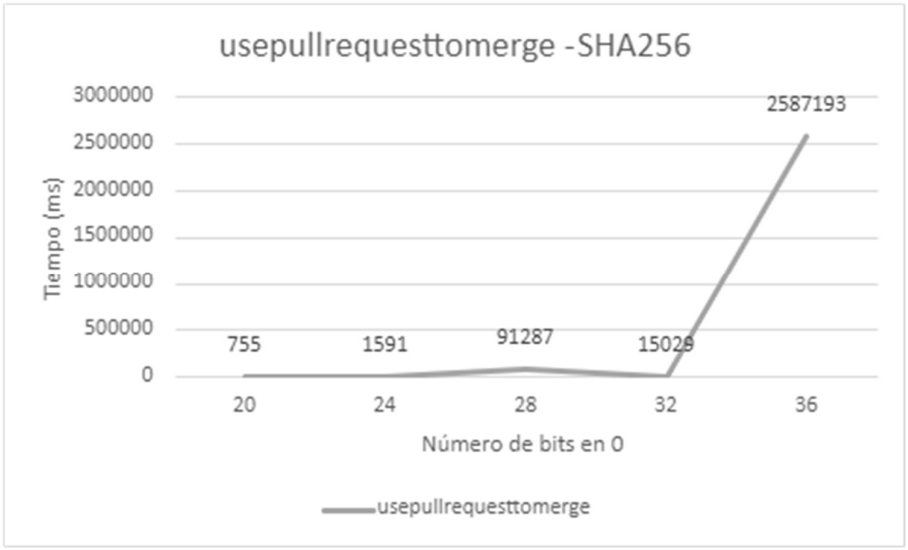
Reporte caso 3
Nicolás Ortega - 201814515
Camilo García - 201821149

