El cuerpo de AES

2^8=256 elementos
(cada elemento es un byte diferente)

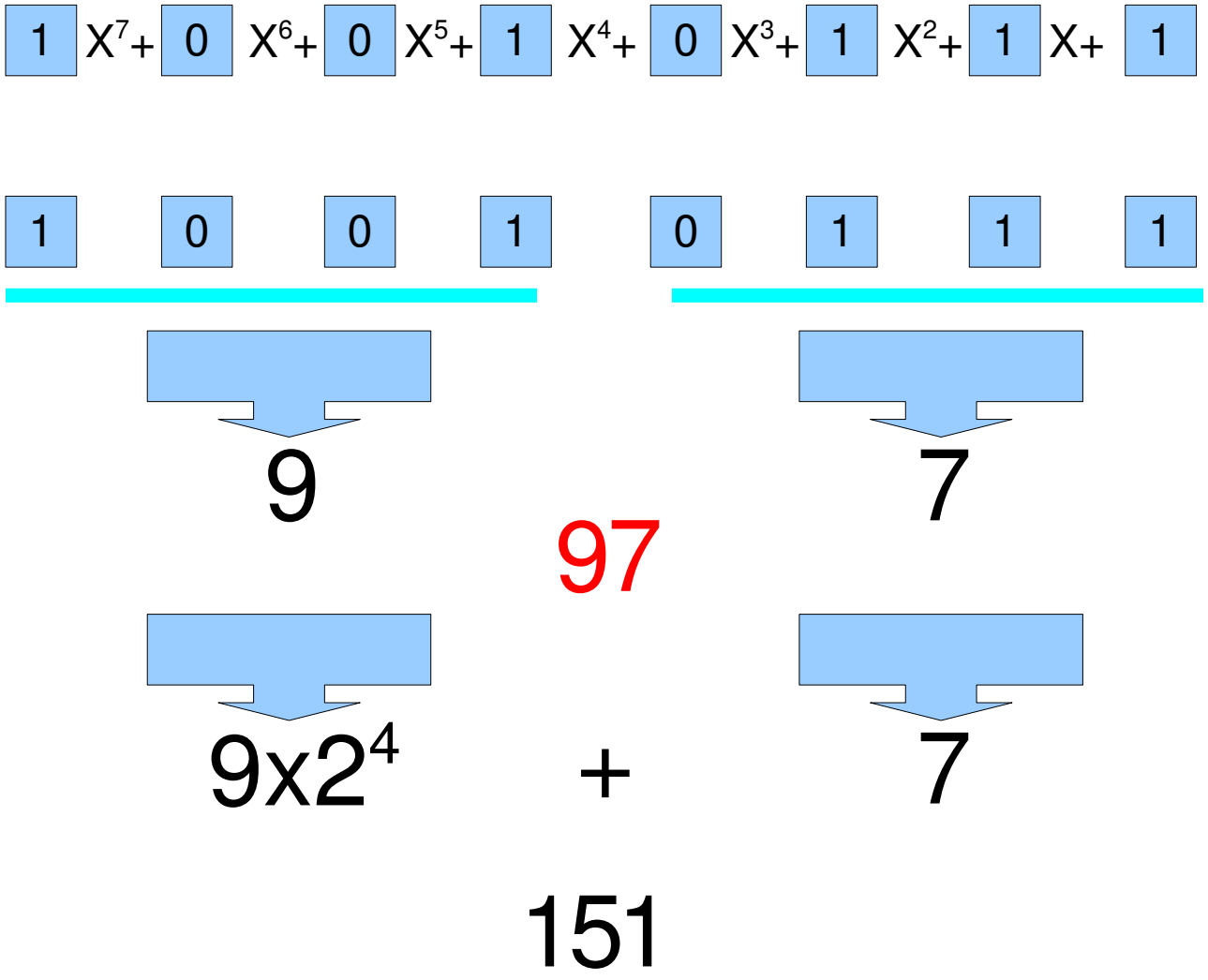
Se construye a partir de los polinomios
con coeficientes 0,1 (polinomios en binario)

aes(X)=$X^8+X^4+X^3+X+1$ (irreducible)

De cada polinomio binario se toma sólo
el resto de dividir por aes(X)

Los posibles restos son polinomios de grado <8, es decir,
tienen 8 coeficientes=1byte

