1. (10 points) Implementar MILLER-RABIN(*n, s*). Colocar el algoritmo en el README.md con una breve explicación. Encontrar todos los primos de 3 cifras utilizando este algoritmo. ¿Cual es el valor apropiado para el parámetro *s*?

   - Código en carpeta: Test Miller Rabin

```
"D:\Gabriel\Programming Projects\Codeblocks Projects\Para probar\Test Miller Rabin\bin\Debug\Test Miller Rabin.exe"
Primos del 100 al 1000:
101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227,
229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367,
373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509,
521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661,
673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829,
839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997,
Process returned 0 (0x0)   execution time : 0.053 s
Press any key to continue.
```

   - El valor mas apropiado para el parámetro s, es 571.
   - Se hicieron pruebas con un ‘s’ que fuera desde 1 hasta 1000 y el que mejor resultado dio fue 571. Acertando 6 de 10 intentos.

```
"D:\Gabriel\Programming Projects\Codeblocks Projects\Para probar\Probabilida
571 acierta 6 veces
701 acierta 4 veces
805 acierta 4 veces
810 acierta 4 veces

Process returned 0 (0x0)   execution time : 0.048 s
Press any key to continue.
```

2. (10 points) Implementar GENERATE-PRIME(*b*). Colocar el algoritmo en el README.md con una breve explicación. Encontrar 100 primos distintos de 10 bits utilizando este algoritmo. ¿Cual es el valor apropiado para el parámetro *s*?
   - Carpeta del código: Trivium/ Trivium
   - No pueden encontrarse 100 primos “distintos” de 100 bits, debido a que solo existen 75 numeros primos de 10 bits.
   - Omitiendo la regla de que deben ser distintos:
   - 188 funciona bien como “s” en este caso

```
"D:\Gabriel\Programming Projects\Codeblocks Projects\Para probar\Trivium\Trivium\bin\Debug\Trivium.exe"
1th prime: 839          2th prime: 809          3th prime: 809          4th prime: 829          5th prime: 733          6th prime: 523          7th prime: 1019

8th prime: 863          9th prime: 569          10th prime: 977         11th prime: 631         12th prime: 523         13th prime: 1013                14th prime: 547

15th prime: 827         16th prime: 947         17th prime: 577         18th prime: 947         19th prime: 811         20th prime: 881         21th prime: 727

22th prime: 977         23th prime: 997         24th prime: 997         25th prime: 991         26th prime: 811         27th prime: 967         28th prime: 701

29th prime: 769         30th prime: 557         31th prime: 587         32th prime: 911         33th prime: 997         34th prime: 563         35th prime: 983

36th prime: 907         37th prime: 857         38th prime: 757         39th prime: 571         40th prime: 797         41th prime: 569         42th prime: 757

43th prime: 797         44th prime: 787         45th prime: 541         46th prime: 991         47th prime: 947         48th prime: 769         49th prime: 859

50th prime: 709         51th prime: 653         52th prime: 857         53th prime: 547         54th prime: 971         55th prime: 643         56th prime: 569

57th prime: 1009                58th prime: 593         59th prime: 1013                60th prime: 569         61th prime: 673         62th prime: 569         63th prime: 541

64th prime: 571         65th prime: 857         66th prime: 739         67th prime: 991         68th prime: 653         69th prime: 953         70th prime: 709

71th prime: 839         72th prime: 541         73th prime: 773         74th prime: 673         75th prime: 1021                76th prime: 967         77th prime: 937

78th prime: 593         79th prime: 1019                80th prime: 1019                81th prime: 863         82th prime: 877         83th prime: 1013                84th prime: 881

85th prime: 653         86th prime: 1021                87th prime: 853         88th prime: 631         89th prime: 1019                90th prime: 703         91th prime: 733

92th prime: 619         93th prime: 739         94th prime: 1013                95th prime: 571         96th prime: 743         97th prime: 569         98th prime: 563

99th prime: 821         100th prime: 887

Process returned 0 (0x0)   execution time : 0.080 s
Press any key to continue.
```