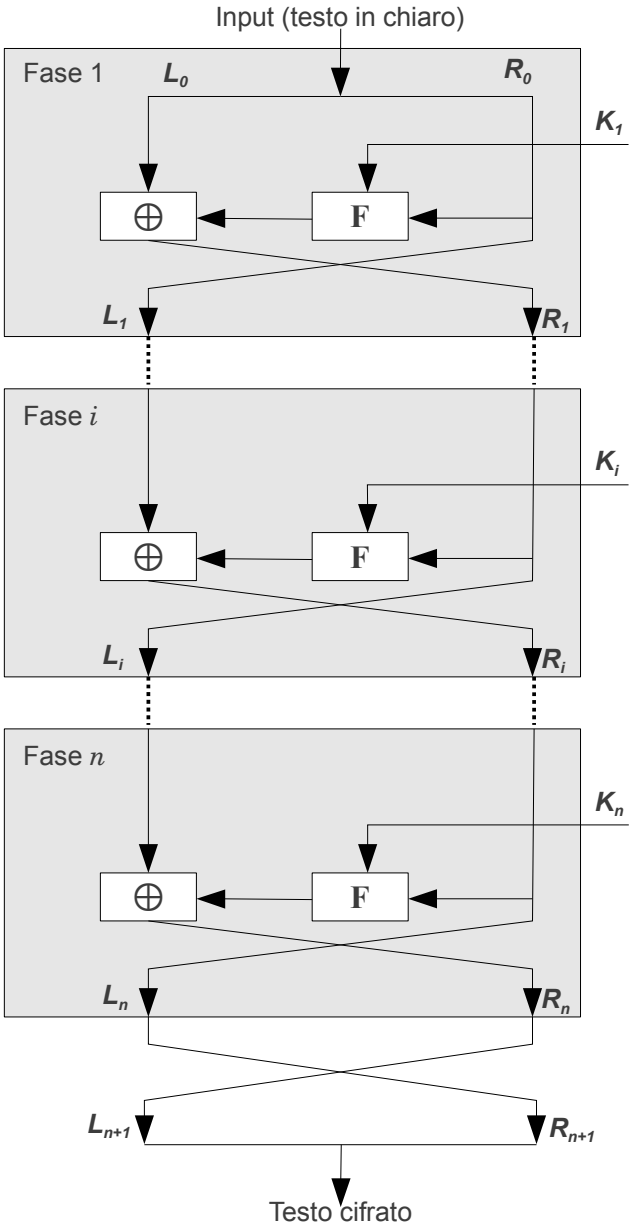
Cifratura di Feistel



