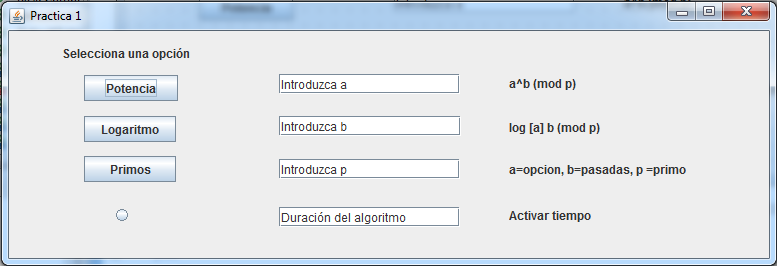
|  |
| --- |
| s tCRIPTOGRAFÍA |
| PRÁCTICA 1 |
| Aritmética modular |
|  |
| **Juan José Segura González**  **Valentín Pérez Carrasco** |
|  |

|  |
| --- |
| 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. |

**29/03/2011**

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 : El valor de a será el parámetro Base, el valor de b el de potencia y p será primo.
* Logaritmo : 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 1, 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 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)** |
| 52691 | 70621 | 21372 | 4903861 | 8 |
| 843587 | 973238 | 431422 | 509172 | 19 |
| 4872961 | 8721432 | 3761215 | 185807 | 11 |
| 29873761 | 16342725 | 7619782 | 1390984 | 52 |
| 537891269 | 27185943 | 16781982 | 1338629 | 129 |
| 1547598739 | 617283627 | 617283612 | 1498259 | 203 |
| 82376849239 | 6172495076 | 5617283945 | 2644410 | 1771 |
| 576382750891 | 472667482885 | 351740985238 | 3227494 | 6178 |
| 5134857695843 | 4664535623833 | 413343239605 | 3241352 | 62493 |

|  |
| --- |
|  |