Programación Concurrente — Trabajo Final — 2012

Maximiliano A. Eschoyez

Resumen

El objetivo de este Trabajo Final es realizar un software para quebrar una encriptación realizada con uno de los siguientes algoritmos: *Blowfish*, *Cast5*. Se deberá implementar el sistema utilizando la *Interfaz de Paso de Mensajes — MPI* y la interfaz de hilos paralelos *OpenMP* para dismimuir el tiempo de ejecución. Además, se debe realizar una serie de mediciones de tiempo de ejecución para comparar el programa secuencial, el comportamiento del programa paralelizado con múltiples hilos y con múltiples procesos en un cluster.

Consigna

En este trabajo se debe desarrollar un programa basado en la biblioteca OpenMP y otro en MPI para encontrar el mensaje oculto en el archivo provisto por el profesor. Las claves a utilizar deben ser números enteros de hasta 16 cifras. Esto se debe a que el algoritmo *Blowfish* (cbc) y *Cast5* con los cuales se generaron los mensajes utilizan claves de 64 bits (16 bytes). El motivo de utilizar sólo números enteros es para reducir el espacio de claves posibles y obtener una respuesta en un tiempo razonable.

El objetivo es dividir el espacio de claves posibles entre todos los procesos que se vayan a ejecutar. De esta forma, la cantidad de procesos dependerá de los recursos disponibles o la configuración de inicio, y cada proceso buscará sólo en el rango que le corresponde. Esta forma de búsqueda de la clave utilizada para la encriptación se llama *decodificación por fuerza bruta*.

La encriptación del mensaje se realizó mediante la utilización de la biblioteca *crypto* del paquete de software OpenSSL (`http://www.openssl.org/`). La clave utilizada debe ser siempre de 16 bytes conocidos, sino el software no funcionará correctamente. Los mensajes a decodificar están encriptados con una clave consistente en un número natural alineado a la derecha, el resto de los caracteres son espacios en blanco. En particular, las claves utilizadas serán de 8 caracteres.

El docente proveerá a cada estudiante de mensajes que debe decodificar. La único que se sabe de antemano es que todos los mensajes comienzan con la palabra “Frase”, tal como está escrita: primera letra en mayúsculas y el resto en minúsculas. Se deberá determinar la clave, la frase encriptada y el algoritmo utilizado.

Una vez terminado el desarrollo del software se deberán realizar mediciones de tiempo para diversa cantidad de procesos/hilos en paralelo. Los resultados obtenidos deberán graficarse a modo de comparación.

Notas: Utilizar la interfaz EVP que provee OpenSSL y como vector de inicialización

```
unsigned char iv[] = {1,2,3,4,5,6,7,8};
```

Presentación del Trabajo Final

Grupos de Trabajo

El trabajo se podrá presentar en forma individual o en grupo de dos integrantes, prefiriéndose la modalidad grupal).

Código Fuente

El código fuente y la versión digital del informe en PDF deben entregarse a través del enlace correspondiente en el Aula Virtual del curso (`http://lms.ubp.edu.ar/`). En dicho enlace se deberá subir un único archivo en formato ZIP conteniendo todos los código fuente que se requieran para la realización del trabajo final.

Informe Escrito

Se entregará al profesor un informe escrito en versión digital donde se debe describir la problemática abordada en el trabajo final, el desarrollo de la solución propuesta, los resultados de las mediciones de tiempo y una conclusión. El texto deberá ser conciso y con descripciones apropiadas. No se debe incluir el código fuente, sino los textos necesarios realizar las explicaciones pertinentes. El formato de entrega es PDF.