《密码学原理》作业 3 答案

1. 首先选择两个消息 m_0 和 m_1，m_0 的所有各块都是全 0，而 m_1 的所有各块都是全 1。然后，在收到相应的密文 c 后，把 c 用以下方法改为 c’：c’中的初始向量与 c 中的初始向量不同，而其它全都与 c 一致。由于 c≠c’，敌方用密文 c’来做查询是合法的。但是，c 的明文和 c’的明文除了第一块之外的所有块全都是一致的。所以，根据查询结果，即可有较大概率判断出明文是 m_0 还是 m_1。

2. 答案是肯定的，用反证法证明如下。假设存在一个敌方在拿到密钥 s 后，找到 $H^s(H^s())$ 的碰撞的概率不是可忽略的（not negligible）。又设(a,b)是所找到的碰撞，亦即 $a \neq b$ 但 $H^s(H^s(a))=H^s(H^s(b))$。我们分两种情况讨论。情况一，$H^s(a)=H^s(b)$。这时，(a,b)也构成 $H^s()$ 的一个碰撞。情况二，$H^s(a) \neq H^s(b)$。这时，$(H^s(a), H^s(b))$ 构成了 $H^s()$ 的一个碰撞。总之，无论在哪种情况下，只要能找到 $H^s(H^s())$ 的碰撞，敌方也能找到 $H^s()$ 的碰撞。因此，同一个敌方找到 $H^s()$ 的碰撞的概率也同样不是可忽略的，而这与 H()的抗碰撞性相矛盾。

3. 助教找出相同比特数最多的 3 名同学，并检查其数据真实性。

4. 构造一个新的加密体系（encryption scheme）(G,E’,D’),其中我们定义 E’(m)=(b,E(m))(b 在{0,1}上均匀分布的并且独立于 E(m))；D’(b，c)=D(c)。首先，我们用反证法证明(G,E’,D’)是 XYZ-安全的。假设对于明文 m_0 和 m_1，存在一个敌方 A’在做了一系列 E’查询和 D’查询后，成功判断挑战密文(b,c)对应明文 m_0 还是 m_1 的概率减去 1/2 不是可以忽略的。基于 A’，我们构造另外一个攻击(G,E,D)的敌方 A。对于 A’产生的每一个 E’查询 m_q，A 把它翻译为 E 查询 m_q 进行查询，再把 E 查询得到的答案 c_q 翻译为(b_q, c_q)交给 A’。对于 A’产生的每一个 D’查询(b_q, c_q)，A 把它翻译为 D 查询 c_q 进行查询，然后再把 D 查询得到的答案 m_q 当成 D’查询的答案交给 A’。当 A 收到挑战密文 c 时，其独立且均匀随机地选择 $b \in \{0,1\}$，并把(b,c)交给 A’。而 A’的输出就会成为 A 的输出。显然，A 判断正确的概率与 A’判断正确的概率完全相同。根据(G,E,D)的 XYZ-安全性，这是不可能的。

最后，我们还需要证明(G,E’,D’)不是 CCA-安全的。构造一个新的敌方 A^*,在收到挑战密文(b,c)后,用(1-b,c)做一个 D’查询,查询结果就会成为 A^*的输出。显然，A^*判断正确的概率为 1。

【注】本题所说的 XYZ-安全，其实在很多文献中被称为 CCA-安全。而本教材所说的 CCA-安全，在这些文献里被称为适应性 CCA-安全，或者 CCA2-安全，或者其它的什么名称。