《密码学原理》作业 1 答案

1. 命题不成立。例如把 one time pad 的密钥空间、明文空间、密文空间、密钥生成算法都保持不变，但加密时直接输出明文作为密文。

2. 答案是否定的。假设一个 H 是一个“正常”的，符合题目中对于 G 的所有要求的伪随机发生器。现在对 H 做一定改造以得到 G：G 与 H 对于后半部分不全是 0 的输入，输出完全相同；当输入后半部分全是 0 时，G 直接输出一个全 0 串。这样构造的 G 显然是一个伪随机发生器，因为对于均匀分布的种子 s，$|D(G(s))-D(H(s))| \leqslant negl(n)$ → 对于均匀分布的 r，$|D(G(s))-D(r)| \leqslant |D(G(s))-D(H(s))|+|D(H(s))-D(r)| = negl(n)+negl(n) = negl(n)$。另一方面，使用这样的 G，可以保证 G’的输出为全 0 串。因此，在此情况下，G’不是一个伪随机发生器。

3. 助教将抽查。

4. 简化符号：记 p_0 为 $\mathcal{A}$ 收到 $E_k(m_0)$ 时输出 1 的概率； p_1 为 $\mathcal{A}$ 收到 $E_k(m_1)$ 时输出 1 的概率。记 q 为 $\mathcal{A}$ 收到 $E_k(m_b)$ 时成功猜到 b 的概率。则有：

$$q=(1-p_0)/2+p_1/2=1/2+(p_1-p_0)/2$$

定义 3.9 要求 $(p_1-p_0)/2 \leqslant negl(n)$，考虑到 m_0 和 m_1 的对称性，同时也应该要求 $(p_0-p_1)/2 \leqslant negl(n)$。把这两者合并，得到 $|(p_1-p_0)/2| \leqslant negl(n)$。而定义 3.10 要求的是 $|(p_1-p_0)| \leqslant negl(n)$，显然与此是等价的。