

The Data Encryption Standard DES

- Por más de 30 años ha sido el cifrado cipher más popular
- Ahora se considera inseguro ya que el espacio de llaves es muy pequeño
- Se sigue usando en algunas aplicaciones y más el 3DES que es usar 3 veces seguidas el cifrado
- ¿Por qué estudiarlo?
 - es el cifrado simétrico más estudiado y ha inspirado muchos otros cifrados cipher.

3.1 Introducción a DES

* 1972: Creación de un estándar de cifrado

- + La Oficina Nacional de Estandares de EU (NBS, ahora NIST) lanzó una convocatoria para un estándar de cifrado en EU.
- + Objetivo: encontrar un algoritmo seguro y único para diversas aplicaciones comerciales.

* Contexto previo:

- + La criptografía era considerada un asunto de seguridad nacional y era mantenida en secreto
- + La demanda comercial de usar cifrados, por ejemplo en los bancos, motivó el desarrollo de un estándar abierto

* 1974: Propuesta de IBM

- + IBM presenta un algoritmo basado en Lucifer, un cifrado de bloques desarrollado por Horst Feistel en los 60s.
- + Lucifer opera en bloques de 64 bits con claves de 128 bits.

* Revisión de la NSA:

- + Hasta entonces la NSA era secreta y no admitía su existencia.
- + El NBS solicitó la ayuda de la Agencia de Seguridad Nacional (NSA) para evaluar la propuesta del IBM.
- + La NSA influyó modificando el algoritmo de IBM, se renombró como DES.
- + Se dice que el DES fue diseñado para resistir ataques de criptanálisis diferencial, un ataque no conocido al público hasta 1990.
- + Presentemente, la NSA redujo la longitud de la llave de 128 bits a 56 bits, lo cual aumenta la vulnerabilidad ante ataques de fuerza bruta.

* Preocupaciones sobre la seguridad:

- + Se temía que la NSA incluyera una puerta secreta que permitiera romper el cifrado y que fuera una propiedad matemática que solo conociera la NSA.
- + Hubo críticas a la reducción del tamaño de la llave, argumentando que esto fue debido a que la NSA tenía la habilidad de buscar en el espacio de llaves de 2^{56} y romper así el cifrado por fuerza bruta.

* 1977: Publicación del DES

- + A pesar de las críticas la NBS publicó el estándar como DES (FIPS PUB 46)
- + El diseño fue descrito hasta el nivel de bits, pero nunca se publicaron los criterios de diseño, como la elección de las cajas de sustitución (S-boxes).

* Análisis y adopción:

- + En los 80's, con el aumento de los computadores personales, el DES fue objeto de intenso escrutinio por la comunidad de criptografía civil
- + No se encontraron serias debilidades hasta 1990.

* Estándar temporal y reemplazo:

- + Originalmente el DES fue estandarizado por 10 años hasta 1987.
- + Debido a la falta de seguridad, el NIST reafirmó su uso hasta 1999 y fue reemplazado por el Advanced Encryption Standard (AES).

3.1.1 Confusión y Difusión.

Según Claude Shannon, hay dos operaciones primitivas que los cifrados deben considerar para ser fueramente seguros:

① Confusión:

- + El objetivo es ocultar la relación entre la clave y el cifrado.
- + Logra que sea difícil para un atacante rastrear como la clave afectó al resultado.
- + Ejemplo: sustitución usada en DES y AES
- + Ejemplo: Sup. que tenemos el texto plano HELLO y queremos usar sustitución de caracteres para cambiar cada letra por otra según una tabla secreta.
 $H \rightarrow M, E \rightarrow P, \dots$

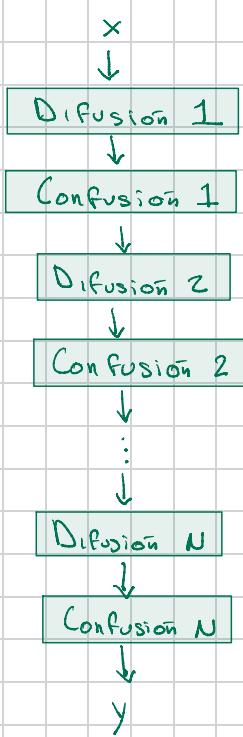
Si cambiamos la llave, todo el mapeo cambia y HELLO podría irse a cifrado completamente diferente como ZYXXO.

② Difusión:

- + Busca disipar la influencia de un símbolo del texto plano en muchos símbolos del texto cifrado.
- + Objetivo es ocultar propiedades estadísticas del texto plano.
- + Ejemplo: Permutación de bits utilizada en DES y operación MixColumn en AES.
- + Despues de aplicar confusión, si usamos una permutación que reorganiza los caracteres o bits, si cambiamos la letra H por G en el texto original, el texto cifrado podría resultar: QRXYP en lugar de ZYXXO.
- + Un ligero cambio en el texto plano se difunde para afectar muchos elementos en el resultado final.

