Cryptography

Lab no. 1

Problem 1. Construct an algorithm which predicts next bits of *linear congruencial generator*, use this algorithm to construct a distinguisher (statistical test) which can distinguish output generated by an instance of LCG from a random string.

Solution:

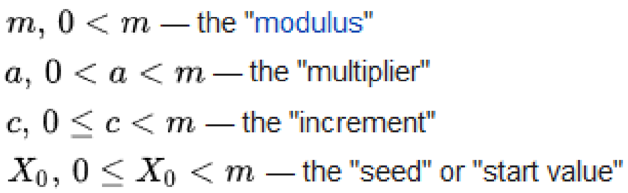
I supposed that multiplier, increment and modulus of linear congruential generator are unknown. Only what is known is the seed and several subsequent states. In my code states are called alternately “states”, “s” or “x” with the same meaning.

I started with finding modulus, in the code it is a function called unknown_modulus. From knowing several subsequent states I could introduce a sequence: $t_{(n)} = s_{(n+1)} - s_{(n)}$. Then, knowing that: x = 0(mod m) is the same as: x = w*m if x≠0 I could generate operations like following: $t_{(n+2)}*t_{(n)}–t_{(n+1)}*t_{(n+1)}$=0(mod m). Using Euclidean Algorythm I could determine the greatest common divisor from number of zeros which is a modulus.

Next, knowing subsequent states and modulus I could determine a multiplier, in the code it is a function called unknown_multiplier. Having linear equations of linear congruential generator such as: $x_{(n+1)}$ = a*$x_{(n)}$ + c (mod m) I could distinguish a multiplier using modular inverse.

Then, the last think to find was increment. In the code the function that deal with it is called unknown_increment. Having subsequent states, multiplier and modulus to find an increment I simply changed over the order of linear congruential generator algorithm.

To distinguish output generated by an instance of LCG from a random string I used conditions of linear congruential generator. They are as follows:



$m,\ 0 < m$ — the "modulus"

$a,\ 0 < a < m$ — the "multiplier"

$c,\ 0 \le c < m$ — the "increment"

$X_0,\ 0 \le X_0 < m$ — the "seed" or "start value"

The function that distinguish output considering given conditions in the code is called conditions.

Using all the known values: start value (seed), increment, multiplier and modulus, function of linear congruential generator called in the code lcd generates n number of states and prints the “next number”.