YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

Solution to 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.)

Solution: IAMASECXEZMESSAGE.

Problem 2: Happy Decryption (5 points)

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

Solution:

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

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?

Solution:

(a) No. Because the encryption function maps odd numbers to odd numbers, and even numbers to even numbers. Haven seen the ciphertext, you know the parity of the plaintext.

(b) No. The same reason as before.

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?

Solution:

(a) You need to consider many interesting cases.

- $k, k' \in \{0\} \cup \{n \in \mathcal{K} \wedge 2 \nmid n\}$;
- $k, k' \in \mathcal{K}$, such that $k + k' = 26$.

(b) No. Here is a simple counter-example. Consider two key pairs $(0, 0)$ and $(0, 1)$. Then $E^2_{(0,0)}(1) = 1$, but $E^2_{(0,1)}(1) = 3$.

Problem 5: Group Property (10 points)

Is Happy a group? Why or why not?

Solution: No. There are two ways to think about this problem.

- Given a pair of keys (k', k'') such that $k' \neq 0$ is even and $k'' \neq 13$ is odd, there is no single key k that gives $E_k = E^2_{(k,k')}$. To see this, consider two different plaintext messages $m_0 = 0$ and $m_1 = 1$. We have

  $$E^2_{(k',k'')}(m_0) = m_0 + 2k' \bmod 26 \neq m_0$$

  and

  $$E^2_{(k',k'')}(m_1) = (m_1 + 2k'') \bmod 26 \neq m_1$$

  However, for any single key $k \in \mathcal{K}$, it either gives $E_k(m_0) = m_0$ or $E_k(m_1) = m_1$. Therefore, for any $k \in \mathcal{K}$, we have

  $$E_k \neq E^2_{(k',k'')}$$

- Note that the identity is 0 in this set. We also know that, the encryption function maps odd numbers to odd numbers, and even numbers to even numbers. Thus, for any odd number $m \in \mathcal{M}$, there does not exist m^{-1} in this set.

Thus, Happy is not a group.