《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。

1. （30 分）《Introduction to Modern Cryptography》42 页,习题 2.5。

   2.5 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.

2. （30 分）《Introduction to Modern Cryptography》104 页，习题 3.6（a）。提示：答案是否定的。可以考虑从一个“正常”的伪随机发生器出发，稍作修改，构造一种特殊的伪随机发生器 G。这样构造的 G 需要满足两个条件：（1）G 确实是一个伪随机发生器；（2）G 对于输入 $s0^{|s|}$ 会有“异常”的表现，从而导致 G’ 不是一个伪随机发生器。请注意你需要证明 G 同时满足这两个条件。

   3.6 Let G be a pseudorandom generator where $|G(s)| \geq 2 \cdot |s|$.

   (a) Define $G'(s) \stackrel{\text{def}}{=} G(s0^{|s|})$. Is G' necessarily a pseudorandom generator?

3. （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。

4. （附加题，做对奖励 30 分，做错或者不做不扣分）《Introduction to Modern Cryptography》104 页，习题 3

   3.4 Prove the equivalence of Definition 3.8 and Definition 3.9.

DEFINITION 3.8 *A private-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *has* indistinguishable encryptions in the presence of an eavesdropper, *or is* EAV-secure, *if for all probabilistic polynomial-time adversaries* $\mathcal{A}$ *there is a negligible function* negl *such that, for all* n,

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n),$$

where the probability is taken over the randomness used by $\mathcal{A}$ *and the randomness used in the experiment (for choosing the key and the bit* b*, as well as any randomness used by* Enc*).*

DEFINITION 3.9 *A private-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *has* indistinguishable encryptions in the presence of an eavesdropper *if for all* PPT *adversaries* $\mathcal{A}$ *there is a negligible function* negl *such that*

$$\left| \Pr[\mathsf{out}_{\mathcal{A}}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,0)) = 1] - \Pr[\mathsf{out}_{\mathcal{A}}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,1)) = 1] \right| \leq \mathsf{negl}(n).$$

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。