Práctica 1 de Criptografía y Computación

Carlos Núñez Molina

6 Elige tres números compuestos n_1, n_2 y n_3. El número n_1 debe ser un número con tres cifras. Para el número n_2 elige 5 primos pequeños (de dos o tres cifras) y multiplícalos. Para el número n_3 elige dos primos grandes (con alguna de las funciones que has implementado en los apartados anteriores) y multiplícalos. Para el número n_1 calcula todos los falsos testigos. Para n_2 y n_3 elige una lista al azar de 200 números y calcula cuáles de ellos (y cuántos) son falsos testigos.

He elegido los números siguientes:

- $n_1 = 225$, que es $5^2 * 3^2$.
- $n_2 = 123358956461$, que es resultado del producto de los primos 13, 71, 277, 563 y 857.
- $n_3 = 12345679009419752461$, que es resultado del producto de los primos 1000000007 y 12345678923.

El número n_1 no tiene ningún falso testigo, es decir, el *Test de Miller-Rabin* devuelve que es un número compuesto para todos los testigos $2 <= a <= n_1 - 2$.

De igual forma, al calcular para los números n_2 y n_3 cuántos testigos, de entre 200 elegidos aleatoriamente, eran falsos, no me salió ninguno.

7 Para el número $n = 3215031751$ elige al azar una lista de 200 números (entre 2 y $n - 2$) y estudia cuántos son falsos testigos.

Para el número 3215031751 he encontrado, de entre 200 testigos elegidos aleatoriamente, a 48 falsos testigos.
Los testigos son: 2935071731, 2931603661, 492933966, 1306278621, 1617551744, 31111325, 1498272839, 2929392930, 134849070, 604718046, 1271080353, 518648904, 2706523043, 947697757, 1981132259, 1985011056, 1478515942, 1835796409, 3000274167, 1332276489, 2497397895, 3176671017, 2954931308, 2303475158, 647172536, 3121660915, 2472553653, 2513988608, 1715030066, 2181060077, 1530369159, 3047639753, 1489381660, 40376247, 783840136, 2449633956, 1660703196, 172367108, 1298928945, 2189953363, 2412866465, 544766023, 1920927519, 702355008, 1876283141, 1807417814,

1996235042, 46896364. A pesar de ser un número para el que el Test de Miller-Rabin funciona mal, el número de testigos falsos no supera el máximo de un cuarto de los testigos totales, 50 en este caso.

8 Para el número $n = 2199733160881$ elige una lista de 100 números (entre 2 y $n - 2$) y para cada uno de ellos estudia si es testigo falso con el test de Fermat y con el test de Miller-Rabin.

Al ejecutar ambos tests con 100 testigos al azar para el número 2199733160881, me salen los siguientes testigos falsos:

- **Test de Fermat** - Todos los testigos (100) son falsos. Los testigos empleados han sido:
  1772366524600, 538468577570, 1839695826187, 1830325115900, 245956300488, 252227361614, 883005771162, 2021500875258, 1403506127642, 1058710820099, 1274965998, 2030564265196, 77194776504, 758906814760, 1388808176848, 1916057635589, 165558076252, 981639518090, 2003188658905, 1802896063434, 31718943680, 1755188885177, 55080159044, 708658801812, 1259837072747, 1249683767330, 545458700298, 2023519069048, 1320752862657, 1256519971144, 43764561062, 663683067093, 741443164060, 352702359926, 1010712566517, 1723847715183, 1512087617015, 3464078178, 2030006524057, 1072795148730, 1746683146928, 471553180675, 2092613404374, 332905792210, 1464046351009, 1899649690036, 1287934280612, 336222710000, 265698880005, 1483512052135, 716810812416, 2166646918644, 1296242564689, 811968931578, 996591533843, 516360696245, 1471477762697, 1230483602460, 656229960390, 888344632866, 2148952297126, 103919305770, 720836525341, 1361348230269, 2032161668090, 15772507540, 1831562525323, 108007918840, 47066868762, 1716363657063, 446304106997, 468875340121, 1218827690995, 41944845957, 1068626703798, 1285685482756, 1199452632461, 588446944227, 2146605465064, 76929896121, 877568880872, 715109297197, 1303152843080, 369200433802, 1748369171515, 1724908326282, 653811897833, 1474083710490, 1040767606137, 2131100465512, 1783945736622, 753710302670, 1893649143413, 1511591654224, 507237636126, 1760298245970, 1225874052858, 1070128630683, 378439231928, 472393159198.
- **Test de Miller-Rabin** - Solo hay 9 testigos falsos:
  2021500875258, 1058710820099, 1916057635589, 1802896063434, 1249683767330, 446304106997, 468875340121, 1068626703798, 1474083710490.

Esto muestra cómo el Test de Miller-Rabin es mucho más fiable que el de Fermat.

Instrucciones de ejecución

Todo el código usado para esta práctica se corresponde con un script de Python denominado *Practica1.py*. Este script ha sido programado en Linux usando Python 3.6.

Este archivo no tiene *main* sino que simplemente se compone de las distintas funciones utilizadas en la práctica. Se pueden ejecutar usando el entorno de **Spyder**. Para ello, simplemente hay que ejecutar una vez el script y, en el terminal de iPython que proporciona Spyder, ejecutar la función deseada.