Instituto Politécnico Nacional

Escuela Superior de Cómputo

Cryptography

Homework 4

SUBBYTES

Santiago Mancera Arturo Samuel

Sánchez José Erick

Carlos Eduardo Caballero Huesca

Brando Josué Martínez García

Grupo: 3CV1

Profesora: Díaz Santiago Sandra

17 de octubre del 2016

1.-

SUBBYTES

Para la operación SUBBYTES existen dos métodos que son equivalentes. Ambos parten de la inicialización de la S-box con los valores en ascendencia fila por fila. Es decir la fila 1 contendrá los valores $00,01,02,\ldots,0F$, la segunda fila será $10.11,\ldots,1F$ y así sucesivamente.

Así mismo en ambos métodos se debe obtener el inverso multiplicativo de cada elemento de la matriz S-box en el campo finito $GF(2^8)$.

Una vez teniendo el inverso multiplicativo de cada elemento (byte) de 8 bits expresados como $(b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0)$ se prosigue de la siguiente manera con la operación llamada **transformación afín**:

Método visto en clase (M1)

Se multiplica cada byte por el polinomio $\boldsymbol{x^4 + x^3 + x^2 + x + 1\ mod\ (x^8 + 1)}$ y al resultado le sumamos $\boldsymbol{x^6 + x^5 + x + 1}$ (se considera la suma como operación XOR). Ambos polinomios establecidos por el estándar.

Método con matriz (M2)

A cada bit de cada byte se le aplica la transformación:

$$b'_i = b_i \oplus b_{(i+4)\ \text{mód}\ 8} \oplus b_{(i+5)\ \text{mód}\ 8} \oplus b_{(i+6)\ \text{mód}\ 8} \oplus b_{(i+7)\ \text{mód}\ 8} \oplus c_i$$

Donde C_i es el bit en la posición i del valor 63 (01100011) y b_i es el mismo bit a transformar.

Esta transformación puede ser vista como la siguiente operación de matrices:

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Para este método cabe hacer las siguientes aclaraciones:

Los subíndices de las expresiones $b_{(i+4)\ \text{mód}\ 8}$ representan corrimientos circulares, los cuales pueden ser visualizados en la matriz de tamaño $8x8$.

De esta forma, los corrimientos en 1 posición, 2 posiciones y 3 posiciones están reflejados como los tres ceros de cada fila en la matriz de tamaño $8x8$, lo que significa que estos corrimientos no existen.

Por otro lado b_i, en la transformación, es multiplicado por el primer 1 (que se va recorriendo de forma circular) de la primer fila de la matriz $8x8$ por lo cual se mantiene en la operación con matrices.

Ambos métodos son equivalentes por las siguientes razones:

En M1, la multiplicación por $\boldsymbol{x^4 + x^3 + x^2 + x + 1\ mod\ (x^8 + 1)}$ puede ser representada de la siguiente manera:

Utilizando como byte de ejemplo $8D = 10001101 = \boldsymbol{x^7 + x^3 + x^2 + 1}$

Y teniendo en cuenta que $\boldsymbol{x^8\ mox\ (x^8 + 1) = 1}$

$$\begin{aligned} &\boldsymbol{x}(x^7 + x^3 + x^2 + 1) \\ &+\boldsymbol{x^2}(x^7 + x^3 + x^2 + 1) \\ &+\boldsymbol{x^3}(x^7 + x^3 + x^2 + 1) \\ &+\boldsymbol{x^4}(x^7 + x^3 + x^2 + 1) \\ &+(x^7 + x^3 + x^2 + 1) \end{aligned}$$

Podemos notar lo siguiente:

$$\begin{aligned} &\boldsymbol{x}(x^7 + x^3 + x^2 + 1) \\ &+\boldsymbol{x^2}(x^7 + x^3 + x^2 + 1) \\ &+\boldsymbol{x^3}(x^7 + x^3 + x^2 + 1) \\ &+\boldsymbol{x^4}(x^7 + x^3 + x^2 + 1) \\ &+(x^7 + x^3 + x^2 + 1) \longrightarrow b_i \end{aligned}$$