El cuerpo de AES



Representaciones de un elemento

polinomio $1X^7+0X^6+0X^5+1X^4+0X^3+1X^2+1X+1$

binario 1 0 0 1 0 1 1 1

hexadecimal 97

decimal 151

Representaciones de un elemento

binario

De 00000000 a 11111111

hexadecimal 97

De 00 a FF

decimal 151

De 0 a 255

Operaciones en F_{256}

Suma

Binario

	1 0 0 1 0 1 1 1
XOR	1 0 1 0 1 0 0 1
	0 0 1 1 1 1 1 0

Operaciones en F_{256}

Producto

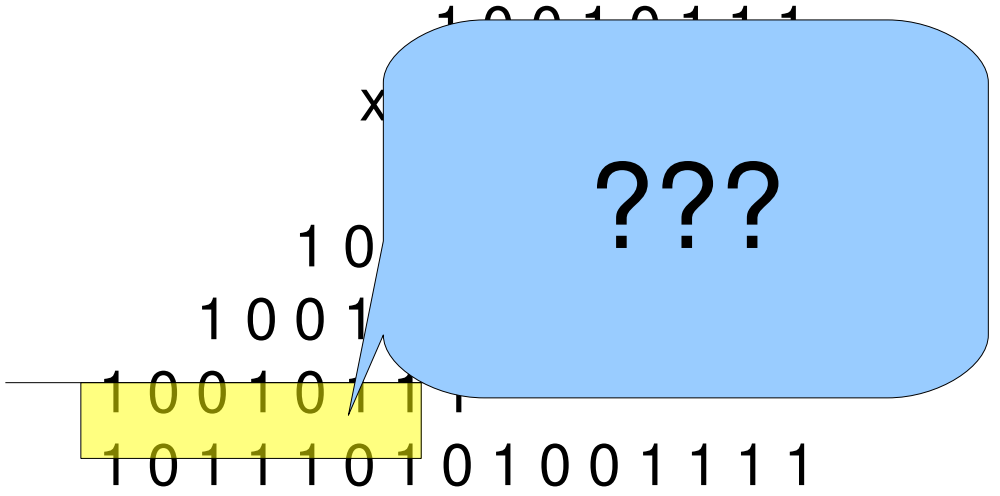
Polinomios

```
                    1 0 0 1 0 1 1 1        97
                x   1 0 1 0 1 0 0 1        A9
                    ---------------
                    1 0 0 1 0 1 1 1
              1 0 0 1 0 1 1 1
          1 0 0 1 0 1 1 1
      1 0 0 1 0 1 1 1
  ---------------------------------------
      1 0 0 1 0 1 1 1
      1 0 1 1 1 0 1 0 1 0 0 1 1 1 1
```

