Iván Risueño Martín y Miguel Moreno Alcaraz

INFORME TABLA COMPARATIVA

Para el ejercicio de Blockchain de la práctica de RSA, hemos generado una tabla comparativa con el tiempo necesario para firmar cien mensajes diferentes con claves de diverso tamaño de bits, usando TCR y sin usarlo.

Primero, explicaremos qué es TCR.
El Teorema Chino del Resto es un resultado en teoría de números que se utiliza para resolver sistemas de congruencias lineales.
Este teorema se puede aplicar en diversos ámbitos, uno de ellos la criptografía, donde se usa para reducir operaciones con números muy grandes pasándolas a congruencias. En RSA se utiliza para hacer que la suma de p y q sean la longitud del bit n, haciendo p y q mucho menores a n, lo cual acelera los cálculos considerablemente.

A continuación tenemos la tabla que hemos generado con nuestro código:

Bits	**TCR**	**Sin TCR**
512	0.031281232833862305	0.06565976142883301
1024	0.13437366485595703	0.3779923915863037
2048	0.860633134841919	2.534207344055176
4096	4.992737293243408	18.377220630645752

En la tabla podemos ver cómo los tiempos para firmar son menores cuando se utiliza TCR. La diferencia es poca en el caso de 512 bits e incluso en el de 1024 bits, pero a medida que los bits aumentan, no sólo aumenta el tiempo para firmar sino también la brecha entre utilizar TCR o no. En el caso mayor, con 4096 bits, podemos ver cómo al no usar TCR el proceso es unas cuatro veces más lento que si lo utilizamos.
Por tanto, con esta tabla podemos afirmar que la eficiencia al utilizar TCR es clara, sobre todo si queremos utilizar mensajes con una clave más larga.