Importancia de combinar difusión y confusión:

- + Cifrar solo con confusión (ej. cifrado por desplazamiento) o solo con difusión no proporciona suficiente seguridad.
- + La combinación de estas dos operaciones conocida como cifrado de producto, ofrece un cifrado fuerte.
- + Los cifrados de bloques modernos son ejemplos de cifrados de producto, con rondas de operaciones aplicadas repetidamente.



Propiedades de difusión en los cifrados de bloques modernos

- + Cambiar un solo bit del texto plano genera un cambio promedio en la mitad de los bits del texto cifrado.
- + Por lo tanto el texto cifrado parece estadísticamente independiente del primero.

Ejemplo: asumamos un cifrado por bloques con bloques de 8 bits de long.

Encriptar dos textos que difieren en un bit:

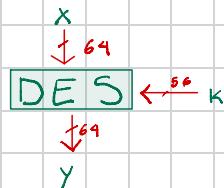
$$\begin{array}{l} X_1 = \underline{00101010} \rightarrow \boxed{\text{Cifrado de}} \\ X_2 = \underline{00001010} \quad \boxed{\text{bloque}} \end{array} \longrightarrow \begin{array}{l} Y_1 = 10111001 \\ Y_2 = 01101100 \end{array}$$

Nota: Los cifrados de bloques modernos tienen bloques de longitud de 64 o 128 bits y pasa lo mismo si se cambia un solo bit.

3.2 Un vistazo al algoritmo DES

* Bloques y clave:

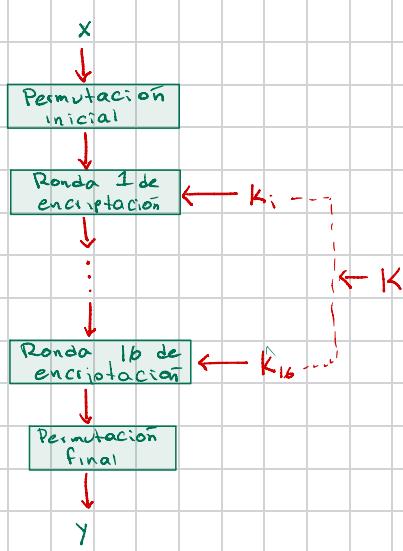
- DES es un cifrado que opera en bloques de 64 bits con una llave de tamaño 56 bits.



- Es un cifrado simétrico, utiliza la misma llave tanto para el cifrado como para el descifrado.

