Cifrado en bloques. El DES (Data Encryption Standard)

Félix Delgado - Ana Núñez

Universidad de Valladolid

Curso 2020 - 2021

Métodos de cifrado en bloques

La mayoría de los métodos clásicos que hemos comentado son métodos de cifrado en bloques. Ahora veremos, ya desde un punto de vista matemático y más sistemático, algunos métodos más.

En un cifrado en bloques de tamaño k (k-bloques), el mensaje original M se divide en *bloques* de tamaño fijo k, es decir,
$M = m_1, \ldots, m_n = M_1, \ldots, M_r$, siendo $M_1 = m_1, \ldots, m_k$,
$M_2 = m_{k+1}, m_{k+2}, \ldots, m_{2k}$, ... :

$$M_i = m_{(i-1)k+1}, m_{(i-1)k+2}, \ldots, m_{ik} \quad (1 \leq i \leq \lfloor r/k \rfloor)$$

El cifrado monoalfabético es el caso particular más simple, con bloques de longitud 1.

Supondremos que el alfabeto $\mathcal{A} = \mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$. Los mensajes M son elementos de $\mathcal{A}^*$. Los k-bloques son por tanto elementos de $(\mathbb{Z}/N\mathbb{Z})^k$ y los denotaremos como vectores.

Cifrado matricial (Hill)

Clave:

Una matriz cuadrada C de tamaño k, con coeficientes en $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ y que sea invertible (es decir con la condición de que su determinante sea una unidad del anillo $\mathbb{Z}_N$).

Cifrado:

El bloque $\underline{z} = (z_1, \ldots, z_k) \in (\mathbb{Z}_N)^k$ se cifra entonces mediante $c(z) = \underline{z}C$.
El mensaje M se cifra mediante $c(M) = c(M_1) \cdots c(M_r)$.

Descifrado:

El destinatario del mensaje conoce C, puede por tanto calcular su inversa, C^{-1}, y descifra el bloque $\underline{w} \in (\mathbb{Z}_N)^k$ mediante $d(\underline{w}) = \underline{w}C^{-1}$.

Cifrado afín

Clave:

Consiste en un par $(C, \underline{x})$, donde C es una matriz inversible $k \times k$ en $\mathbb{Z}_N$ y $\underline{x} \in (\mathbb{Z}_N)^k$.

Cifrado:

Para un bloque $\underline{z} \in (\mathbb{Z}_N)^k$ es:

$$\underline{z} \mapsto c(\underline{z}) = \underline{z}C + \underline{x}$$

Descifrado:

Para un bloque $\underline{w} \in (\mathbb{Z}_N)^k$:

$$\underline{w} \mapsto d(\underline{w}) = (\underline{w} - \underline{x})C^{-1}$$

El cifrado de Vigenère es un caso particular de cifrado afín, donde C es la matriz identidad y $\underline{x}$ es la clave.

Cifrado afín variable

Hay diferentes formas de "complicar" un poco las cosas mediante la implementación en flujo del sistema de bloques. Esto, en general, es un tema que veremos más adelante. Aquí daremos un ejemplo sencillo.

Clave: Una terna $(C, D, \underline{x})$ formada por dos matrices inversibles y $\underline{x} \in (\mathbb{Z}_N)^k$.

Cifrado: El primer bloque se cifra mediante $c(M_1) = M_1 C + \underline{x} D$ y los restantes:

$$c(M_i) = M_i C + M_{i-1} D$$

Para cifrar el bloque i-ésimo también podemos usar el mensaje cifrado anterior, en lugar del propio mensaje M_{i-1}:

Cifrado: $c(M_1) = M_1 C + \underline{x} D$ y los restantes:

$$c(M_i) = M_i C + c(M_{i-1}) D \quad \text{para } i \geq 2$$

Seguridad de los métodos matriciales:

Los cifrados matriciales son muy vulnerables a los ataques a texto claro conocido.

Esto se debe a que si conocemos el cifrado $\underline{w}_1, \ldots, \underline{w}_k$ de k bloques en claro $\underline{z}_1, \ldots, \underline{z}_k$ que sean linealmente independientes podemos determinar la matriz de cifrado resolviendo los k sistemas de ecuaciones con k incógnitas resultantes de plantear:

$$\underline{z}_i \begin{pmatrix} X_{11} & \ldots & X_{1k} \\ \vdots & & \vdots \\ X_{k1} & \ldots & X_{kk} \end{pmatrix} = \underline{w}_i$$

Para el cifrado afín son necesarios $k+1$ bloques en claro y sus correspondientes cifrados.

