密码学大作业

作业对象：信安 1601 班，1602 班作业

提交时间：2017-2018 学年第二学期第 13 教学周

作业内容：

利用古典密码算法的思想，设计一种新密码算法，使用编程语言对上述密码算法进行实现，并利用差分密码分析方法对设计的密码算法进行分析。

作业要求：

（1）使用不少于 2 种古典密码算法思想；

（2）明文要求是 26 个字母符号，或者二进制数据（分组长度不少于 8）；

（3）要求使用编程语言对上述设计算法进行实现，编程语言自选；

（4）要求实现加密过程和解密过程；

（5）利用差分密码分析方法，对所设计的密码算法进行分析，要求通过编程方法的实现差分分析，编程语言自选；

（6）完成密码设计及分析报告，加解密执行过程，以及明文、密钥、密文内容要通过截图体现；

作业提交内容：

（1）密码设计及分析报告（文档格式自定，要求章节清晰，内容明确，文件格式为 PDF）；

（2）密码算法实现（源码，可执行代码）；

（3）分析实现（源码，可执行代码）；

（4）上述内容压缩打包，命名格式为：学号_姓名.rar

（5）不提交纸质材料，所有压缩包各班交由学习委员汇总后，发送到老师这里（邮箱，QQ 在线等方式均可，学习委员同时提交为交作业同学名单）。不接受各位同学单独提交作业，不接受迟交作业。

注：大作业要求个人独立完成。提交作业中，如发现两人所使用的算法或代码相同，则均记 0 分。迟交作业等于未交作业。