Extra Credit 4

Due: May 25, 2018 at 11:59pm **Extended; due date is now May 30** **Points:** 20

Questions

1. (*40 points*) Consider double encryption, where $c = E_{k'}(E_k(m))$ and the keys k and k' are each n bits long. Assume that each encipherment takes one time unit. A cryptanalyst will use a known plaintext attack to determine the key from two messages m_0 and m_1 and their corresponding ciphertexts c_0 and c_1.

   (a) The cryptanalyst computes $E_x(m_0)$ for each possible key x and stores each in a table. How many bits of memory does the table require? How many time units does it take to compute the entry?

   (b) The cryptanalyst computes $y = D_{x'}(c_0)$, where D is the decipherment function corresponding to E, for each possible key x', and then checks the table to see if y is in it. If so, (x,x') is a candidate for the key pair. How should the table be organized to allow the cryptographer to find a match for y in time $O(1)$? How many time units will pass before a match must occur?

   (c) How can the cryptographer confirm that (x,x') is in fact the desired key pair?

   (d) What are the maximum amounts of time and memory needed for the attack? What are the expected amounts of time and memory?