Sieć Feistela

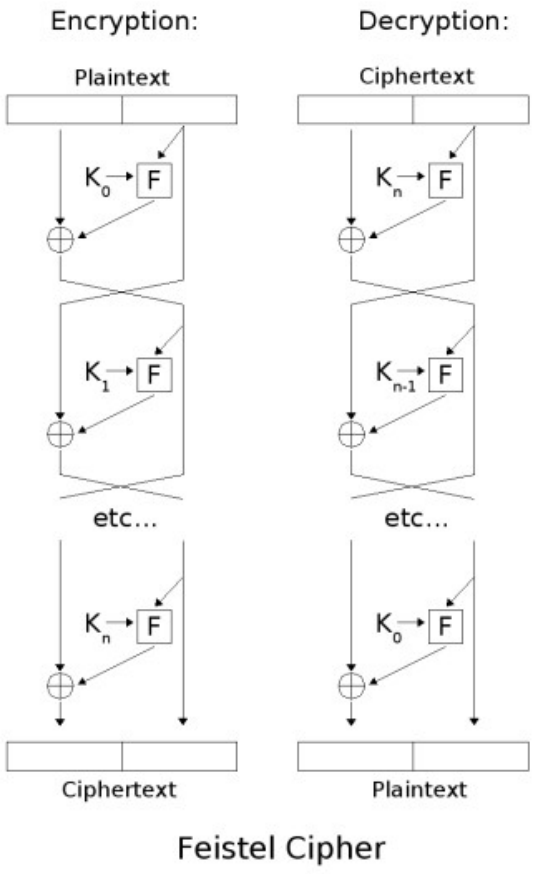
Istotą działania wielu algorytmów szyfrujących, w tym DES, jest tzw. **sieć Feistela**. Jest to schemat działania, który pozwala na szyfrowanie i deszyfrowanie informacji tym samym algorytmem, mimo iż sama funkcja szyfrująca **F** nie jest odwracalna. Sieć Feistela generuje z tekstu jawnego szyfrogram, a z szyfrogramu tekst jawny.

Sieci Feistela składa się z n+1 rund szyfrowania, oznaczonych 0, 1, 2 ... n. Do każdej rundy wchodzą dwa równe bloki tekstu, A_i i B_i.

W pierwszej rundzie (nr. 0), dzielimy oryginalny tekst jawny na pół, tworząc dwa bloki A_0 i B_0. Jeden z tych dwóch bloków (załóżmy, że B_0) jest szyfrowany funkcją **F** (z odpowiednim dla danej rundy kluczem: K_0, K_1, K_2 ... K_n) dając wynik $\mathbf{F}(B_0)$, i następnie połączony z drugim blokiem (czyli A_0) za pomocą operacji logicznej XOR (oznaczonej symbolem $\oplus$), dając $A_0 \oplus \mathbf{F}(B_0)$.

Do następnej rundy (nr 1) wchodzą A_1 i B_1. W miejsce bloku A_1 podstawiamy niezmieniony blok B_0 z poprzedniej rundy, a zamiast B_1 wynik poprzedniej rundy, czyli $A_0 \oplus \mathbf{F}(B_0)$. (Bloki zostały więc zamienione miejscami).

Każda kolejna runda powtarza ten schemat:



Feistel Cipher

Analizując trzy rundy szyfrujące i trzy deszyfrujące, pokaż dlaczego sieć Feistela pozwala szyfrować i rozszyfrować wiadomość tym samym algorytmem, niezależnie od postaci funkcji szyfrującej **F**.