UNIVERSIDAD DEL VALLE DE GUATEMALA
Computación Paralela y Distribuida
Ing. Juan Jose Celada

Proyecto no. 2
Programación Paralela con MPI

Maria Isabel Ortiz Naranjo 18176

GUATEMALA, 13 de mayo de 2022

I. Antecedentes

DES

DES (Data Encryption Standard) es un esquema de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de ordenadores.

Estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fue sometido a las leyes de USA.

Posteriormente se sacó una versión de DES implementada por hardware, que entró a formar parte de los estándares de la ISO con el nombre de DEA.

Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

Como la clave efectiva es de 56 bits, son posible un total de 2 elevado a 56 = 72.057.594.037.927.936 claves posibles, es decir, unos 72.000 billones de claves, por lo que la ruptura del sistema por fuerza bruta o diccionario es sumamente improbable, aunque no imposible si se dispone de suerte y una gran potencia de cálculo.

Actualmente DES ya no es estándar y fueron en Enero de 1999 con un poder de cómputo que efectuaba aproximadamente 250 mil millones de ensayos en un segundo.

- Los principales inconvenientes que presenta DES son:

  Se considera un secreto nacional de EEUU, por lo que está protegido por leyes específicas, y no se puede comercializar ni en hardware ni en software fuera de ese país sin permiso específico del Departamento de Estado.

La clave es corta, tanto que no asegura una fortaleza adecuada. Hasta ahora había resultado suficiente, y nunca había sido roto el sistema. Pero con la potencia de cálculo actual y venidera de los computadores y con el trabajo en equipo por Internet se cree que se puede violar el algoritmo, como ya ha ocurrido una vez, aunque eso sí, en un plazo de tiempo que no resultó peligroso para la información cifrada.

No permite longitud de clave variable, con lo que sus posibilidades de configuración son muy limitadas, además de permitirse con ello la creación de limitaciones legales.

La seguridad del sistema se ve reducida considerablemente si se conoce un número suficiente textos elegidos, ya que existe un sistema matemático, llamado Criptoanálisis Diferencial, que puede en ese caso romper el sistema en 2 elevado a 47 iteraciones.

- Entre sus ventajas cabe citar:

Es el sistema más extendido del mundo, el que más máquinas usan, el más barato y el más probado.

Es muy rápido y fácil de implementar.

Desde su aparición nunca ha sido roto con un sistema práctico.

Pasos a seguir para el algoritmo

1. Expansión de la clave: para que DES pueda utilizar una nueva subclave en cada ronda, derivada por recursión de la primera clave, esta se ha de expandir a una longitud que permita generar el número necesario de subclaves de 128 bits. Así, cada subclave se basa en un fragmento de la clave de salida expandida. El número de subclaves necesarias comprende el número de rondas (R), incluida la ronda final y una subclave para la ronda previa (R + 1).

2. Ronda previa: en la ronda previa el bloque de 128 bits se transpone en una tabla bidimensional o matriz (state) y se une con la primera subclave mediante XOR (Key Addition). La tabla comprende 4 columnas y 4 líneas. Cada casilla contiene 1 byte (8 bits) del bloque que se ha de encriptar.

3. Rondas de cifrado: el número de rondas depende de la longitud de clave utilizada, esto es, 10 rondas en AES128, 12 en AES192 o 14 en AES256. En cada ronda tienen lugar las siguientes operaciones:

SubBytes: se trata de una sustitución alfabética simple, en la cual cada byte del bloque original se sustituye por un equivalente mediante una caja-S.

ShiftRows: en la transformación ShiftRow los bytes de las casillas de la matriz se desplazan cíclicamente hacia la izquierda.

MixColumns: esta transformación contenida en el algoritmo AES consiste en mezclar los datos dentro de las columnas de la tabla. Este paso se basa en un recálculo de cada casilla, para lo cual las columnas se someten a una multiplicación matricial. Los resultados se unen mediante XOR.

KeyAddition: al final de cada ronda se produce una nueva KeyAddition, es decir, una unión con la subclave, que se apoya, como en la etapa inicial, en la unión por XOR del bloque de datos o los bytes de la matriz con la subclave actual.

4. Etapa final: Esta es la última ronda de cifrado que, al contrario que las rondas anteriores, no contiene transformaciones del tipo MixColumns, comprendiendo únicamente las operaciones SubBytes, ShiftRows y KeyAddition. El resultado de esta ronda final es el texto cifrado.

El descifrado de datos encriptados con AES se basa en la inversión del algoritmo, que no solo guarda relación con la secuencia de pasos sino también con las operaciones ShiftRow, MixColumns und SubBytes, que también han de ver invertida su orientación.

II. Fuente de información