Proyecto No.2:
OpenMPI

Oliver Graf 17190
Estuardo Ureta 17010
Kristen Brandt 171482

Índice

Antecedentes conceptuales

GitHub

GitHub es una herramienta para el control de versiones de proyectos, normalmente este se utiliza para proyectos de código. Esta herramienta permite que haya varios colaboradores en el desarrollo del proyecto y se mantenga un orden en el trabajo de los mismos (Github, 2022).

OpenMPI

OpenMPI es una biblioteca estándar para realizar procesamiento en paralelo haciendo uso de un modelo de memoria distribuida. Esta biblioteca es open source y se puede correr en Linux, OS, Windows (Open MPI, 2022).

Cifrado/Decifrado

El cifrado es el proceso que traduce los datos sin formato especial (“plaintext") a algo que no parece tener sentido y parece ser aleatorio (“ciphertext”). Descifrado es el proceso para pasar de los datos “sin sentido” de regreso a un texto sin formato especial. La idea de hacer un proceso de cifrado es que solo las personas autorizadas a ver los datos los puedan ver mientras que personas no autorizadas no puedan tener acceso a la información inicial. Ahora este proceso de cifrado y descifrado se utiliza en las computadoras y las comunicaciones que se tienen a través de ellas (Fox, 2022).

Bruteforce

Un ataque de brute force o fuerza bruta es un método de hacking que utiliza el método de prueba y error para poder descifrar todo tipo de documentos o información (Fortinet, 2020). En el caso del proyecto se utilizará un programa de bruteforce para poder descubrir la llave privada usada para cifrar un texto. Dicho programa tendrá iteraciones hasta encontrar la clave deseada.

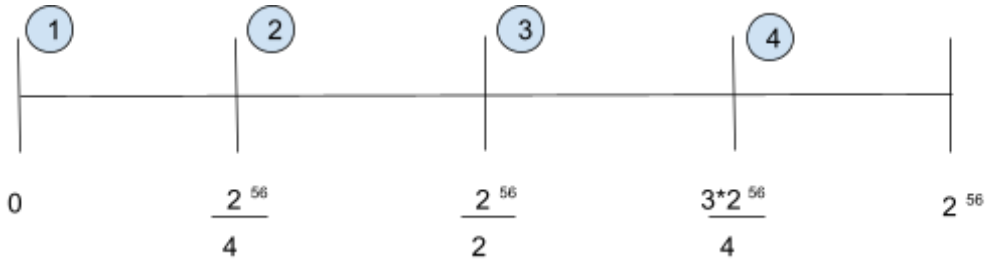
Algoritmo DES

Data Encryption Standard, también conocido como DES, es un algoritmo de cifrado para data digital. Aunque este algoritmo ya no es considerado como uno seguro por su clave de solamente 56 bits este ha influenciado un gran avance en la criptografía que se utiliza hoy en día. Este algoritmo fue desarrollado en los 1970 en International Business Machines Corporation (IBM) y fue seleccionado por el National Security Agency (NSA) para la protección de datos gubernamentales electrónicos confidenciales y no clasificados. Aunque este algoritmo era reforzado contra el criptoanálisis diferencial no era muy bueno en contra de ataque de fuerza bruta. En 1977 este algoritmo se volvió el estándar federal de procesamiento de información (FIPS) para los Estados Unidos (DES, 2020).

Antecedentes numéricos

Speedups inconsistentes

Se pueden dar speedups inconsistentes y dependientes de la llave elegida dado a que se recorre el espacio de datos de forma incremental y en orden, aparte se dividen equitativamente los espacios.



Posibles claves y cómo los speedups pueden ser inconsistentes

Los speedups dependen mucho de la llave que se elige.

Si se corre el programa de manera paralela con 4 distintos procesos, si se escoge una llave de $\frac{2^{56}}{2} + 1$ se encontrara la llave en la primera iteración por el 3er proceso pero si se utiliza la misma clave de $\frac{2^{56}}{2} + 1$ en el programa secuencial el programa se toma $\frac{2^{56}}{2} + 1$ iteraciones para encontrar la respuesta. Aquí se daría un speedup extremadamente alto.

Otro ejemplo de las inconsistencia es si se escoge una llave de $\frac{2^{56}}{4}$ se encontrará la llave en exactamente la misma iteración sin importar si el programa es paralelo o no. En este caso no se daría ningún speedup en el programa.

Diagrama de flujo del algoritmo DES

DES se fundamenta de dos atributos fundamentales de la criptografía. La primera es la sustitución (también llamada confusión) y la segundo es la transposición (también llamada difusión). El algoritmo en cuestión consta de 16 pasos, cada uno de los cuales se les llaman una ronda. Cada ronda realiza los pasos de sustitución y transposición. Hablando de los pasos tenemos los siguientes: En el primer paso, el bloque de texto sin formato de 64 bits se transfiere a una función de permutación en el inicial (PI) . La permutación inicial se realiza en texto sin formato. Luego, la PI produce dos mitades del bloque permutado. Una de las mitades denominándose LPT o permutación izquierda de texto por su siglas en inglés. La otra mitad denominada permutación derecha de texto sin formato (RPT). Luego, cada LPT y RPT pasan por 16 rondas del proceso de encriptación. Al final, LPT y RPT se vuelven a unir y se realiza una permutación final (FP) en el bloque combinado el resultado de este proceso produce texto cifrado de 64 bits.

