

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

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

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

