



Actividad 10.-Multiplicación en GF(2⁸)

Por equipos (a,b,c.. f)

Resolver la siguiente multiplicacion en GF(2⁸)

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 82 & B2 & 63 & 77 \\ 63 & C5 & 9C & E2 \\ A2 & FC & 93 & F2 \\ 20 & E2 & 67 & AD \end{pmatrix} = \begin{pmatrix} 38 & 35 & 8D & 8C \\ 99 & DE & 8B & 08 \\ DE & A9 & 6B & 86 \\ 1C & 2B & 64 & C8 \end{pmatrix}$$

Para repartir los ejercicios seguir las instrucciones del video de clase.
Reemplazar los valores de las variables a,b,c, ..., p por los resultados obtenidos.

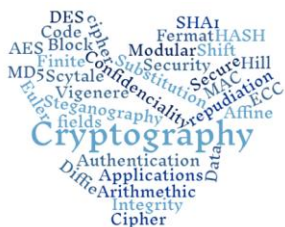
El coordinador designará al responsable de juntar los procedimientos, elaborar este documento y subirlo a classroom. El resto solo debe marcar su tarea como entregada y poner en comentarios el nombre de quien sube el archivo.

Nota: Los procedimientos deben realizarse a mano, debes escanear tus notas y juntarlas con este documento o tomar una foto e incluirla como imagen al final de este archivo.

Trabajos sin procedimientos a mano valen 0 puntos.

Al finalizar guarda un sólo archivo como PDF para subirlo a Classroom.

M. en C. Nidia A. Cortez Duarte





Actividad 10.-Multiplicación en GF(2⁸)

- RAMIREZ OLVERA GUILLERMO

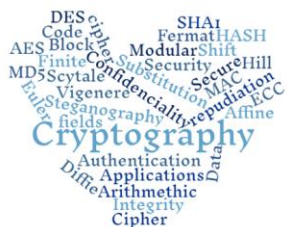
$$e = 82 \times 1 + 63 \times 2 + A2 \times 3 + 20 \times 1$$

(1) (2) (3) (4)

(2) $\Rightarrow 0x63 = 0110\ 0011$
 $0x63 \times 2 = 1100\ 0110 = 0xC6$

(3) $\Rightarrow 0xA2 = 1010\ 0010$
 $0xA2 \times 2 = 101\ 0001\ 00$
 $0101\ 0001\ 0$
 $111\ 1001\ 10$
 $1000\ 1101\ 1$
 $0111\ 1101$
F D

82
xor C6
FD
20
99





Actividad 10.-Multiplicación en GF(2⁸)

$F = 02 * 1 + 05 * 2 + FC * 3 + E2 * 1$
① ② ③ ④

② $\Rightarrow 2 \Rightarrow 0 \times 02 = 0000\ 0010 = X$

$05 = 1100\ 0101 = X^7 + X^6 + X^2 + 1$

$$\begin{array}{r} X^7 + X^6 + X^2 + 1 \\ \times X \\ \hline X^8 + X^7 + X^3 + X \end{array}$$

$$\begin{array}{r} 1 \\ X^8 + X^4 + X^3 + X + 1 \overline{) X^8 + X^7 + X^3 + X} \\ \hline X^7 + X^4 + 1 \\ 1001\ 0001 \\ \underline{9\ 1} \end{array}$$

③ $\Rightarrow 3 \Rightarrow 0011 = X + 1$

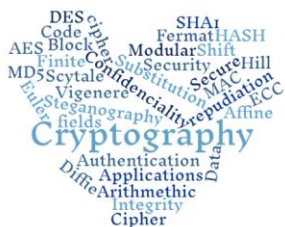
$0X\ FC = 1111\ 1100 = X^7 + X^6 + X^5 + X^4 + X^3 + X^2$

$$\begin{array}{r} X^7 + X^6 + X^5 + X^4 + X^3 + X^2 \\ \times X + 1 \\ \hline X^8 + X^7 + X^6 + X^5 + X^4 + X^3 + X^2 + X^7 + X^6 + X^5 + X^4 + X^3 \\ \hline X^8 + X^2 \end{array}$$

$$\begin{array}{r} 1 \\ X^8 + X^4 + X^3 + X + 1 \overline{) X^8 + X^2} \\ \hline X^4 + X^3 + X^2 + X + 1 \\ 0001\ 1111 \\ \underline{1\ F} \end{array}$$

$$\begin{array}{r} X^8 + X^2 \\ \text{xor } 02 \\ \hline 91 \\ \text{xor } 91 \\ \hline 1F \\ \text{xor } 1F \\ \hline E2 \\ \text{xor } E2 \\ \hline DE \end{array}$$

M. en C. Nidia A. Cortez Duarte





Actividad 10.-Multiplicación en GF(2⁸)

