Informe Caso 2.

A1. Algoritmos de Cifrado

* MD5 (Message-Digest Algorithm 5): Es un algoritmo de reducción criptográfica de 128 bits y se usa para comprobar que un archivo no haya sido alterado. Este algoritmo aún se usa, pero debido a que con el tiempo se descubrieron muchas vulnerabilidades, muchas organizaciones lo dejaron de usar.
* SHA-256 (Secure Hash Algorithm 256): Es un algoritmo de seguridad criptográfica de 256 bits y se utiliza en diferentes herramientas de seguridad y protocolos como TLS, SSL, PGP, SSH, S/MIME, IPsec y Bitcoin. Este algoritmo se sigue utilizando más que todo en Bitcoin.
* SHA-384 (Secure Hash Algorithm 384): Es un algoritmo de seguridad criptográfica de 384 bits, es del mismo conjunto de algoritmos criptográficos que el SHA-256 y el SHA-512 y aún se utiliza.
* SHA-512 (Secure Hash Algorithm 512): Es un algoritmo de seguridad criptográfica de 512 bits, es el más seguro del conjunto de algoritmos criptográficos SHA-2 y el más lento. Aún se usa este algoritmo.

A2. Tiempos de Solución

Para ejecutar el programa se tiene que ingresar el algoritmo con el que se desea encriptar seguido de la palabra a encriptar. Ej: 2 caso.

Para los tiempos de solución, se resolvió en una maquina con un procesador Intel Core i5-8400 de 2.80Ghz.

Para el funcionamiento de la solución se creó una clase que implementa Runnable llamada “CrackerContrasenia”. Esta lo que hace es que genera cadenas candidatas de manera recursiva por orden lexicográfico, y compara estas candidatas con la cadena cifrada. Es importante recalcar que solo genera cadenas candidatas cuya longitud se encuentra dentro de un intervalo cerrado que se da por parámetro. El método “identificar\_entrada” calcula la longitud de los intervalos cerrados y crea un Thread Pool dependiendo del número de núcleos disponibles, y a través de este Thread Pool ejecutan las instancias de CrackerContrasenia.

Finalmente, para la toma de tiempos se tiene en cuenta como tiempo inicial el instante antes de que las instancias de CrackerContrasenia se ejecuten en el ThreadPool y como tiempo final, el tiempo que demora CrackerContrasenia en encontrar la solución o notificar por consola que no la encontró.

Se identifico como el peor caso las cadenas que son válidas para la expresión regular , que hacen referencia a las cadenas que contengan solo el carácter “z” con longitud de 1 a 7. Este es el peor caso debido a que las cadenas se generan desde el carácter “a” y sus respectivas combinaciones.

Los tiempos registrados son los siguientes:

