《密码学原理》作业1

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。

作业提交格式：客观题，请大家在 Deadline 那天课上提交纸质版作业；

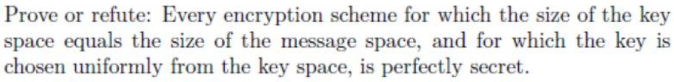
实验题，请将源码和运行结果打包（文件名为学号+姓名）发到助教邮箱。

1.（20 分）《Introduction to Modern Cryptography》38 页，习题 2.5。

Prove Lemma 2.6 :

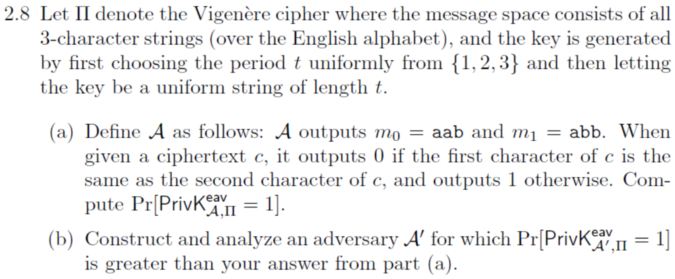
Encryption scheme Π is perfectly secret if and only if it is perfectly indistinguishable.

2.（20 分）



Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

3.（20 分）Introduction to Modern Cryptography》38 页，习题 2.8。



2.8 Let Π denote the Vigenère cipher where the message space consists of all 3-character strings (over the English alphabet), and the key is generated by first choosing the period t uniformly from $\{1, 2, 3\}$ and then letting the key be a uniform string of length t.

(a) Define $\mathcal{A}$ as follows: $\mathcal{A}$ outputs $m_0 = \texttt{aab}$ and $m_1 = \texttt{abb}$. When given a ciphertext c, it outputs 0 if the first character of c is the same as the second character of c, and outputs 1 otherwise. Compute $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1]$.

(b) Construct and analyze an adversary $\mathcal{A}'$ for which $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A}',\Pi} = 1]$ is greater than your answer from part (a).

4.（40 分）请用 Crypto++或者 Java Cryptography Architecture(JCA)实现一个 one time pad。请提交全部源代码，以及把“hello world”加密后产生的密文。