Píldora nº 23: ¿Qué son los inversos aditivos en un cuerpo?

Escena 1: Importancia de los inversos en la criptografía

Al cifrar un mensaje, aplicamos ciertas operaciones matemáticas sobre un texto en claro de forma que lo convierten en un criptograma. Estas operaciones no pueden ser cualesquiera porque es necesario asegurar que el destinatario sea capaz de realizar sobre el criptograma la operación inversa a la que hizo el emisor, descifrando y recuperando así el texto en claro.

Un criptograma puede descifrarse aplicando en destino la operación inversa a la usada por el emisor utilizando la misma clave, o bien aplicando la misma operación que en emisión pero usando como clave en este caso el valor inverso dentro de un cuerpo de la clave utilizada en el proceso de cifra.

En los algoritmos criptográficos utilizaremos el concepto de inverso en operaciones de suma, multiplicación, or exclusivo e incluso en operaciones con polinomios.

Escena 2: Inversos en la suma módulo n

El inverso de un número en una operación suma dentro de un cuerpo será el complemento de ese número dentro del cuerpo.

Así, el inverso de 12 en el cuerpo 27 es 15, dado que 12+15 = 27 mod 27 = 0; esto es, la identidad de la suma. Por tanto, si ciframos la letra F = 5 sumándole un desplazamiento de 12 espacios, obtenemos el valor 17, es decir la letra Q. Para recuperar el texto en claro podemos restarle al criptograma Q este desplazamiento de 12 posiciones, con lo que obviamente recuperamos la letra F, o bien sumarle el complemento de 12 en el módulo 27, que era 15, obteniendo 17+15 = 32 mod 27 = 5 = F.

Escena 3: Inversos en xor o suma módulo 2

El inverso del or exclusivo es el mismo valor, dado que la operación xor es involutiva.

Así, si se desea descifrar una operación xor realizada sobre un texto en claro con una clave y que ha dado origen a un criptograma, se aplica el xor con el mismo valor de la clave a ese criptograma para recuperar el texto en claro. Por ejemplo si en ASCII se cifra la A con la clave w se obtiene A xor w = 0100 0001 xor 0111 0111 = 0011 0110 = 6 en valor ASCII. Para descifrar este criptograma, hacemos 6 xor w = 0011 0110 xor 0111 0111 = 0100 0001 = A, recuperando el texto en claro.

Escena 4: De momento todo va muy bien

Dado que resulta obvio que en ambos casos el inverso siempre existirá, se podrá recuperar el texto en claro en cualquier cifra que haya hecho uso de estas operaciones. Pero, ¿qué ocurriría ahora si en vez de estas sumas, la operación es una multiplicación?

Esta operación de multiplicación, y más en particular la de elevar a potencia, será muy común en criptografía moderna, especialmente en criptografía de clave pública, pero la solución en este caso ya no es tan sencilla.

Madrid, enero de 2015

Autor del guion: *Jorge Ramió Aguirre*
Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*