2.1 Finding the Round Subkey of the F Function

Throughout these notes, we make repeated use of the following lemma.

Lemma 2.1. *Suppose that $F_k(x) = X$, where x denotes the XOR of the inputs, X denotes the XOR of the outputs and k denotes the subkey used in F. Then, given x and X, we can extract k efficiently.*

Proof. Since we know x, we know S_E and thus we know S_I. Now, we also know □

2.2 Cryptanalysis of DES Reduced to 4 Rounds