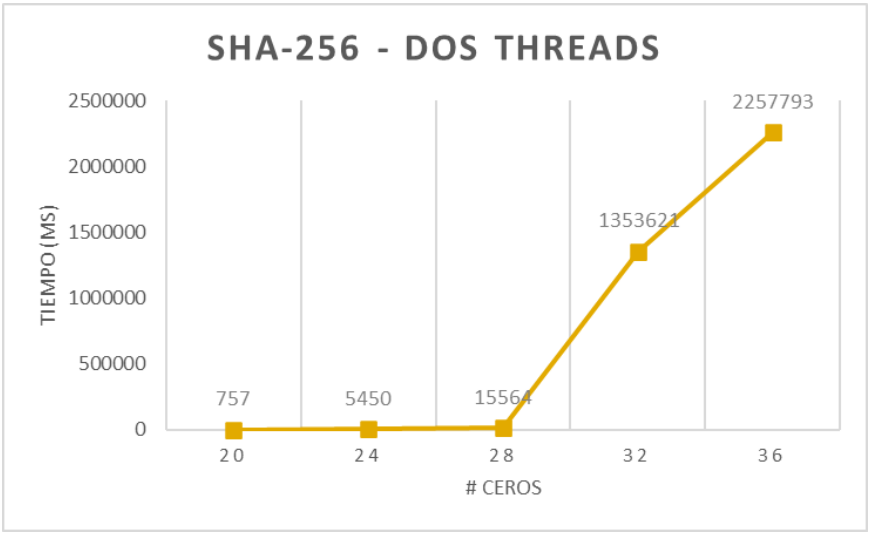




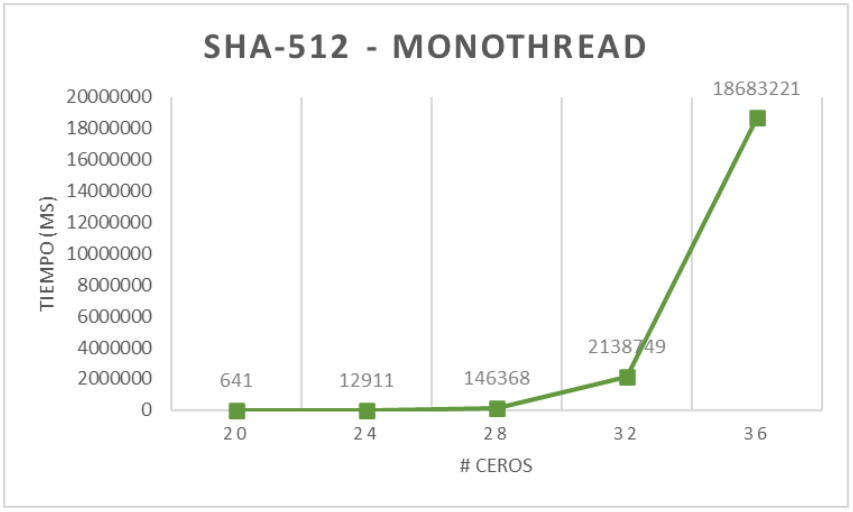
Gráficas Cadena #2 : infracomputacional

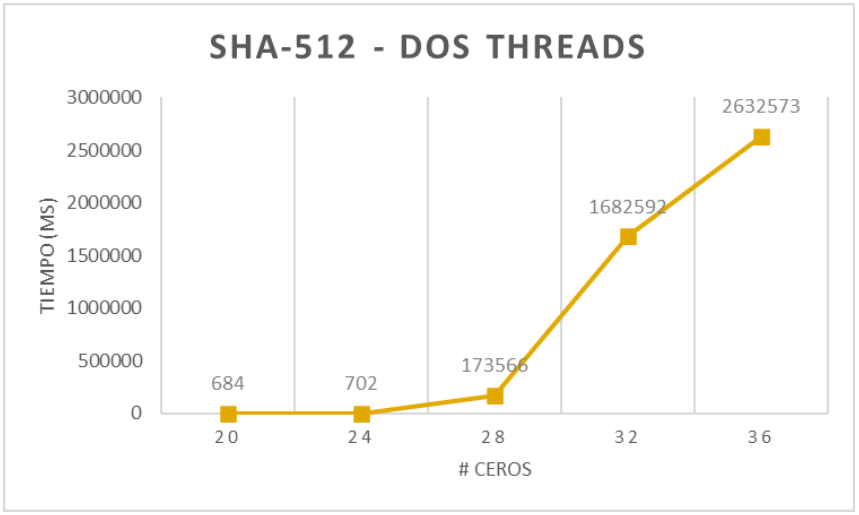
Utilizando algoritmo SHA-256:





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

```
Ingrese el valor de inputString: testblock
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 24
Ingrese el valor de numThreads (1 o 2): 1
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-256
Cadena de entrada: testblock
Valor v: 7438519
Hash: 0000009c3a9c048613f6df46ca999d07a38f92355ee6f477eb602ab02dbefc44
Tiempo de búsqueda: 8883 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 7438520
Tiempo total de ejecución (segundos): 8.883
Ciclos de procesador promedio por hash: 4.431E11
```

