**Laboratorio 8 - Maria Camila Londoño**

1. **¿Tendría sentido mostrar la representación ASCII del texto cifrado? ¿Por qué?**

Pues podría mostrarse para entendimiento de la persona, pero no es necesario. Basta con tener la llave en hexadecimal y el mensaje también en hexadecimal, para encriptar o desencriptar, y el texto cifrado se puede mostrar en hexa.

1. **¿Cambia en algo el texto cifrado al hacer esta alteración? ¿Por qué?**

Depende de cual byte sea el que se modifique, pues para las llaves cada octavo bit es ignorado, lo que implica que si la posición del numero en hexadecimal es impar (iniciando el conteo desde 0), el ultimo bit que lo compone es ignorado. Entonces si por ejemplo tengo la llave A0A1A2A3A4A5A6A7 y cambio A1 por A2 se altera el texto cifrado con respecto al original, pues al ser el segundo número hexadecimal su ultimo bit es el octavo bit de los 64 que lo componen, lo mismo pasaría si se cambia A3 por A4, A5 por A6, o A7 por A8. En cambio, sí se modifica A0, A2, A4 o A6 no se altera el mensaje, pues los cuatro bits que componen al número hexa no contienen a un bit con posición divisible entre ocho.

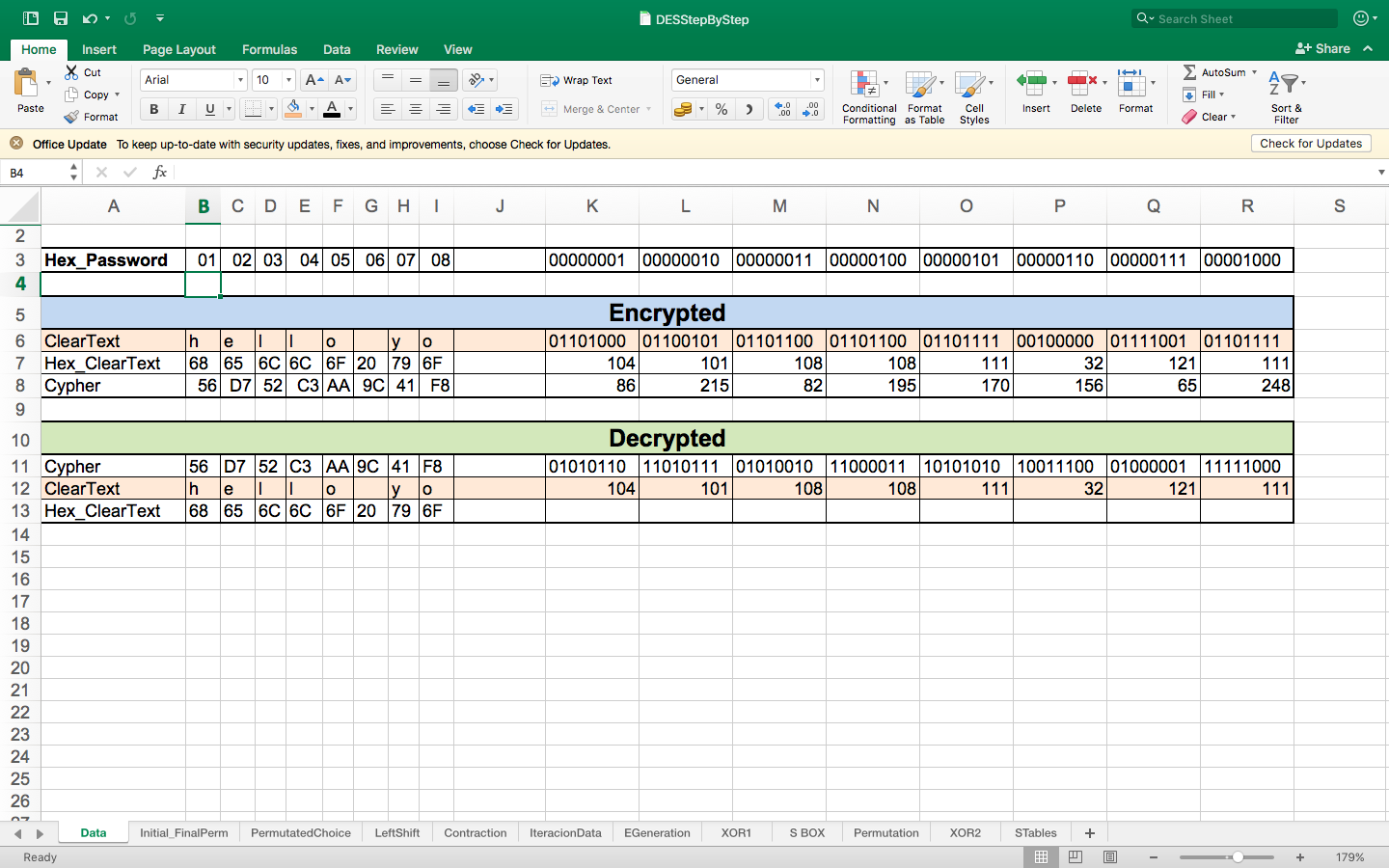
1. **¿Tiene esto alguna relación con el hecho de que la clave de DES sea únicamente de 56 bits?**

