现代密码学 6. 离散对数.

6.1

(1) $e_k(x,b) = (y_1, y_2)$ $y_1 = \alpha^k$. $y_2 = x + \beta^k$.

$d_k(y_1,y_2) = y_2 - \beta^k = y_2 - (\alpha^a)^k = y_2 - y_1^a$.

(2) 1°. 证明任何与 CDH 问题等价的算法, 都可以用来解密 ElGamal 密文:

设 OracleCDH 是一个解 CDH 问题的算法.

$\delta = \text{OracleCDH}(\alpha, \beta, y_1) = \text{OracleCDH}(\alpha, \alpha^a, \alpha^k) = \alpha^{ak} = \beta^k$

$x = y_2 - \beta^k = y_2 - \delta = x + \beta^k - \beta^k$

2° 证明任何用于 ElGamal 密文的算法, 都可以用来解 CDH:

设 ~~Oracle-ElGamal-Decrypt~~ Oracle-ElGamal 是解密 ElGamal 的算法.

CDH: 已知 $\alpha, \alpha^a, \alpha^b$

$\delta = \text{Oracle-ElGamal}(\alpha, \beta = \alpha^a, (y_1 = \alpha^b, y_2)) = y_2 - y_1^a = y_2 - \alpha^{ab}$.

↳ 作为 $d_k(y_1, y_2)$

$\alpha^{ab} = y_2 - \delta$

∴ 得证.

6.2. 攻击者已知: 公钥 $\alpha, \beta = \alpha^a$, 泄露的 k. 密文 y_1, y_2

$\beta^k = \alpha^{ak}$ $y_2 = x \cdot \beta^k$. $\Rightarrow x = y_2 \cdot (\beta^k)^{-1}$. 求直接求得明文