easy_ECC　Writeup

该题目思路比较简单，利用椭圆曲线计算 xG 的方法即可求出公钥对（具体原理见 https://www.jianshu.com/p/e41bc1eb1d81），一个较重要的点是利用逆元求分数的取模，有两种方法：费马小定理和欧几里得算法，这里我采用了费马小定理计算，编写脚本即可获得 flag。

脚本如下：

```
#求 x 的 y 次方的模
def power(x, y, mod):
    r = 1
    while( y ):
        if y & 1:
            r = (r * x) % mod
        x = (x * x) % mod
        y >>= 1
    return r


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 = power(2*Gy, p-2,p)
        temp = (3*Gx*Gx+a)*inv%p
    else:
        inv = power((x-Gx), p-2,p)
        temp = (y-Gy)*inv%p
    #print(temp)
    xr = (temp*temp-Gx-x)%p
    yr = (temp*(x-xr)-y)%p
    #print(i,xr,yr)
    x = xr
    y = yr
print(x+y)
```

求得 flag 为：cyberpeace{19477226185390}