CS 555, Fall, 2017, Homework 0

Due: September 5, 2017, 1:30 PM.

1. (a) Let X' denote the bit-by-bit complement of a bit string X. Show that if $C = \mathrm{DES}_K(M)$, then $C' = \mathrm{DES}_{K'}(M')$. (Hint: Compare the two encipherings. At each step, tell which quantities are complemented and which are not.)

(b) Explain how this property can be exploited in a chosen-plaintext attack to reduce the search effort by roughly 50%. Assume that comparing two 64-bit strings takes negligible time compared to computing $\mathrm{DES}_K(M)$ once. Part of your answer should be an algorithm which tells exactly what to do. (Hint: Obtain the ciphertext for a plaintext M and for its complement M'.)