# DES

*José Galaviz*

# Horst Feistel

- Inmigrante alemán llegado a EEUU en 1932
- Después de muchos intentos losgra trabajar en criptografía.
- IBM TJ Watson Research Lab, 1967.
- Lucifer

# Lucifer

- Red de Feistel:
  - Cifrado de bloque.
  - El bloque se  divide en 2 partes que sontratadas de manera diferente.
  - Funciona por rondas.
- 128 bits de clave (aunque sólo se usan 112 porque el octavo bit de cada bytes es de verificación de paridad) y de tamaño de bloque de cifrado.
- Basado en un concepto llamado Caja-S (caja de substitución).

# Convocatoria del NBS

National Bureau of Standards hoy National Institute of Standards and Technology (NIST) lanza una convocatoria en 1973 (segunda en 1974) para propuestas de algoritmo criptográfico..

- Alto nivel de seguridad.
- Completamente especificado y fácil de entender.
- La seguridad debe residir en la clave, no en mantener el algoritmo en secreto.
- Debe poder ponerse a disposición del pblico sin restricciones.

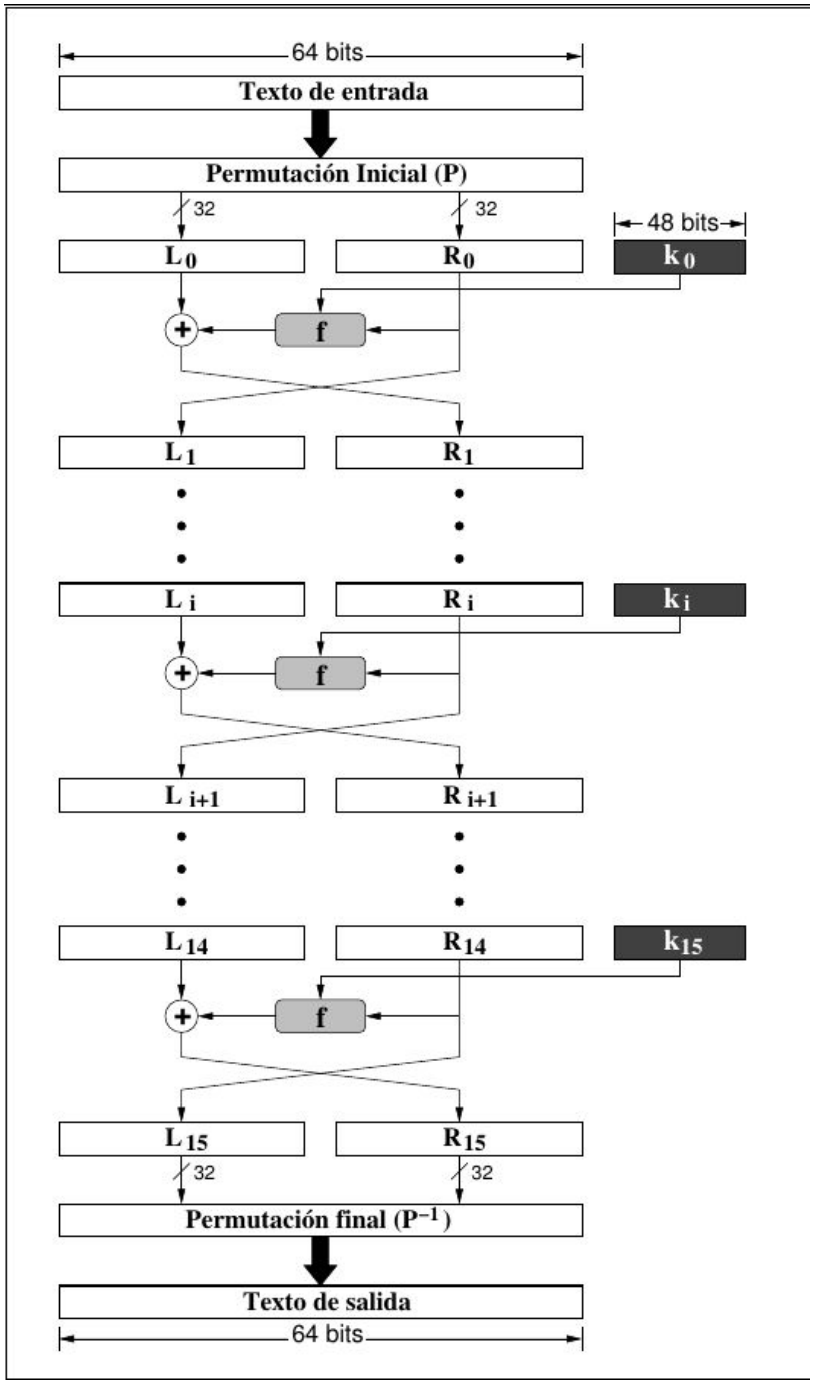
En la segunda convocatoria se presentó Lucifer