• Los métodos de cifrado en bloque se se usan hoy en día son bastante más complicados. En general, cada bloque se cifra usando varias iteraciones de una mezcla de cifrados de sustitución y trasposición.

• Habitualmente también se incluyen técnicas de difusión o propagación cuyo efecto es que la alteración de unos pocos caracteres (por ejemplo un sólo bit) se propaga, provocando una alteración muy grande en el mensaje cifrado. Esta técnica evita el éxito de técnicas criptográficas basados el seguimiento de introducir pequeñas alteraciones.

• Además cualquier método de cifrado tiene que incluir alguna operación no lineal. De no ser así siempre son frágiles ante criptoanálisis lineales como los descritos.

Vamos a comentar dos de ellos que han sido o son estándares en la transmisión de mensajes:

- DES (Data Encryption System)
- AES (Advanced Encryption Standard)

El DES

El sistema de cifrado DES (*Data Encryption System*) fue adoptado en 1977 por el National Bureau of Standards como estándar federal en los Estados Unidos para aplicaciones no clasificadas.

Es una extensión de un sistema desarrollado por IBM llamado *Lucifer* y utiliza una clave de 56 bits.

Hasta 1998 se ha estando utilizando sistemáticamente, en esa fecha se ha sustituido por el *AES* (*Advanced Encryption Standard*) que utiliza claves de 128 bits que se pueden extender de ser necesario en el futuro hasta los 256.

El DES

A mediados de 1998, se demostró que un ataque por la fuerza bruta a DES era viable, debido a la escasa longitud que emplea en su clave. No obstante, el algoritmo aún no ha demostrado ninguna debilidad grave desde el punto de vista teórico, por lo que su estudio sigue siendo plenamente interesante.

El DES se implementa bien mediante hardware (hay varias compañías que fabricaron microchips para ello), bien mediante software (por ejemplo en los navegadores). Se pueden encontrar varios programas de cifrado con DES en la red.

Elementos básicos

El sistema cifra bloques de información M de 64 bits.

Los elementos básicos del sistema son:

1. Una clave K de 64 bits con ciertas condiciones.
2. 16 subclaves de longitud 48, $K_1, K_2, \ldots, K_{16}$, generadas sucesivamente por la clave original K.
3. Una permutación inicial fija IP, y la permutación final IP^{-1}, ambas de 64 elementos.
4. Para cada subclave de K de 48 bits, una función de "encriptado interno", $f_K : \{0,1\}^{32} \to \{0,1\}^{32}$.

La permutación inicial

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Cifrado

La forma en que se cifra cada bloque M de longitud 64 a partir de estos elementos es la siguiente:

1. Se aplica a M la permutación inicial IP.
2. El resultado se divide justo por la mitad en dos subbloques, $P(M) = (L_0, R_0)$, cada uno de 32 bits.
3. Para $i = 1, \ldots, 16$ se aplica el proceso siguiente:

$$L_i := R_{i-1}$$
$$R_i := L_{i-1} \oplus f_{K_i}(R_{i-1}).$$

4. El resultado final del proceso anterior, (L_{16}, R_{16}) se cambia de orden, y a (R_{16}, L_{16}) se le aplica la permutación IP^{-1}. El resultado de esta operación es el cifrado del bloque M.

Redes de Feistel

El proceso descrito en el tercer paso del proceso anterior que produce un par (R_n, L_n) a partir de (L_0, R_0) y unas claves $K_1, \ldots, K_n$ se denomina *red de Feistel*.

Tiene la propiedad de que si se invierte el proceso, partiendo de (R_n, L_n) y de las claves $K_n, \ldots, K_1$, se obtiene de nuevo (L_0, R_0). Esto es sencillo de comprobar usando inducción en el número n de pasos.

Por lo tanto, el descifrado del DES se realiza igual que el cifrado pero utilizando la sucesión de subclaves en sentido inverso.

La clave

Una clave DES está formada por 64 bits, es decir, es un elemento $K \in \{0,1\}^{64}$.

