**Министерство образования и науки Российской Федерации**

федеральное государственное автономное образовательное учреждение

высшего образования

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ**

**ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**Классические криптографические системы**

**经典密码系统**

Методические указания для проведения

лабораторной работы № 3 по дисциплине

«Информационная безопасность автоматизированных систем».

Томск – 2022

**Цель работы**: изучить классические методы шифрования и программно реализовать алгоритмы шифрования текстовых сообщений. 学习经典加密方法，并在软件中实现文本信息加密算法。

**Теоретические сведения**

**Шифр Цезаря**

В I в. н.э. Ю.Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (*А*) на четвертую (*D*), вторую (*B)* – на пятую (*E*), наконец последнюю – на третью: 公元 1 世纪，J.Caesar 在与高卢人的战争中，与他在罗马的朋友通信时，用第四个字母（D）代替了拉丁字母的第一个字母（A），用第五个字母（E）代替了第二个字母（B），最后用第三个字母代替了最后一个字母：

**ABCDEFGHIJKLMNOPQRSTUVWXYZ YHQL YLGL YLFL**

**DEFGHIJKLMNOPQRSTUVWXYZABC Veni vidi vici -** “Пришел, увидел,

победил”

С современной точки зрения, в шифре Цезаря каждая буква замещается на букву, находящуюся *k* символами правее по модулю равному количеству букв в алфавите. 从现代的角度来看，在凯撒密码中，每个字母都被右边 k 个字符的字母所取代，其模数等于字母表中的字母数。

*Ck*(*j*) *=*(*j+k*)(mod *n*),

где *n* *—* количество букв в алфавите (мощность алфавита).

Очевидно, что обратной подстановкой является

*Ck*-1(*j*) *= Сn-k=*(*j*+*n*-*k*)(mod *n*).

**Шифр Цезаря с ключевым словом**

В данной разновидности шифра Цезаря ключ задается числом *k*(0<= *k* <=*n*-1) и коротким ключевым словом или предложением. Выписывается алфавит, а под ним, начиная с *k*-й позиции, ключевое слово. Оставшиеся буквы записываются в алфавитном порядке после ключевого слова. В итоге мы получаем подстановку для каждой буквы. Требование, чтобы все буквы ключевого слова были различными не обязательно *—* можно записывать ключевое слово без повторения одинаковых букв. 在凯撒密码的这一变体中，密钥由一个数字 k（0<= k <=n-1）和一个简短的关键词或句子给出。字母表被写出，关键词从第 k 个位置开始写在字母表下方。其余字母按字母顺序写在关键词之后。最后，每个字母都有一个替代词。关键词的所有字母都必须是不同的这一要求并无必要--不重复相同的字母也可以写出关键词。

**Пример**: *k* = 5;ключевое слово *КЛЮЧ*

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Ъ У Ь Э Я **К Л Ю Ч** А Б В Г Д Е Ж З И Л М Н О П Р С Т У Ф Х Ц Ш Щ

*Исходное сообщение*: РИМ

*Шифротекст*: ЗЧГ

**Аффинная криптосистема**

Обобщением системы Цезаря является аффинная криптосистема. Она определяется двумя числами *a* и *b*, где ***0 <=*** *a,b* <= *n*-1 и *n* —является мощностью алфавита. Числа *a* и *n* должны быть взаимно простыми. Соответствующими заменами являются: 仿射密码系统是对凯撒系统的概括。它由两个数字 a 和 b 定义，其中 0 <= a,b <= n-1，n 是字母表的幂次。a 和 n 必须互质。相应的替换为

*Aa,b*(*j*)=(*a\*j+b*)(mod *n*),

Обратную замену также можно получить, просто поменяв местами строки в таблице замен. 只需交换替换表中的行，也可实现反向替换。

*A*-1*a,b*(*j*)=(*j-b*)\**a*-1(mod *n*).

Взаимная простота *a* и *n* необходима для однозначности отображения, в противном случае возможны отображения различных символов в один и неоднозначность дешифрирования. a 和 n 的相互简单性是确保映射明确无误的必要条件，否则就可能出现不同符号映射成一个符号以及解释含糊不清的情况。

**Квадрат Полибия**

Система Цезаря не является старейшей. Возможно, что наиболее древней из известных является система греческого историка Полибия, умершего за 30 лет до рождения Цезаря. В Древней Греции (II в. до н.э.) был известен шифр, называемый “*квадрат Полибия”*. Это устройство представляло собой квадрат 5\*5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку записывалась одна буква (в греческом варианте одна клетка оказывалась пустой, а в латинском - в одну клетку помещали две буквы *I,J*). В результате каждой букве отвечала пара чисел по номеру строки и столбца. 凯撒的体系并不是最古老的。已知最古老的系统可能是希腊历史学家波利比乌斯的系统，他比凯撒早出生 30 年。 在古希腊（公元前 2 世纪），人们知道一种叫做波利比乌斯方阵的密码。这个装置是一个 5\*5 的正方形，其中的列和行用 1 到 5 的数字编号。每个方格中都写有一个字母（在希腊文版本中，一个方格是空的，而在拉丁文版本中，两个字母 I,J 被放在一个方格中）。因此，每个字母的行数和列数都与一对数字相对应。