- SANCHEZ MENDEZ EDMUNDO JOSUE

Calculando h "Cajas"

$$h = 01 \times 77 + 02 \times E2 + 03 \times F2 + 01 \times AD$$

$01 \times 77 = 77$

$02 \times E2 = 111000100 = DF$

$03 \times F2 = 11116010 = 0D$

$01 \times AD = AD$

h = 0x08

Calculando y "Polinomio"

$$y = 01 \times 63 + 02 \times 9C + 03 \times 93 + 01 \times 67$$

$01 \times 63 = 63$

$02 \times 9C = 100111000 = x^8 + x^5 + x^4 + x^3 = 23$

$03 \times 93 = 02 \times 93 = 100100110 = AE$

$93 = 10010011$

$110110101 = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$





Actividad 10.-Multiplicación en GF(2⁸)

Handwritten work on graph paper showing polynomial multiplication in GF(2⁸).

Top part: Polynomial multiplication of $x^0 + x^4 + x^3 + x^1$ and $x^0 + x^7 + x^5 + x^4 + x^2 + 1$.

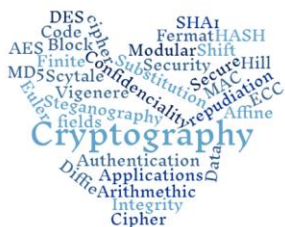
Bottom part: XOR operation on hexadecimal values.

XOR:

$$\begin{array}{r} 63 \\ 23 \\ \oplus \\ AC \\ \hline 67 \\ \oplus \\ 8B \end{array}$$

Result: 01x67 = 67

Equation: $y = 0x8B$





Actividad 10.-Multiplicación en GF(2⁸)

- BERNAL RAMIREZ ANDRE

Handwritten work on grid paper showing calculations in GF(2⁸).

Initial values:

02	03	01	01
01	02	03	03
01	01	02	02
03	01	01	02

82	B2	63	77
63	C5	9C	E2
A2	FC	93	F2
20	E2	67	AD

9	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

Calculation for i:

$$i = (01 * 82) + (01 * 63) + (02 * A2) + (03 * 20)$$

02 x A2 x 2 = 10 10 0 0 1 0 0

XOR 1000 1 1 0 1 1

00 10 1 1 1 1 1

S F

20 x 2 = 00 1 0 0 0 0 0 0

20 00 1 0 0 0 0 0

XOR 0 1 1 0 0 0 0 0

6 0

Calculation for j:

$$j = (01 * B2) + (01 * C5) + (02 * FC) + (03 * E2)$$

A = FC = $x^7 + x^6 + x^5 + x^4 + x^3 + x^2$

B = 00 00 00 10 = x

$x^8 + x^4 + x^3 + x + 1$

Polynomial division:

$$\begin{array}{r} x^8 + x^4 + x^3 + x + 1 \\ - (x^8 + x^4 + x^3 + x + 1) \\ \hline 0 \end{array}$$

Result: 1 1 1 0 0 0 1 1

E 7 6 5 4 3 2 1

E 3



Actividad 10.-Multiplicación en GF(2⁸)

$$\begin{array}{l} A \quad 11100010 = x^7 + x^6 + x^5 + x \\ B \quad 00000011 = x + 1 \end{array}$$

$$\begin{array}{r} x^7 + x^6 + x^5 + x \\ x + 1 \\ \hline x^8 + x^7 + x^6 + x^2 \\ + \quad x^7 + x^6 + x^5 + x \\ \hline x^8 + x^5 + x^2 + x \end{array}$$

$$\begin{array}{r} x^8 + x^4 + x^3 + 1 \overline{) x^8 + x^5 + x^2 + x} \\ -x^8 + x^4 + x^3 - x - 1 \\ \hline x^5 + x^3 + x^2 + 1 \end{array}$$

$$\begin{array}{r} 00111101 \\ 3 \quad D \end{array}$$

$$\begin{array}{r} J = B2 \\ C5 \\ \text{xOR } F3 \\ 3B \\ \hline A9 \end{array}$$

$$K = (01 \times 63) + (01 \times 9C) + (02 \times 93) + (03 \times 67)$$

$$\begin{array}{r} 02 \times 93 \times 2 = 100100110 \\ 100011011 \\ \hline 000111101 \\ 3 \quad D \end{array}$$

$$\begin{array}{r} K = 63 \\ 9C \\ \text{xOR } 3D \\ A9 \\ \hline 6B \end{array}$$

$$\begin{array}{r} 0 \times 67 \times 02 = 011001110 \\ 67 = 01100111 \\ \hline 10101001 \\ A \quad 9 \end{array}$$



Actividad 10.-Multiplicación en GF(2⁸)

CEDILLO HERNANDEZ JUAN DANIEL

Handwritten work on grid paper showing the multiplication of two 4x4 matrices in GF(2⁸).