Sí, ya que, aunque es una llave de 64 bits al ignorar cada octavo bit terminan siendo realmente 8 bits los que ignoran y por ende una llave de 56.

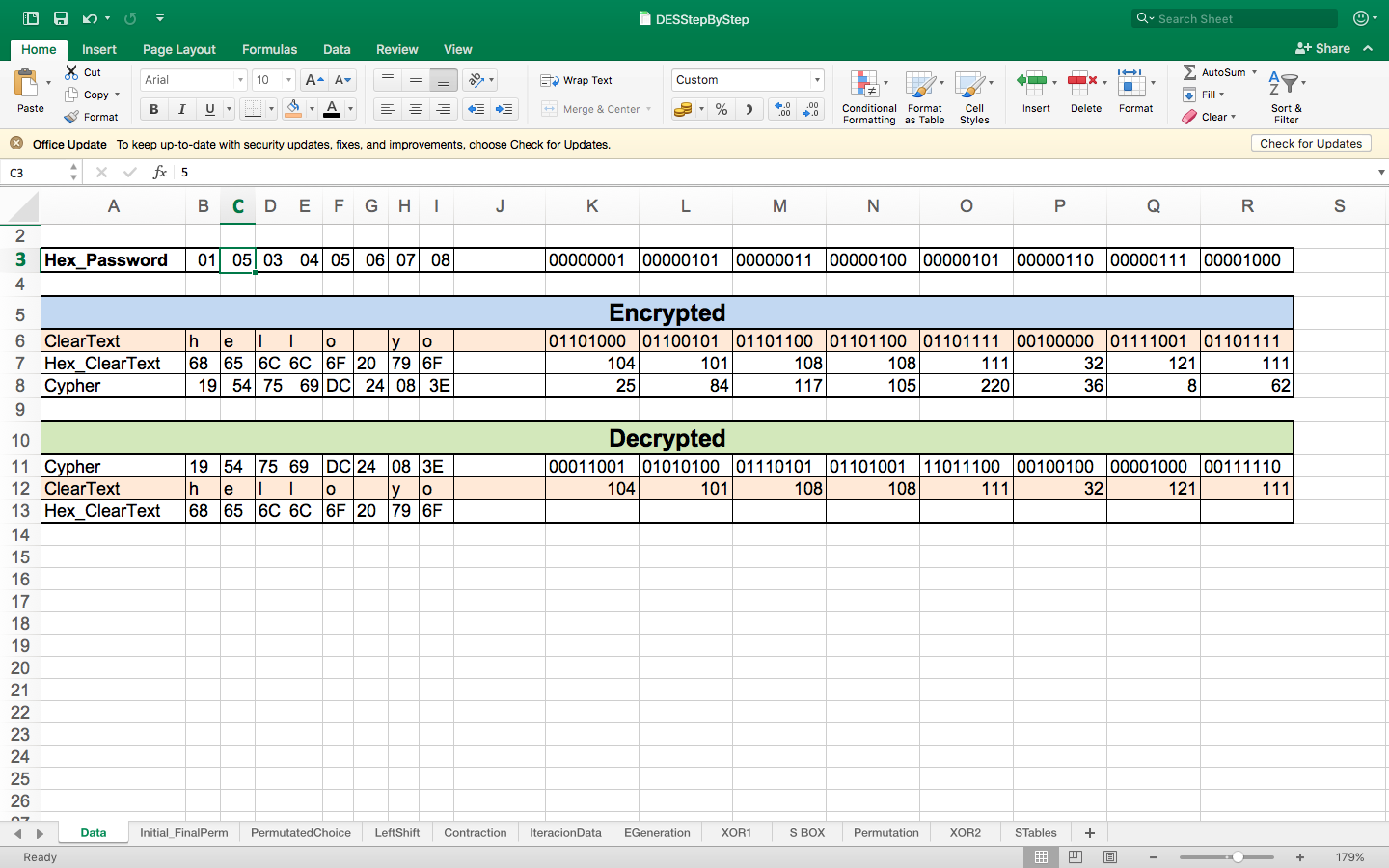
