Homework 24

Joe Baker, Brett Schreiber, Brian Knotten

March 20, 2018

42

Consider the example where $|m| = 2$ and $|k| = 1$. Therefore there are $2^2 = 4$ possible messages and $2^1 = 2$ possible keys. An eavesdropper Carol intercepts an encrypted message c. The encryption-decryption scheme (E, D) is public and so Carol knows it. But she doesn't know the key, so she tries all possible keys: 0 and 1. Carol runs $D_0(c)$ and gets m_0. Then she runs $D_1(c)$ and gets m_1. So Carol knows that the original message $m \in m_0, m_1$. So Carol can guess the message with probability 1/2.

43

Assume that $f^k(x)$ is not a one-way permutation of x. $f^k(x)$ is still a permutation, since $f(x)$ is a permutation. So therefore $f^k(x)$ is not one-way. That means an algorithm A, given y and f will output the x such that $f^k(x) = y$ in polynomial time.

Construct an algorithm B as follows:
Given y and the one-way permutation f:
    Run A on f, y to get x such that $f^k(x) = y$.
    Repeat the following procedure $k - 1$ times:
        $x' := f(x)$
        $x := x'$
    Return x'

Since k is polynomial on n, then B is a polynomial algorithm, since it loops only $k - 1$ times. B returns the final value x' such that $f(x') = y$. Therefore B can reverse f. But f is a one way permutation. It cannot be cracked in polynomial time. There is a contradiction. Therefore f^k must also be a one-way permutation.