

E.6.1

① 首先由 $y_1 = \alpha^k \pmod{p}$, 根据 a 计算 $y_1^a = (\alpha^k)^a = \alpha^{ak} \pmod{p}$

又因 $\beta = \alpha^a \pmod{p}$, 所以 $y_1^a = \beta^k \pmod{p}$

而 $y_2 = x + \beta^k \pmod{p}$, 那么 $x = y_2 - \beta^k \pmod{p}$, 将 $\beta^k = y_1^a \pmod{p}$ 代入得

$$x = y_2 - y_1^a \pmod{p}$$

② I. 解密 \rightarrow 解决 CDH.

已知 (y_1, y_2) , 且能解密出 x , 已知 $y_2 = x + \beta^k \pmod{p}$, 那么 $\beta^k = y_2 - x \pmod{p}$

这里 $y_1 = \alpha^k \pmod{p}$, $\beta = \alpha^a \pmod{p}$

$\therefore \beta^k = \alpha^{ak} \pmod{p}$, 即 CDH 问题的解

II. 密文为 (y_1, y_2) , 其中 $y_1 = \alpha^k \pmod{p}$, $\beta = \alpha^a \pmod{p}$,

如有解 CDH 的算法, 则可根据 y_1 和 β 计算出 $\beta^k = \alpha^{ak} \pmod{p}$

\therefore 可通过 $x = y_2 - \beta^k \pmod{p}$ 得到 x

习题 6.20

源代码:

```
def modinv(a, p):
    return pow(a, -1, p)

def L1_table_gen(alpha, p):
    table = {}
    val = 1
    for i in range(p):
        table[val] = i
        val = (val * alpha) % p
    return table

def L2_oracle(beta):
    if beta in [25219, 841]:
        return 1
    elif beta in [163, 532, 625, 656]:
        return 0
    else:
        return -1 # undefined
```

```

def log_discrete(p, alpha, beta):
    L1 = L1_table_gen(alpha, p)
    x = []
    b = beta

    x0 = L1[b]
    x.append(x0)
    b = (b * modinv(pow(alpha, x0, p), p)) % p

    i = 1
    while b != 1:
        xi = L2_oracle(b)
        x.append(xi)
        gamma = pow(b, (p + 1) // 4, p)
        if L1[gamma] == xi:
            b = gamma
        else:
            b = (p - gamma) % p
        b = (b * modinv(pow(alpha, xi, p), p)) % p
        i += 1

    return sum(xi * (1 << i) for i, xi in enumerate(reversed(x)))

# 使用
p = 1103
alpha = 5
beta = 896
result = log_discrete(p, alpha, beta)
print("log_5 896 =", result)

```

结果:

log_5 896 = 147