Práctica 4
Facultad de Ciencias
Criptografía y Seguridad

José de Jesús Galaviz Casas
galaviz@ciencias.unam.mx

Edgar Omar Arroyo Munguía
omar.am@ciencias.unam.mx

Luis Fernando Yang Fong Baeza
fernandofong@ciencias.unam.mx

26 de Febrero 2020

1. Generación de números primos aleatorios arbitrariamente grandes y tests de primalidad

Como primer tarea, deberán de generar un script de Python en el cual, se puedan generar números arbitrariamente grandes (Al menos 100 dígitos), sin importar cómo funcione el algoritmo o qué biblioteca(s) de Python3 utilicen, pero ésto debe de ser generado correctamente y será evaluado en las pruebas unitarias.

Uno de los retos más grandes de la computación, es trabajar con poder trabajar con primos de manera eficiente, ya sea su factorización o su generación mediante un algoritmo, sin embargo, estos son problemas, computacionalmente hablando, muy complejos que podría tardar demasiado, sin embargo para ésto existen los tests de primalidad, en ésta práctica se van a implementar el más conocido, Miller-Rabin y el menos conocido pero más curioso por ser el peor, el test de primalidad de Wilson. Obviamente estos tests de primalidad, no tiene sentido que preguntemos para primos relativamente pequeños como 101 o 107, hablamos de números demasiado grandes, tan grandes que desborden a un `long long int`.

2. Test de primalidad de Miller-Rabin

El test de primalidad de Miller-Rabin, es considerado como uno de los mejores tests de primalidad, si no es que el mejor, aunque en realidad se les considera como *Pseudoprimos fuertes*.

La idea del test es encontrar raíces no triviales de 1 $mod\ n$. Recordando un poco el Pequeño Teorema de Fermat, tenemos que $a^{n-1} \equiv 1\ mod\ n$, entonces Miller-Rabin lo que hace es encontrar un par de números r y s tales que $(n-1) = r(2^s)$ con r par, de manera que el test procede de la siguiente manera:

1. Escoger un número aleatorio a en el rango $[1, n-1]$
2. Si $a^{r-1} \not\equiv\ mod\ n$ y $a^{(2^j)r} \not\equiv -1\ mod\ n$ para toda j en el rango $[0, s-1]$, entonces n no es primo.
3. En otro caso, entonces n sí es primo.

3. Test de primalidad de Wilson

El test de primalidad de Wilson, nace del teorema de Wilson, el cual no será demostrado en este PDF pero pueden ver la demostración en las notas de *A Complete Course on Number Theory*, que establece lo siguiente:

$$\textit{Para cada primo } p\textit{, tenemos que } (p-1)! \equiv -1 \textit{ mod } p$$

De manera que es el peor test de primalidad puesto que hay que calcullar $(p-1)!$, aunque sea con aritmética modular, el resultado es monstruoso, sin embargo éste test es para notar que, Miller-Rabin, no es el único test de primalidad y lo denso que puede llegar a ser un número grande arbitario.