* Algoritmo MD5



* Algoritmo SHA-256



* Algoritmo SHA-384



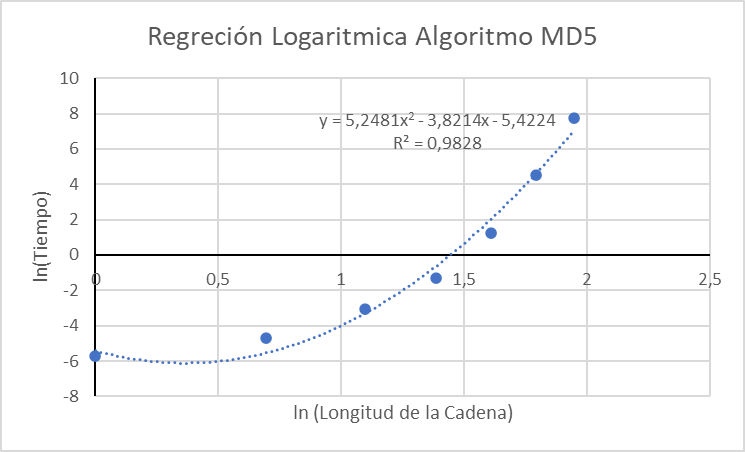
* Algoritmo SHA-512

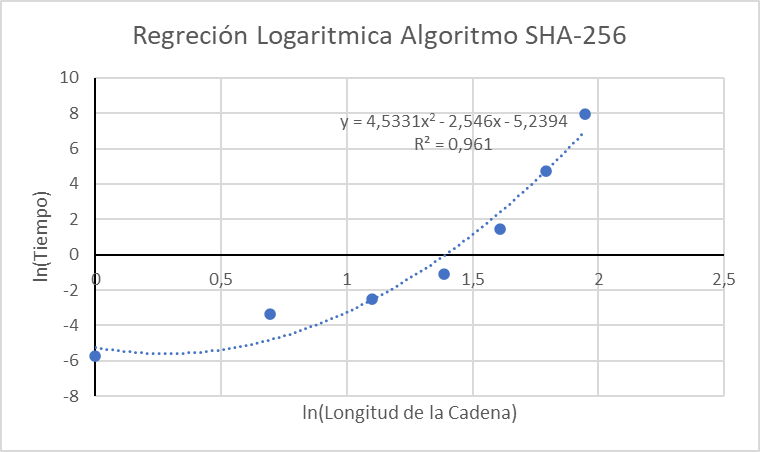


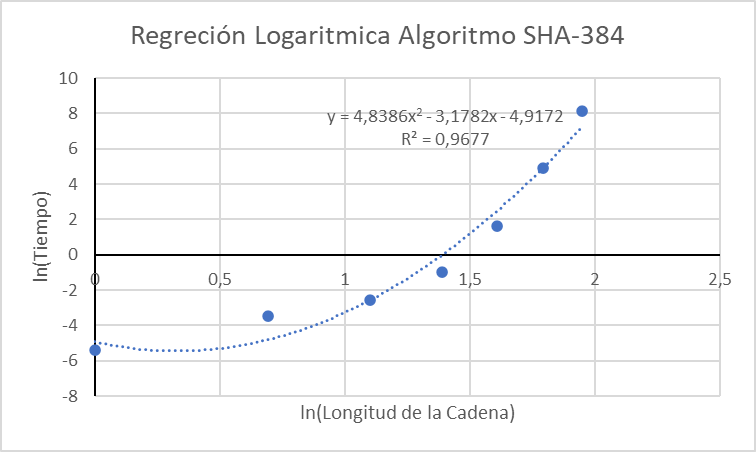
A3. Estimación cadena de 16 caracteres.

Para realizar la estimación se hizo una regresión logarítmica a los datos, y a esta se le encontró la función que mejor se ajustara. Finalmente se encuentra el valor del tiempo estimado y se aplica la función exponencial a este valor para encontrarlo en segundos. El valor a determinar es cuando la función de regresión logarítmica es evaluada en

