題目: 有兩次簽證並且有 Key1,Key2 的前半部分
,想要推出 Key1,Key2 後半部分,推出後就可以透過公式反推 d,就可以自己創造簽證了

解法:

把 Key1,Key2 拆成 (a+k1) (a+k2)
把這個帶進去 DSA 的那個公式

$$s_1 \equiv k_1^{-1}(h_1 + dr_1) \bmod n$$
$$s_2 \equiv k_2^{-1}(h_2 + dr_2) \bmod n$$

可以推出

$$k1 - r1*s2*k2/(r2*s1) + r1*h2/(r2*s1) - h1/s1 - r1*s2*a/(r2*s1) + a = 0$$

參考 slide 上面找 k1,k2 的方式:使用 LLL 找短向量(因為-k1,k2,K)的數量級幾乎是 n^(1/2) 所以很短，剛好 LLL 是找短向量用的

$$k_1 - s_1^{-1}s_2r_1r_2^{-1}k_2 + s_1^{-1}r_1h_2r_2^{-1} - s_1^{-1}h_1 \equiv 0 \bmod n$$

$$\text{Let } t = -s_1^{-1}s_2r_1r_2^{-1},\ u = s_1^{-1}r_1h_2r_2^{-1} - s_1^{-1}h_1$$
$$\text{o}\quad k_1 + tk_2 + u \equiv 0 \bmod n$$

只要照著擺出這個矩陣,並且執行 LLL 就有機會解出 k1,k2
這邊有個重點是 d 是隨機的並且這個 d 弄出來的簽證,不一定可以讓我們解到正確的 k1,k2,因為 LLL 並不一定可以找到最小解，並不一定可以找到我們要的答案,所以要用個 while 迴圈去跑幾次,直到 d 可以被 LLL 找出

$$\begin{bmatrix} n & 0 & 0 \\ t & 1 & 0 \\ u & 0 & K \end{bmatrix}$$

$$(-q,\ k_2,\ 1)B = (-k_1,\ k_2,\ K)$$

K = 2^128 (k1,k2 的上界)
t = -1*inverse(s1,n) * s2 * r1 * inverse(r2,n) %n
u = (inverse(s1,n)*r1*h2* inverse(r2,n) - h1* inverse(s1,n) -

inverse(s1,n)*inverse(r2,n)*r1*s2*a + a)%n

找到後因為只是 key 的後半段,要記得加上 a,a
兩個 key 都找到之後就可以回推 d,並且作簽證的動作