Taules RSA

Comparació desxifrat/firma amb i sense TCR

Mida de la clau (bits)	**Temps mitj amb TCR (s)**	**Temps mitj sense TCR (s)**
512	0,00030460	0,00067994
1024	0,00136945	0,00376248
2048	0,00766940	0,02390725
4096	0,04829465	0,16696047
8192	0,33660203	1,19817270

Els resultats mostren que l'ús de TCR (Teorema Xinès del Resto) accelera de forma significativa l'operació de firma RSA. Això es deu a que per calcular l'RSA sense TCR, s'ha de calcular s = md mod n, amb una n té la mida de la clau completa, que pot ser considerablement gran. Per altre part, usant el TCR, reduïm aquesta expressió a dues exponenciacions més petites, mdp mod p i mdq mod q, i això fa que el cost es redueixi.

Aquesta reducció es nota significantment en la clau de 8192, on la diferència és de aproximadament 0,86 segons per firma, que s'amplifica quan es fan 1024 signatures. De fet, per tal de poder executar probes amb aquesta mida de clau, s'han hagut de fer modificacions a algunes funcions:

- S'ha hagut de cambiar la funció extended_gcd de recursiva a iterativa, ja que sinó es produia un error de "RecursionError: maximum recursion depth exceeded".
- S'ha hagut d'optimitzar el test de primalitat Miller-Rabin per reduir el nombre de bases utilitzades en claus grans i millorar el cribatge inicial.
- Ha calgut canviar també la generació de primers, modificant l'eficiència generant candidats més adequats i amb menys iteracions de comprovació.

Gràcies a aquestes modificacions, ha estat possible generar claus grans i calcular els temps de la pràctica en un temps raonable.

Comparació temps xifrat i verificació

Mida de la clau (bits)	**Temps mitj xifrat (s)**	**Temps mitj verificació (s)**
512	0,00001847	0,00001832
1024	0,00005270	0,00005225
2048	0,00016630	0,00016586
4096	0,00058325	0,00058487
8192	0,00205853	0,00207389

Els temps de xifrat i verificació són molt més petits que els de firma. Això es deu al fet que aquestes dues operacions utilitzen l'exponent públic e=65537, que és molt petit i té molt pocs bits a 1. Això fa que l'exponenciació modular sigui extremadament ràpida.

També s'observa que els temps de xifrat i verificació són gairebé idèntics, la qual cosa és normal perquè matemàticament són la mateixa operació ($m^e \bmod n$).