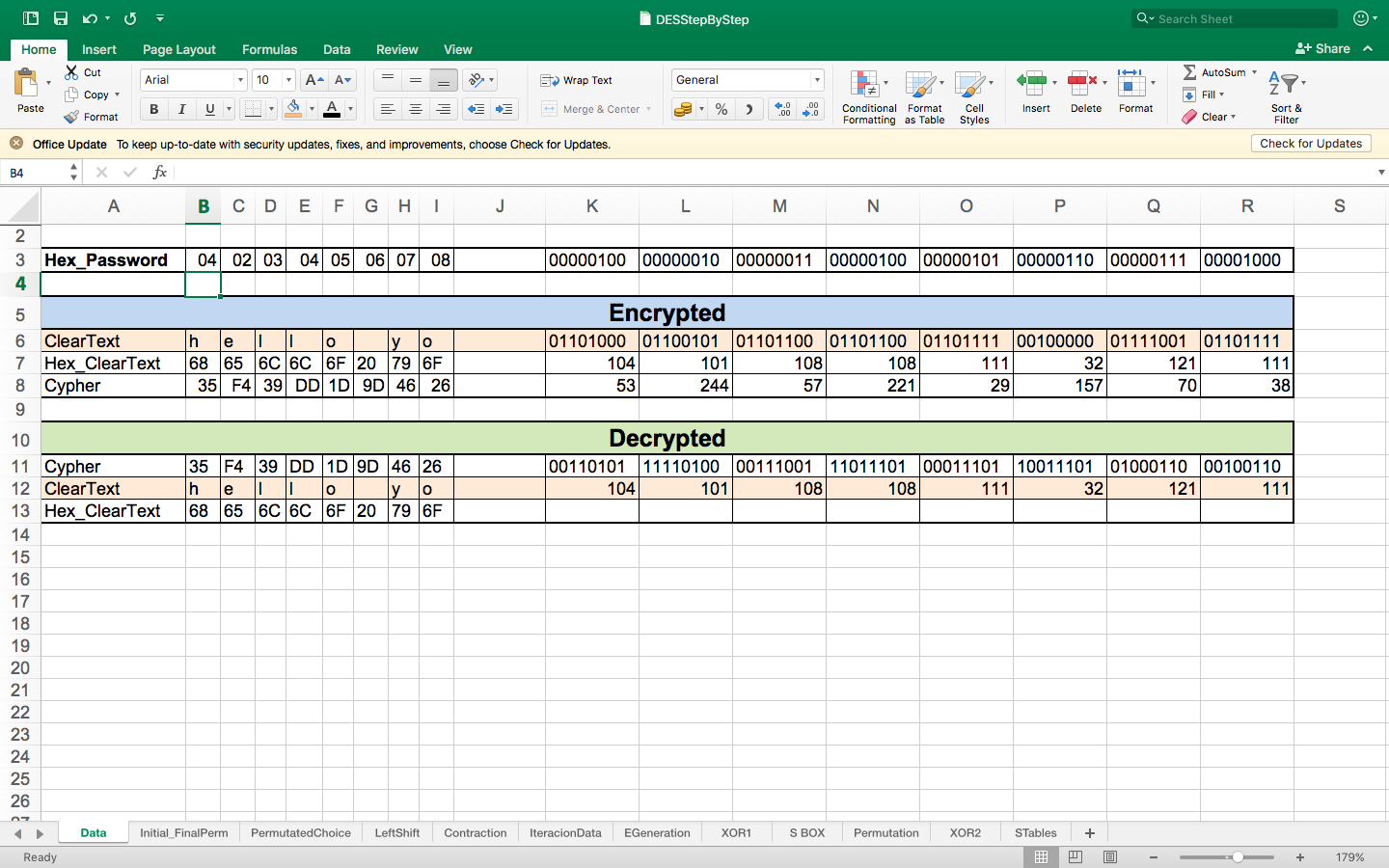
1. **¿Qué sucede? ¿Cuántos bytes del texto cifrado se alteran cuando se cambia un solo bit (que no es el último de algún byte)? Tome algunas capturas de pantalla (screenshots).**

