Problem Set 2

Due on Friday, October 3, 2008.

In this problem set, we consider a variant of the Caesar cipher which we call the "Happy" cipher (named after the venerable "Happy Hacker" of CPSC 223 fame). Happy (E, D) is defined as follows: Let $X_1 = \{0, \ldots, 12\}$ and $X_2 = \{13, \ldots, 25\}$. Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = X = X_1 \cup X_2$, and let $n = |X| = 26$. Define

$$E_k(m) = \begin{cases} (m+k) \bmod 13 & \text{if } k \in X_1 \wedge m \in X_1 \\ m & \text{if } k \in X_1 \wedge m \in X_2 \\ m & \text{if } k \in X_2 \wedge m \in X_1 \\ ((m+k) \bmod 13) + 13 & \text{if } k \in X_2 \wedge m \in X_2 \end{cases}$$

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

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?

The following problems ask you to compute probabilities. You may do so either analytically (if you're facile with combinatorial counting techniques) or experimentally by writing a program to simulate 1000 random trials and reporting the fraction of times that the desired result is obtained. Either way, you should show your work – analytic derivation, or program and simulation results.

Problem 6: Birthday Problem (20 points)

Suppose $u_1, \ldots, u_6$ and $v_1, \ldots, v_6$ are chosen uniformly and independently at random from X (so duplicates are possible. Find the probability that $\{u_1, \ldots, u_6\} \cap \{v_1, \ldots, v_6\} \neq \emptyset$. (Note that $6 = \lceil \sqrt{n} \rceil$.)

Problem 7: Birthday Attack on Double Happy (40 points)

Assume Alice chooses a random key pair (k_0, k_0') and a random message m and computes $c = E^2_{(k_0,k_0')}(m)$ using Double Happy. Eve learns the plaintext-ciphertext pair (m, c) and then carries out the *Birthday Attack* for $m \in \mathcal{M}$ and $c \in \mathcal{C}$ as follows:

- She chooses $k_1, \ldots, k_6$ uniformly at random from $\mathcal{K}$ and computes $u_i = E_{k_i}(m)$ for $i = 1, \ldots, 6$.
- She chooses $k_1', \ldots, k_6'$ uniformly at random from $\mathcal{K}$ and computes $v_j = D_{k_j'}(c)$ for $j = 1, \ldots, 6$.
- If $\{u_1, \ldots, u_6\} \cap \{v_1, \ldots, v_6\} \neq \emptyset$, we say the Birthday Attack *succeeds in producing a candidate key pair*. In that case, Eve obtains the candidate key pair $(k, k') = (k_i, k_j')$, where (i, j) is the lexicographically smallest pair such that $u_i = v_j$.
- If a candidate key pair (k, k') is produced and (k, k') can be used to decrypt any message Alice might send using her key, that is, if $D^2_{(k,k')}(E^2_{(k_0,k_0')}(m)) = m$ for all $m \in \mathcal{M}$, then we say the Birthday Attack *succeeds in breaking Double Happy*.

(a) Find the probability that the Birthday Attack succeeds in producing a candidate key pair, and compare your result with your answer to problem 6.

(b) Find the probability that the Birthday Attack succeeds in breaking Double Happy.