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:

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 $B = 2 \Rightarrow C = 0$ 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 $y_i=a_ix_i+b_i$ 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 inițiale:

```
\begin{aligned} 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)). \end{aligned}
```

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

Enunt.

Utilizand polinomul primitiv f(t), $t^3 + 2t + 1 = 0$, 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 date sunt:

-
$$a_{i+2} = a_{i+1} + a_i$$

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

iar valorile inițiale:

- $a_1=(0,0,1)=26$; $a_2=(1,2,0)=4$

- $b_1=(0,1,0)=3$; $b_2=(1,0,2)=12$

	G			
exp-n	F			f _n
0	0	0	0	0
1	0	1	0	3
	1	0	0	9
3	0	1	2	5
4	1	2	0	15
2 3 4 5 6 7	2	1	2	23
6	1	1	1	13
7	1	2	2	17
8	2	0	2	20
9	0	1	1	4
10	1	1	0	12
11	1	1	2	14
12	1	0		11
13	0	0	2	2
14	0	2		6
15	2	0	0 0	18
16	0	2	1	7
17	2	1	0	21
18	1	2	1	16
19	2	2	2	26
20	2	1	1	22
21	1	0	1	10
22	0	2	2	8
23	2	2	0	24
24	2	2	1	25
25	2	0	1	19
26	0	0	1	1

a _{i+2} =a _{i+1} +a _i						
a _i Polinom						
a1	0	0	1			
a2	1	2	0			
a3	1	2	1			
a4	2	1	1			
a5	0	0	2			
a6	2	1	0			
a7	2	1	2			
a8	1	2	2			
a9	0	0	1			
a10	1	2	0			
a11	1	2	1			
a12	2	1	1			
a13	0	0	2			
a14	2	1	0			
a15	2	1	2			
a16	1	2	2			
a17	0	0	1			
a18	1	2	0			
a19	1	2	1			
a20	2	1	1			
a21	0	0	2			
a22	2	1	0			
a23	2	1	2			
a24	1	2	2			
a25	0	0	1			
a26	1	2	0			

$b_{i+2} = b_{i+1} * b_i$					
b_i	Polinon	1		Exponent_26	
b1	0	1	0	3	
b2	1	0	2	12	
b3	2	0	0	15	
b4	0	1	0	1	
b5	0	2	1	16	
b6	2	1	0	17	
b7	1	2	2	7	
b8	2	2	1	24	
b9	2	1	2	5	
b10	0	1	2	3	
b11	2	0	2	8	
b12	1	1	2	11	
b13	2	2	2	19	
b14	1	2	0	4	
b15	0	0	2	23	
b16	0	1	0	1	
b17	2	2	1	24	
b18	2	0	1	25	
b19	2	2	0	23	
b20	0	2	2	22	
b21	2	2	2	19	
b22	2	0	0	15	
b23	2	0	2	8	
b24	2	2	0	23	
b25	2	1	2	5	
b26	1	0	0	2	

Sa se cifreze cuvantul COD.

	С			0			D		
Х	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
а-ехр	18			5			20		
b-pol	2	0	0	0	0	2	0	1	0
b-exp	15			13			1		
a _i *x _i exp	19			9			3		
a _i *x _i pol	2	2	2	0	1	1	0	1	2
a _i *x _i +b _i pol	1	2	2	0	1	0	0	2	2
a _i *x _i +b _i exp	7			1			22		
		17		С	3			8	