Data Encryption Standard

FIPS PUB 46-3

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

Reaffirmed
1999 October 25

U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

DATA ENCRYPTION STANDARD (DES)

Algoritmo DES

- ***Data Encryption Standard***.
- Algoritmo di cifratura simmetrico.
- Adottato come standard ufficiale dal NBS, oggi NIST, nel 1977.
- Ampiamente utilizzato in molti ambiti commerciali, ad esempio nel settore bancario.
- Veloce e "moderatamente" sicuro.
- Se due utenti desiderano scambiarsi dati, hanno bisogno di una chiave segreta pre-condivisa (eventualmente scambiata con un metodo a chiave pubblica).

Algoritmo DES (ctd.)

- Nel 1990 Eli Biham e Adi Shamir hanno mostrato che la crittanalisi differenziale rompe DES.

- In realtà, questo non era del tutto vero, perché la crittoanalisi differenziale sarebbe più efficace della ricerca esaustiva di tutte le chiavi possibili se l'algoritmo utilizza al massimo 15 round.

- DES usava 16 round.

- Più tardi, Biham e Shamir ha pubblicato un attacco di crittoanalisi differenziale più efficiente della ricerca esaustiva anche contro il DES con 16 round.

Algoritmo DES (ctd.)

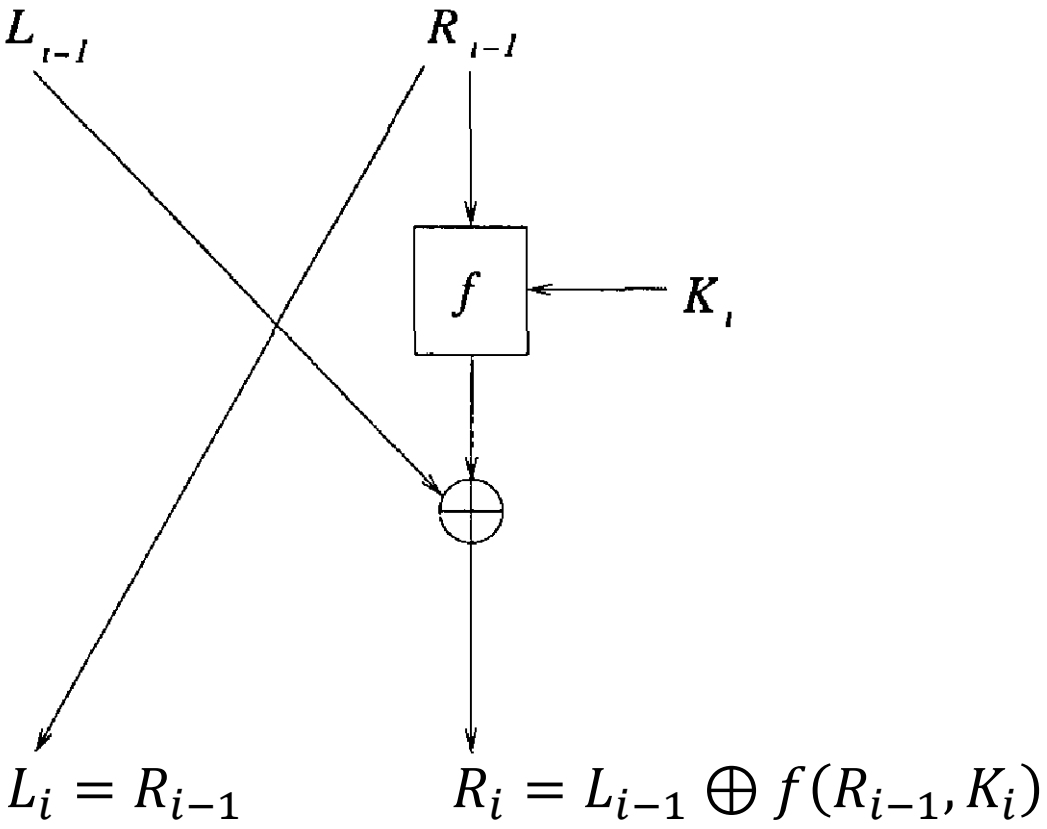
- Il DES è durato a lungo, anche se ora è diventato obsoleto.
- Gli attacchi a forza bruta, sebbene costosi, sono ora possibili.
- Nel 2000, il NIST lo ha sostituito con un nuovo crittosistema (AES).
- Il DES è un cifrario a blocchi: spezza il testo in chiaro in blocchi di 64 bit ciascuno e cripta ogni blocco separatamente.
- Il principio alla base del DES è chiamato sistema Feistel (in onore di Horst Feistel, noto per aver sviluppato il cifrario Lucifero all'IBM).
- Le procedure di cifratura e decifratura di Feistel sono molto simili e basta invertire l'operazione di generazione delle chiavi per ottenere la decifratura dalla cifratura.

