task.md 2025-04-25

Завдання

Час – великий учитель. Біда в тому, що він вбиває своїх учнів. (с) Будда

Це особливий підписаний документ за допомогою бібліотеки

При підписі використовується алгоритм ECDSA з геш функцією SHA3-256. Параметри кривої в формі Едвардса:

 $n = 400000000000000000000000000000029 \\ E26087789 \\ BC2815 \\ BDFF97093543 \\ CCF$

d = 18

G.y = 742F27A268641C9D7DDF69892BE3DF3D8F9CC52260B89A4953C8379C7C0A212B

G.x = 91F5D0E7E2D417E3108B13B075CDC7756045F8424479FCFE8F23D27250A0883F

Бібіліотека має вразливість. Ваша задача полягає в тому щоб знайти приватний ключ, який використовувася для підпису документу.