Debe cumplir la propiedad de que dividiendo K en 8 grupos de 8 bits (es decir, en bytes), la suma de los 8 bits de cada grupo es impar, es decir, $\sum_{i=1}^{8} b_{8k+i} = 1 \mod 2$ para $k = 0, \ldots, 7$.

Por tanto, en cada byte 7 de los bits determinan el octavo (*bit de paridad*), y en una clave DES hay en realidad 56 bits significativos, el resto sirven para detectar errores.

Generación de las subclaves

Se consideran las funciones $PC1 : \{0,1\}^{64} \to \{0,1\}^{28} \times \{0,1\}^{28}$ y $PC2 : \{0,1\}^{28} \times \{0,1\}^{28} \to \{0,1\}^{48}$ dadas por

$PC1$						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

$PC2$					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Generación de las subclaves

Es decir, $PC1$ transforma una sucesión de 64 bits, $k = k_1, \ldots, k_{64}$, en dos bloques de 28 bits, (C, D), donde $C = k_{57}k_{49}k_{41}\ldots k_{36}$ y $D = k_{63}k_{55}k_{47}\ldots k_4$. La función $PC2$ transforma de igual manera un par de bloques de 28 bits en uno de 48.
El proceso de generación de las subclaves a a partir de la clave K es el siguiente:

1. Se calculan $(C_0, D_0) = PC1(K)$.
2. Para $1 \leq i \leq 16$, se calculan

$$C_i = LS(C_{i-1}) \ , \quad D_i = LS(D_{i-1}) \ , \quad K_i = PC2(C_i, D_i),$$

donde LS es una permutación circular a la izquierda de una posición para $i = 1, 2, 16$ y de dos posiciones para los restantes índices.

La función de encriptado interno

Se consideran una función de expansión $E : \{0,1\}^{32} \to \{0,1\}^{48}$ y una permutación P de $\{0,1\}^{32}$ dadas por

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

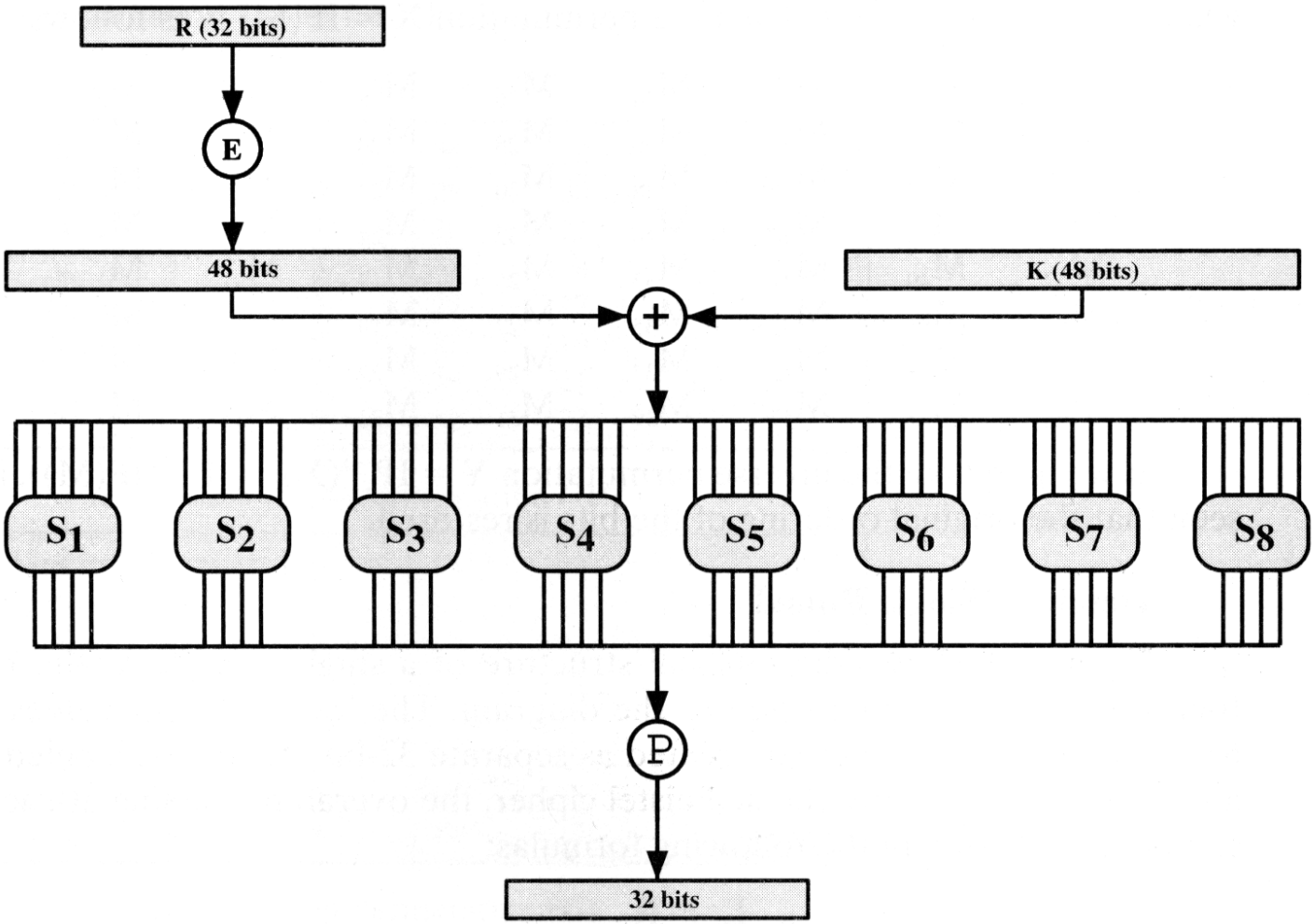
P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