# NSA

La National Security Agency evalúa a los candidatos y emite recomendaciones.

- Se reduce el tamaño de clave y de bloque a 64 bits.
- Se cambia la función alambrada en las Cajas-S
- Se convierte en estándar para cifrado de datos que no comprometan la seguridad nacional en 1976 y se mantiene hasta 2002.

# DES


64 bits
Texto de entrada
Permutación Inicial (P)
32
32
48 bits
L0
R0
k0
f
L1
R1
Li
Ri
ki
f
Li+1
Ri+1
L14
R14
k15
f
L15
R15
32
32
Permutación final (P−1)
Texto de salida
64 bits

# DES Permutación inicial

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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 |

# Ecuaciones de DES

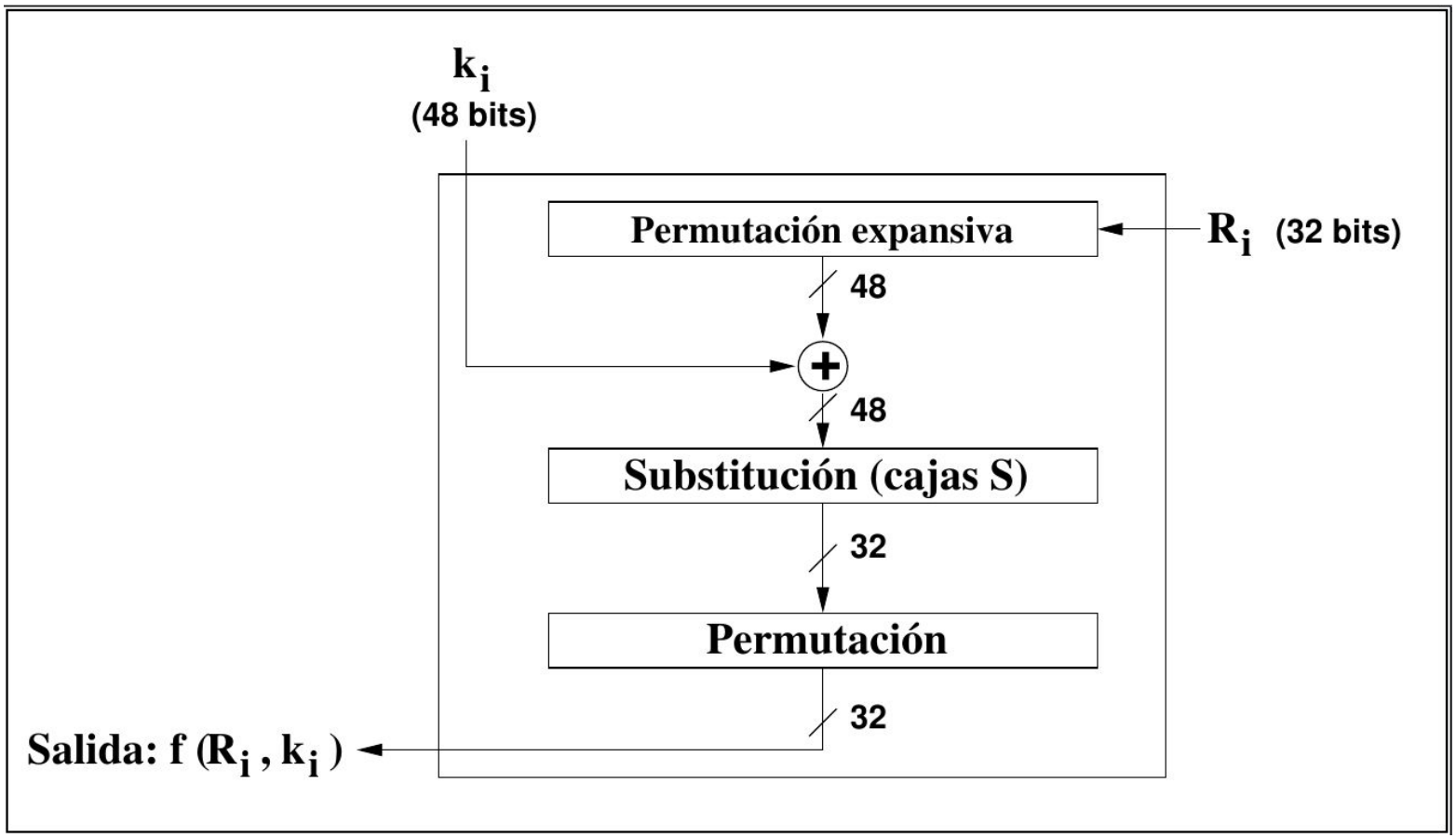
En el diagrama es claro que:

$$L_{i+1} = R_i$$

$$R_{i+1} = L_I \oplus f(R_i, k_i)$$

# La función criptográfica

La función f recibe dos argumentos: la llave de ronda (48 bits) y la parte derecha de la ronda previa (32 bits)



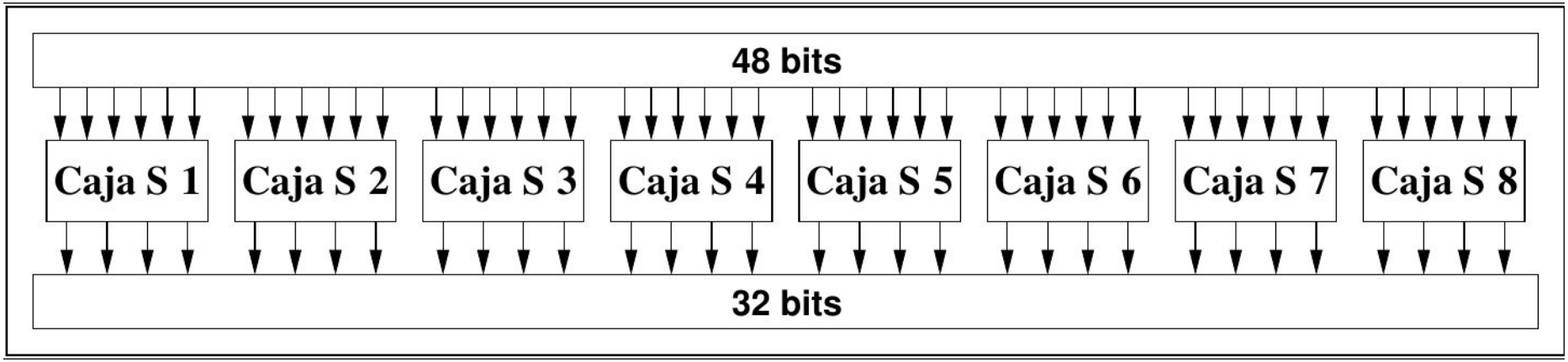
# Permutación expansiva

La permutación expansiva no es, formalmente hablando, una permutación, pero sí altera el orden de los bits y duplica algunos.

| | | | | | |
|---|---|---|---|---|---|
| 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 |

# Substitución

A la salida de la permutación expansiva se le hace un XOR con los 48 bits de la clave de ronda y el resultado de eso se pasa a la etapa de substitución. Cada Caja-S de esta etapa recibe 6 bits y entrega 4.



