

# Instituto Politécnico Nacional

## Escuela Superior de Cómputo

Cryptography

### Práctica 6: Block ciphers 21/02/19



Nombres:

- Santuario Parra Luis Fernando
- Varela Cruz Cesar Alejandro

Grupo: 3CM6

---

<b>Introducción</b>	<b>3</b>
<b>Objetivo</b>	<b>3</b>
<b>Desarrollo</b>	<b>3</b>
Ejercicio 1	3
Ejercicio Programación	4
Función 1 (Multiplicación)	4
Función 2 (Representación polinomial)	5
Función 3 (S-box)	6
<b>Conclusiones</b>	<b>7</b>
Santuario Parra Luis Fernando	7
César Alejandro Varela Cruz	7
<b>Referencias</b>	<b>7</b>
<b>Anexo</b>	<b>8</b>

## Introducción

En el sistema de cifrado AES es necesario realizar operaciones de campo [4] y para poder lograr esto se necesita trabajar con polinomios, sin embargo un algoritmo con matrices o que use una representación de dichos polinomios como usualmente los manejamos es ineficiente y poco práctico a la hora de programar, es por ello que para realizar estas operaciones tenemos que recurrir a las operaciones a nivel de bits que nos permiten obtener una representación binaria de dichos polinomios así como poder trabajar con ellos de una forma más eficiente.

## Objetivo

Implementar la operación de multiplicación en  $GF(2)$  para polinomios de longitud  $n$  y generar la S-Box de AES utilizando los inversos multiplicativos de  $GF(2^8)$ .

## Desarrollo

### Ejercicio 1

Siendo  $a=25$  obtener  $b$  que es el valor de la S-box de AES de la fila 2 columna 5:

$a = 25$  entonces  $a = 4D$  por lo que puede ser representada como  $a = 0100\ 1101$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \text{mod}2$$

Al realizar la multiplicación de la matriz de 8x8 por el valor de  $a$  nos queda


$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \text{mod}2$$

Y al realizar la operación obtenemos:

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = 3F$$

## Ejercicio Programación

### Función 1 (Multiplicación)

 Símbolo del sistema - java multirred.MultIrred

Opciones:

- 1.-Multiplicación
- 2.-Representación Polinomial
- 3.-S-box
- 4.-Salir

1

Escriba un (a) numero en binario

10110100

Escriba un (b) numero en binario

11111

Escriba el polinomio irreducible

10000001

Resultado

11100001 = e1

Código:

```
int sum=0,num=0;
```


```
for(int i=0;i<=(int)(Math.log(a)/Math.log(2));i++){
    if(((int)Math.pow(2, i)&a)!=0){
        num=b;
        for(int j=0;j<i;j++){
            num=num<<1;
            if((int)(Math.log(num)/Math.log(2))>=(int)(Math.log(m)/Math.log(2))){
```

```

        num^=m;
    }
}
sum^=num;
}
}
return sum;

```

## Función 2 (Representación polinomial)

 Símbolo del sistema - java multirred.Multlrred

Opciones:

- 1.-Multiplicación
- 2.-Representación Polinomial
- 3.-S-box
- 4.-Salir

2

Escriba un (a) numero en binario

100011011

$X^8 + X^4 + X^3 + X^1 + 1$

Código:

String polinomio = "";

```

for(int i=(int)(Math.log(a)/Math.log(2));i>=0;i--){
    if(((int)Math.pow(2, i)&a)!=0){
        if(polinomio.equals("")){
            if(i!=0){
                polinomio += "X^"+i;
            }
            else{
                polinomio += "1";
            }
        }
        else{
            if(i!=0){

```


```

        polinomio += " + X^"+i;
    }
    else{
        polinomio += " + 1";
    }
}
}
}

System.out.println("\n\n"+polinomio"\n");

```

### Función 3 (S-box)

 Símbolo del sistema - java multirred.MultIrrred

Opciones:

- 1.-Multiplicación
- 2.-Representación Polinomial
- 3.-S-box
- 4.-Salir

3

Escriba un numero en Hexadecimal para calcular el equivalente de la S-box de aes

25

$25^{-1} = 111111 = 3F$

Código:

```

int c = Integer.parseInt("10001111",2);
    int b = 0;
    int val = 0;

    for(int i=0;i<8;i++){
        val=0;
        for(int j=0;j<8;j++){
            val ^= c>>(7-j) & a>>j;
        }
        val&=1;
        c |= c<<8;
        c >>= 1;
        c &= 255;

        b |= val<<i;
    }
    b^=Integer.parseInt("01100011",2);
    return b;

```

## Conclusiones

Santuario Parra Luis Fernando

En el desarrollo de esta práctica se implementó la multiplicación en GF(2) en el lenguaje de programación Java para poder generar la S-box utilizando la tabla de inversos multiplicativos de , así también como la representación polinomial de dicha multiplicación.

César Alejandro Varela Cruz

En ésta práctica realizamos 1 programa con 3 subprogramas (multiplicación, representación polinomial y sbox), los cuales son importante entender cómo se realizan para poder entender después como es que se realiza cada uno de los pasos de otros tipos de cifrado como el AES por ejemplo, ya que este realiza multiplicaciones, sustituciones de Sbox entro otras cosas.

## Referencias

- [1]Egov.ufsc.br, 2019. [Online]. Available: [http://www.egov.ufsc.br/portal/sites/default/files/la\\_criptografia\\_desde\\_la\\_antigua\\_grecia\\_hasta\\_la\\_maquina\\_enigma1.pdf](http://www.egov.ufsc.br/portal/sites/default/files/la_criptografia_desde_la_antigua_grecia_hasta_la_maquina_enigma1.pdf). [Accessed: 12- Feb- 2019].
- [2]"Historia de la Criptografía | Seguridad en Cómputo", Blogs.acatlan.unam.mx, 2019. [Online]. Available: <http://blogs.acatlan.unam.mx/lasc/2016/06/15/historia-de-la-criptografia/>. [Accessed: 12- Feb- 2019].
- [3]"Criptografía y criptoanálisis: la dialéctica de la seguridad | Revista .Seguridad", Revista.seguridad.unam.mx, 2019. [Online]. Available: <https://revista.seguridad.unam.mx/numero-17/criptograf%C3%AD-y-criptoan%C3%A1lisis-la-dial%C3%A9ctica-de-la-seguridad>. [Accessed: 27- Feb- 2019].
- [4]B. Preneel, *Understanding cryptography*. [Place of publication not identified]: Springer, 2014.

## Anexo

FECHA / DATE  
/ /

$a = 25$      $R = 2$      $C = 5 \Rightarrow 40$   
 40 = 0100 1101 Menor Significativo

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \pmod{2}$$

$$\begin{matrix} 1+0+0+0+0+0+1+0 \\ 1+0+0+0+0+0+1+0 \\ 1+0+1+0+0+0+1+0 \\ 1+0+1+1+0+0+0+0 \end{matrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \pmod{2}$$

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \begin{matrix} 0011 & 1111 \\ 3 & F \end{matrix}$$

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = 3F$$