Problem Set 2

Due on Monday, February 15, 2010

In this problem set, we consider a variant of the Caesar cipher which we call the "Happy-2010" cipher (named after the venerable "Happy Hacker" of CPSC 223 fame). Happy-2010 (E, D) is defined as follows: Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, \ldots, 25\}$. Define

$$E_k(m) = \begin{cases} (m + 2k) \bmod 26 & \text{if } m + k \text{ is even} \\ m & \text{if } m + k \text{ is odd} \end{cases}$$

We also consider Double Happy (E^2, D^2). Here, $\mathcal{K}^2 = \mathcal{K} \times \mathcal{K}$, and $E^2_{(k_1,k_2)} = E_{k_1}(E_{k_2}(m))$.

Feel free to write programs to help you solve these problems. If you do, include the programs and their output along with your solutions, and say how the computer was used.

Problem 1: Happy Encryption (5 points)

Encrypt the plaintext "i am a secret message" using Happy with key $k = 3$. (As usual, we will ignore spaces.)

Problem 2: Happy Decryption (5 points)

Describe the Happy decryption function $D_k(c)$.

Problem 3: Security (10 points)

(a) Is Happy information-theoretically secure? Why or why not?

(b) Is Double Happy information-theoretically secure? Why or why not?

Problem 4: Equivalent Key Pairs (10 points)

Suppose $m_0 = c_0 = 4$.

(a) Find all key pairs (k, k') such that $E^2_{(k,k')}(m_0) = c_0$.

(b) Do all such key pairs give rise to the same function $E^2_{(k,k')}$? That is, if $E^2_{(\hat{k},\hat{k'})}(m_0) = E^2_{(k,k')}(m_0) = c_0$, does $E^2_{(\hat{k},\hat{k'})}(m) = E^2_{(k,k')}(m)$ for all $m \in \mathcal{M}$? Why or why not?

Problem 5: Group Property (10 points)

Is Happy a group? Why or why not?