由攻破 IND-CPA 安全性的敌手 $\mathcal{A}$ 来构造解决 CDH 问题的敌手 $\mathcal{B}$:

1. 首先挑战者生成 (G, p, g, g^x, g^y), 并发送给敌手 $\mathcal{B}$;
2. 敌手 $\mathcal{B}$ 构造信息 $PK = (G, p, g, h = g^x)$ 发送给敌手 $\mathcal{A}$;
3. 敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 查询预言机, 若输入 x_i 为新, 返回 $H(x_i)$, 若不为新, 则返回对应结果;
4. 敌手 $\mathcal{A}$ 发送明文信息 M_0, M_1 给敌手 $\mathcal{B}$;
5. 敌手 $\mathcal{B}$ 构造信息 $C = (c_1 = g^y, c_2 \in \{0,1\}^m)$ 发送给敌手 $\mathcal{A}$;
6. 敌手 $\mathcal{A}$ 运行算法, 由于 $H(h^y) = H(g^{xy})$, 故敌手 $\mathcal{A}$ 有不可忽略的概率会向敌手 $\mathcal{B}$ 查询 g^{xy} 的预言机输出;
7. 此时敌手 $\mathcal{B}$ 即可以不可忽略的概率获得 g^{xy} 解决 CDH 问题;