DES

- Un testo in chiaro (m) consiste in 64 bit divisi in due vettori di 32 bit ognuno: [L | R]
- La chiave segreta ha 56 bit, ma si esprime come stringa di 64 bit.
- I bit della chiave segreta nelle posizioni 8, 16, 24, ..., sono di parità, e i loro valori sono scelti in modo che ogni blocco di 8 bit abbia un numero dispari di uno.
- Ciò consente il rilevamento di un singolo errore su qualsiasi byte della chiave.
- Il risultato della crittografia è un blocco di testo cifrato di 64 bit.

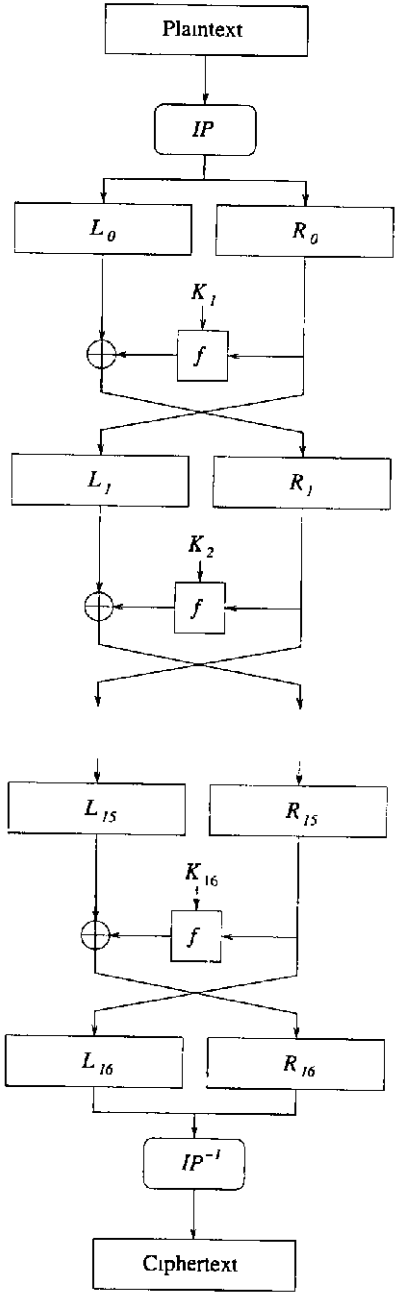
Round

- Dati in input $[L_{i-1} \mid R_{i-1}]$, l'output di un round è $[L_i \mid R_i]$:



- Dopo *n* round, otteniamo il testo cifrato

Algoritmo DES



Fasi dell'algoritmo

1. I bit di m sono permutati tramite una permutazione iniziale (IP), e si ottiene $m_0 = IP(m)$, scritto come $[L_0 \mid R_0]$.

2. Per $1 \leq i \leq 16$ (i = numero di round) si calcola:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f\left(R_{i-1}, K_i\right)$$

dove K_i è una stringa di 48 bit ottenuta dalla chiave K, mentre f è una funzione progettata ad hoc. (Per gli scopi del Corso non si approfondiscono questi due aspetti)

3. Si scambiano le parti destra e sinistra, ottenendo $R_{16}L_{16}$ e si applica l'inversa della permutazione inizialeper ottenere il ciphertext $c = IP^{-1}(R_{16}L_{16})$.

Decifratura

- Stessi passi, ma usando le chiavi in ordine inverso.

Features of DES encryption

- Ogni bit della chiave segreta *K* è usato in 14 dei 16 round.
  → **confusione**

- In un buon sistema crittografico, ogni bit del testo cifrato deve dipendere da tutti i bit del testo in chiaro.
  → **diffusione**

- L'espansione *E*(*R*) ha il ruolo di soddisfare questa condizione entro pochi round.