Matrix 1 (Left):

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

Matrix 2 (Right):

$$\begin{pmatrix} 82 & B2 & 63 & 77 \\ 63 & C5 & 9C & E2 \\ A2 & FC & 93 & F2 \\ 20 & 1E2 & 67 & AD \end{pmatrix}$$

Result Matrix (Far Right):

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix}$$

Calculation for element 'l':

$$l = (01 * 77) + (01 * E2) + (02 * F2) + (03 * AD)$$

Handwritten notes:

Como sabemos todo número multiplicado por 1 es el número mismo. 77 y E2 se quedan así.

Binary conversions:

0xF2 = 1111 0010
0xF2 x2 = 1110 0100
XOR: 1000 1101
F

0xAD x2 = 1010 1101
AD = 1010 1101
XOR: 1111 1011
XOR: 1000 1101
E

Final result for 'l':

l = 77
E2
XOR: FF
EC
0x86
134 decimal

Methodo puros

Calculation for 'm':

$$m = (03 * 82) + (01 * 63) + (01 * A2) + (02 * 20)$$

Polynomial representations:

A = 0000 0011 = x + 1
B = 1000 1010 = x⁷ + x

Reduction:

reduciendo x⁸ + x⁴ + x³ + x + 1

Final result for 'm':

1001 1101
9 D

M. en C. Nidia A. Cortez Duarte



Actividad 10.-Multiplicación en GF(2⁸)

A 0000 0010 = X⁵
B 0010 0000 = X⁵

$$\begin{array}{r} * X^5 \\ X \\ \hline X^6 \end{array}$$

$$\begin{array}{r} 0100 \quad 0000 \\ 4 \quad 0 \end{array}$$

m = 90
63
A2
90
1C = 28 decimal

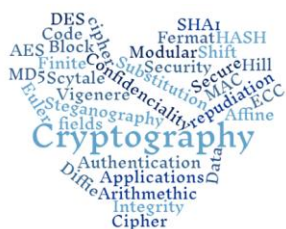
$$n = (03 * B2) + (01 * C5) + (01 * FC) + (02 * E2)$$

$$\begin{array}{r} 0x B2 \times 2 = 1011 \ 0010 \ 0 \\ 0x B2 = 101 \ 1001 \ 0 \\ \hline \text{XOR} \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \\ \text{XOR} \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \\ \hline 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \\ \hline \quad \quad C \quad \quad D \end{array}$$

$$n = 0xE2 \times 2 = 1110 \ 0010 \ 0$$
$$\begin{array}{r} 1000 \ 1101 \ 1 \\ \hline 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \\ \hline \quad \quad D \quad \quad F \end{array}$$

n = CD
C5
FC
DF
2B = 43 decimal

Metodo cajas





Actividad 10.-Multiplicación en GF(2⁸)

- COVARRUBIAS SANCHEZ DANIEL

Handwritten work on lined paper showing the multiplication of 03 and 63 in GF(2⁸).

Top part: A table of hexadecimal values and their corresponding letters.

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

B2	B2	63	77
63	C5	9C	E2
A2	FC	93	F2
20	E2	67	A0

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

Para 0)

$0 = 03 \cdot 63 + 01 \cdot 9C + 01 \cdot 93 + 02 \cdot 67$

$0 \times 63 \cdot 3 = 0 \times 63 \cdot 2 + 0 \times 63$

$0 \times 63 \cdot 2 = 011000110$

$+ 0 \times 63 = 01100011$

10100101

$0 \times 67 \cdot 2 = 11001110 = 0 \times CE$

A5

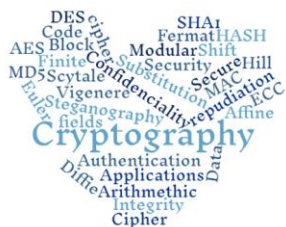
9C

0) XOR 93

CE

64

0) 0x64





Actividad 10.-Multiplicación en GF(2⁸)

Para p) $p = 03 \cdot 77 + 01 \cdot E2 + 01 \cdot F2 + 02 \cdot AD$

$A = 77 = 0111\ 0111 = x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + x^0$
 $B = 0000\ 0011 = x^1 + x^0$

$$\begin{array}{r} x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1 \\ \underline{x^1 + 1} \\ x^7 + x^6 + x^5 + x^3 + x^2 + x \\ \underline{x^6 + x^5 + x^4 + x^3 + x^2 + x + 1} \\ x^7 + x^4 + x^3 + 1 \end{array}$$

$A = AD = 1010\ 1101 = x^7 + x^5 + x^3 + x^2 + 1$
 $B = 0000\ 0010 = x$
 $= x^8 + x^6 + x^4 + x^3 + x$

$$\begin{array}{r} x^8 + x^4 + x^3 + x + 1 \mid x^8 + x^6 + x^4 + x^3 + x \\ \underline{-x^8 - x^4 - x^3 - x - 1} \\ x^6 + 1 \end{array} \rightarrow \begin{array}{r} 1001, 0001 \\ 4 \quad 1 \end{array}$$

99
E2
p) XOR F2
41
C8

M. en C. Nidia A. Cortez Duarte

