《密码学课程设计》课程任务及考核方式

密码学课程设计是信息安全专业的专业实践课程。课程要求如下：

1. **实验内容**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设计内容 | 设计要求 | 学时（天） | 备注 |
| 1 | 古典密码算法 | 1. 实现维吉尼亚密码算法的加解密过程，并能正确的加解密教材P65页习题5（6）。 2. 实现Hill密码算法的加解密过程，并能正确的加解密教材P65页习题5（7）。 | 2 | 1.所有程序优先使用Python3版本完成；如使用其他编程语言，将会适当扣分。  2.实现密码算法时不允许使用现有库，解题时可以使用扩展库完成。  3.对完成其他非课程要求的密码学题目（提供题目、wp和结题脚本）者可进行额外加分。 |
| 2 | 序列密码 | 1. 选择一个15次以上的不可约多项式，编写一个线性反馈移位寄存器。验证生成序列的周期。 2. 完成题目LFSRXOR.py并提交WP（完整的结题思路和代码） | 2 |
| 3 | DES加解密或AES的加密算法 | 1. 编写DES加解密或AES的加密算法，使算法能够运行成功。并利用分组密码的工作模式对一段明文进行加解密。 2. 编程解决AES2和DES3，并提交WP（完整的结题思路和代码） | 10 |
| 4 | RSA加密算法 | 1. 利用所学的生成素数的算法，生成两个尽可能的素数，进一步实现RSA的加密算法。 2. 解决mediumRSA，hardRSA，veryhardRSA、cipher和RSA题目，并提交WP（完整的结题思路和代码） | 6 |
| 5 | Hash函数 | 1. 选择MD5或其它的Hash函数进行编程实现 2. 解决md51题目，并提交WP（完整的结题思路和代码） | 6 |
| 6 | 综合实验 | Alice想通过公共信道给Bob传输一份秘密文件（文件非常大），又知道，很多人和机构想得到这份文件。如果你是Alice，你应该怎样做？请设计一个方案。，并编程实现。 | 6 |
| **合 计** | |  | 32 |  |

**三．成绩评定**

1．根据大家的具体工作量和难度进行权衡得分。主要包括成果演示和课程报告部分。

2.成功完成的每个实验都要记录在课程报告中，课程报告中要详细记录每个实验的步骤和相应截图，严禁互相抄袭，凡发现两份报告雷同者，两份报告都做不及格处理。  
3.课程报告封面及目录见群文件。