Operaciones en F_{256}

Producto

Polinomios



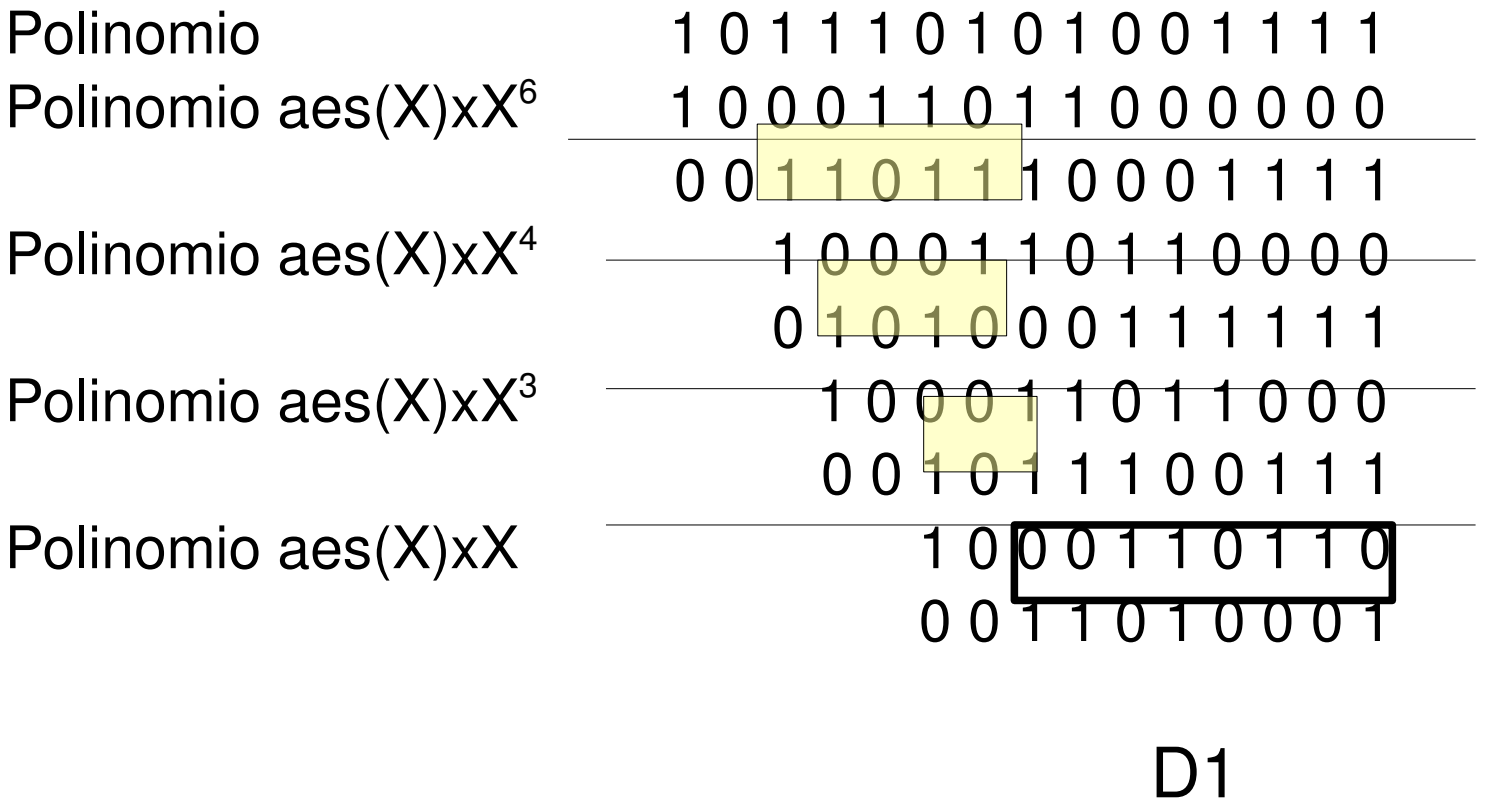
Operaciones en F_{256}

Producto

Polinomio	1 0 1 1 1 0 1 0 1 0 0 1 1 1 1
Polinomio aes(X)xX^6	1 0 0 0 1 1 0 1 1 0 0 0 0 0 0
	0 0 1 1 0 1 1 1 0 0 0 1 1 1 1

Operaciones en F_{256}

Producto



Operaciones en F_{256}

Un método alternativo para el producto:

La idea es ordenar los elementos de F_{256} de un modo diferente

Se usa que todos los elementos (menos el 0) pueden generarse como potencias de uno dado:elemento primitivo.

El elemento primitivo más sencillo es X+1=00000011=03

Se elabora una tabla con todas las potencias de X+1

Hacer el producto por X+1 es sencillo

Multiplicando un polinomio por X+1

```
  1 0 0 1 0 1 1 1          97
          X  1 1           03
  1 0 0 1 0 1 1 1
1 0 0 1 0 1 1 1
1 1 0 1 1 1 0 0 1
```

Se desplaza un lugar a la izquierda
y se hace XOR con el original.

Si el primer dígito a la izquierda es 0 ya está;
Si es 1 se hace XOR con 100011011.

En este caso

```
          1 1 0 1 1 1 0 0 1
  XOR     1 0 0 0 1 1 0 1 1
          0 1 0 1 0 0 0 1 0
```

Tabla de potencias o antilogaritmos (en base X+1=03)

0	01
1	03
2	05
3	0F
4	11
5	33
6	55
7	FF
8	1A
.	.
.	.
.	.
255	01

Se ordenan en una tabla 16x16
con los exponentes escritos
también en hexadecimal

Cálculo del producto usando las tablas de logaritmos y antilogaritmos

Ejemplo: 97xA9

Primer paso: se buscan los logaritmos correspondientes

Cálculo del producto usando las tablas de logaritmos y antilogaritmos

Ejemplo: 97xA9

Primer paso: se buscan los logaritmos correspondientes

log(97)=F5
log(A9)=43

Cálculo del producto usando las tablas de logaritmos y antilogaritmos

Ejemplo: 97xA9

Primer paso: se buscan los logaritmos correspondientes
Segundo paso: se suman módulo 255 (por qué??)

$\log(97)=F5_h=245$

$\log(A9)=43_h=67$

$245+67=57=39_h$

Cálculo del producto usando las tablas de logaritmos y antilogaritmos

Ejemplo: 97xA9

Primer paso: se buscan los logaritmos correspondientes

Segundo paso: se suman módulo 255

$\log(97)=F5_h=245$

$\log(A9)=43_h=67$

$$245+67=57=39_h$$

Tercer paso:En la tabla de antilogaritmos se busca qué elemento es ésta potencia:

Cálculo del producto usando las tablas de logaritmos y antilogaritmos

Ejemplo: 97xA9

Primer paso: se buscan los logaritmos correspondientes

Segundo paso: se suman módulo 255

$\log(97)=F5_h=245$

$\log(A9)=43_h=67$

$$245+67=57=39_h$$

Tercer paso:En la tabla de antilogaritmos se busca qué elemento es ésta potencia:

D1 ¡¡¡¡bien!!!!!

Cálculo del inverso usando las tablas:

Dado un elemento b

$$b^{-1}=Alog(FF-log(b))$$

Puesto que si $b=(03)^s$

$(03)^s(03)^{255-s}=(03)^{255}=1$