*****Instituto Politécnico Nacional***

***Escuela Superior de Cómputo***

*Criptography*

***Ejercicios Capítulo VI***

***Nombre:*** *Sampayo Hernández Mauro*

***Grupo:*** *3CV17*

***Profesor:*** *Víctor Manuel Silva García*

**Ejercicios**

1. **Construya el primo cuando tienen los siguientes valores:**
2. **y**

Realizamos el análisis de enteros de la forma con los valores de m:

**Si es Primo**

Comprobando con la ayuda del programa desarrollado para el algoritmo de Miller Rabin, comprobamos que el número es primo:



Por lo tanto

1. **y**

Realizamos el análisis de enteros de la forma con los valores de m:

**No es Primo**

**No es Primo**

**No es Primo**

**No es Primo**

**No es Primo**

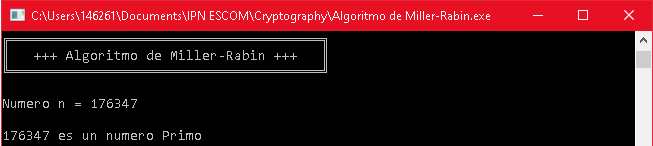
**No es Primo**

**No es Primo**

**No es Primo**

**Si es Primo**

Comprobando con la ayuda del programa desarrollado para el algoritmo de Miller Rabin, comprobamos que el número es primo:



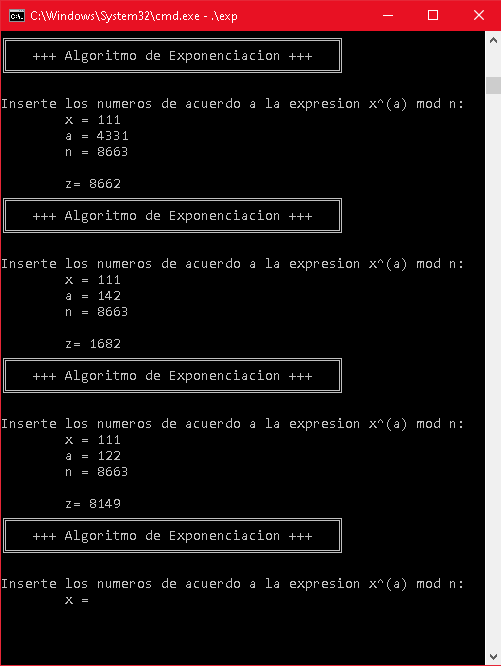
Por lo tanto

1. **Encuentre un elemento generador para cada uno de los casos del problema anterior.**

tanto, los primos serán 2, 61 y 71.

Proponemos , y comprobamos que sea un elemento generador por medio de la operación para todo primo:

Nos auxiliamos del programa del Algoritmo de Exponenciación para comprobar los resultados:

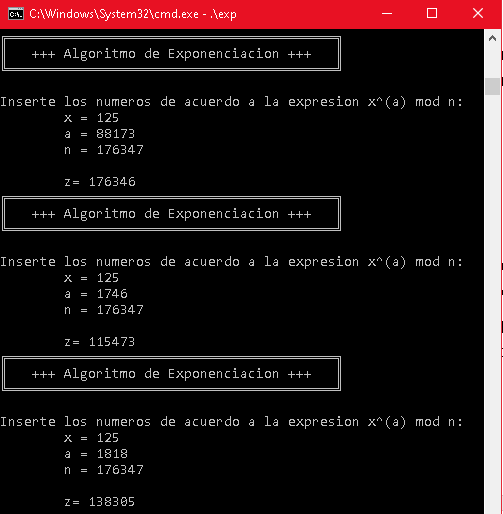


Ningún valor de para todo primo fue equivalente a 1, por lo cuál se cumple la condición de que para todo primo. Por lo tanto**: es un elemento generador**

tanto, los primos serán 2, 101 y 97.

Proponemos , y comprobamos que sea un elemento generador por medio de la operación para todo primo:

Nos auxiliamos del programa del Algoritmo de Exponenciación para comprobar los resultados:



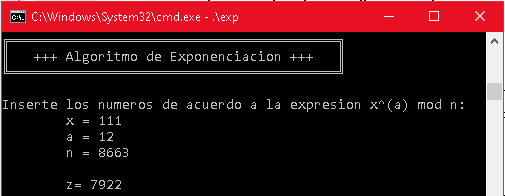
Ningún valor de para todo primo fue equivalente a 1, por lo cuál se cumple la condición de que para todo primo. Por lo tanto**: es un elemento generador**

1. **Dado un elemento generador, , del problema uno realice los siguientes cálculos**
2. **Proponga un valor aleatorio que cumpla con la condición; , y lleve a cabo el cálculo .**

Considerando que para este ejercicio se usará el inciso a) del problema uno, se tiene que:

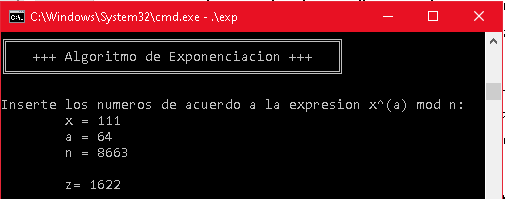
Proponiendo se tiene:

Resolviendo, auxiliándonos del programa del Algoritmo de Exponenciación:



1. **Plantee un valor para la variable y otro para la clave privada . Con estos datos calcule a y .**

Proponiendo y se tiene:



1. **Utilizando la expresión , descifre el resultado del problema 3.**

1. **Resuelva el problema anterior de acuerdo con la expresión 6.3.5.**
2. **Diga porqué el cifrado de ElGamal se considera aleatorio.**

Se considera aleatorio debido a que las variables de cifrado se construyen a partir de un entero aleatorio, pues cada vez que se cifra un valor los valores de serán diferentes.