Universidad
Carlos III de Madrid

***COSEC LAB** · Dpto. Informática*

Universidad Carlos III de Madrid

Ejercicios de cifrado simétrico. SOLUCIONES - DES

Seguridad en las Tecnologías de la Información
Curso 2016/2017

Cifradores de bloque

Parte I – DES

1. Suponiendo que la clave utilizada en el algoritmo DES es: **10000101 10100100 10001111 10001111 10000101 10100100 10001111 10001111.**

a) Calcular la 1ª clave interna que genera el algoritmo, para cifrar un texto en claro.

b) Calcular L_1 y R_1 partiendo del mensaje en claro siguiente: **10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101010**

Clave inicial:

1-8: 1 0 0 0 0 1 0 1

9-16: 1 0 1 0 0 1 0 0

17-24: 1 0 0 0 1 1 1 1

25-32: 1 0 0 0 1 1 1 1

33-40: 1 0 0 0 0 1 0 1

41-48: 1 0 1 0 0 1 0 0

49-56: 1 0 0 0 1 1 1 1

57-64: 1 0 0 0 1 1 1 1.

Permutación PC-1	Permutación PC-2
57 49	14 17 11

Clave tras la primera permutación PC-1**:**

1	1	1	1	1	1	1
1	0	0	0	0	0	0
0	0	0	0	1	0	0
0	1	0	0	0	0	0
1	1	0	0	1	1	0
0	1	1	1	1	1	1
1	1	1	1	0	0	1
1	0	0	0	0	0	0

2. Desplazamiento a la izquierda de 1 posición en cada mitad.

C0: 1111111 1000000 0000100 0100000

C0 tras el desplazamiento: 1111111 0000000 0001000 1000001

D0: 1100110 0111111 1111001 1000000

D0 tras el desplazamiento: 1001100 1111111 1110011 0000001

3. Segunda permutación PC-2, reduce a 48 bits, siendo el resultado final

000011 110100 000100 010001 100100 010111 111100 010111

b) 1. Realizamos la permutación inicial IP, obteniendo L_0 y R_0

1-8: **10101010**
9-16: **10101010**
17-24: **10101010**
25-32: **10101010**
33-40: **10101010**
41-48: **10101010**
49-56: **10101010**
57-64: **10101010**

Permutación inicial IP:

58 50 42
34 26

L_0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0
R_0	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1

2. Obtenemos la salida de la caja E (expansión) tomando como entrada R_0

Caja E:

```
32   1   2
   3   4   5
```

La salida de la caja E:

111111
111111
111111
111111
111111
111111
111111
111111

3. A continuación combinamos los bits de la caja E o-exclusivo con los bits de la clave interna generada anteriormente, obteniendo los bits de entrada a la caja S.

Subclave	Caja E	Salida de caja E = Entrada a caja S
000011	111111	**111100**
110100	111111	**001011**
000100	111111	**111011**
010001	111111	**101110**
100100	111111	**011011**
010111	111111	**101000**
111100	111111	**000011**
010111	111111	**101000**

4. Obtenemos las salidas de las cajas S

S1: 5 = 0101; S2: 2 = 0010; S3: 5 = 0101; S4: 13 = 1101

S5: 9 = 1001; S6: 2 = 0010; S7: 0 = 0000; S8: 9 = 1001

Luego nos quedará: Salida caja S

0101 0010 0101 1101 1001 0010 0000 1001

5. Obtenemos la caja P

- De 32 bits a 32 bits

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6

Recordatorio: Caja P:

Salida de la Caja P
1110 1101 0010 0001 1001 1000 0100 0010

6. La salida de la caja P se combina o-exclusivo con L_0 y obtenemos R_1:

Caja P
1110 1101 0010 0001 1001 1000 0100 0010

L_0
0000 0000 0000 0000 0000 0000 0000 0000

R_1
1110 1101 0010 0001 1001 1000 0100 0010

7. L_1 se corresponderá con R_0. Por lo tanto quedará:

R_1
1110 1101 0010 0001 1001 1000 0100 0010

L_1 = R_0 (ver paso 1)
1111 1111 1111 1111 1111 1111 1111 1111

2. Se dispone de un cifrador DES en modo CBC donde:

El mensaje a cifrar es M = **10101010 10101010 10101010 10101010 10101010 10101010 10101010 10101010 01010101 01010101 01010101 01010101 01010101 01010101 01010101 01010101**

El valor inicial del registro **C_o=11111111 00000000 11111111 00000000 11111111 00000000 11111111 00000000**

a) Calcule el valor que habrá a la entrada de la caja S, en la primera iteración, teniendo en cuenta que no se realiza la transformación IP y que el valor de la primera clave interna es **k_1= 000000 111111 000000 111111 000000 111111 000000 111111.**

b) Suponiendo que después de realizar el primer cifrado tenemos a la salida del cifrador **C_1= 01010101 01010101 01010101 01010101 01010101 01010101 01010101 01010101**, calcule lo que habrá a la entrada del cifrador, en el cifrado del siguiente bloque.

c) Se envía C_1 a través de una línea de comunicación, produciéndose un error que afecta dos bits de este bloque. Explique razonadamente como afectaría esto al descifrado del mensaje.

a) 1. En primer lugar debemos realizar la suma OR-exclusivo del primer bloque del mensaje con C_o, que resulta $M_1 \oplus C_o$ = 01010101 10101010 01010101 10101010 01010101 10101010 01010101 10101010. Este resultado será la entrada al cifrador.

2. A continuación se distribuye en Lo y Ro

0 1 0 1 0 1 0 1
1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1
1 0 1 0 1 0 1 0 } Lo

0 1 0 1 0 1 0 1
1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1
1 0 1 0 1 0 1 0 } Ro

3. Obtenemos la salida de la caja E a partir de Ro

Salida de Caja E	
0 0 1 0	1 0
1 0 1 0	1 1
1 1 0 1	0 1
0 1 0 1	0 0
0 0 1 0	1 0
1 0 1 0	1 1
1 1 0 1	0 1
0 1 0 1	0 0

4. A continuación combinamos los bits de salida de la caja E o-exclusivo con los bits de la clave interna generada anteriormente, obteniendo los bits de entrada a la caja S.

Clave	Salida de Caja E		Entrada a caja S	
000000	0 0 1 0	1 0	0 0 1 0	1 0
111111	1 0 1 0	1 1	0 1 0 1	0 0
000000	1 1 0 1	0 1	1 1 0 1	0 1
111111	0 1 0 1	0 0	1 0 1 0	1 1
000000	0 0 1 0	1 0	0 0 1 0	1 0
111111	1 0 1 0	1 1	0 1 0 1	0 0
000000	1 1 0 1	0 1	1 1 0 1	0 1
111111	0 1 0 1	0 0	1 0 1 0	1 1

b) Se nos pide el cálculo de $M_2 \oplus C_1$, como los dos bloques son iguales el resultado es 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

c) Ya que $M_i = D(C_i, K) \oplus C_{i-1}$ un error en el bloque C_1 afectará en el descifrado a los bloques M_1 y M_2. $M_1 = D(C_1, K) \oplus C_0$ se verá afectado en gran cantidad de sus bits, con respecto al resultado que debía de salir si C_1 hubiera llegado correctamente, debido al efecto avalancha que se produce en el DES. $M_2 = D(C_2, K) \oplus C_1$ se verá afectado en dos bits, en las posiciones de los dos bits erróneos de C_1

3. Si supiéramos que la clave que un usuario usa en el algoritmo de cifrado DES está compuesta por ocho letras del alfabeto (26 letras), y tomando que el tiempo de cálculo necesario para, haciendo una búsqueda exhaustiva, probar una clave es 1 microsegundo. Se pide:

a) Calcular el tiempo necesario para romper un criptograma.

b) Calcularlo también para el caso que el alfabeto sea alfanumérico.

SOLUCIÓN:

a.- El problema se reduce a calcular las variaciones con repetición de 26 elementos tomados de 8 en 8. Esto es 26^8 = 208827064576 microsegundos, o lo que es lo mismo 2,41 días.

b.- El problema se reduce a calcular las variaciones con repetición de 36 (26 + 10) elementos tomados de 8 en 8. Esto es 36^8 = 2821109907456 microsegundos, o lo que es lo mismo 32,65 días.