CRIPTORED

talentum Startups

PROYECTO THOTH Píldoras Formativas

http://www.criptored.upm.es/thoth/index.php

Píldora nº 25: ¿Cómo calculamos inversos con el algoritmo extendido de Euclides?

Escena 1: Intentando minimizar el trabajo de encontrar el inverso

Como ya se ha explicado en píldoras anteriores, en criptografía es de vital importancia conocer el valor del inverso de un número dentro de un cuerpo. Sin ir más lejos, ello nos permitirá generar las claves pública y privada en un sistema de cifra asimétrica, entre ellos el conocido estándar RSA.

Hemos visto además que a partir del algoritmo de Euclides, que nos permitía demostrar que dos números eran primos entre sí o coprimos si el máximo común divisor entre ellos era igual a 1, se podía llegar a ese inverso. No obstante, su desarrollo conceptual era poco práctico y muy propenso a equivocaciones. Nos hace falta un algoritmo que sea sencillo y, además, eficiente. Este será el algoritmo extendido de Euclides.

Escena 2: El algoritmo extendido de Euclides

Existen diversas formas de encontrar el inverso multiplicativo mediante este algoritmo; a continuación se describe una de ellas. Las ecuaciones que regirán para calcular x = inv (A, B) son las siguientes:

Hacer $(g_0, g_1, u_0, u_1, v_0, v_1, i) = (B, A, 1, 0, 0, 1, 1)$
Mientras $g_i \neq 0$ hacer
    Hacer y_{i+1} = parte entera (g_{i-1}/g_i)
    Hacer $g_{i+1} = g_{i-1} - y_{i+1} \times g_i$
    Hacer $u_{i+1} = u_{i-1} - y_{i+1} \times u_i$
    Hacer $v_{i+1} = v_{i-1} - y_{i+1} \times v_i$
    Hacer $i = i+1$
Si $(v_{i-1} < 0)$
    Hacer $v_{i-1} = v_{i-1} + B$
    Hacer $x = v_{i-1}$

Vamos a encontrar el inverso de 9 en el cuerpo 275, esto es inv (9, 275). Sabemos que el inverso existe pues mcd (9, 275) = 1, dado que 9 = 3^2 y 275 = 5^2x11.

Escena 3: Encontrando el inverso de 9 en 275

i	y_i	g_i	u_i	v_i
0	-	**275**	1	0
1	-	**9**	0	1
2	30	5	1	-30
3	1	4	-1	31
4	1	1	2	**-61**
5	4	0	-**9**	**275**

- Recuerdo de la operatividad del último cálculo: -**9** = -1 - (4x2) y **275** = 31 - [4x(-61)]
- Como v_{i-1} = -61 ha salido un valor negativo, entonces **X** = - 61 + 275 = **214**

Efectivamente, inv (9, 275) = 214 pues 214 x 9 = 1.926 mod 275 = 1, ya que 1.926 = 7 x 275 + 1.

Escena 4: ¿Cuán rápido es el algoritmo extendido de Euclides?

Es un algoritmo muy rápido y además por lo general llega a la solución en muy pocos pasos. Por ejemplo, encontrar la clave la privada de RSA, inversa de la clave pública que típicamente es el valor 65.537, dentro de un cuerpo de 2.048 bits, puede decirse que es instantáneo.

Madrid, enero de 2015

Autor del guion: *Jorge Ramió Aguirre*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*