**A B C D E 13 34 22 24 44 34 15 42 22 34 43 45 32**

**F G H I,J K**

**L M N O P Cogito ergo sum -** лат. “Я мыслю, следовательно, существую”

**Q R S T U** Р.Декарт **V W X Y Z**

**Решетка Кардано**

Широко известны шифры, принадлежащие к классу “перестановка”, в частности “*решетка Кардано*”. Это прямоугольная карточка с отверстиями, чаще всего квадратная, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. Число строк и столбцов на карточке четно. Карточка сделана так, что при последовательном ее поворачивании каждая клетка лежащего под ней листа окажется занятой. Карточку поворачивают сначала вдоль вертикальной оси симметрии на 180, а затем вдоль горизонтально оси также на 180. И вновь повторяют ту же процедуру. 属于 "置换 "类的密码广为人知，尤其是 "卡达诺网格"。这是一张带孔的长方形卡片，多为正方形，将其重叠在一张纸上，只留下部分空白。卡片上的行数和列数都是偶数。卡片的制作方式是，当卡片连续转动时，下面纸张的每个单元格都会被占满。先将卡片沿垂直对称轴旋转 180，然后再沿水平轴旋转 180。重复同样的步骤。

**Таблица Виженера**

Неудобство рассмотренных выше шифров очевидно, т.к. в случае использования стандартного алфавита таблица частот встречаемости букв алфавита позволяет определить один или несколько символов, а этого иногда достаточно для вскрытия шифра (например, “Плящущие человечки” Конан Дойля). Поэтому использовались различные приемы для того чтобы затруднить дешифрование, например использование “*таблицы Виженера”*, которая представляет собой квадратную таблицу с числом строк и столбцов равным количеству букв алфавита. Чтобы зашифровать какое-либо сообщение выбирают слово - *лозунг* (например, “монастырь”) и надписывают его над сообщением с необходимым повторением. 上述密码的不便之处显而易见，因为在使用标准字母表的情况下，通过字母出现频率表可以识别出一个或多个字符，有时这就足以打开密码（例如柯南道尔的《跳舞的人》）。因此，人们使用了各种技术来增加解密的难度，例如使用 "维基涅尔表"，这是一个行列数等于字母表字母数的方形表。为了对信息进行加密，可以选择一个口号词（如 "修道院"），并在信息上方刻上必要的重复词。

Чтобы получить шифрованный текст, находят очередной знак лозунга, начиная с первого в вертикальном алфавите, а ему соответствующий знак сообщения в горизонтальном алфавите. На пересечении выделенных столбца и строки находим первую букву шифра. Очевидно, что ключом к такому шифру является используемый лозунг. 要获得密码文本，需要从纵向字母表中的第一个符号开始，找到标语的下一个符号，并在横向字母表中找到信息的相应符号。在所选列和行的交叉点上，我们就能找到密码的第一个字母。显然，这种密码的关键在于所使用的口号。

Если *n {\displaystyle n}n* – количество букв в алфавите, *m j {\displaystyle m\_{j}}mj*– буквы открытого текста, *kj* – k j {\displaystyle k\_{j}} kj буквы ключа, то шифрование Виженера можно записать следующим образом:

*cj* = (*mj* + *kj*) (mod *n*). c j = m j + k j ( mod n ) {\displaystyle c\_{j}=m\_{j}+k\_{j}{\pmod {n}}}

Дешифровывание:

*mj* = (*cj* – *kj*) (mod *n*). c j = m j + k j ( mod n ) {\displaystyle c\_{j}=m\_{j}+k\_{j}{\pmod {n}}}