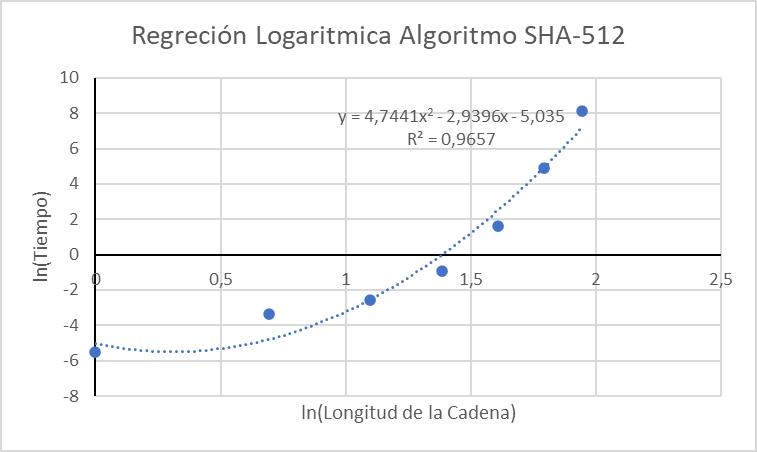
* Algoritmo MD5



* Algoritmo SHA-25  
  
* Algoritmo SHA-384

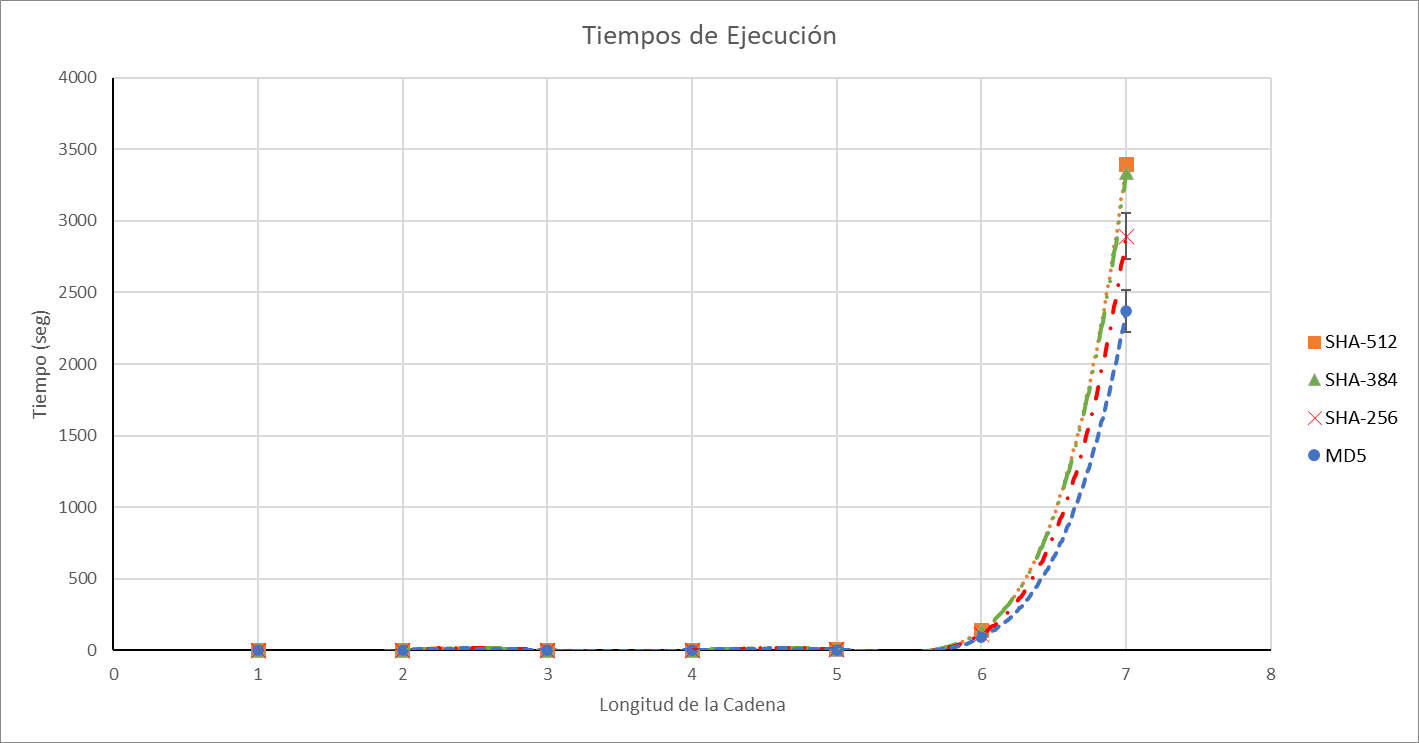


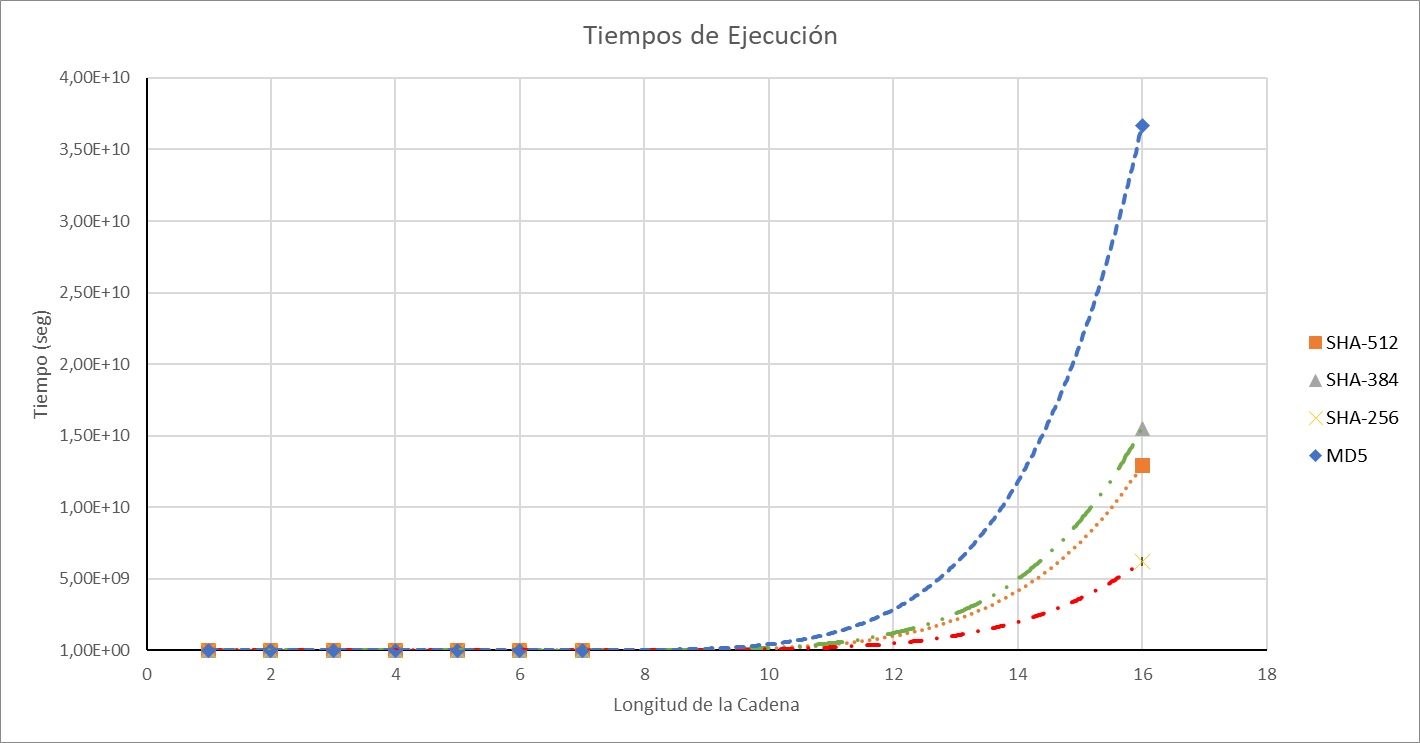
* Algoritmo SHA-512



A4. Graficas

Se mostrarán dos gráficas, en la primera están los tiempos de ejecución solo de los datos registrados, la segunda contiene los tiempos registrados y la predicción para una cadena de 16 caracteres.





A5. Caso promedio

Para encontrar cuantos ciclos de reloj se demora en promedio, se pasarán los tiempos obtenidos para cada algoritmo a ciclos de reloj, y este tiempo se dividirá en dos, dado que el caso promedio corresponde a evaluar la mitad de los casos de todos los posibles evaluados. Se usará la siguiente conversión para los datos:

Aplicando la conversión se obtienen los siguientes resultados:



B1. Los datos que deben ser protegidos y que maneja el sistema de rastreo de unidades de distribución y paquetes son:

* El estado del paquete (entrega o recolección)
* Las rutas de distribución
* La localización de las unidades de distribución
* El documento legal del paquete o contrato de transporte (remitente, destinatario, contenido, horas de recogida y entrega, etc.)

B2.

* Estado del paquete: Como cliente (remitente o destinatario), cuando quiera consultar el estado de mi paquete dado que el sistema opera normalmente quiero que la información sea actualizada únicamente por la empresa, esto debe suceder el 100% de las consultas.

Si no se garantiza este requerimiento, los clientes se verían afectados ya que un tercero podría influir en el estado del paquete y generar confusiones tanto para los clientes como para la empresa.

* Las rutas de distribución: Como operador, cuando necesite cambiar la ruta de distribución dado que el sistema opera normalmente quiero que la información sólo pueda ser aprobada por el sistema de gestión y rastreo de unidades de distribución, esto debe suceder el 100% de las actualizaciones de las rutas.

