HNP-revenge

先向 server 拿兩個 message 的 signature，接著解方程式，想要求出 k1 及 k2：

$s_1k_1 - h_1 = d * r_1$ and $s_2k_2 - h_2 = d * r_2$

$(s_1k_1 - h_1)/(s_2k_2 - h_2) = r_1/r_2$

$\rightarrow (s_1k_1 - h_1) * r_2 = (s_2k_2 - h_2) * r_1$

$\rightarrow s_1k_1r_2 - h_1r_2 = s_2k_2r_1 - h_2r_1$

$\rightarrow s_1k_1r_2 - s_2k_2r_1 - h_1r_2 + h_2r_1 = 0$

$\rightarrow k_1 - s_1^{-1}r_2^{-1}s_2r_1k_2 - s_1^{-1}h_1 + s_1^{-1}r_2^{-1}h_2r_1 = 0$

let $t = -s_1^{-1}r_2^{-1}s_2r_1$ and $u = s_1^{-1}r_2^{-1}h_2r_1 - s_1^{-1}h_1$

$\rightarrow k_1 + tk_2 + u = 0 \ (mod\ n)$

因為 k1, k2 有相同的前綴 `a = int(md5(b'secret').hexdigest(), 16) << 128`，把式子整理後，可以使用 lattices 去解 p1, p2：

$k_1 + tk_2 + u = 0 \ (mod\ n)$

$\rightarrow (a + p_1) + t(a + p_2) + u = 0 \ (mod\ n)$

$\rightarrow p_1 + tp_2 + (1 + t)a + u = 0 \ (mod\ n)$

$|p_1|, |p_2| < 128$

構建 lattice basic，設定 $K = 2^{128}$，並使用 LLL 求 reduce basic，可以看到 $v = (-p_1, p_2, K)$ 存在這個 reduce basic 中：

```
L = matrix(ZZ, [[n, 0, 0], [t, 1, 0], [a * (1+t) + u, 0, 2^128]])
L.LLL()
```

```
[-159821575041606419486715044730765694571   384710661893270773752008618930402124820]
[  -285788667382032639487999010709678291 2632246685618559545443528487477873481040]
[  346909083829111687918362389719995500531 4536212198753846690690224105901539410210]
```

有 p_1, p_2 後就可以還原回 k_1, k_2：

```
v = L.LLL()[1]
p1 = -v[0]
p2 = v[1]
k1 = a + p1
k2 = a + p2
k1, k2
```

```
(428533473835224596820615420326027243265496308682266701863195340338059073680000,
 428533473835224596820615420326027243268099976501147058144690068924465979331920)
```

有 k_1, k_2 後就可以還原出 d，驗證 d 是否跟 public key 的點相同：

```
d = (s2 * k2 - h2) * r2^(-1)
(int(d)*G).x(), Px
```

```
(mpz(113551801687420176889825240584277746938287326030292027522704591303296956035 77),
 '113551801687420176889825240584277746938287326030292027522704591303296956035 77')
```

有 d 後就可以還原出 private key，就可以送進 `Kuruwa` 到 server，就可以拿到 flag：

```
h = sha256('Kuruwa'.encode()).digest()
k = int(md5(b'secret').hexdigest() + md5(long_to_bytes(int(d)) + h).hexdigest(), 16)
prikey = Private_key(pubkey, d)
sig = prikey.sign(bytes_to_long(h), k)
str(sig.r), str(sig.s)
```

```
('63825320594311623643769791740580330406314025161475446258801230035581964411195',
 '113387105831969992999296008760571004273107175410665454360839926815706465618861')
```

```
r.recvline()
r.recvline()
r.recvline()
r.recvline()
```

```
b'3) exit\n'
```

```
r.sendline(b"2")
r.sendlineafter(b'username: ', b"Kuruwa")
r.sendlineafter(b'r: ', str(sig.r).encode())
r.sendlineafter(b's: ', str(sig.s).encode())
```

```
b's: '
```

```
r.recvline()
```

```
b'FLAG{adfc9b68bd6ec6dbf6b3c9ddd46aafaea06a97ee}\n'
```