Özge Öneyman 24906

Homework 2

(1)

$n = 326$

$t = 81$

a) There are 162 elements in the group.

↳ There are 162 pos ints that relatively prime to 326.

b) Generators are 3, 7, 11, 19, 29, 45, 63, 67, 73, 75, 79, 89, 101, 103, 107 ...

c) $|\mathbb{Z}_{326}| = 81$

?

(2) $n = p \times q$

Compute $m = c^d \bmod n$ $(d = e^{-1} \bmod \phi(n))$

Plaintext = Answer to the ultimate question of life, the universe, and everything is not 42. it is 517.

(3)

plaintext1:

plaintext2: Our knowledge can only be finite, while our ignorance must necessarily be infinite

plaintext3:

(4) $ax \equiv b \mod n$

a) $\gcd(a,n) = 1$ → solution exist for this 56884393062303769019751449983. ~

b) $\gcd(a,n) = 3$ ⇒ solution not exist

c) $\gcd(a,n) = 3$ ⇒ solution not exist

> gcd = 3 cannot devided b.

(5)

$P_1(x) = x^5 + x^2 + 1$

the output of LFSR can have maximum period of $2^L - 1 = 2^L - 1 = 31$

$P_2(x) = x^5 + x^3 + x^2 + 1$ → Period = 12 → Its not generated.

L=5

Period = 31 ⇒ It generated maximum period sequence

(6) For the 3 sequence. When we use BM fonction it gives us binary sequence. ⇒ This connection is polynomial. ⇒ Thus, LFSR is predictable.

(7)