《密码学原理》作业 2

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.（20 分）《Introduction to Modern Cryptography》156 页，习题 4.9（a）。

4.9 Prove that the following modifications of CBC-MAC do not yield a secure fixed-length MAC:

(a) Modify CBC-MAC so that a random IV is used each time a tag is computed (and the IV is output along with t_ℓ). I.e., $t_0 \leftarrow \{0,1\}^n$ is chosen uniformly at random rather than being fixed to 0^n, and the tag is t_0, t_ℓ.

提示：敌方可以向 MAC Oracle 提交一个查询 m，从而得到相应的(t_0, t_l)。显然有 $Vrfy_k(m, t_0, t_l)=1$。然后，把(m, t_0, t_l)稍作修改，得到(m’, t_0’, t_l’)，使其满足 m’≠m 但 $Vrfy_k(m', t_0', t_l')=1$。

2.（20 分）《Introduction to Modern Cryptography》190 页，习题 5.5(a)。

5.5 What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

(a) Each round function outputs all 0s, regardless of the input.

3.（20 分）《Introduction to Modern Cryptography》190 页，习题 5.5(b)。
提示：我们只要求你考虑 r 是 3 的倍数的情况，其它情况可以忽略。

5.5 What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

(b) Each round function is the identity function.

4. (40 分）请用 Crypto++或者 Java Cryptography Architecture(JCA)实现一个程序，读出一个名为“key.txt”的文件中的 128 位的密钥，一个名为“plain.txt”的文件中的 128 位的明文，用 TripleDES 加密后，密文写入一个叫做“encrypted.txt”的文件。所有文件格式均为纯文本,密钥、明文、密文均用二进制书写，形如“00111010……”。请提交全部源代码。提示：网上可以找到类似的源代码，但需要稍加修改才能达到本作业题的要求。

5. （附加题，做对奖励 20 分，做错或者不做不扣分）《Introduction to Modern Cryptography》104 页，习题 4.9（b）。

4.9 Prove that the following modifications of CBC-MAC do not yield a secure fixed-length MAC:

(b) Modify CBC-MAC so that all blocks $t_1, \ldots, t_\ell$ are output (rather than just t_ℓ).

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。