Homework 24

Austin Frownfelter   Matthew Bialecki

March 21, 2018

1 Problem 42

$E_{u_n}(x)$ will produce a y in the range 2^n. Since there are 2^m possible x values, then $E_{u_n}(x)$ is not one-to-one. Thus, there must be some form of "padding" or other method of converting the n-bit string to at least m-bits to make $E_{u_n}(x)$ one-to-one. This padding must be trivial, which means some number of bits (greater than 0) must be non-random. Since some portion of the key is non-random, the distributions of $E_{u_n}(x)$ and $E_{u_n}(x')$ are not equal.

2 Problem 43

Assume f is a one-way permutation. After $f(x)$, the result is some random permutation of x (having n bits). After k iterations of permuting these strings, the result is still some random permutation. $f(x)$ runs in polynomial time. Therefore, $f^k(x)$ is a one-way permutation.