Objetivo

Explorar la operación del algoritmo DES mediante el rastreo de la ejecución, mediante el cálculo de una ronda de forma manual, y posteriormente se explora los diferentes modos de uso del cifrado de bloques.

Desarrollo

Junto con este documento encontrará una calculadora DES. Utilice la calculadora DES para cifrar y descifrar bloques de datos de prueba. La calculadora puede generar información de las rondas ejecutadas, con múltiples detalles del cálculo.

Para este taller cada estudiante tendrá tres valores, un texto plano, una clave, y un texto cifrado. Si cifra el texto plano con la clave dada, deberá obtener el texto cifrado dado; de la misma forma, si descifra el texto cifrado con la clave dada, deberá obtener el texto plano. La aplicación de DES permite también obtener detalles del procesamiento y obtiene los resultados para cada una de las rondas del algoritmo.

Parte A: núcleo del cifrador de bloques

La parte inicial del taller consiste en utilizar los valores de texto plano, clave y texto cifrado dados.

a) Cifre el texto plano utilizando la clave dada, identifique los valores de salida de cada ronda. Note que los bits de datos cambian en cada ronda. ¿cuál es el valor de los datos al inicio de la ronda 5?

b) Cambie el bit 10 del texto plano, si es 1 por 0 o si es 0 por 1, asuma que la numeración es de izquierda (MSB) bit 1 a derecha (LSB) bit 64. Cifre este nuevo valor, utilice la salida de los resultados de las rondas y liste en una tabla la cantidad de bits que cambian de una ronda a otra para las primeras diez rondas. Se recomienda convertir de hexadecimal a binario para comparar y contar los bits que cambian.

c) Describa el proceso de DES para encontrar las subclaves de cada ronda.

d) Cambie el bit 20 de la clave, si es 1 por 0 o si es 0 por 1, asuma que la numeración es de izquierda (MSB) bit 1 a derecha (LSB) bit 64. Cifre el valor original, utilice la salida de los resultados de las rondas y liste en una tabla la cantidad de bits que cambian de una ronda a otra para las primeras diez rondas.

e) Describa las características de confusión y difusión de DES, y muestre ejemplos de las características con los datos del cifrador obtenidos de la calculadora.

Parte B: Ronda del cifrador de bloque

Utilice los datos originales y siga el detalle de las permutaciones, sustituciones, datos y claves de la segunda ronda según el algoritmo y el procedimiento de la calculadora DES. Utilice el valor de los datos y de las subclaves como se muestran en la calculadora DES, y verifique que obtiene los mismos valores como se muestran al inicio de la tercera ronda. Utilice una calculadora científica que le permia trabajar con números en varias bases y ejecutar operaciones lógicas.

En el informe incluya una sección, sección 4, con los detalles de cómo calcula cada uno de los pasos de la segunda ronda, y muestre validez de los resultados de los datos obtenidos versus el resultado de la calculadora DES.

Informe

Escribe un informe con una sección para cda una de las partes mencionadas arriba. El informe debe incluir: 1) abstract en inglés, 2) introducción, 3) desarrollo de la parte A, 4) desarrollo de la parte B, 5) conclusiones y 6) bibliografía. Para la parte A, incluya el detalle registros obtenidos de la calculadora DES, datos, claves, resultados, y los valores iniciales y finales de las rondas. Para la parte B, muestre el detalle de la segunda ronda; adicionalmente, muestre los valores internos. Utilice el formato de informe acordado para el curso. La longitud del documento debe ser 4 páginas máximo, incluyendo tablas, figuras, y bibliografía.

Entrega

Cargue solo un (1) documento en WORD, con el informe, al Teams del curso. El plazo de entrega es el 16 de febrero, antes de las 23:59. Modifica el nombre del archivo, debe ser `<usuario Unisabana>-Tarea02.docx`, por ejemplo: `ferneymallo-Tarea02.docx`.