**Пример:** **Шифрование сообщения с использованием таблицы Виженера**

*Лозунг*: **м о н а с т ы р ь м о н а с т ы р ь м о н**

*Исходный текст*: **р а с к и н у л о с ь м о р е ш и р о к о**

*Шифротекст:* **э о я к щ а п ы й ю й щ о в ч ф ш л ь ш ы**

***Таблица Виженера***

**АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ**

**БВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯА**

**ВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБ**

**ГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВ**

**ДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯФБВГ**

**ЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯФБВГД**

**ЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯФБВГДЕ**

**ЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖ**

**ИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗ**

**ЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИ**

**КЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙ**

**ЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙК**

**МНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛ**

**НОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМ**

**ОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМН**

**ПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНО**

**РСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОП**

**СТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПР**

**ТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРС**

**УФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТ**

**ФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУ**

**ХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФ**

**ЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХ**

**ЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦ**

**ШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ**

**ЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШ**

**ЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ**

**ЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬ**

**ЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧЩШЬЫ**

**ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭ**

**ЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮ**

**Одноразовый шифровальный блокнот**

Примером нераскрываемого шифра может служить так называемый “*одноразовый шифровальный блокнот*” - шифр, в основе которого лежит та же идея, что в шифре Цезаря. Назовем *расширенным алфавитом* совокупность букв алфавита, знаков препинания {. , : ; ! ? () – “ <пробел>}, число символов расширенного русского алфавита в данном варианте будет равно *44*. Занумеруем символы расширенного алфавита числами от *0* до *43.* Тогда любой передаваемый текст можно рассматривать как последовательность {*an*} чисел множества *A*={0,1,2,…,43}. 无法破译的密码的一个例子是所谓的 "一次性密码垫"，这是一种基于与凯撒密码相同的思想的密码。我们把扩展字母表称为由字母、标点符号 {. , : ; ! ? () - " <空格>}，在这种变体中，扩展俄语字母表的字符数等于 44 个。让我们用 0 到 43 之间的数字对扩展字母表的字符进行编号。这样，任何传输的文本都可以视为集合 A={0,1,2,...43} 中的数字序列 {an}。

Предположим, что имеем случайную последовательность {*cn*} из чисел множества *А* той же длины, что и передаваемый текст - *ключ*. Складывая по модулю *44* число из передаваемого текста *an* с соответствующим числом из множества ключа *cn*:

*an* + *cn*  *bn* (mod 44), 0 <= *bn* <= 43

получим последовательность {*bn*} знаков шифрованного текста. Чтобы получить передаваемый текст, можно воспользоваться тем же ключом:

*an*  *bn* - *cn* (mod 44),0 <= *an* <= 43

У двух абонентов, находящихся в секретной переписке, имеются два одинаковых блокнота. В каждом из них на нескольких листах напечатана случайная последовательность чисел множества *А.* Отправитель свой текст шифрует указанным выше способом при помощи первой страницы блокнота. Зашифровав сообщение, он уничтожает использованную страницу и отправляет текст сообщения второму абоненту, получатель шифрованного текста расшифровывает его и также уничтожает использованный лист блокнота. Нетрудно видеть, что одноразовый шифр не раскрываем в принципе, так как символ в тексте может быть заменен любым другим символом и этот выбор совершенно случаен.秘密通信中的两个订户有两个完全相同的笔记本。发送者用笔记本的第一页按上述方法加密文本。加密后，他销毁用过的那一页，然后将信息文本发送给第二个订户，密码文本的接收者解密后也销毁笔记本用过的那一页。不难看出，一次性密码原则上是不可泄露的，因为文本中的一个字符可以被任何其他字符替换，而这种选择是完全随机的。

**Задание на лабораторную работу**

1. Выбрать любые два классических криптоалгоритма из представленных в методических указаниях. 从指南中介绍的经典加密算法中任选两种。

2. Реализовать программу для шифрования и дешифрования текстовых сообщений. Программа должна осуществлять шифрование текста, введенного пользователем, с помощью выбранных алгоритмов. При необходимости указания параметров шифрования (например, сдвига в алгоритме Цезаря) пользователь должен также вводить их в командную строку в ответ на соответствующий запрос. Оформить классы в виде dll библиотек. 执行一个加密和解密文本信息的程序。程序应使用选定的算法对用户输入的文本进行加密。如果需要指定加密参数（例如凯撒算法中的移位），用户也应在响应相应请求时在命令行中输入这些参数。将类组织为 dll 库。

3. Осущест вить проверку правильности работы программы. Для этого необходимо вручную зашифровать некоторое сообщение в соответствии с выбранным алгоритмом и сравнить полученный результат с результатом работы программы. В качестве сообщения используйте Вашу фамилию, записанную латиницей. 检查程序操作的正确性。为此，请根据所选算法手动加密一些信息，并将结果与程序结果进行比较。用拉丁文书写您的姓氏作为信息。

4. Оформить отчет по лабораторной работе.

***\*Дополнительно***

Реализовать программу для дешифровки текстовых сообщений на основе выбранных криптоалгоритмов.

**Содержание отчета**

Форма сдачи лабораторной работы предполагает демонстрацию выполненного задания (программы) и подготовку отчета.

Отчет по лабораторной работе должен содержать:

1. Тему и цель лабораторной работы;

2. Краткие теоретические сведения;

3. