Tablas del Campo

$f(x) = x^4 + x + 1$ sea a raíz del polinomio

$a^4 + a + 1 = 0$ → $a^4 = -a - 1$ → $a^4 = a + 1$ Xor

$$GF(2^4)$$

			decimal	binario
a^0	1		1	0001
a^1	x	$\to x \cdot a^{n-1}$	2	0010
a^2	x^2	idem todos	4	0100
a^3	x^3		8	1000
a^4	$x(x^3) = x^4 = x+1$		3	0011
a^5	$x \cdot (x+1) = x^2 + x$		6	0110
a^6	$x^3 + x^2$		12	1100
a^7	$x^3 + x + 1$	$(x+1)$	11	1011
a^8	$x^2 + 1 = x \cdot (x^3 + x + 1) = x^4 + x^2 + x$		5	0101
a^9	$x^3 + x$		10	1010
a^{10}	$x^2 + x + 1$		7	0111
a^{11}	$x^3 + x^2 + x$		14	1110
a^{12}	$x^3 + x^2 + x + 1$		15	1111
a^{13}	$x^3 + x^2 + 1$		13	1101
a^{14}	$x^3 + 1$		9	1001
a^{15}	$x \cdot (x^3 + 1) = x^4 + x = (x+1) + x = 1$		1	0001

Xor

Polinomio Generador

$$g(x) = (x + \alpha) \cdot (x + a^2) \cdot \ldots \cdot (x + \alpha^{n-k})$$

$$\frac{n-k}{2} = t \rightarrow \text{puede corregir} \checkmark$$

$$\frac{6}{2} = t \rightarrow \boxed{t = 3} \,\hat{}$$

$$g(x) = \underbrace{(x + a^1) \cdot (x + a^2)}_{A} \cdot \underbrace{(x + a^3)(x + a^4)}_{B} \underbrace{(x + a^5)(x + a^6)}_{C}$$

$$\underbrace{\qquad\qquad\qquad}_{I} \qquad \underbrace{\qquad\qquad}_{C.}$$

$A = x^2 + x a^2 + a^1 x + a^1 a^2$

$\quad x^2 + x(2^1 + 2^2) + 2^1 2^2$

$\quad x^2 + x(x + x^2) + 2^3$

$\qquad 6 = a^5 + 2^3 \quad = x^2 + a^5 x + 2^3$

$B = x^2 + x a^4 + 2^3 x + 2^3 2^4 \qquad\qquad A \times B = I$

$\qquad\qquad\qquad\qquad\qquad (x^2 + a^5 x + 2^3) \cdot (x^2 + 2^9 x + 2^7)$

$x^2 + x(2^4 + 2^3) + 2^3 2^4 \qquad x^4 + x^3 2^7 + x^2 2^7 + a^5 x^3 + 2^{12} x^2 + 2^{12} x$

$\quad x(2^7) + 2^2 \qquad\qquad + 2^3 x^2 + 2^6 x + 2^{10}$

$x^2 + 2^7 x + 2^7 \qquad\qquad x^4 + x^3 a^{13} + x^2 a^6 + a^{10}$

$\qquad\qquad\qquad\qquad\qquad\quad \uparrow$

$\qquad\qquad\qquad\qquad\text{Simbinatria}$

$C = x^2 + a^9 x + a^{11}$

$$\boxed{I \times C}$$

$$g(x) = x^6 + x^5 a^{10} + x^4 a^{19} + x^3 a^4 + x^2 a^6 + x a^9 + a^6$$

$$I(x) = a + a^4x + a^{15}x^2 + a^{10}x^3 + a^4x^4 + a^5x^5 + a^6x^6 + a^3x^7 + a^8x^8$$

$$\overset{15}{\underset{nk}{X}}\overset{9}{}$$

$$x^6 \cdot I(x) = x^6 \cdot I(x) = a x^{14} + a^3 x^{13} + a x^{12} + a x^{11} + a^9 x^{10} + a^{10} x^9$$
$$a^{15} x^8 + a^4 x^7 + a x^6$$

$$x^6 \cdot I(x) \lfloor g(x)$$
$$a x^8 + a^6 x^7 + a x^6 + a^{12} x^5 + a^7 x^4 + a^{11} x^3 + a^2 x^2$$
$$\cdots \quad + a^{13} x + a^3$$

Resto $x^5 a^6 + x^4 a^3 + x^3 a^2 + x^2 a^0 + x a^9 + a^{14} \rightarrow$ Paridad

$$V(x) = a^{14} + a^9 x + a^0 x^2 + a^2 x^3 + a^{-3} x^4 + a^6 x^5 + a x^6 + a^4 x^7 \cdots \sqcup I$$
$$\underbrace{}_{} \quad \underbrace{}_{\text{Paridad}} \quad \underbrace{}_{\text{Información}}$$

$$E(x) = a^7 x^2 + a^{13} x^8 + a^3 x^{10}$$

$$B(x) = V(x) + E(x)$$

$$E_n \ x^2 = a^0 \oplus a^7 = a^9$$
$$x^8 = a^{15} \oplus a^{13} = a^6$$
$$x^{10} = a^4 \oplus a^3 = a^7$$