La función de encriptado interno

Para cada subclave K de 48 bits, la función $f_K : \{0,1\}^{32} \to \{0,1\}^{32}$ se define de la siguiente manera:

1. Dado R de 32 bits, se le aplica la función E de expansión y se suma con XOR el resultado a K, $E(R) \oplus K$.
2. El resultado se divide en 8 bloques de 6 bits $E(R) \oplus K = B_1, \ldots, B_8$.
3. Se usan las **S-cajas** $S_i : \{0,1\}^6 \to \{0,1\}^4$, $1 \leq i \leq 8$, para cifrar los bloques, $C_i = S_i(B_i)$.
4. A los 32 bits obtenidos, $C = C_1 \ldots C_8$, se le aplica P. El resultado es $f_K(R)$.

Esquema del encriptado interno



Las S-cajas

Las cajas S_i, $i = 1, \ldots, 8$ son una de las razones de la robustez del método.

Cada una de ellas, S, es una tabla de doble entrada formada por 16 columnas (numeradas en binario $0000, 0001, \ldots$) y 4 filas (numeradas $00, 01, 10, 11$). Cada fila de la tabla contiene una permutación de los enteros $0, 1, \ldots, 15$.
Si el bloque de entrada es $b = (b_6 b_5 \ldots b_1)$, la salida $S(b)$ viene dada por la representación binaria del entero que corresponde a la fila $b_6 b_1$ y la columna $b_5 b_4 b_3 b_2$.

Se pueden encontrar todos los valores de estas tablas en los libros especializados o en la red.

	S[4]															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

$S[4] : (x_0, x_1, x_2, x_3, x_4, x_5) \rightarrow (y_0, y_1, y_2, y_3)$

$(1, 0, 1, 0, 1, 1)$: row 3, column 5, $S[4](1, 0, 1, 0, 1, 1) = 14 = (1, 1, 1, 0)$

S6		Middle 4 bits of input															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Criptoanálisis

El criptoanálisis del DES se ha realizado de varias maneras, algunas más eficaces que otras. Desde el sistema de fuerza bruta (probando todas las claves posibles) hasta métodos bastante elaborados basados casi todos ellos en ataques con grandes cantidades de texto a texto claro elegido (criptoanálisis diferencial –Biham y Shamir– y lineal –Matsui–).

En Enero de 1997, durante la conferencia anual de la compañía RSA, se ofreció un premio de 100.000 dólares por romper el DES. El reto se llevó a cabo con éxito el 17 de Junio de 1997 mediante 75.000 ordenadores coordinados por Internet que consiguieron romper el sistema después de explorar aproximadamente un 25% de las claves posibles (aproximadamente $17 \cdot 10^{15}$).