*****Instituto Politécnico Nacional***

***Escuela Superior de Cómputo***

*Criptography*

***Ejercicios Capítulo V***

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

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

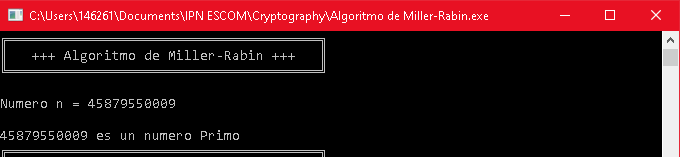
***Profesor:*** *Víctor Manuel Silva García*

**Ejercicios**

1. **Construya un número de 11 dígitos que tenga terminación en 1, 3 7 o 9. Aplique el algoritmo de primalidad hasta 10 veces en caso de que el resultado sea es primo. Si el resultado indica que es compuesto, entonces proponga otro número con las características anteriores.**

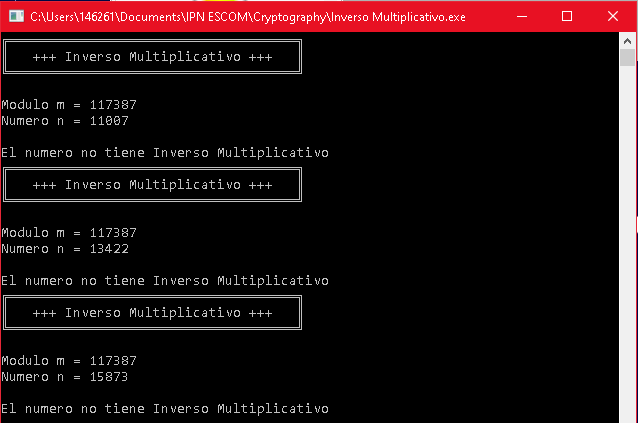
Número a testear: 45879550009



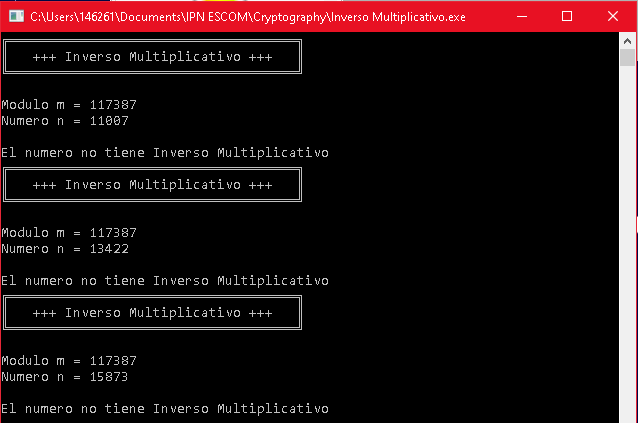


1. **Dado el módulo , encuentre los inversos multiplicativos en caso de que existan de los siguientes números: 11007, 13422 y 15873.**

