XCTF easy_ECC WP

原创

lqvir 于 2020-12-22 19:50:12 发布

文章标签： ecc 密码学

本文链接：https://blog.csdn.net/weixin_46227016/article/details/111565136

ECC

第一次做椭圆曲线公钥加密方法，了解了一些ECC公钥加密的原理，

> 已知椭圆曲线加密Ep(a,b)参数为
> p = 15424654874903
> a = 16546484
> b = 4548674875
> G(6478678675,5636379357093)
> 私钥为
> k = 546768
> 求公钥K(x,y)

根据博客学习了ECC公钥的加密原理ECC

根据题目与ECC的性质，可以构建脚本实现解密过程：

```
Gx = 6478678675
Gy = 5636379357093
a = 16546484
b = 4548674875
p = 15424654874903
k = 546768
x = Gx
y = Gy
for i in range(k-1):
    if (x==Gx and y==Gy):
        inv = pow(2*Gy, p-2,p)
        temp = (3*Gx*Gx+a)*inv%p
    else:
        inv = pow((x-Gx), p-2,p)
        temp = (y-Gy)*inv%p

    xr = (temp*temp-Gx-x)%p
    yr = (temp*(x-xr)-y)%p
 #print(i,xr,yr)
    x = xr
    y = yr
print(x+y)
```