Se alteran todos los bytes del texto

Original:

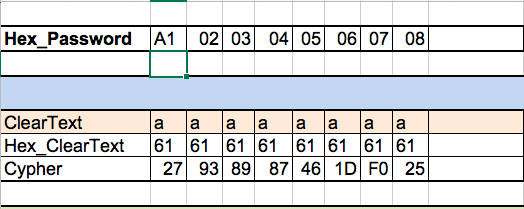
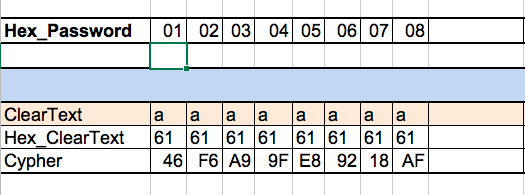
****

Modificando el primer número hexadecimal: Modificando el segundo número hexadecimal:

****

Ej 2 (cambiando de mensaje):

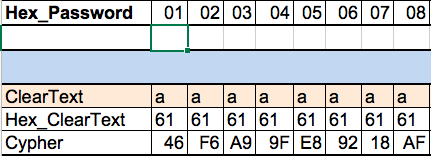
Original:Modificando el primer número hexadecimal:



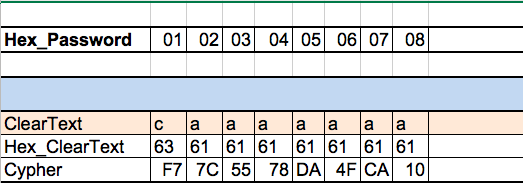
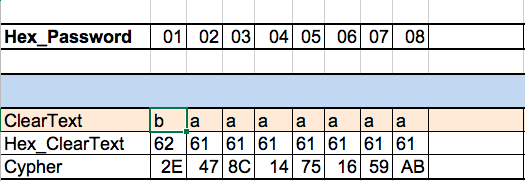
1. **¿Qué sucede? ¿Cuántos bytes del texto cifrado se alteran cuando se cambia un solo bit del texto plano? Tome algunas capturas de pantalla (screenshots).**

Se alteran todos los bytes del texto

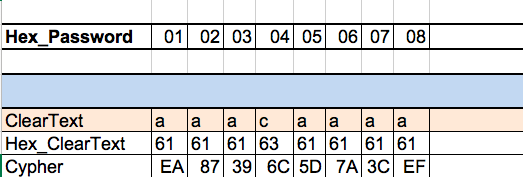
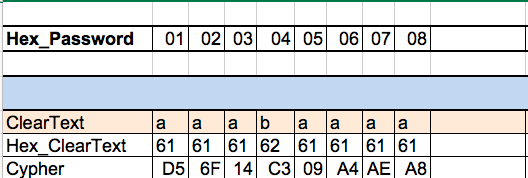
Original:

****

Cambiando el primer byte: Cambiando un bit:

****

Cambiando el otro byte: Cambiando un bit:

****

1. **¿Puede establecer un patrón en la permutación? ¿A qué corresponden los primeros 8 bits? ¿Los segundos? ¿Los demás?**

En el n byte del output queda el n\*2 bit de cada byte del input. (el orden es: el primero de derecha a izquierda del input es el primero izquierda del output)

En el primer byte del output queda el segundo bit de cada byte del input.

