CRIPTOGRAFÍA

PRÁCTICA 1

Aritmética modular

Juan José Segura González

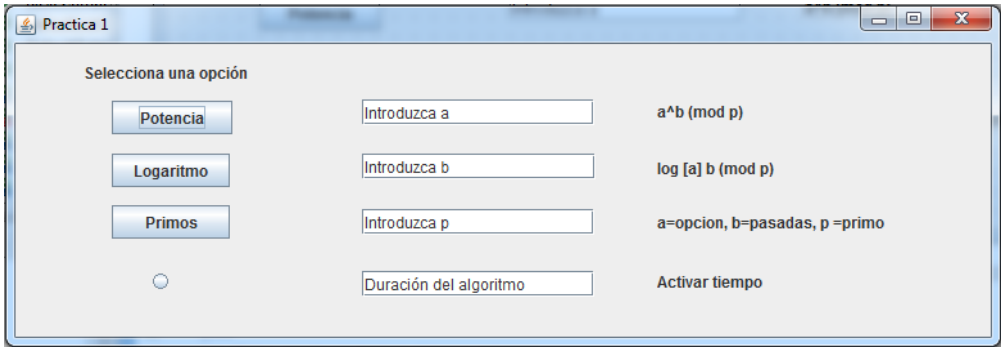
Valentín Pérez Carrasco

29/03/2011

Esta práctica nos introduce en algunos algoritmos de aritmética modular que son necesarios para el desarrollo de la criptografía de clave pública. Se trata de conocer e implementar algunos de ellos, y de observar las diferencias del tiempo de cálculo entre distintas operaciones.

Manual de usuario

A continuación se muestra una pequeña captura de la aplicación creada, para facilitar su uso ya que no dispone de la explicación de los campos a rellenar. Así para el cálculo de las distintas opciones se haría de la siguiente forma:



- Potencia $a^b (mod\ p)$: El valor de a será el parámetro Base, el valor de b el de potencia y p será primo.

- Logaritmo $\log_a b\ (mod\ p)$: Igual que el usado en potencia.

- Primos: Para calcular si un valor es primo se realiza de dos formas distintas,
    - Dando el valor del número a calcular, para calcular si un valor es primo en el campo Base se insertará un 0, en Potencia se trata del número n necesaria para saber con cuantos valores realizar la prueba y en Primo se insertará el valor a calcular.
    - Sin dar el valor, se calcula un valor aleatorio sin insertarlo por parte del usuario, en el campo Base se usará un valor distinto de 1, Potencia es el mismo que el anterior caso y el campo Primo se puede omitir ya que se mostrará en ese campo el valor aleatorio usado para la prueba, el valor aleatorio será de tantas dígitos como inserte en el campo Base.
    - El campo potencia puede ser también la probabilidad de acierto y calculará el número de pasadas, y viceversa mostrando el resultado al final en el campo potencia.

- El botón debajo de primo sirve para mostrar en el último campo el tiempo que ha tardado el algoritmo en calcular un resultado.

Para ejecutar el programa en una consola de Linux con una distribución jre de java instalada ejecute java –jar <nombre_archivo>.

Tabla comparativa de tiempos

Las pruebas se han realizado en un ordenador con las siguientes características:

- Intel core 2 Duo 64 bits 2.2ghz.
- 4 GB de memoria RAM.

P	A	B	Tiempo Potencia (ns)	Tiempo Logaritmo (ms)
13177	23457	12382	1130603	10
251477	671234	251472	780176	30
4461881	9735462	9761235	851568	100
9843079	6142715	5612781	1011617	130
15444521	27185943	16781982	1015350	165
472251991	617283627	617283612	1244456	243
5463458053	6172895076	5617283945	2153418	526
7357734241449	572667482885	351740985238	2839805	6260
5746175430239	4664535623833	413343239605	2672758	32493