《密码学原理》作业 3

注意：因为课本版本不同，以下习题的题号可能会有出入，有的习题甚至在某些版本中不存在。请大家以以下影印内容为准。

作业格式要求：客观题提交格式“学号+姓名.pdf”；实验题，只提交.cpp 和.h 源码；最后将两份文件打包，格式为“学号+姓名.rar”

1.（30 分）Prove the CBC mode does not yield a CCA secure encryption scheme regardless of F. 提示：可以模仿书上的一个例子。首先选择两个消息 m_0 和 m_1，然后在收到相应的密文 c 后，把 c 改为 c’，用密文 c’来做查询。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.（30 分）《Introduction to Modern Cryptography》190 页，习题 5.3。

5.3 Let (Gen, H) be a collision-resistant hash function. Is $(\mathsf{Gen}, \hat{H})$ defined by $\hat{H}^s(x) \stackrel{\text{def}}{=} H^s(H^s(x))$ necessarily collision resistant?

提示：如果答案是肯定的，你需要提供严格的证明；如果答案是否定的，你需要举一个反例。

3.（40 分）请用 Crypto++或者 Java Cryptography Architecture(JCA)实现一个程序，寻找 SHA-1 的“近似碰撞”。也就是说，要找到两个输入 a 和 b，使得 a≠b，但是 SHA1(a)和 SHA1(b)有尽可能多的对应比特相同。请说明你找到的 SHA1(a)和 SHA1(b)有多少个比特相同。**对于相同比特数最多的三位同学，我们将公开表扬，并分别额外奖励 50 分、30 分、20 分**。请提交你找到的 a 和 b 的值，以及它们的 Hash 值。

请注意：**请对你找到的 a 和 b 的值绝对保密。**在没有抄袭的情况下，不同同学提交的 a 和 b 的值几乎不可能相同。所以，如果有 2 位或者更多同学提交了一组相同的(a,b)，我们将视为严重抄袭嫌疑。有严重抄袭嫌疑者，将不会得到表扬和公开奖励，并且会受到调查。一旦调查证实了抄袭行为，我们将予以严惩。

4.（附加题，做对奖励 30 分，做错或者不做不扣分）We can define “XYZ security” for private key encryption schemes by slightly modifying the definition of CCA security: We no longer allow the adversary to make encryption and decryption queries after the challenge ciphertext c is received; everything else remains the same. Assume there exists an

XYZ-secure encryption scheme (G,E,D). Prove there exists a private key encryption scheme that is XYZ-secure but not CCA secure.

关于参考别人的作业：如果你参考了别人的作业，请在显眼处明确指出自己参考了谁的作业（姓名、学号一定要写清楚，参考了哪一题也请写清楚）。我们会在对方得分的基础上，适当降低一些，作为你的得分。如果你不做这样的说明，那么就会被视为抄袭，有可能受到严惩。无理由雷同的作业有可能全部得 0 分。