Universidad Del Valle de Guatemala
Computación Paralela
Miguel Novella

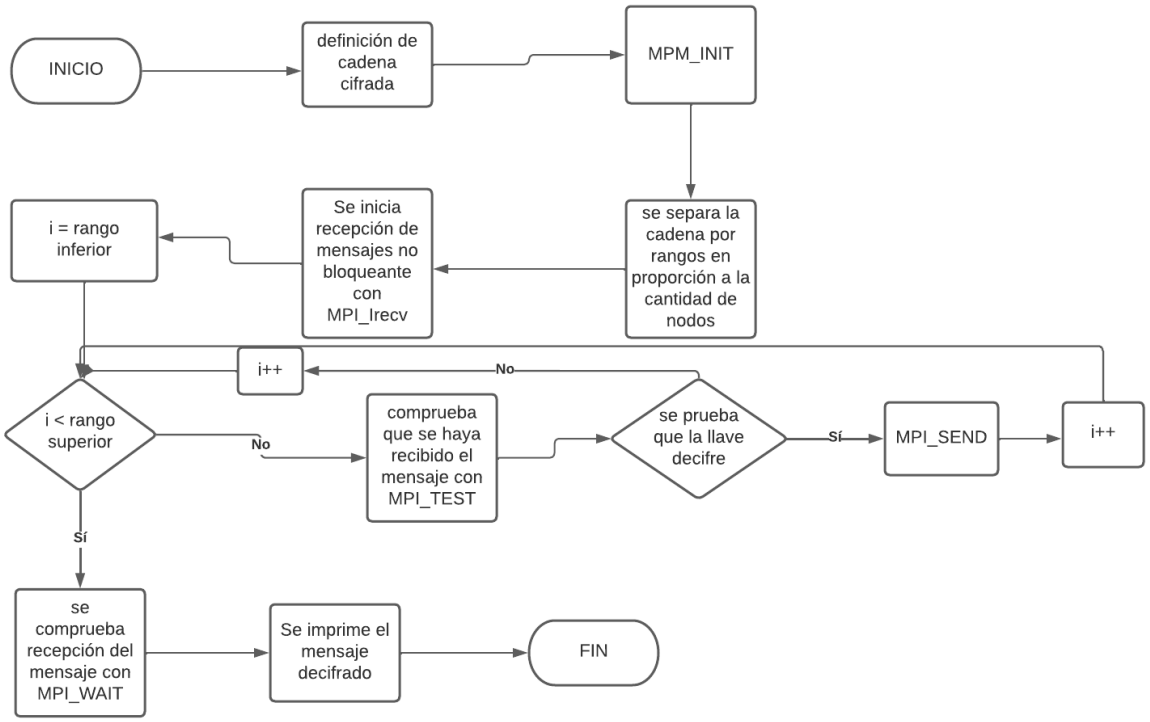
Proyecto # 2

29/04/2022
Augusto Alonso #181085
Esteban Cabrera #17781
Mario Sarmientos #17055

DES

DES o Data Encryption Standard es un algoritmo de cifrado simétrico, es un prototipo del cifrado por bloques. Se basa en la estructura de red de Feistel que tiene 16 rondas. Utiliza una clave criptográfica para modificar la transformación, así el descifrado se realiza solo para quienes tienen la clave.

Diagrama de flujo



Una vez funcionando su programa base, explique mediante diagramas como funcionan las rutinas:

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

Decrypt es un método que recibe la llave a utilizar, el mensaje cifrado como siguiente parámetro y por último, la longitud de la cadena recibida. Su función es desencriptar un mensaje.

Ecrypt es un método que recibe la llave a utilizar, el mensaje cifrado como siguiente parámetro y por último, la longitud de la cadena recibida. Su función es encriptar un mensaje.

b. tryKey (key, *ciph, len)

Recibe la llave, el mensaje cifrado y la longitud del mensaje. Prueba si la llave es válida para poder descifrar el mensaje.

c. memcpy

Copia los valores de num bytes desde la ubicación a la que apunta el origen directamente al bloque de memoria al que apunta el destino. El resultado es una copia binaria de los datos.

d. strstr

Devuelve un puntero a la primera aparición de str2 en str1, o un puntero nulo si str2 no forma parte de str1. El proceso de coincidencia no incluye los caracteres nulos finales, pero se detiene ahí.

