HGAME 2022 WEEEK4 容世

Crypto

ECC

线上网站

sagecell.sagemath.org

常规ECC

```
E =EllipticCurve(GF(p),[a,b])
c1 = E(14455613666211899576018835165132438102011988264607146511938249744871964946084,25506582570581289714612640493258299813803157561796247330693768146763035791942)
c2 = E(37554871162619456709183509122673929636457622251880199235054734523782483869931,71392055540616736539267960989304287083629288530398474590782366384873814477806)

m=c1-k*c2
print(m)

cipher_left = 27453988545002384546706933590432585006240439443312571008791835203660152890619
cipher_right = 27453988545002384546706933590432585006240439443312571008791835203660152890619

c1=cipher_left/m[1]
print(c1)
```

Evaluate

Language: Sage

```
(57824879640955326550732559538097319221644125075532201058220628014917816573008 : 5447527586617964725403656557946739867751179615886683290766862044853251052675 7 : 1)
1274809002565510220953939 17
```

n2s可得

```
import libnum

z1=49303314923700944603626 0
z2=12748090025655102209539 3917

print(libnum.n2s(int(z2)))

#hgame{Ecc$ is!sO@HaRd}
```