GEORGIA INSTITUTE OF TECHNOLOGY
School of Electrical and Computer Engineering

ECE 6280
Cryptography

HWK #2, Due: Thursday Feb. 6

Problem 1: Prove that if $\mathcal{S}_1$ and $\mathcal{S}_2$ have perfect secrecy, then so does $\mathcal{S}_1 * \mathcal{S}_2$ (their product).

Problem 2: Show that, in a perfect cryptosystem, $H(K|C) = H(K)$.

Problem 3 Solve question 3.3 from the textbook.

Problem 4: A Lucifer (Feistel-type) cryptosystem operates on block of $2n$ message symblos by the rule $M_{i+2} = M_i + f(M_{i+1}, K_{i+1})$ in which $f(M_{i+1}, K_{i+1})$ is just the permutation of M_{i+1} determined by the key (permutation) K_{i+1}. Given the additional side information that the keys are equal to the same permutation π, prove that the system is vulnerable to a chosen plaintext attack (assume L iterations of Lucifer system).

Problem 5^***:** Compute $H(K|C)$ for the affine cipher, assuming that keys are used equiprobably and the plaintext are equiprobable.

Problem 6^* Solve question 2.15 from the textbook.