4 corrimientos

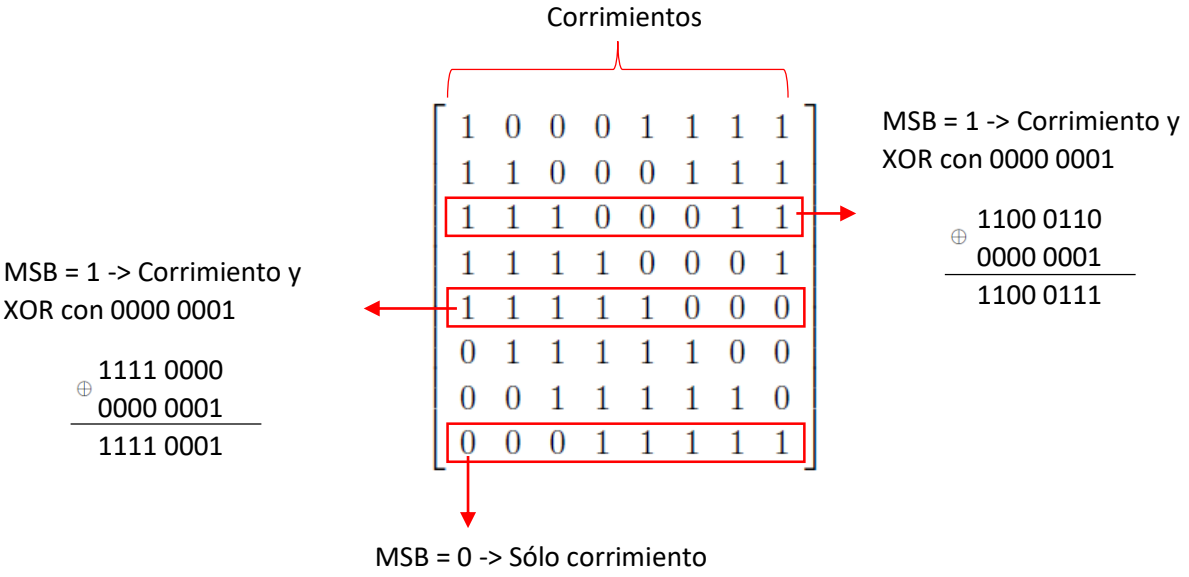
Debido a que la multiplicación por $\boldsymbol{x}$ es equivalente a realizar corrimientos (como lo hemos visto en clase), se obtiene que la multiplicación por $\boldsymbol{x^4 + x^3 + x^2 + x + 1\ mod\ (x^8 + 1)}$ corresponde a realizar 4 corrimientos, es decir, el primer bit quedará en la posición 4, el segundo en la posición 5, el tercero en la posición 6 y el cuarto en la posición 7. Lo anterior es igual a tomar desde un principio el cuarto, quinto, sexto y séptimo bit como lo hace la transformación de M2 en la parte de $\oplus\, b_{(i+4)\ \text{mód}\ 8} \oplus b_{(i+5)\ \text{mód}\ 8} \oplus b_{(i+6)\ \text{mód}\ 8} \oplus b_{(i+7)\ \text{mód}\ 8}$

Mientras tanto, debido a que al final de la multiplicación de M1 sumamos $\boldsymbol{(x^7 + x^3 + x^2 + 1)}$ (porque se multiplica por 1) es equivalente a decir que todos los bits del byte permanecen como lo indica la parte de $b'_i = b_i \oplus$ en la transformación de M2.

Ahora bien, se sabe que en la multiplicación de polinomios en campos finitos se debe considerar $m(x)$, que en nuestro caso y como lo establece el estándar en M1 es $\boldsymbol{(x^8 + 1)}$, para realizar los corrimientos al multiplicar por otra $\boldsymbol{x}$. Es decir, si vemos al polinomio como representación binaria, se debe considerar si el bit más significativo del polinomio a multiplicar es $\boldsymbol{0}$ ó $\boldsymbol{1}$, si es cero, se realiza el corrimiento. Si es uno, se debe realizar el corrimiento (no circular) y la operación XOR con $m(x)$.

En este caso sabemos que $\boldsymbol{x^8\ mox\ (x^8 + 1) = 1}$, por lo tanto cuando el bit más significativo sea 1 se realiza el corrimiento y luego XOR con $\boldsymbol{0000\ 0001}$. Lo anterior se sigue cumpliendo en la matriz de M2:

Por ejemplo:



Debido a lo anterior es que se crea un corrimiento circular como lo indica la transformación de M2 al ser cada corrimiento $\boldsymbol{mox\ 8}$.

Como se mencionaba anteriormente los corrimientos en 1 posición, 2 posiciones y 3 posiciones que están reflejados como los tres ceros de cada fila en la matriz de tamaño $8x8$ no existen. Esto se refleja en el polinomio $\boldsymbol{x^4 + x^3 + x^2 + x + 1}$ de M1 al no existir $\boldsymbol{x^5}, \boldsymbol{x^6}$ ni $\boldsymbol{x^7}$, ya que al realizar el corrimiento circular terminarían en las posiciones 1, 2 y 3 respectivamente.

Por último, en ambos métodos se realiza la suma (XOR) después de realizar los corrimientos (multiplicaciones), el valor que se suma es el mismo en los dos cosos. En M1 se representa como $\boldsymbol{x^6 + x^5 + x + 1}$, mientras que en M2 es 01100011. La equivalencia se muestra de la siguiente manera:

$$\boldsymbol{63_{16} = 0110\ 0011 = x^6 + x^5 + x + 1 = 99_{10}}$$