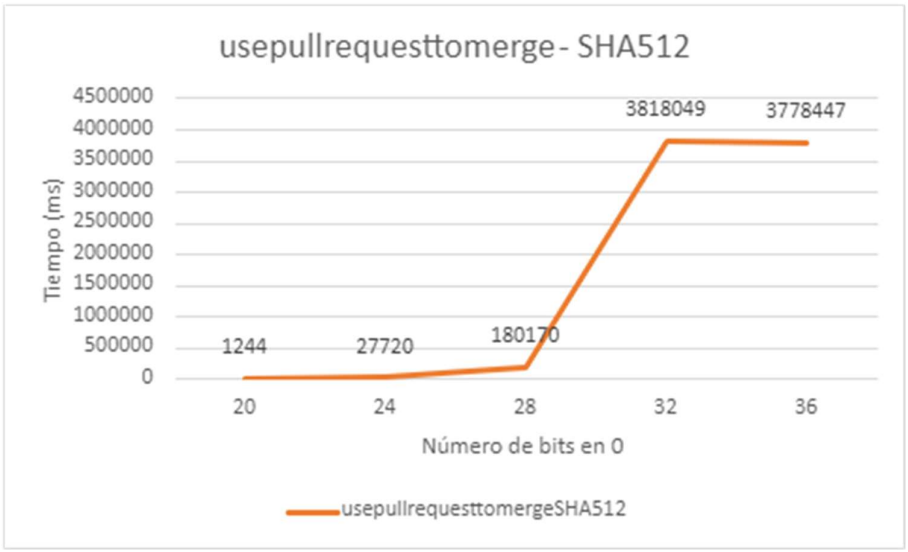
Sección A

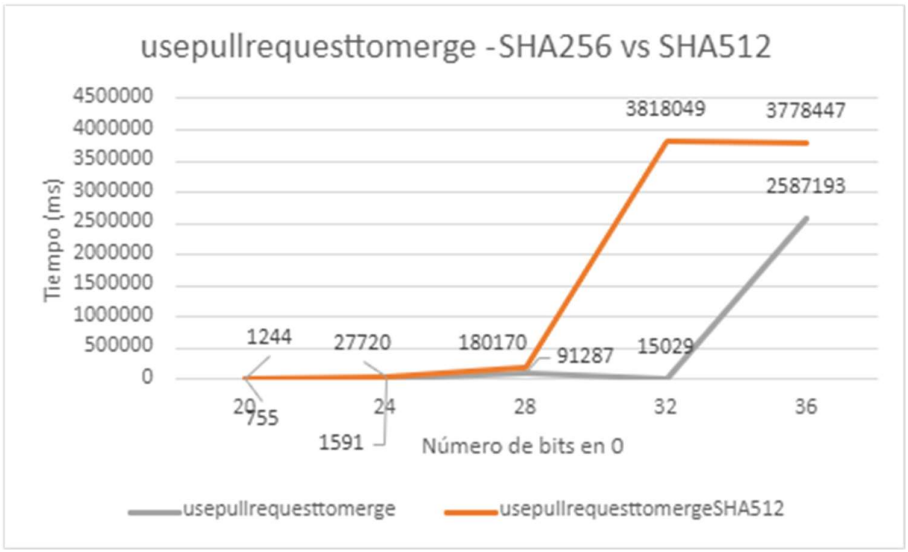
1. **Recolección de datos**
   A continuación, se encuentra una tabla que contiene los datos recopilados a partir de la elaboración de nuestro algoritmo. Se utilizaron 2 cadenas diferentes, con los algoritmos SHA-256 y SHA-512 y los diferentes números de 0 solicitados.

Algoritmo usado	Cadena de prueba	Número de 0's buscado	Cadena de respuesta v	Tiempo(ms)
SHA-256	usepullrequesttomerge	20	zaaavvn	755
		24	maaeevt	1591
		28	kaxbjhy	91287
		32	iaemyxv	15029
		36	No encontró	2587193
	hazpausasactivas	20	taacnik	1158
		24	naboynz	6343
		28	saaajsa	492
		32	xhkxquz	688187
		36	No encontró	2389179
SHA-512	usepullrequesttomerge	20	iaabqvo	1244
		24	vactqon	27720
		28	uaordsy	180170
		32	prnvhnb	3818049
		36	No encontró	3778447
	hazpausasactivas	20	laabjfk	758
		24	sabgchl	11039
		28	dbgvtvy	363959
		32	yaxpabh	278884
		36	No encontró	3637602

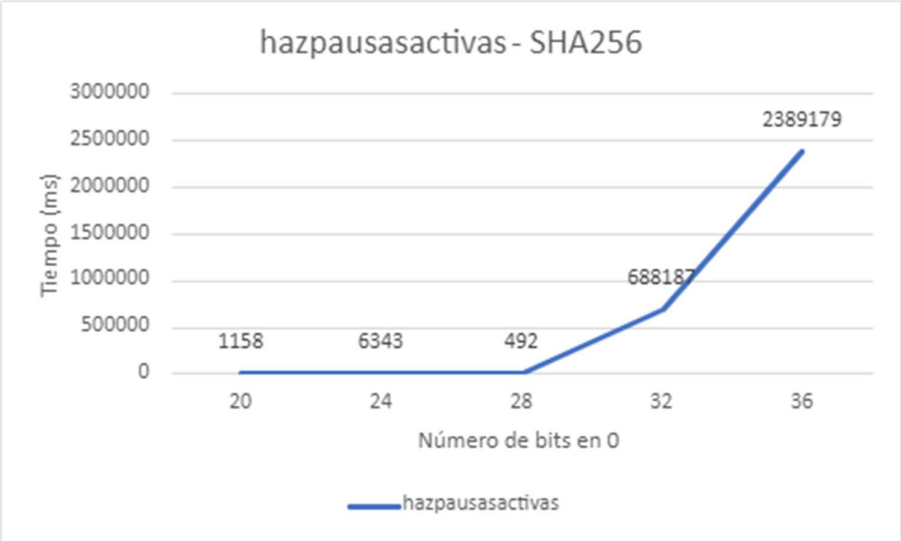
2. **Graficación de los datos recolectados**
   A continuación, se pueden encontrar los tiempos para la cadena “usepullrequesttomerge” con cada uno de los algoritmos y al final una combinación de ambos