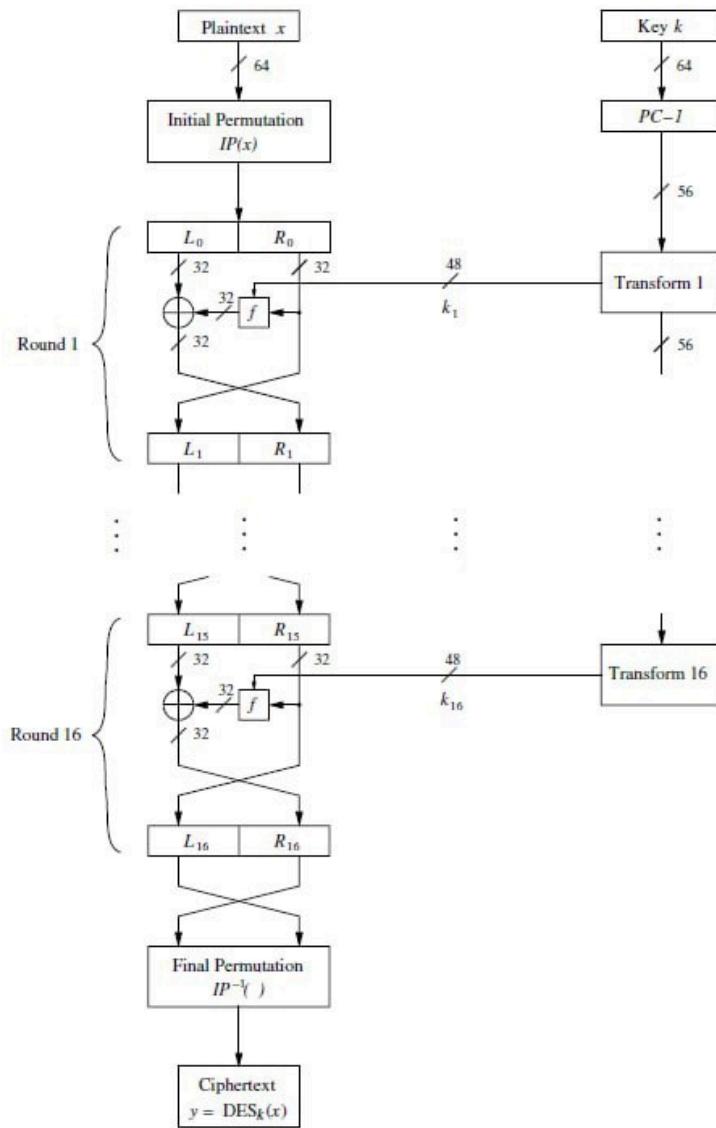
* Estructura general

- DES es un algoritmo iterativo que se efectúa en 16 rondas
- En cada ronda, se utiliza una subllave K_i diferente derivada de la llave principal K .
- Es similar a los cifrados modernos de bloques.



* Red Feistel

- El corazón de DES es una red Feistel
- Estas redes se usan en muchos códigos de bloques modernos (no en AES)
- Si se usan correctamente puede generar códigos muy seguros.
- Ventaja: La encriptación y desencriptación son esencialmente el mismo proceso, pero con las subllaves aplicadas en orden inverso. Cifrado ... X



* Proceso

① Permutación inicial

- El bloque de texto plano de 64 bits pasa por una permutación inicial P_1

② División de mitades

- El bloque se divide en dos mitades de 32 bits: L_0 (izq) y R_0 (derecha)
- Estas serán el input de la red Feistel

③ Rondas (16 en total)

- En cada ronda, la mitad derecha R_i pasa por una función de cifrado f
- El resultado de f se combina mediante una operación XOR con la mitad izquierda L_i
- Las mitades se intercambian y el proceso se repite.

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$$

- Al finalizar la ronda 16 las dos mitades de 32 bits L_{16} y R_{16} se intercambian de nuevo.
- En cada ronda, una llave k_i se obtiene la la clave principal de 56 bits usando un "esquema de llaves"

④ Permutación Final $(P_1)^{-1}$

- Despues de los 16 rondas se realiza una permutación final inversa $(P_1)^{-1}$ para obtener el texto cifrado

* Función de cifrado f :

- La función f toma dos entradas R_{i-1} y la llave k_i
- **Objetivo:** Generar un valor "pseudorandomo" que se combine con la mitad izquierda L_i mediante XOR
- **Confusión y difusión:** La función f es la responsable de la confusión (relación no obvia entre la clave y el texto cifrado) y difusión (propagación del cambio de un bit).
- La función f se debe diseñar con cuidado, una vez que ha sido creada seguramente, la seguridad del cifrado Feistel aumenta con el número de bits de la llave que se usan y el número de rondas.

* Consideraciones finales:

- La seguridad de DES depende del diseño de la función F y el uso de subllaves y rondas múltiples.
- **Perfeccional es un mapeo biyectivo:** Cada bloque de entrada de 64 bits se transforma de manera única en un bloque de salida de 64 bits. Permanece biyectivo aunque F no lo sea.
- En el caso de DES, la función F es sobreyectiva. Usa bloques no lineales y una llave de 48 bits para transformar 32 bits de entrada en 32 de salida.

Nota: Feistel solo encripta el lado izquierdo en cada ronda, el derecho permanece igual.

Ejemplo:

① Entrada: texto plano de 8 bits: 10101010
clave de 8 bits: 11001100

Actualizamos L y R : $L_0 = R_0 = 1010$

$$R_1 = L_0 \text{ XOR } F(R_0, k_1)$$

$$= 1010 \text{ XOR } 0110 = 1100$$

② IP: "divide en 2 mitades":

$$L_0 = 1010$$

$$R_0 = 1010$$

③ F : tomar R y llave k_1 y aplicar XOR

④ Ronda 1: Entrada: $L_0 = 1010$

$$R_0 = 1010$$

$$\text{Subclave} = 1100$$

$$\text{Aplicar } F: F(R_0, k_1) = R_0 \text{ XOR } k_1$$

$$F(1010, 1100) = 0110$$

⑤ Ronda 2: Entrada $L_1 = 1010$

$$R_1 = 1100$$

$$\text{Subclave} = 0011$$

$$\text{Aplicar } F: F(R_1, k_2) = F(1100, 0011) = 1111$$

$$\text{Actualizamos } L, R: L_2 = R_1 = 1100$$

$$R_2 = L_1 \text{ XOR } F(R_1, k_2)$$

$$1010 \text{ XOR } 1111 = 0101$$

⑥ Permutación Final: ninguna

⑦ Resultado: $L_2 \cup R_2 = 11000101$