1. Suppose $M = 10001010$ and $C = 11110011$ are corresponding bit streams in a known plaintext attack on a four-bit LFSR. $M$ was enciphered from left to right, that is, the bit at the left end (1 for $M$) was enciphered first. Each bit of $M$ was XORed with the next bit output by the LFSR to produce the next bit of $C$. Find the matrix $H$, the tap sequence $T$, and the initial contents of the register. Show all of your work.

2. (a) Let $X'$ denote the bit-by-bit complement of a bit string $X$. Show that if $C = \text{DES}_K(M)$, then $C' = \text{DES}_{K'}(M')$. (Hint: Compare the two encipherings. At each step of DES, 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 nearly 50%. Assume that comparing two 64-bit strings takes negligible time compared to computing $\text{DES}_K(M)$ 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 $M'$.)