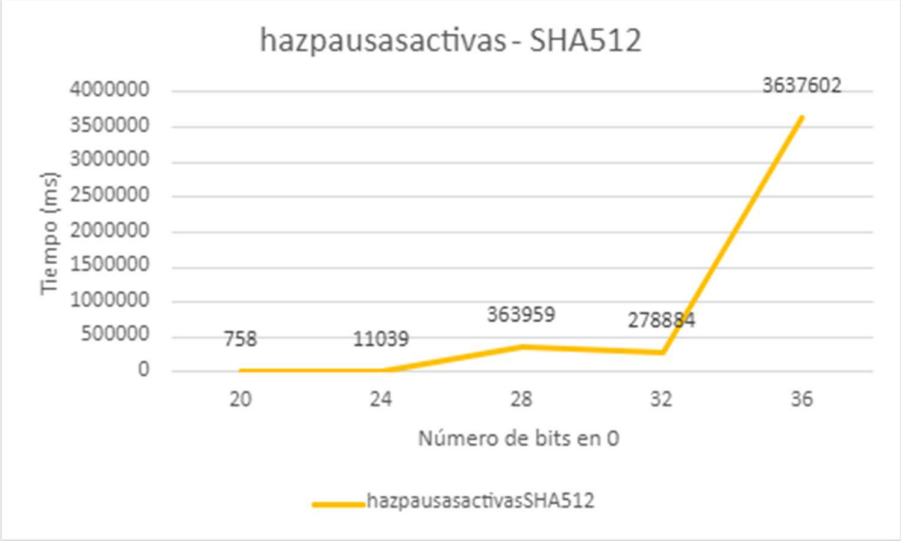

usepullrequesttomerge -SHA256
3000000
2500000
2000000
1500000
1000000
500000
0
Tiempo (ms)
755
1591
91287
15029
2587193
20
24
28
32
36
Número de bits en 0
usepullrequesttomerge

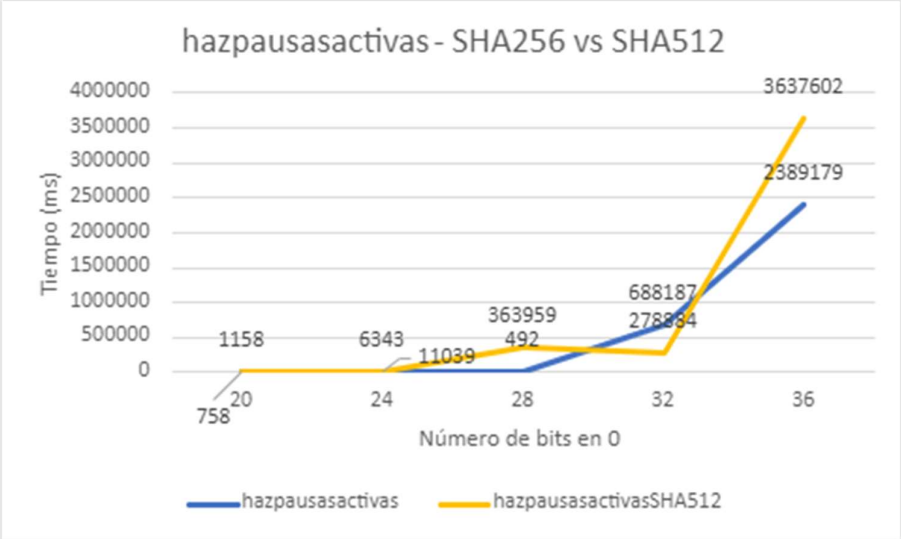

usepullrequesttomerge- SHA512
4500000
4000000
3500000
3000000
2500000
2000000
1500000
1000000
500000
0
Tiempo (ms)
1244
27720
180170
3818049
3778447
20
24
28
32
36
Número de bits en 0
usepullrequesttomergeSHA512


usepullrequesttomerge -SHA256 vs SHA512
4500000
4000000
3500000
3000000
2500000
2000000
1500000
1000000
500000
0
Tiempo (ms)
1244
27720
180170
91287
15029
3818049
3778447
2587193
20
755
24
1591
28
32
36
Número de bits en 0
usepullrequesttomerge
usepullrequesttomergeSHA512

A continuación, se pueden encontrar los tiempos para la cadena “hazpausasactivas” con cada uno de los algoritmos y al final una combinación de ambos.







3. Cálculos sobre el tiempo de un ciclo

Las pruebas se desarrollaron en un computador con un procesador de 3 Ghz. Esto significa que el procesador realiza $3x10^9$ ciclos por segundo. Para calcular cuántos ciclos de procesador toma en promedio en generar y evaluar el valor para determinar si cumple o no con la condición buscada, lo primero que se hizo fue determinar una búsqueda tal que se encontrara con un solo proceso de generación y evaluación. Esta cadena fue "pruebaparaquefuncioesdcv" y, cumplía la condición de prueba (4 ceros) simplemente agregando la letra a. Además, para efectos de esta prueba, solo se lanzó el thread encargado de generar las cadenas con los valores v de longitud 1, para que el threading del desarrollo no alterara los resultados.

