$0 = (0,0,0)$ ou $f_0 = 0$

$t = (0,1,0)$ $f_1 = 3$

$t^2 = (1,0,0)$ $f_2 = 9$

$t^3 = (0,1,2)$ $f_3 = ?$

$GF(3^3)$ $f(t) = t^3 + 2t + 1 = 0$

$t^3 = -2t - 1$

$|-2| \bmod(3) = 1$

$|-1| \bmod(3) = 2$

$t^3 = 1 \cdot t + 2$

$1 \cdot t + 2 = (0,1,2) \Rightarrow 1 \cdot 3 + 2 = 5$

$GF(3^3)$ N $3^3 = 27$

$y_1 = a_1 x_1 + b_1$, $a_1 \neq 0$

$a_{i+2} = a_{i+1} + a_i$ $\quad i = 1,2,3$

$b_{i+2} = b_{i+1} \cdot b_i$ $\quad i = 1,2,3$

de adunat mod(3)

$a_1 = (0,2,1) = t^{16}$

$a_2 = (1,1,1) = t^{6}$

$b_1 = (0,0,2) = t^{13}$

$b_2 = (1,1,0) = t^{10}$

$(13 + 10) \bmod (26) = 23$

valoarea din camp GALOIS

Cifrare litere

(a)	S
i(b)	19 (index literă alfabet)
x(c)	(2,0,1)
x(d)	25
a(e)	(1,0,2) (indexul din tabelă pag 2 a_{19})
a(f)	12 (t-ul pentru a(e) tot pag 2)
b(g)	(0,1,1) (ne ia puterea din tabelul Galois t pentru a(f))
b	9 (din tabel, valoarea lui b(g))
(h)	26
(i)	E (index literă)

în câmpul Galois, $19 = t^{25}$

$= (2,0,1)$

$0 = (0,0,0)$ $f_0 = 0$

$t = (0,1,0)$ $f_1 = 3$

$t^2 = (1,0,0)$ $f_2 = 9$

$t^3 = (0,1,2)$ $f_3 = 5$

$t^4 = (1,2,0)$ $f_4 = 15$

$t^5 = (2,1,2)$ $f_5 = 23$

$t^6 = (1,1,1)$ $f_6 = 13$

$t^7 = (1,2,2)$ $f_7 = 17$

$t^8 = (2,0,2)$ $f_8 = 20$

$t^9 = (0,1,1)$ $f_9 = 4$

$t^{10} = (1,1,0)$ $f_{10} = 12$

$t^{11} = (1,1,2)$ $f_{11} = 14$

$t^{12} = (1,0,2)$ $f_{12} = 11$

$t^{13} = (0,0,2)$ $f_{13} = 2$

$t^{14} = (0,2,0)$ $f_{14} = 6$

$t^{15} = (2,0,0)$ $f_{15} = 18$

$t^{16} = (0,2,1)$ $f_{16} = 7$

$t^{17} = (2,1,0)$ $f_{17} = 21$

$t^{18} = (1,2,1)$ $f_{18} = 16$

$t^{19} = (2,2,2)$ $f_{19} = 26$

$t^{20} = (2,1,1)$ $f_{20} = 22$

$t^{21} = (1,0,1)$ $f_{21} = 10$

$t^{22} = (0,2,2)$ $f_{22} = 8$

$t^{23} = (2,2,0)$ $f_{23} = 24$

$t^{24} = (2,2,1)$ $f_{24} = 25$

$t^{25} = (2,0,1)$ $f_{25} = 19$

$t^{26} = (0,0,1)$ $f_{26} = 1$

a_i			
a_1	0	1	1
a_2	1	2	1
a_3	1	0	2
a_4	2	2	0
a_5	0	2	2
a_6	2	1	2
a_7	2	0	1
a_8	1	1	0
a_9	0	1	1
a_{10}	1	2	1
a_{11}	1	0	2
a_{12}	2	2	0
a_{13}	0	2	2
a_{14}	2	1	2
a_{15}	2	0	1
a_{16}	1	1	0
a_{17}	0	1	1
a_{18}	1	2	1
a_{19}	1	0	2
a_{20}	2	2	0
a_{21}	0	2	2
a_{22}	2	1	2
a_{23}	2	0	1
a_{24}	1	1	0
a_{25}	0	1	1
a_{26}	1	2	1

b_i				
b_1	0	0	2	13
b_2	1	1	0	10
b_3	2	2	0	23
b_4	1	2	2	7
b_5	1	2	0	4
b_6	1	1	2	11
b_7	2	0	0	15
b_8	0	0	1	26
b_9	2	0	0	15
b_{10}	2	0	0	15
b_{11}	1	2	0	4
b_{12}	2	2	2	19
b_{13}	2	2	0	23
b_{14}	0	2	1	16
b_{15}	0	0	2	13
b_{16}	0	1	2	3
b_{17}	0	2	1	16
b_{18}	2	2	2	19
b_{19}	0	1	1	9
b_{20}	1	0	0	2
b_{21}	1	1	2	11
b_{22}	0	0	2	13
b_{23}	2	2	1	24
b_{24}	1	1	2	11
b_{25}	0	1	1	9
b_{26}	2	1	1	20

	D	A
x	4	1
x-pol	(0,1,1)	(0,0,1)
x-exp	3	26
a-pol	(2,2,0)	(0,1,1)
a-exp	23	9
b-pol	(1,2,2)	(0,0,2)
b-exp	7	13
h	18	3
i	R	C

$y_4 = t^{23} \cdot t^{9} + (1,2,2)$

$= t^{6} + (1,2,2) =$

$= (1,1,1) + (1,2,2) = (2,0,0) = 18$

$y_1 = t^{9} \cdot t^{26} + (0,0,2)$

$= t^{9} + (0,0,2)$

$= (0,1,1) + (0,0,2) = (0,1,0)$

$= 3$