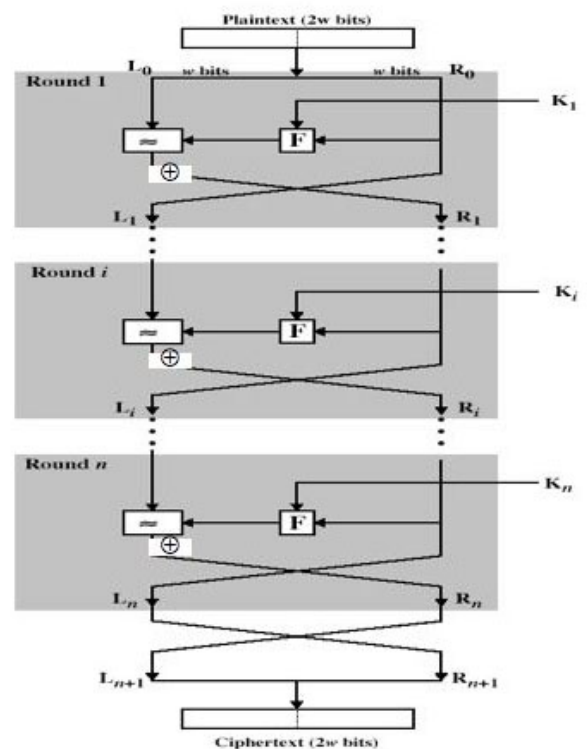


cifrario di Feistel

- Horst Feistel (IBM) ha introdotto uno schema di cifrario nei primi anni 70.
- il DES è un cifrario di Feistel
- molti cifrari a blocchi sono cifrari di Feistel - per esempio i due finalisti AES MARS e twofish
- la cifratura e la decifratura funzionano essenzialmente allo stesso modo

cifrario di Feistel

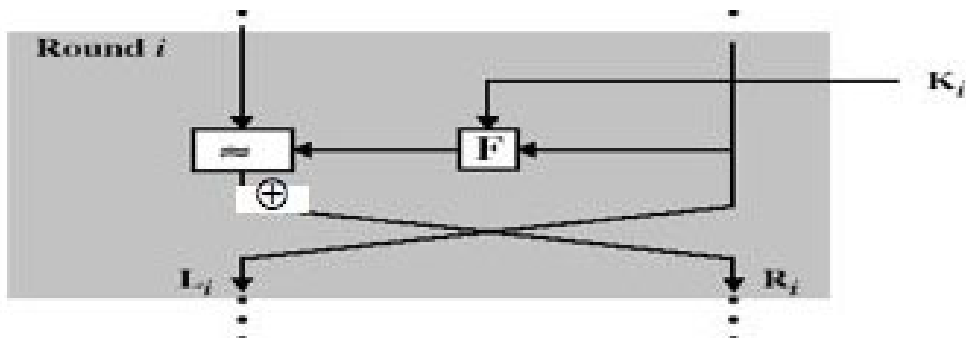
In un cifrario di Feistel, i blocchi hanno lunghezza $m = 2w$: a ogni iterazione, ogni stato è diviso in due blocchi di lung. w , (L_i, R_i) . Servono R chiavi di round $(k_1, \dots, k_R)$.



funzione di round

la funzione di round ha la seguente forma:

input: (L_{i-1}, R_{i-1}, k_i) , output (L_i, R_i)



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

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

cifrario di Feistel - invertibilità

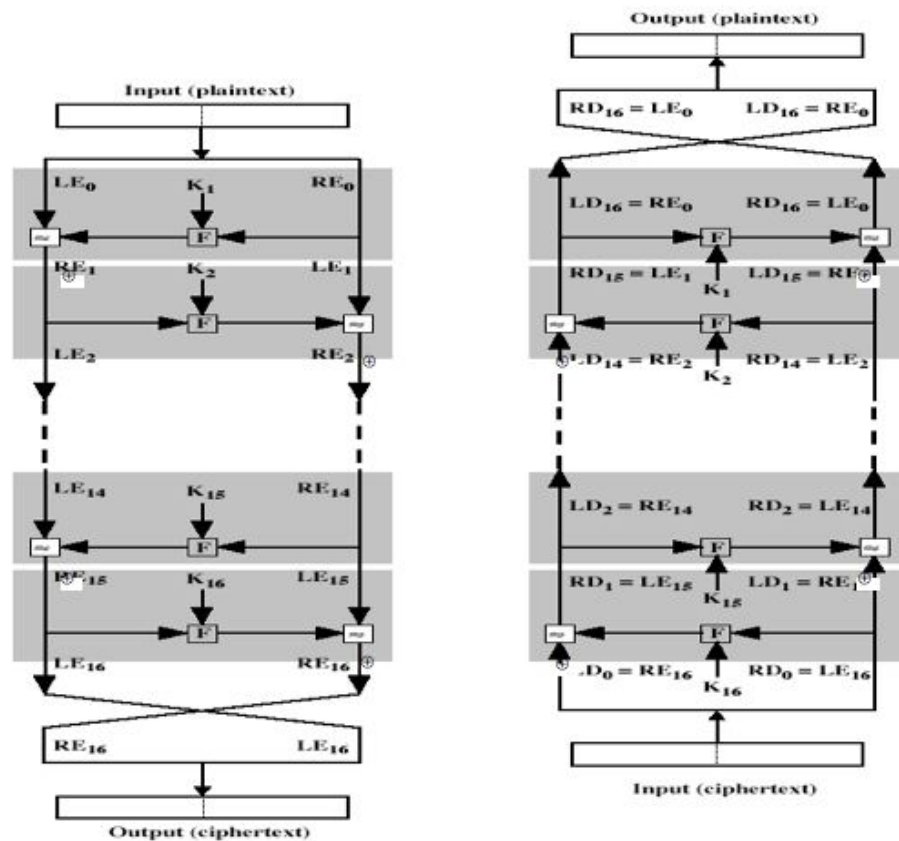
- la funzione di round è una funzione $f : \{0, 1\}^{2w} \rightarrow \{0, 1\}^{2w}$
- la F è una funzione arbitraria $F : \{0, 1\}^w \rightarrow \{0, 1\}^w$
- comunque sia scelta la F (invertibile o non invertibile) la funzione di round f è comunque invertibile
- da

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

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

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

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



Dimensione del blocco L' aumento della grandezza del blocco aumenta la sicurezza ma rallenta la velocità di cifratura e decifratura

Dimensione della chiave L' aumento della lunghezza della chiave aumenta la sicurezza e rende la ricerca esaustiva più difficile ma rallenta l'algoritmo

Numero di round L' aumento del numero di round aumenta la sicurezza ma rallenta l'algoritmo

Funzione F L' aumento di complessità rende l'analisi più difficile ma rallenta l'algoritmo

risultati teorici

- se la funzione $F : k \times \{0, 1\}^w \rightarrow \{0, 1\}^w$ è una funzione pseudocasuale sicura
- allora bastano 3 round alla Feistel
- $f : k^3 \times \{0, 1\}^{2w} \rightarrow \{0, 1\}^{2w}$ è una permutazione pseudocasuale sicura
- Luby - Rackoff ca 1985