# Cajas-S

- El primero y el último bit de entrada son el índice de un reglón ( r )  en una matriz.
- Los 4 de enmedio son el índice de una columna ( c ) de esa misma matriz.
- La Caja-S entrega el valor que tiene en la entrada (r,c).

| **Caja** $S_1$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

| **Caja** $S_2$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

| **Caja** $S_3$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

| **Caja** $S_4$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

| **Caja** $S_5$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |

| **Caja** $S_6$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |

| **Caja** $S_7$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |

| **Caja** $S_8$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

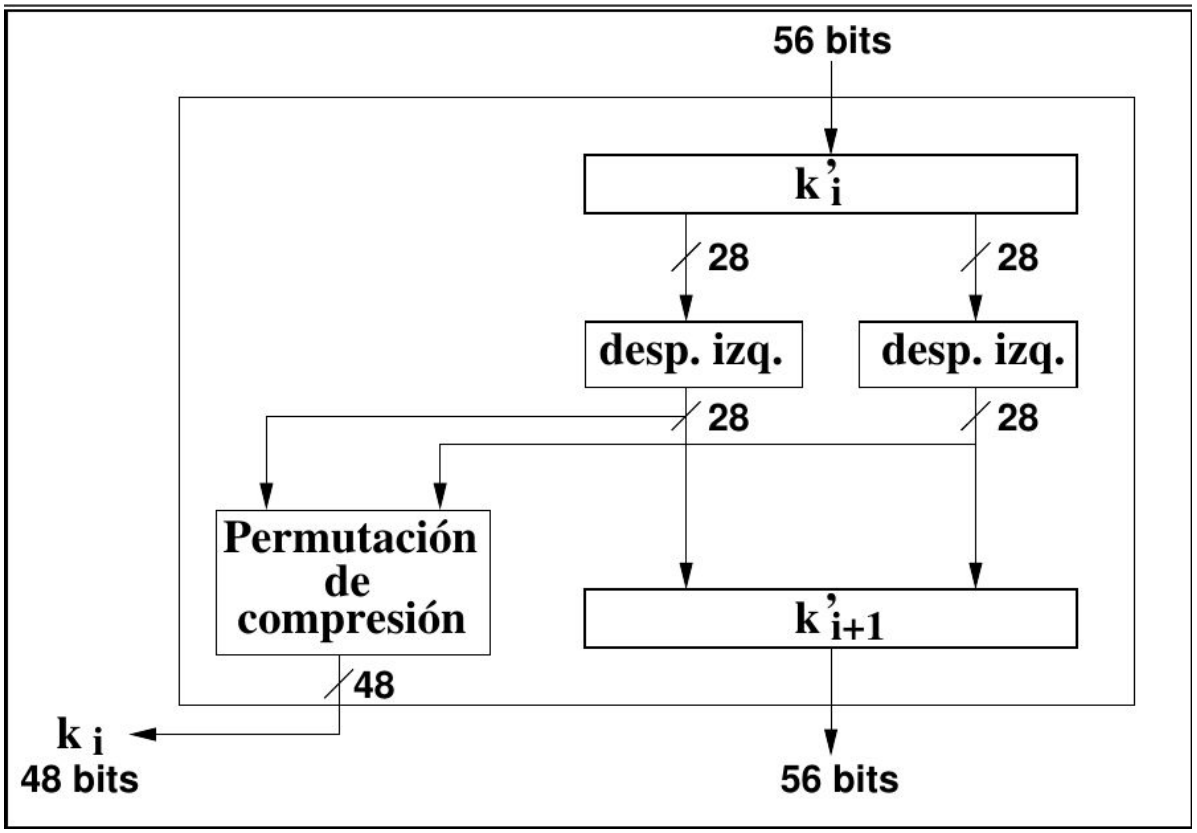
# Permutación

A la salida de la etapa de substitución se le aplica, ahora sí, una permutación de verdad.