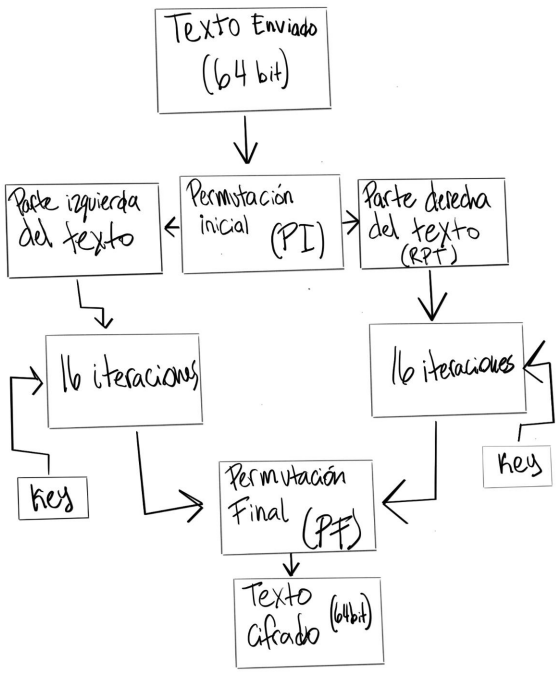


Diagrama 1. Flujo del algoritmo DES (Data Encryption Standard)

El algoritmo DES es usado como un cifrado de bloque de clave simétrica. El algoritmo toma el texto sin formato en bloques de 64 bits y los convierte en texto cifrado utilizando claves de 48 bits. Se puede utilizar para prácticamente cualquier tipo de cifrado. Pero siendo prácticos y estando actualizados con nuevas tecnologías podemos saber que el único uso práctico actual de DES es como bloque de construcción para llegar a Triple DES. Al momento de ser usado ya

hace décadas se utilizaba para todo tipo de cifrado, como se menciona anteriormente. En ese momento, este era simila y usado con igual o parecida frecuencia a AES, por ejemplo.

Introducción

En el proyecto No.2 de computación paralela y distribuida se utilizó OpenMPI, para diseñar un programa que sea capaz de encontrar una llave privada con la cual fue cifrado un texto sin formato (“plain text”). Este proyecto se hizo con el objetivo de diseñar programas para la paralelización de procesos con memoria distribuida utilizando la librería de OpenMPI además de optimizar el uso de recursos distribuidos y mejorar el speedup del programa paralelo.

Se utilizó el algoritmo de DES mencionado en los antecedentes conceptuales para poder cifrar un texto y descubrir la llave privada utilizada. Este algoritmo se escribió utilizando C.

Metodología

Diagrama de rutinas

decrypt (key, *ciph, len) y encrypt (key, *ciph, len)

tryKey (key, *ciph, len)

memcpy

strstr

Funciones primitivas de MPI

MPI_Irecv

Esta función es para comenzar el recibimiento de un mensaje. Lo que hace es bloquear el proceso hasta que se le notifique la llegada de un mensaje. Cuando esto suceda, pedirá que se comience a recibir el mensaje, a la vez que continúa la ejecución del resto del proceso. Una vez nos es necesario utilizar el mensaje, es obligatorio utilizar alguna directiva de MPI para detener la ejecución (como MPI_Wait), o bien comprobar el estado del recibo (por ejemplo con MPI_Test).

MPI_Send

Funcion de envío de mensaje bloqueante de un proceso de origen a uno de destino. Al ser bloqueante significa que hasta que el mensaje no haya sido enviado (que salga del buffer de salida) no se continúa la ejecución.

MPI_Wait

Este método bloquea el proceso que lo invoca hasta que la operación indicada en request se complete. Una vez se completa, se rellena la variable en el parámetro de salida status con los datos propios del objeto de tipo MPI_Status.

Resultados

Discusión

- Pendiente de hacer

Conclusiones/Recomendaciones

- Pendiente de hacer

Anexos

- Cronograma de actividades

UNIVERSIDAD DEL VALLE DE GUATEMALA
Proyecto 2 MPI
CRONOGRAMA DE ACTIVIDADES

FASE	ACTIVIDADES / ESTRATEGIAS	RESPONSABLE	Abril			Mayo	
			2	3	4	1	2
Etapa 1	Planificación de actividades						
	Inicializar GIT						
	Documentación preliminar						
	Bosquejo de Informe						
	Código parcial						
	Mediciones de tiempo sobre código base						
Etapa 2	Programación defensiva						
	Antecedentes numéricos						
	Codigo (inicial)						
	Diagrama de flujo de su programa						
	catálogo de las funciones						
	Revision						
	Mediciones de tiempo						
	Modificaciones						
	Calculo de Speed up						
	Correcciones de parametros						
FINAL	Reporte						
	Retos encontrados para la implementación						
	Bitacora						
	Recomendaciones						
	Resultados						
	Discusión y conclusiones						

- Catálogo de funciones

- Bitácora de pruebas

Literatura Citada

Fox, P. (2022). *Cifrado, Descifrado y cracking (artículo)*. Khan Academy. Retrieved from https://es.khanacademy.org/computing/ap-computer-science-principles/x2d2f703b37b450a3:online-data-security/x2d2f703b37b450a3:data-encryption/a/encryption-decryption-and-code-cracking

Lecture 4 data encryption standard (DES) - LRI. (2020). Retrieved from https://www.lri.fr/~fmartignon/documenti/systemesecurite/4-DES.pdf

Open MPI: Open source high performance computing. Open MPI: Open Source High Performance Computing. (2022). Retrieved from https://www.open-mpi.org/

What is a brute force attack?: Definition, Types & How It Works. Fortinet. (2020). Retrieved from https://www.fortinet.com/resources/cyberglossary/brute-force-attack

Where the world builds software. GitHub. (2022). Retrieved from http://github.com/