No.
Date. / /

E6.1

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 → 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 $y_1=\alpha^k \pmod p$，$\beta=\alpha^a \pmod p$

∴ $\beta^k=\alpha^{ak} \pmod p$，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 $\beta^k=\alpha^{ak} \pmod p$

∴可通过 $x=y_2-\beta^k \pmod p$ 得到x

E6.2

若泄露了随机数k，则若攻击者已知道密文以及公钥 α,β,p

则 因 $\beta=\alpha^a$，∴可知 $\beta^k=\alpha^{ak}=K$

则 可由 $y_2=x\cdot K$ 解密得到 $x=y_2\cdot K^{-1}$

则 此次ElGamal 加密被破解