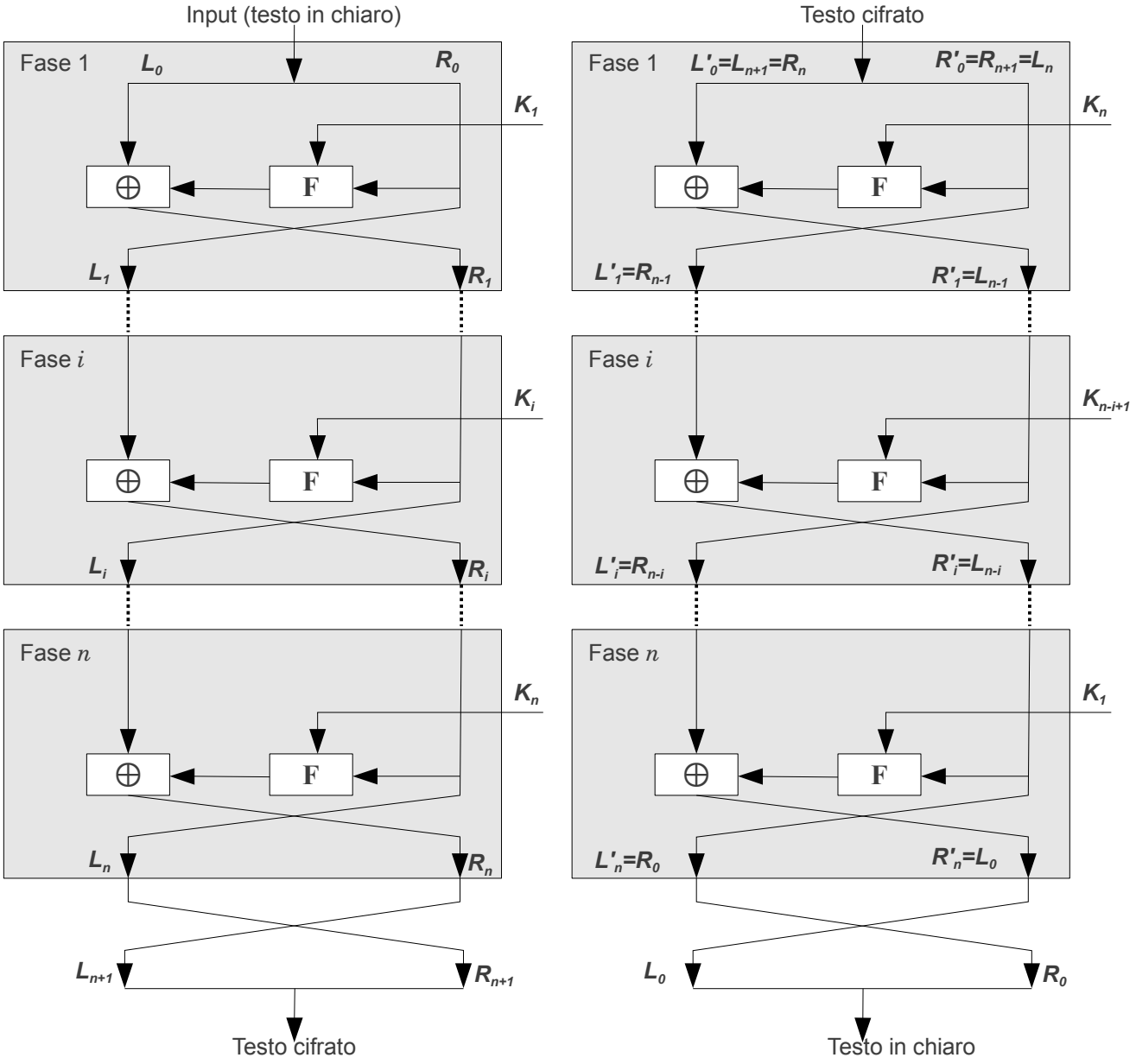
L'input viene diviso in due parti uguali, L_0, R_0

Lo stesso viene fatto per l'output di ogni fase, L_i, R_i

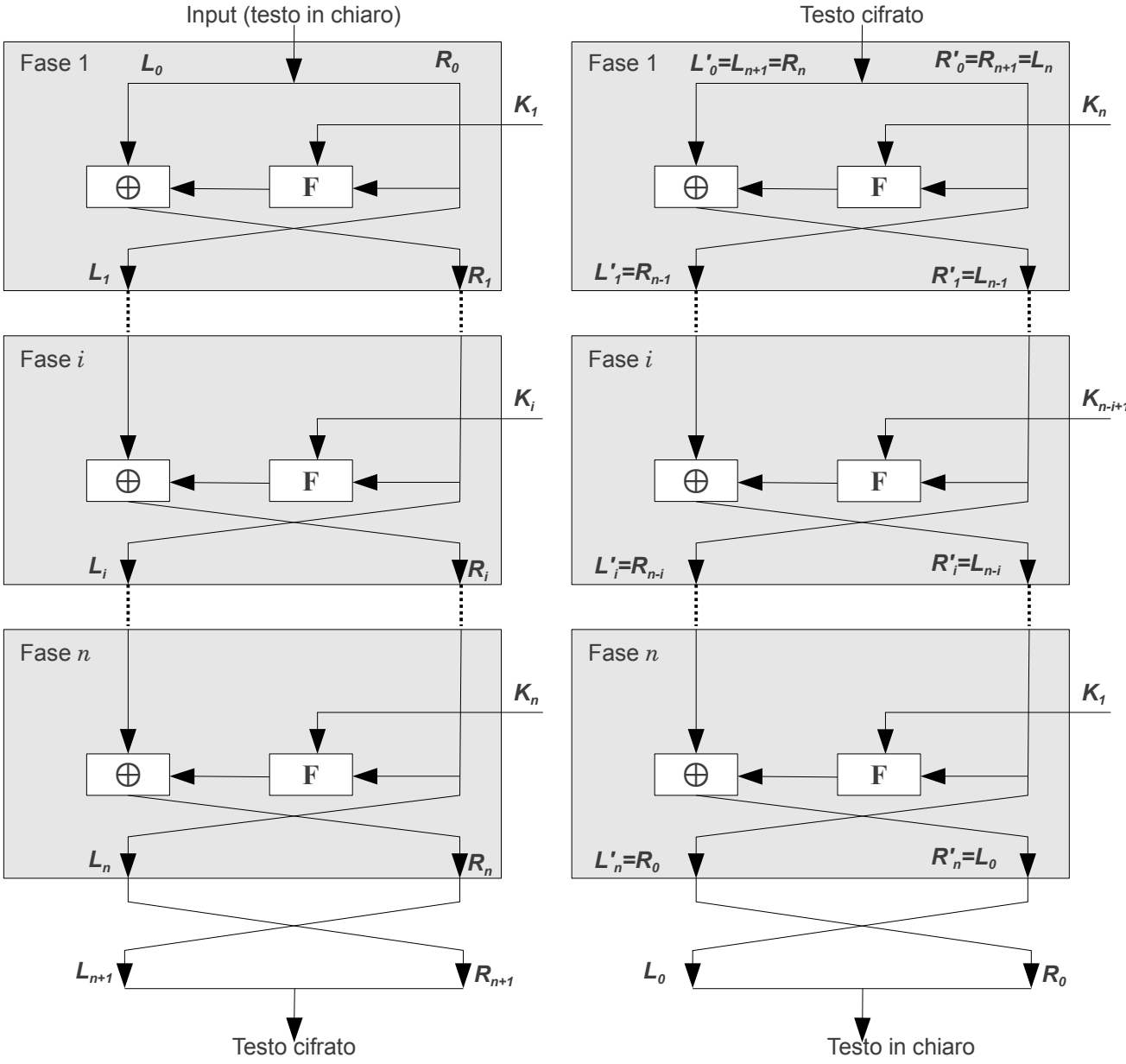
Ad ogni passo

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

Cifratura di Feistel



Cifratura di Feistel



Se n=16:

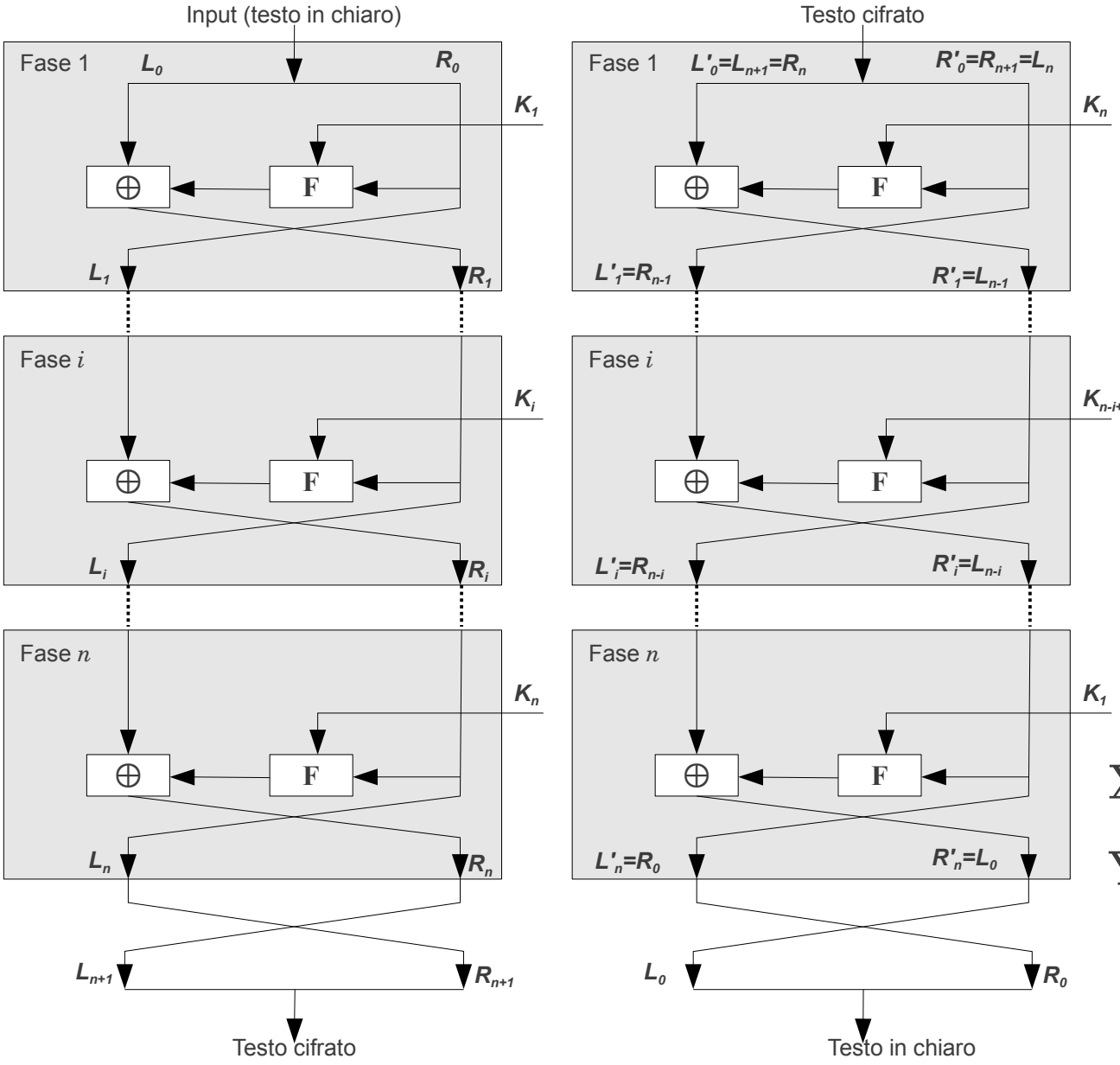
- $L'_1 = R'_0 = L_{16} = R_{15}$
- $R'_1 = L'_0 \oplus \mathrm{F}(R'_0, K_{16}) =$

  $= R_{16} \oplus \mathrm{F}(R_{15}, K_{16}) =$

  $= [L_{15} \oplus \mathrm{F}(R_{15}, K_{16})] \oplus \mathrm{F}(R_{15}, K_{16})$

  $= L_{15} \oplus [\mathrm{F}(R_{15}, K_{16}) \oplus \mathrm{F}(R_{15}, K_{16})]$

Cifratura di Feistel



Se n=16:

- $L'_1 = R'_0 = L_{16} = R_{15}$
- $R'_1 = L'_0 \oplus \mathrm{F}(R'_0, K_{16}) =$

$= R_{16} \oplus \mathrm{F}(R_{15}, K_{16}) =$

$= [L_{15} \oplus \mathrm{F}(R_{15}, K_{16})] \oplus \mathrm{F}(R_{15}, K_{16})$

$= L_{15} \oplus [\mathrm{F}(R_{15}, K_{16}) \oplus \mathrm{F}(R_{15}, K_{16})]$

$= L_{15}$

perchè

$\mathrm{X} \oplus \mathrm{X} = 0$

$\mathrm{Y} \oplus 0 = \mathrm{Y}$