

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 urmatoarul 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:

- Daca B = 0 => C=2 chiar daca din calcul rezulta alta valoare
- Daca B = 1 => C=2 chiar daca din calcul rezulta alta valoare
- 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 cuvântul „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 - spațiu), si fie polinomul de permutare $y_i = a_i x_i + b_i$ cu $a_i \neq 0$, iar pentru parametrii a_i și b_i regulile de recurență sunt:

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

cu valorile inițiale:

$$a_1 = (A \bmod(3), B \bmod(3), C \bmod(3))$$

$$a_2 = (D \bmod(3), C \bmod(3), A \bmod(3))$$

$$b_1 = ((A + 1) \bmod(3), (B + 1) \bmod(3), (C + 1) \bmod(3))$$

$$b_2 = ((D + 1) \bmod(3), (C + 1) \bmod(3), (A + 1) \bmod(3)).$$

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

Sa se cifreze cuvantul COD.

	C	O	D
x	3	15	4
x-pol	0 1 0	1 2 0	0 1 1
x-exp	1	4	9
a-pol	1 2 1	2 1 2	2 1 1
a-exp	18	5	20
b-pol	2 0 0	0 0 2	0 1 0
b-exp	15	13	1
$a_i * x_i \text{ exp}$	19	9	3
$a_i * x_i \text{ pol}$	2 2 2	0 1 1	0 1 2
$a_i * x_i + b_i \text{ pol}$	1 2 2	0 1 0	0 2 2
$a_i * x_i + b_i \text{ exp}$	7	1	22
	17	C 3	8