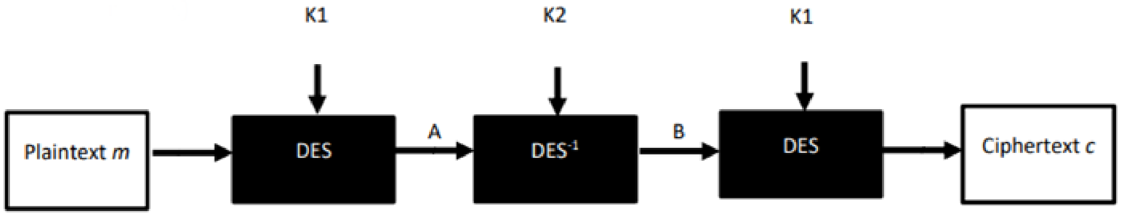
Note: Please cite any resources used, and mention any classmates that you worked with on this assignment. If you worked alone, please also say so. We will start taking points off if this is missing.

Problem 1. 3DES

We discussed how use a meet in the middle attack to break 2DES using a known-plaintext attack. Now we want to adapt it to break 3DES. We use the following diagram. Here, we are attempting to break $DES_{K1}(DES^{-1}_{K2}(DES_{K1}(m)))$ by attempting to find K_1 and K_2. Show that you can find K_1 and K_2 with a **chosen** plaintext using attack 2^{56} chosen plaintexts and two tables of 2^{56} entries of DES inverse operations.

(Hint: start by constructing a table with all 2^{56} possible values for K_1 and corresponding $DES^{-1}_{k1}(0)$ (that is, assume $A = 0$). Then, using $A = 0$, meet in the middle.)



Problem 2. Super One-Time Pad

Consider the following improvement to one-time pad encryption, which we will call super one-time pad encryption. As before our message and encryption key is a string of bits. But for super one-time pad encryption we compute:

$$c = \ m \ xor \ k \ xor \ k^R$$

where k^R denotes key reversal (so, for example, $11010001^R = 10001011$).

Is super one-time pad encryption perfectly secure (that is, does it leak no information about the contents of the plaintext other than the length of the plaintext)?

Problem 3. Feistel Cipher

Let F be a single round of a Feistel cipher operating on 64-bit blocks. That means an input $a = (a_L,\ a_R)$ where a_L and a_R are 32 bits long each, and $F(a_L,\ a_R) = \ (a_R,\ a_L \ xor \ f(a_R,\ k))$. f is the Feistel cipher's "secret" function.

Suppose that $(a_L,\ a_R)$ and $(b_L,\ b_R)$ are a pair of plaintexts such that $a_R \ xor \ b_R = \ q$ for some number q.

Consider what happens when we run two rounds of the Feistel Cipher on the input a, and two rounds of the Feistel Cipher on b:

$$(c_L,\ c_R) = F(F(a_L,\ a_R)),\ (d_L,\ d_R) = F(F(b_L,\ b_R))$$

.

Show that if $c_L = d_L$, then $c_R \ xor \ d_R = q$.