En el segundo byte del output queda el cuarto bit de cada byte del input.

En el tercer byte del output queda el sexto bit de cada byte del input.

En el cuarto byte del output queda el octavo bit de cada byte del input.

En los otros 4 bytes se vuelve a inciar n en 1 y cada iteración se van sumando dos al acomulado.

En el quinto byte del output sería 1 + 0 queda el 1 bit de cada byte del input.

En el sexto byte del output sería 1 + 2 queda el 3 bit de cada byte del input.

En el septimo byte del output sería 1 + 4 queda el 5 bit de cada byte del input.

En el octavo byte del output sería 1 + 6 queda el 7 bit de cada byte del input.

Otro patrón es que para el output del primer byte del mensaje: si todo el mensaje son letra se ponen todos los bits en 1. Si hay algún espacio u otro símbolo en vez de una letra se pone un cero en la ubicación que sea contraria del mensaje original, por ejemplo, para a$aaaaaa el signo “$” se encuentra en la segunda posición, entonces en el output el cero ira en la segunda posición de derecha a izquierda es decir 111111101.

Para el output del segundo byte: si todo el mensaje son letras pone todos los bits 0

1. **¿Por qué se dice que estas permutaciones no agregan ningún valor criptográfico? Explique**
2. **Trate de identificar en qué hoja de cálculo está cada uno de los siguientes elementos de la función F (tome screenshots):**
3. **La función de Expansión.**

En la hoja de cálculo llamada “EGeneration”

../../Desktop/Screen%20Shot%202019-04-22%20at%201.41.56%20PM.png

1. **El fragmento de la clave que se escoge en cada ciclo.**

En la hoja de cálculo llamada “Left Shift” **../../Desktop/Screen%20Shot%202019-04-22%20at%208.06.25%20PM.png**

**3. El XOR entre el fragmento de la clave y el resultado de la expansión.**

En la hoja de cálculo llamada “XO-1”

**../../Desktop/Screen%20Shot%202019-04-22%20at%208.08.43%20PM.png**

**4. Las funciones de sustitución**

En la hoja de cálculo llamada “S-Box”

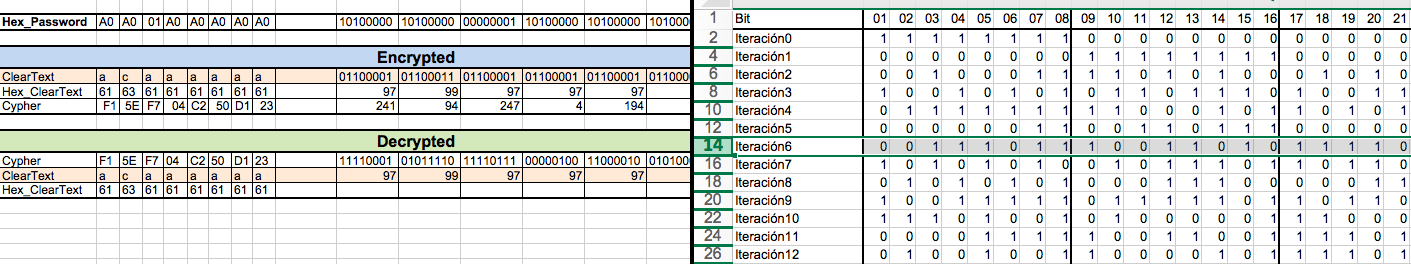
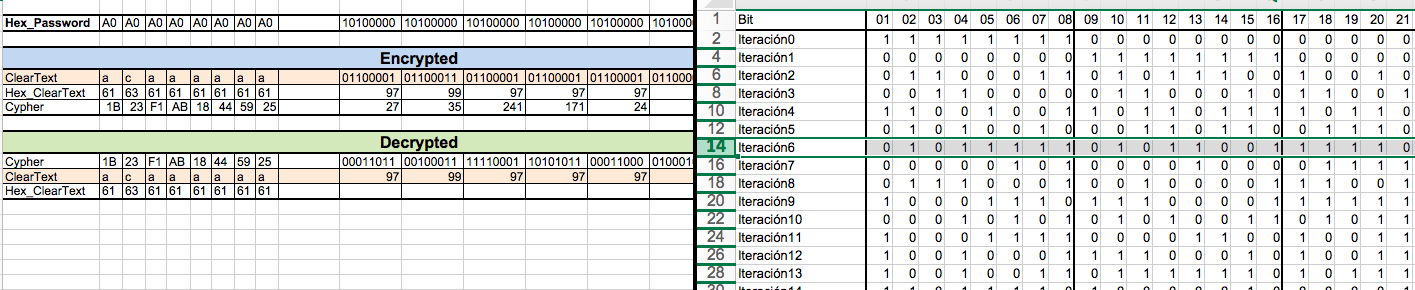
../../Desktop/Screen%20Shot%202019-04-22%20at%208.09.45%20PM.png­­­