Cálculo 2

```
Ingrese el valor de inputString: infracomp
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 24
Ingrese el valor de numThreads (1 o 2): 2
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-256
Cadena de entrada: infracomp
Valor v: 1094962657
Hash: 000000187b5d043b61963f33ed5a952aa45b4d42943bf11cae7062c4d212c3f8
Tiempo de búsqueda: 44293 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 42515177
Tiempo total de ejecución (segundos): 44.293
Ciclos de procesador promedio por hash: 7.665E11
```

Cálculo 3

```
Ingrese el valor de inputString: infracomp
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 28
Ingrese el valor de numThreads (1 o 2): 2
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-256
Cadena de entrada: infracomp
Valor v: 506275629
Hash: 0000000122fcffced7268d3f069714cc23464fdafdd0d516f287e521aad5aa1a
Tiempo de búsqueda: 783188 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 1012484953
Tiempo total de ejecución (segundos): 783.188
Ciclos de procesador promedio por hash: 5.523E11
```

Cálculo 4

```
Ingrese el valor de inputString: infracomp
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 20
Ingrese el valor de numThreads (1 o 2): 2
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-512
Cadena de entrada: infracomp
Valor v: 353607
Hash: 00000b9a997e6b319fe4fa0b14c55e6aa694c3c12873c0869a0a2a7fdfea0644650dd7c6fdeb4ecdd5b3482d0a5c5796ba265bc05157eec71ffea9b9a77e094f
Tiempo de búsqueda: 1085 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 695890
Tiempo total de ejecución (segundos): 1.085
Ciclos de procesador promedio por hash: 1.5729E12
```

Cálculo 5

```
Ingrese el valor de inputString: infracomp
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 24
Ingrese el valor de numThreads (1 o 2): 2
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-512
Cadena de entrada: infracomp
Valor v: 12137348
Hash: 000000f9635f03b0f0861dc07445b6c3636d971b4c05f8c930a39cf05e06596c21aa54057818d7b7c45ceb7bb93ffc9ae76c0ba9567fc17c9315f88a61448c4f
Tiempo de búsqueda: 30625 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 24300564
Tiempo total de ejecución (segundos): 30.625
Ciclos de procesador promedio por hash: 1.2432E12
```

Cálculo 6

```
Ingrese el valor de inputString: infracomp
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 28
Ingrese el valor de numThreads (1 o 2): 2
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-512
Cadena de entrada: infracomp
Valor v: 1703141396
Hash: 0000000e0ba8d1017617fece6362bee3e1836ce5353ad70cc2d58dde31910cae53ef52c2a0b14777009755597ecc1c899774acca25f336c97f4ab2e3e9564ff1
Tiempo de búsqueda: 1427742 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 1259174662
Tiempo total de ejecución (segundos): 1427.742
Ciclos de procesador promedio por hash: 1.1172E12
```

Cálculo 7

```
Ingrese el valor de inputString: testblock
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 20
Ingrese el valor de numThreads (1 o 2): 1
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-256
Cadena de entrada: testblock
Valor v: 1977688
Hash: 00000e3068378f9935379946c55a4ff4f1107a6ee3ad27bf624ee1672a14431c
Tiempo de búsqueda: 2487 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 1977689
Tiempo total de ejecución (segundos): 2.487
Ciclos de procesador promedio por hash: 4.977E11
```

Cálculo 8

```
Ingrese el valor de inputString: testblock
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 20
Ingrese el valor de numThreads (1 o 2): 1
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-512
Cadena de entrada: testblock
Valor v: 1210914
Hash: 0000027719e3f5e01355c4f27a020a1406a3d81ab7f32f3657ee5a0151d6d144b8dd7c16d629d57972be766a15cd6901d5646f5e303969bdd550a763230cef29
Tiempo de búsqueda: 2787 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 1210915
Tiempo total de ejecución (segundos): 2.787
Ciclos de procesador promedio por hash: 1.092E12
```

Cálculo 9

```
Ingrese el valor de inputString: testblock
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 24
Ingrese el valor de numThreads (1 o 2): 1
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-256
Cadena de entrada: testblock
Valor v: 7438519
Hash: 0000009c3a9c048613f6df46ca999d07a38f92355ee6f477eb602ab02dbefc44
Tiempo de búsqueda: 8883 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 7438520
Tiempo total de ejecución (segundos): 8.883
Ciclos de procesador promedio por hash: 4.431E11
```

Cálculo 10

```
Ingrese el valor de inputString: testblock
Ingrese el valor de numZeros (20, 24, 28, 32 o 36): 24
Ingrese el valor de numThreads (1 o 2): 1
Ingrese el valor de algorithm (SHA-256 o SHA-512): SHA-512
Cadena de entrada: testblock
Valor v: 15011155
Hash: 000000e95ea72977b4bc1f41c96d5b69ae21d895865400d1622b60d015001457c5754858ea0c5b8e44186545f042c0530e38362bbe215984e9f4692492bbe360
Tiempo de búsqueda: 31842 ms
Velocidad del procesador: 2.1 GHz
Total de operaciones de hash: 15011156
Tiempo total de ejecución (segundos): 31.842
Ciclos de procesador promedio por hash: 1.0227E12
```

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 = $26 + 26^2 + 26^3 + 26^4 + 26^5 + 26^6 + 26^7$

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.