Tema 8 - Criptografie

20. Se folosește alfabetul de la ex. anterior, iar unitățile de mesaj sunt blocuri de 3 caractere.

Vom folosi criptosistemul ElGamal pentru a decripta mesajul.

Pasul 1: Identificarea cheilor și parametrilor:

Parametrii p și g sunt cei folosiți în criptosistemul ElGamal.
Cheia publică a lui Alice este: p, g, g^{α}.
Cheia privată este: α.

Pasul 2: Determinarea parametrilor de criptare / decriptare:

$p = 65537 \quad g = 5 \quad \alpha = 13908$

Mesajul criptat $(u, v) = (29095, 23946)$

Pasul 3:

Se calculează $w = u^{p-1-\alpha} \bmod p$

$mP = (v \cdot w) \bmod p$

MI: Vom implementa un cod C++ pentru a ne ușura munca:

tema8_20.cpp

Mesajul este: "G!T", am rulat de 2 ori, nu sunt sigură de rezultat

M II:

$w = u^{p-1-\alpha} \bmod p$

$w = 29095^{65536-13908} \bmod 65537$

Vom folosi exponențierea modulară rapidă:

mod_exp(29095, 51628, 65537) = 12345

$m' = (23846 \cdot w) \bmod 65537$

$m' = (23846 \cdot 12345) \bmod 65537$

$= 294590670 \bmod 65537$

$= 46790$

Împărțim m' în baza 30: 46790 : 30 = 1559 rest 10

1559 : 30 = 51 rest 29

51 : 30 = 1 rest 21

1 : 30 = 0 rest 1

Blocurile sunt: 1, 21, 29, 10

B = 1 V = 21 29 = . K = 10

→ Cred că am greșit la calcule.