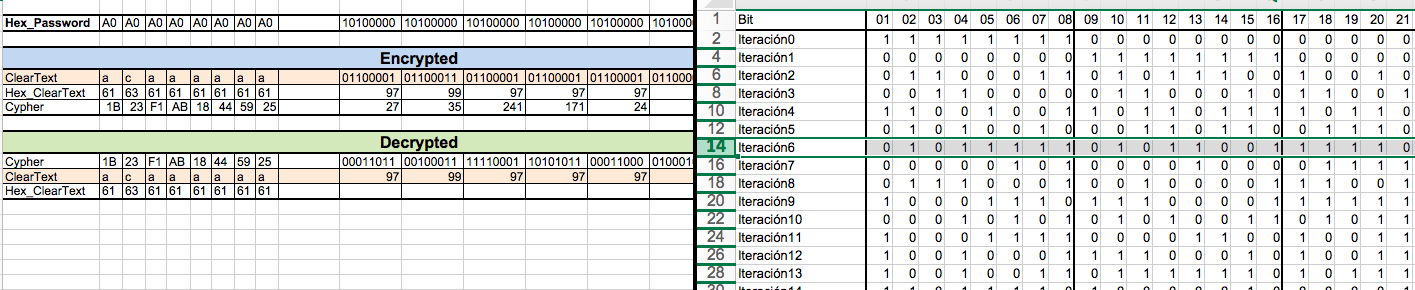
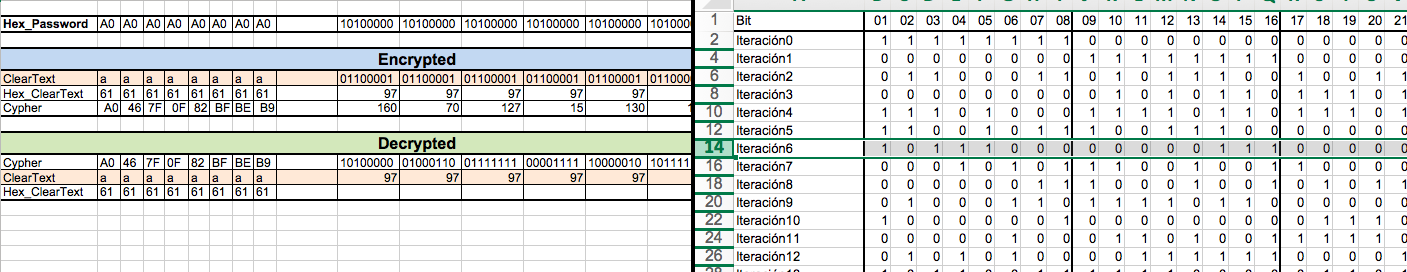
**5. La permutación.**

Permuted choice

**../../Desktop/Screen%20Shot%202019-04-22%20at%208.10.26%20PM.png**

1. **¿Qué sucede con los datos de las iteraciones cuando cambia un bit? ¿Qué tan diferentes son las primeras iteraciones? ¿Qué tan diferentes son las últimas iteraciones? Muestre un par de screenshots con la comparación.**

