PRÁCTICA: MULTIPLICACIÓN EN SNOW 3G y AES

Objetivo: Implementar la multiplicación binaria usada tanto en SNOW 3G como en AES.

Desarrollo:

En SNOW 3G las dos multiplicaciones de 32 bits por 32 bits implicadas en el LFSR se corresponden con productos de polinomios en módulo $x^8+x^7+x^5+x^3+1$, que pueden ser implementadas como una sucesión de desplazamientos de bytes y XORs con el byte $A9_{16}=10101001_2$.

En AES la multiplicación de bytes utilizada se corresponde con el producto de polinomios en módulo $x^8+x^4+x^3+x+1$, que puede ser implementado como una sucesión de desplazamientos de bytes y XORs con el byte $1B_{16}=00011011_2$.

En ambos casos, implica aplicar operación distributiva sobre los dos bytes multiplicandos, usando para ello el byte de menor peso, y luego para cada bit 1 de ese byte, desplazar a izquierda el otro byte, de forma que cada vez que su bit más significativo antes del desplazamiento sea 1, hay que hacer, tras el desplazamiento, una XOR bit a bit con el byte A9 o 1B.

Ejemplo:

Entradas:

- Primer byte: 57
- Segundo byte: 83
- Algoritmo: AES

Salida:

- Primer byte: 01010111
- Segundo byte: 10000011
- Byte Algoritmo: 00011011
- Multiplicación: 11000001

Resultante de la operación:

01010111x10000011= 01010111x00000001 + 01010111x00000010 + 01010111x10000000= 01010111+10101110+01010111x10000000= 01010111+10101110+00111000= 11000001

Donde la operación 01010111x10000000 resulta de los pasos:

0	1	2	3	4	5	6	7
01010111	10101110	01011100+00011011= 01000111	10001110	00011100+00011011= 00000111	00001110	00011100	00111000