Si no se garantiza este requerimiento, los conductores, los clientes y la empresa pueden verse afectados ya que un tercero podría aprobar el cambio de ruta y causar retraso en las entregas de los paquetes.

* La localización de las unidades de distribución: Como controlador, cuando esté consultando la información de la ubicación de las unidades de distribución dado que el sistema opera normalmente quiero que la información sea real y exacta, esto debe suceder el 100% de las consultas.

Si no se garantiza este requerimiento, la empresa y los clientes se pueden ver afectados ya que se causarían confusiones de los horarios de entrega de los paquetes.

* El documento legal del paquete o contrato de transporte: Como cliente, cuando genere un contrato de transporte con la empresa dado que el sistema opera normalmente quiero que la información sólo la pueda ver la empresa, esto debe suceder el 100% de las veces.

Si no se garantiza este requerimiento, los clientes se pueden ver afectados en gran medida, ya que la información que contiene el documento legal es del cliente y puede ser delicada.

B3. Vulnerabilidades del sistema:

* Ya que los puntos de atención al cliente se comunican con el servidor de manejo de órdenes por medio de internet para registrar pedidos y contratos, una vulnerabilidad en este sistema sería que un atacante pudiera acceder al servidor y consultar los contratos que contienen información de los clientes, ya que las comunicaciones están protegidas para garantizar integridad, pero no confidencialidad.
* En el servidor de manejo administrativo contable un atacante podría inyectar consultas maliciosas para lograr acceder a la base de datos y modificar los datos o eliminarlos. Aparte de afectar la privacidad de los clientes y de la compañía afectaría también el rendimiento del servidor.
* Ya que las unidades se comunican con el servidor de manejo de unidades de distribución y paquetes para informar su estado y estas comunicaciones están protegidas para garantizar integridad, un atacante podría acceder al servidor y ver las rutas que las unidades van a tomar porque no están protegidas para garantizar confidencialidad.