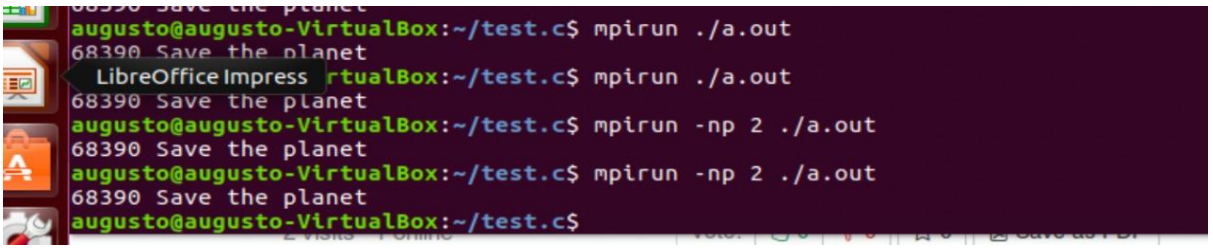
Describa el uso y flujo de comunicación de las primitivas de MPI:

a. 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.
b. 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.
c. MPI_Wait: Este método bloquea el proceso que lo invoca hasta que la operación indicada en request se complete.

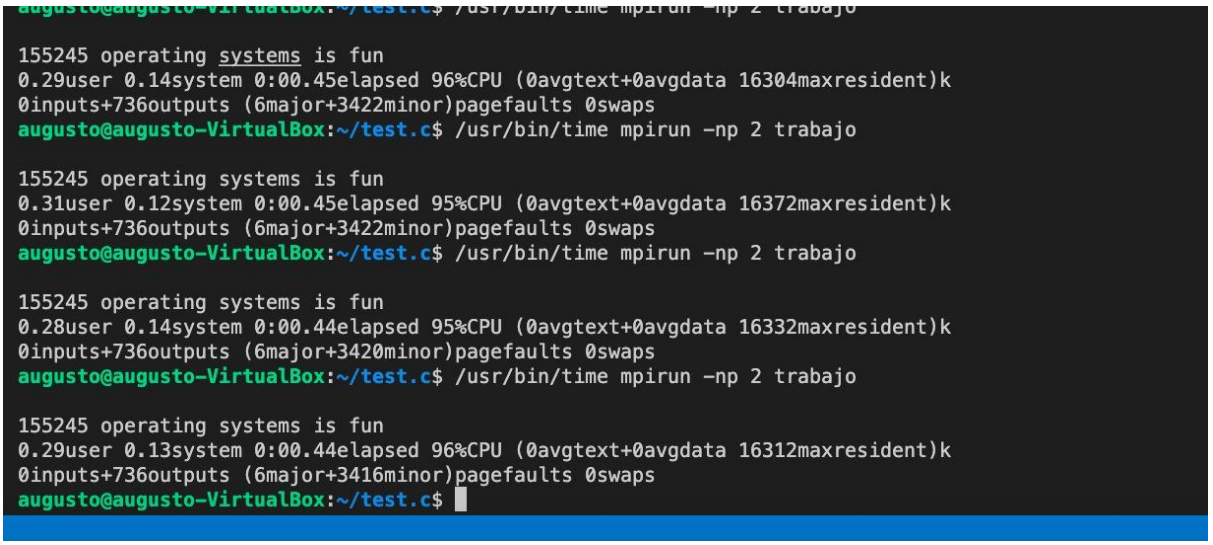
Cronograma de actividades

Día / Task	Implementacion de MPI	Paralelizacion en los metodos	Mediciones de tiempos nuevos	Pruebas de cifrado y decifrado	Trabajo en documento	Trabajo en documento
lunes						
martes						
miércoles						
jueves						
viernes						

Ejecución del programa (y mediciones)



Promedio de tiempo de ejecución


augusto@augusto-VirtualBox:~/test.c$ /usr/bin/time mpirun -np 2 trabajo
155245 operating systems is fun
0.29user 0.14system 0:00.45elapsed 96%CPU (0avgtext+0avgdata 16304maxresident)k
0inputs+736outputs (6major+3422minor)pagefaults 0swaps
augusto@augusto-VirtualBox:~/test.c$ /usr/bin/time mpirun -np 2 trabajo
155245 operating systems is fun
0.31user 0.12system 0:00.45elapsed 95%CPU (0avgtext+0avgdata 16372maxresident)k
0inputs+736outputs (6major+3422minor)pagefaults 0swaps
augusto@augusto-VirtualBox:~/test.c$ /usr/bin/time mpirun -np 2 trabajo
155245 operating systems is fun
0.28user 0.14system 0:00.44elapsed 95%CPU (0avgtext+0avgdata 16332maxresident)k
0inputs+736outputs (6major+3420minor)pagefaults 0swaps
augusto@augusto-VirtualBox:~/test.c$ /usr/bin/time mpirun -np 2 trabajo
155245 operating systems is fun
0.29user 0.13system 0:00.44elapsed 96%CPU (0avgtext+0avgdata 16312maxresident)k
0inputs+736outputs (6major+3416minor)pagefaults 0swaps
augusto@augusto-VirtualBox:~/test.c$