| | | | |
|---|---|---|---|
| 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 |

# Planificación de clave (key schedule)

El el algoritmo que genera las claves de ronda a partir de la clave general de entrada.



# Desplazamientos

La mitad izquierda y derecha se rotan un cierto número de bits a la izquierda en función del número de ronda.

| **Ronda** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Desp.** | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

# Permutación de compresión

La salida de los desplazamientos se pasa a una permutación de compresión que, formalmente hablando, nuevamente no es una permutación.

| | | | | | |
|---|---|---|---|---|---|
| 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 |

# Descifrado

Si se introduce a DES un texto cifrado con él, pero invirtiendo las claves de ronda (la 15 entra como la 0, la 14 como la 1, etc.) se obtiene el texto claro.

# 3DES

Una variante de uso de DES que aún se utiliza es “triple DES” o 3DES:

$$E_{K_3}\left(E_{K_2}^{-1}(E_{K_1}(P))\right)$$

Nótese que la aplicación de enmedio es un descifrado ¿por qué?

# Efectos

De acuerdo con la clasificación de Shannon:

- Confusión: Cajas-S
- Difusión: Permutaciones y cambios derecha-izquierda.

Cada bit de salida del texto cifrado es función de TODOS los bits del texto de entrada y de TODOS los bits de la clave.

Un cambio en un bit de entrada, genera cambios en el 50% de los bits de salida.

# Análisis

De acuerdo con eso para fortalecer un esquema de cifrado podríamos hacer:

- Más confusión.
- Más difusión.

Es decir componer las funciones que hacen esas operaciones.

¿Es igual de efectivo?

# Llaves

Piensen en la llave completa y en cómo se generan las llaves de ronda....

¿Pueden construir una llave global para la que sepan en toda ronda, cuál será la llave de esa ronda sin pensar mucho?

# Llaves débiles

En cada ronda siempre entra la misma llave

| Llave con bits de paridad | Llave |
|---|---|
| 0101 0101 0101 0101 | 0000000 0000000 |
| 1F1F 1F1F 0E0E 0E0E | 0000000 FFFFFFF |
| E0E0 E0E0 F1F1 F1F1 | FFFFFFF 0000000 |
| FEFE FEFE FEFE FEFE | FFFFFFF FFFFFFF |

# Y otras menos débiles

- Las débiles son tales que en cada ronda siempre entra la misma llave de ronda en vez de las 16 esperadas.
- Pero el problema se generaliza:
  - Hay llaves que sólo generan dos posibles llaves de ronda.
  - Hay otras que sólo generan 4.
  - Hay otras que sólo generan 8.
- DES tiene problemas con 64 llaves débiles o con algún grado de debilidad, de un total de aprox $72X10^{15}$ llaves.

# Propiedades algebraicas

Un algoritmo de cifrado E es cerrado si y sólo si, para todo mensaje M y llaves K1 y K2, existe K3 tal que:

$$E(K2, E(K1,M)) = E(K3, M)$$

Por ejemplo la sustitución monoalfabética es cerrada.

# ¿DES es un grupo?

En el caso de DES, tenemos la propiedad de que el mismo algoritmo se usa para cifrar y descifrar, así que si fuera cerrado cumpliría todos los requisitos para ser grupo algebraico.

Si lo fuera sería vulnerable a cierto tipo de ataques y no serviría de nada componerlo consigo mismo.

# DES no es un grupo

En 1992 Campbell y Wiener demostraron que DES no es un grupo.