Al correr este caso de prueba múltiples veces, obtuvimos que se demoró en promedio 14ms, lo que quiere decir que generar y evaluar el valor para determina si cumple o no con la condición buscada toma 0.014 segundos.

Posteriormente, pasamos el valor de frecuencia del procesador a su contraparte en forma de periodo, de tal forma que pudiéramos hacer la división de este valor con el número de segundos que toma el proceso, de la siguiente forma

$$\frac{1}{3x10^9\ segundos/ciclo} = \frac{1}{0{,}014\ segundos} = \frac{1}{2.38x10^{-8}} ciclos = 42.016.807\ ciclos$$

Obteniendo así que se llevan a cabo 42.016.807 ciclos en la operación para realizar este proceso.

Sección B

1. Algoritmos de Hash

Las funciones criptográficas de hash se utilizan principalmente para proteger contraseñas y almacenarlas de forma segura y no como texto plano en una base de

datos. Sin embargo, no solo se utilizan de esta forma, existen otros usos para las funciones de hash. Algunos algoritmos de hash se utilizan para detectar malware, y otros se usan en las comunicaciones para asegurar la integridad de los mensajes[1]. Entre los algoritmos más utilizados actualmente se encuentran:

- **SHA2 (Secure Hash Algorithm):** dentro de este encontramos múltiples variaciones:
  - SHA-256
  - SHA-384
  - SHA-512
  - SHA2-224
- **SHA3:** es menos popular, pero sigue siendo una alternativa existente
- **Algoritmos Hash KDF (Key Derivation Function):** entre los cuales encontramos los algoritmos más populares para protección de contraseñas:
  - Argon2
  - Scrypt
  - Bcrypt
  - PBKDF2

Desafortunadamente, aunque los algoritmos criptográficos de hash suelen proveer alta seguridad, no son completamente invencibles. Es por esto que a lo largo de los años se han hecho pruebas de atacantes para medir la seguridad los algoritmos, y en algunas ocasiones se han logrado vulnerar. Estos ataques se pueden hacer principalmente de dos formas: por "fuerza bruta" o buscando debilidades matemáticas del algoritmo[2].

Entre los algoritmos de hash que se consideran obsoletos, porque ya no dan la garantía suficiente en seguridad, se encuentran:

- **MD2, MD4 y MD5**
- **RIPEMD**
- **SHA-1**
- **CRC**

2. Un posible uso adicional de la tecnología del Blockchain

Un caso de uso en el cuál almacenar información en una cadena de bloques (Blockchain) sería de mucha utilidad es en la regulación de los servicios públicos y gubernamentales. Actualmente toda la gestión pública se maneja de forma tradicional, con una entidad central que realiza todas las operaciones y administra un registro de estas. En este caso, aquella entidad está representada por el gobierno. Sin embargo, como bien es conocido en nuestro país, esta entidad central se compone de personas que son altamente corruptibles y que por lo tanto no ofrecen muy altas garantías sobre la veracidad de las operaciones. Es aquí donde el blockchain entra a presumir su valor. Integrar el blockchain a las operaciones gubernamentales les permitiría presumir de una transparencia definitiva. Esto se podría aplicar en múltiples ámbitos: gestión de licencias, transacciones, votaciones, manejo y distribución de recursos, entre otras. Si se guardara la información de todas estas transacciones u

operaciones en una cadena de bloques, la información real sería rastreable, se vería altamente protegida, no sería repudiable y se mantendría su integridad. Como bien sabemos, el blockchain permite que la comunidad (que tiene acceso a la cadena) se entere en todo momento de la nueva información que se agregue, por lo tanto, cualquier intento de manipular la información sería fácilmente detenido[3]. De esta forma, la información almacenada en cada bloque sería transparente, toda la comunidad tendría acceso a ella y se garantizaría la veracidad.

Bibliografía

1. Algoritmos HASH: Qué son, seguridad, uso y funcionamiento. *RedesZone* https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-hash/.

2. Escritor, G. Á. M. & ElevenPaths, científico y conferenciante E. del Á. de I. y L. en. La criptografía insegura que deberías dejar de usar - Think Big Empresas. *Think Big* https://empresas.blogthinkbig.com/la-criptografia-insegura-que-deberias-dejar-de-usar/ (2019).

3. PlayGround. *Qué es 'Blockchain' en 5 minutos*. (2018).