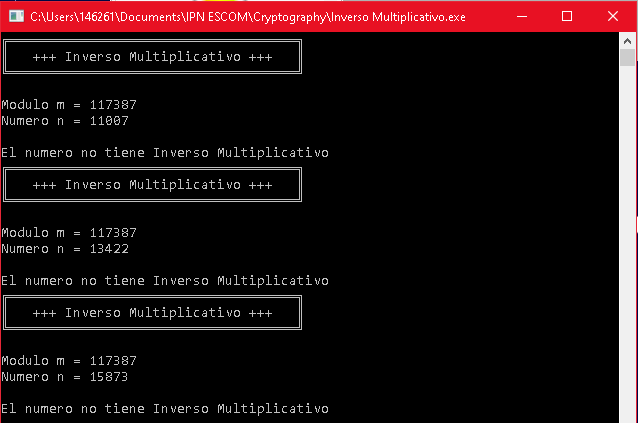
* Para 11007



* Para 13422

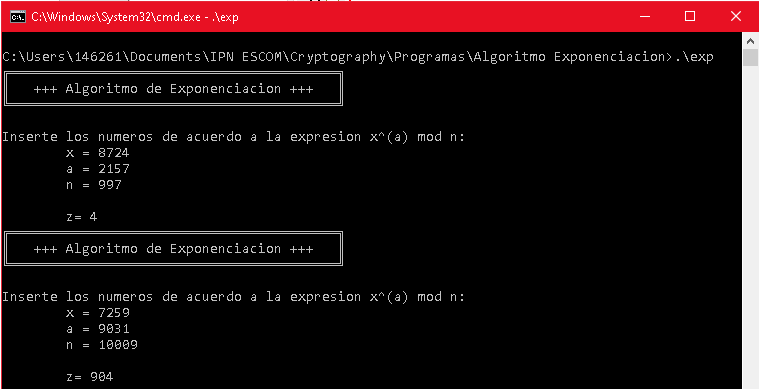


* Para 15873

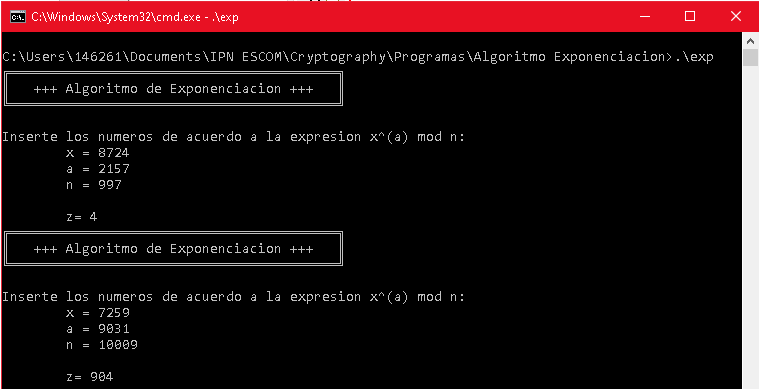


1. **Realice los siguientes cálculos de exponenciación:,**

* Para

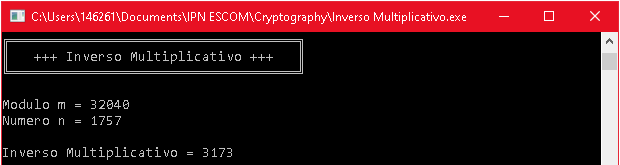


* Para



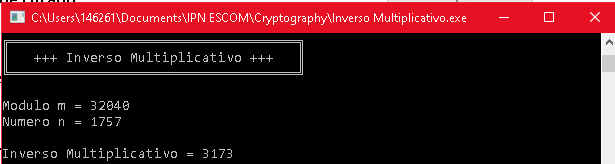
1. **Desarrolle un programa para realizar la operación de exponenciación con números de 50 dígitos y presente un ejemplo.**
2. **Dados los valores de en un esquema RSA, encuentre los siguientes elementos: .**

Proponiendo , comprobamos que este entero impar sea válido verificando que :

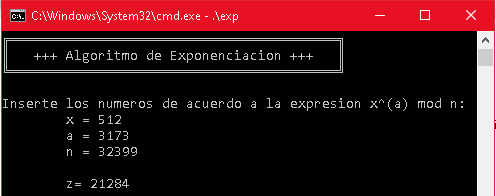


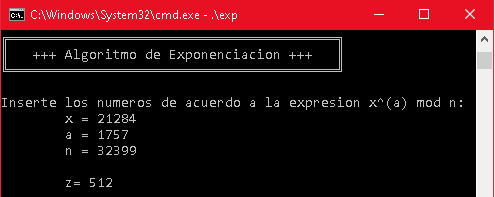
Como los valores de y cuentan con un Inverso Multiplicativo, entonces forzosamente , por lo tanto , es un entero válido.

Así para el cálculo de se obtiene el inverso multiplicativo de módulo :



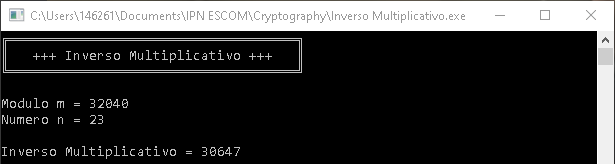
Así





1. **Utilizando los valores de del problema 6, proponga un valor privado y un valor público ; además, considere el caso hipotético de que la función Has Sha de un mensaje es 53. Con esta información, lleve a cabo la firma digital del mensaje.**

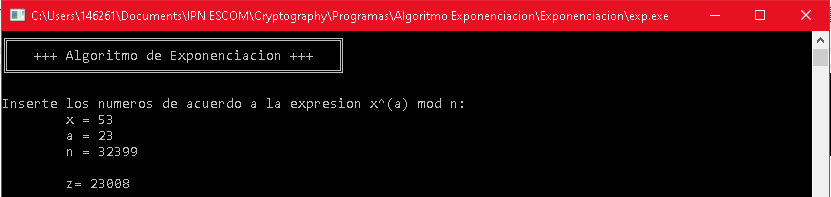
Considerando que y ; se propone y comprobamos que este entero impar sea válido si :



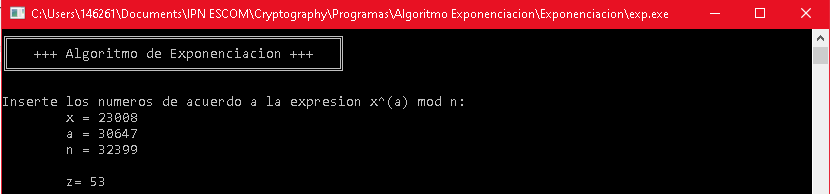
y cuentan con un Inverso Multiplicativo, por lo que ,ypor lo tanto , es un entero válido.

El valor de será el valor del inverso multiplicativo de módulo , es decir:

Ahora considerando que H (M)= , obtenemos la firma digital:



Comprobamos por medio de:



Se puede observar que se obtuvo el valor para esperado, por lo cvual podemos comprobar que la Firma Digital es correcta.