Enunt

I. Polinomul primitiv

Forma generala a polinomului primitiv este $f(t) = At^3 + Bt^2 + Ct + D$.

Parametrii A, B, C si D vor fi calculati in urmatorul mod:

- A = 1;
- B - index alfabetic a celei de-a 2-a litera din numele de familie
- C este indexul alfabetic a primei litere din numele propriu
- D = 1;

Dar, cum exista patru polinoamele primitive de ordin 3:

1021
1121
1201
1211

Atunci:

a) Daca B = 0 => C=2 chiar daca din calcul rezulta alta valoare
b) Daca B = 1 => C=2 chiar daca din calcul rezulta alta valoare
c) Daca B = 2 atunci C poate lua numai valorile 0 sau 1; daca C are valoarea 2 din calcul, vom lua C=1;
   Adica B = 2 => C= 0 sau C=1.

Exemplu. Dan Ionescu -> A=1, B=15, C=4, D=1 => $t^3 + 2t + 1 = 0$.

II. Sa se cifreze cuvantul „COD" utilizand polinomul primitiv $f(t)$, pentru câmpul $GF(3^3)$, adica $N = 3^3 = 27$ litere (cele 26 de litere ale alfabetului plus cuvântul - spaţiu), si fie polinomul de permutare $y_i = a_i x_i + b_i$ cu $a_i \neq 0$, iar pentru parametrii a_i şi b_i regulile de recurenţă sunt:

- $a_{i+2}=a_{i+1}+a_i$
- $b_{i+2}=b_{i+1}*b_i$

cu valorile iniţiale:

$a_1 = (A\ mod(3), B\ mod(3), C\ mod(3))$
$a_2 = (D\ mod(3), C\ mod(3), A\ mod(3))$
$b_1 = ((A+1)\ mod(3), (B+1)\ mod(3), (C+1)\ mod(3))$
$b_2 = ((D+1)\ mod(3), (C+1)\ mod(3), (A+1)\ mod(3)).$

Se vor completa toate etapele (tabelele) ca in exemplul primit la seminar.