Paso 4 (cambiando byte de la llave distinto al ultimo)

Paso 5 (cambiando byte del texto y luego bit distinto al ultimo)

Al ejecutar el mismo procedimiento del paso 4 se puede ver que la iteración 6 cambia totalmente al cambiar un byte de la llave, sin embargo, permanece igual durante las dos primeras iteraciones, en la tercera ya se ve cambio. En el paso 5 cambia desde la primera iteración al modificar un byte del mensaje, cuando se modifica aumentando un bit el único cabio que se ve con respecto a la anterior es que hay un corrimiento de bits hacia la izquierda.

1. **Explique qué sucede con las sub-claves de cada iteración. ¿Son iguales? ¿Son diferentes?**

Son diferentes, para cada paso se va generando una nueva clave después de hacer el corrimiento de bits a la izquierda

1. **¿Podría explicar en qué consiste una “clave débil”? ¿Qué otras claves débiles se le ocurren?**

Una clave débil es cuando se usa una clave que hace que el algoritmo funcione de formas distintas a las esperadas, por ejemplo, si toda la clave son ceros o unos es una clave débil, ya que, al hacer las modificaciones, todos los left shifts van a poner ceros al igual que las contracciones.

1. **¿Qué sucede con las sub-claves de cada iteración al usar claves semi-débiles?**

Dan todas cero en todos los bits

1. **Suponga que un procesador como el de su PC necesita 20 ciclos de procesador para cifrar un bloque de 64 bits con DES. (16 ciclos para cada iteración, 2 ciclos para la**

**permutación inicial, y 2 ciclos para la permutación final). ¿Cuánto demoraría un ataque de fuerza bruta, con un tamaño de clave de 56 bits? Muestre los cálculos usando la velocidad del procesador de su PC.**

1. **Intente explicar por qué este procedimiento funciona para descifrar un archivo. Tenga en cuenta lasiguiente identidad:**

**A XOR A XOR B = B**

Para des encriptar se hace el proceso, pero las subllaves en el orden opuesto, entonces en el momento

Por propiedades de XOR sabemos que A XOR A = 0. Entonces se remplaza por 0 el A XOR A y quedaría 0 XOR B = B. Teniendo en cuenta esto, sabemos que si hacemos el proceso invirtiendo que al hacer los dos XOR se haría primero el de el grupo de 32 bits de la izquierda con la permutación de la derecha después de hacer la sustitución, y luego el XOR de la expansión con la contracción entonces sería aplicar lo mismo pero en otro orden, ya que para A XOR B XOR A, A XOR B = 1 y 1 XOR A = A entonces se iría obteniendo lo contrario a partir de B

1. **Teniendo en cuenta la pregunta anterior. ¿Qué efectos tiene una clave débil sobre las funciones Fi en cada iteración? ¿Qué pasaría si cifráramos un mensaje con una clave**

**débil, y el resultado lo volviéramos a cifrar con la misma clave débil?**

Que los bits resultantes serían cero y que si se cifra dos veces con la clave débil vuelve a generarse el mensaje inicial, por ejemplo, si el mensaje es 6262626262626262 con la llave 0000000000000000 el mensaje encriptado sería 045DCAC6B3DA0AA2 y si 045DCAC6B3DA0AA2 se encripta con la misma llave el mensaje encriptado seria 6262626262626262, pues no habría cambios en las subllaves ni modificaciones en el proceso al tener una llave de solo 1s o 0s o la mitad 1s y la mitad 0s

1. **¿Qué efectos tiene una clave semi-débil sobre las funciones Fi en cada iteración? ¿Qué pasaría si cifráramos un mensaje con una clave semi-débil, y el resultado lo cifráramos con su pareja?**

Las llaves semidébiles son las que solo generan dos llaves distintas como A1F6A1F6A1F6A1F6 que solo sería A1 y F6, y esto afecta en los desplazamientos ya que se ve que de la iteración 2 a la 8 no cambia nada ni de la 9 a la 15… Si lo ciframos dos veces da un mensaje distinto al inicial