实验一 古典密码实验报告

1. 实验目的
2. 掌握单表代替密码；
3. 掌握多表代替密码，重点是多表代替密码的实现；
4. 掌握置换密码；
5. 掌握对单表、多表密码体制的攻击；
6. 掌握16进制转换与读写。
7. 实验背景

（介绍实验所涉及的知识，包括：代替密码、维吉尼亚密码、希尔密码、置换密码、密码统计分析、base64编码）

1. 实验内容

plaintext = cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

注意：标点符号和空格不加密

1）实现单表代替密码：凯撒密码,实现对英文消息plainxtext的代替加密；

2）实现多表代替密码：维吉尼亚密码、希尔密码,实现对英文消息的代替加密；

3）实现分组大小为8的置换密码，实现对英文消息plainxtext的置换加密；

4）实现对代替密码的攻击,找到1）中密文对应的解密密钥；

5）实现二进制文件读写、字节替换密码，读取二进制文件cryptointro.txt，并对其进行加密，把密文写到文件cipher.txt。

6）了解base64编码，读取上述cryptointro.txt和cipher.txt，并以base64编码输出并显示。

1. 实验过程
2. 实验心得