**实验二 凯撒密码及单表置换**

**一、实验目的**

1. 掌握凯撒密码的基本原理，了解其加密和解密的具体过程。

2. 学习实现凯撒密码的移位置换操作，输出不同形式的密文，包括大小写混合、全大写和全小写形式。

3. 理解单表置换的基本概念和实现方法，掌握其在加密中的应用。

**二、实验原理**

**1. 凯撒密码**

替代密码算法的原理是使用替代法进行加密，就是将明文中的字符用其它字符替代后形成密文。例如，明文字母a、b、c、d，用D、E、F、G做对应替换后形成密文。

替代密码包括多种类型，如单表替代密码、多明码替代密码、多字母替代密码、多表替代密码等。凯撒密码是一种简单的替换加密技术，其基本思想是将字母表中的每个字母通过固定的偏移量进行移位替换。例如，假设偏移量为*k*，则明文中的每个字母*c*替换为，其中，*n*为字母表的长度，*c*和*c′*分别表示明文和密文字母对应的索引值。凯撒密码的解密过程是加密的逆过程，偏移量为*−k* ：。

此外，为了适应不同的输出需求，可以在加密完成后对密文格式进行处理（如转换为全大写、全小写或大小写混合）。

**2.置换密码**

置换密码算法的原理是不改变明文字符，只将字符在明文中的排列顺序改变，从而实现明文信息的加密。置换密码有时又称为换位密码。

单表置换是实现置换密码的一种常用方法，在算法中维护着一个置换表，这个置换表记录了明文和密文的对照关系。当没有发生加密（即没有发生置换）之前，其置换表如表1所示。

**表1 加密前的置换表**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i | j | k | l | m |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

在单表置换算法中，密钥是由一组英文字符和空格组成的，称之为密钥词组。将密钥填入置换表，如果遇到重复的字符则忽略，接着按原表顺序填充，忽略重复字符。例如当输入密钥词组：CRYPTO后，对应的置换表如表2所示。

**表2 加密后·的置换表**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i | j | k | l | m |
| C | R | Y | P | T | O | A | B | D | E | F | G | H |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| I | J | K | L | M | N | Q | S | U | V | W | X | Z |

密钥CRYPTO，后序ABD……WXZ则是密钥词组中未出现的字母按照英文字母表顺序排列成的。密钥词组是生成置换表的核心参数，它为加密过程提供了灵活性和可定制性，同时也直接影响了密文的形式和解密的难度。

**三、实验内容**

1. 凯撒密码的移位置换

 输入明文字符串和偏移量*k*。

 实现凯撒密码的加密算法，输出以下四种格式的密文：大小写不变、大小写互换、全大写、全小写。

 实现凯撒密码的解密算法，验证加密和解密的正确性。

2. 单表置换

实现基于置换表的加密和解密算法。输入明文字符串，通过置换表加密生成密文，随后解密以恢复原始明文。

**四、实验报告要求**

实验报告正文部分格式及内容如下：

实验目的：给出本次实验所涉及并要求掌握的知识点。

实验内容：给出实验的具体内容。

实验代码：给出实验时所实现的核心代码，展示算法的实现过程。

实验结果：给出实验的实际运行结果，并分析实验结果，验证算法的正确性和效率。

实验总结与心得：总结实验过程，分析实验中出现的问题及解决方法，总结实验的心得体会，并提出实验的改进意见。