第 4-6 讲: 加密算法

姓名：_ **学号：**_

评分：_____ **评阅：**_____

2021 年 3 月 30 日

请独立完成作业，不得抄袭。
若得到他人帮助, 请致谢。
若参考了其它资料，请给出引用。
鼓励讨论，但需独立书写解题过程。

1 作业 (必做部分)

题目 1 (TJ 7-7(a,b))

解答：

题目 2 (TJ 7-9(b))

解答：

题目 3 (TJ 7-12)

解答：

题目 4 (TC 31.7-1)

解答：

题目 5 (TC 31.7-2)

解答:

题目 6 (TC Problem 31-3)

解答:

---

2 作业 (选做部分)

题目 1 (TC Problem 31-4)

解答:

---

3 Open Topics

Open Topics 1 (中国剩余定理)
向同学介绍中国剩余定理及其应用。

Open Topics 2 (椭圆曲线加密 (Elliptic Curve Cryptography, ECC))
椭圆曲线加密是基于椭圆曲线数学理论实现的一种非对称加密算法。相比 RSA, ECC 优势是可以使用更短的密钥, 来实现与 RSA 相当或更高的安全。(参考资料-1: https://medium.com/dev-genius/introduction-to-elliptic-curve-cryptography-567e47b0e49e) (参考资料-2: https://en.wikipedia.org/wiki/Elliptic-curve_cryptography) (参考资料-3: https://www.jianshu.com/p/e41bc1eb1d81)

4 反馈