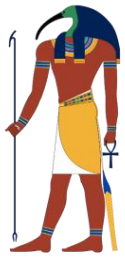

Píldora nº 11: ¿Cifrando dentro de un cuerpo?

Escena 1: El concepto de módulo

En criptografía las operaciones se realizan dentro de un cuerpo de cifra o módulo, siendo este concepto distinto cuando hablamos de criptografía clásica o de criptografía moderna. Vamos a explicar qué significa esto y cuáles son esas diferencias.

De la misma manera que el segundero de un reloj al llegar a los 60 segundos se posiciona en el valor inicial 0 y en el minutero se apunta que ha transcurrido otro minuto, en matemática discreta decimos que un cuerpo finito n está conformado por n números enteros, que van desde el valor 0 hasta el valor n-1, siendo n otra vez el 0, n+1 el valor 1, etc.

Por lo tanto, si el valor de n fuese el número 77 con elementos {0, 1, 2,… 74, 75, 76}, tendríamos entre otros los siguientes resultados modulares posibles:

a) 22 mod 77 = 22 (porque 22 está contenido en 77)
b) 100 mod 77 = 33 (porque 100 contiene una vez al 77 y el resto o residuo es 33)
c) 450 mod 77 = 65 (porque 450 contiene cinco veces al 77 y el resto o residuo es 65)
d) -200 mod 77 = 31 (porque sumando 3x77 a -200 se obtiene un valor entre 0 y 76, el 31)

Escena 2: El cuerpo de cifra en la criptografía clásica

En criptografía clásica el cuerpo de cifra será el número de elementos que conforman el alfabeto del texto en claro. Aunque este alfabeto puede ser cualquier conjunto de letras y/o signos, es habitual trabajar en módulo 27 ya que es el número de letras mayúsculas del alfabeto español, es decir de la A hasta la Z incluyendo la Ñ, codificando por lo general la letra A con el valor 0, la B con el 1, etc., terminando con la Z en el valor 26. Sobre esos números se

realizarán operaciones de suma, resta y producto para cifrar cada letra o un conjunto de letras del texto en claro en módulo 27.

Escena 3: El cuerpo de cifra en la criptografía moderna

Por el contrario, en la cifra moderna el cuerpo en el que se realizan las operaciones no tiene relación alguna con el alfabeto utilizado en el texto en claro, por ejemplo los 256 caracteres del código ASCII. Es más, por lo general ese cuerpo de cifra suele ser un número mucho mayor, como por ejemplo 65.536 y 65.537 en el algoritmo de clave secreta IDEA, o bien un número de unos 300 dígitos decimales o 1.024 bits, que se utiliza como valor mínimo del módulo en el algoritmo de clave pública RSA.

Madrid, octubre de 2014

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