Problem 1 (设计一种密钥分享方案)

设 $E=(E,D)$ 是加密算法, 密钥空间 $K=\{0,1\}^l$. 一家银行总行想将密钥 k 分散为 p_0,p_1,p_2 给 3 家分行, 使得任何两家都可以解密, 任何一家都得不到密钥的任何信息.

为此总行产生两个随机数对 (k_0,k_0') 和 (k_1,k_1') 使得 $k_0\oplus k_0'=k_1\oplus k_1'=k$. 请给出一个密钥分配方案.

分行 1 所持密钥为：(k_0, k_1)

分行 2 所持密钥为：(k_0', k_1')

分行 3 所持密钥为：(k_0, k_1')