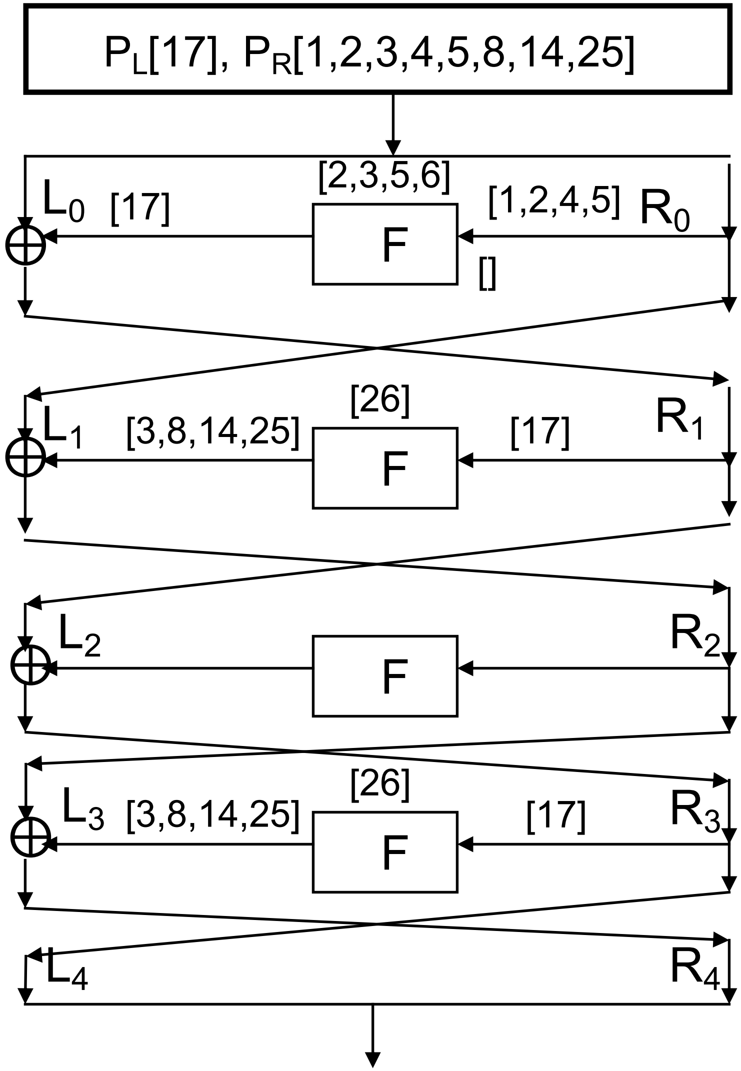
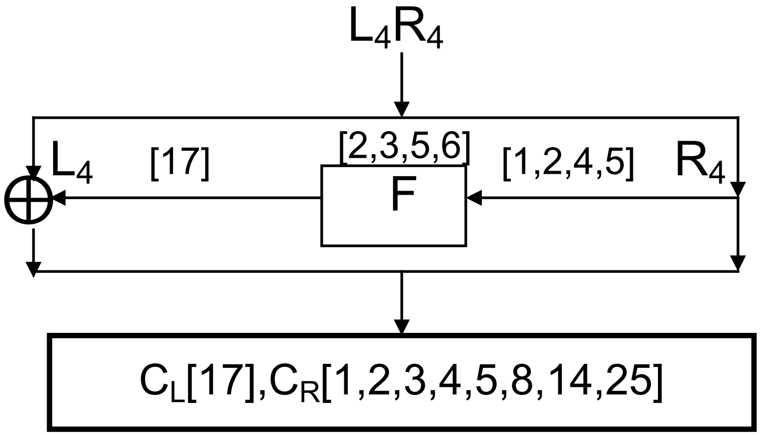
Linear Cryptanalysis of DES, 5 rounds





1. $P_L[17] \oplus R_1[17] = K_1[2,3,5,6] \oplus P_R[1,2,4,5] \oplus 1$
2. $P_R[3,8,14,25] \oplus R_2[3,8,14,25] = K_2[26] \oplus R_1[17] \oplus 1$
   $R_2[3,8,14,25] \oplus C_R[3,8,14,25] = K_4[26] \oplus C_R[17] \oplus 1$
   $C_L[17] \oplus R_3[17] = K_5[2,3,5,6] \oplus C_R[1,2,4,5] \oplus 1$

- Adding yields: $P_L[17] \oplus P_R[1,2,3,4,5,8,14,25] \oplus C_L[17] \oplus C_R[1,2,3,4,5,8,14,25] = K_1[2,3,5,6] \oplus K_2[26] \oplus K_4[26] \oplus K_5[2,3,5,6]$
- This holds with probability:

$p= p_B^2 p_A^2 + p_B^2 q_A^2 + p_A^2 q_B^2 + 4(q_A p_B q_B p_A) + q_B^2 q_A^2 \cong .519,$

where $q_i = 1 - p_i$. $p/q = 1.07927..$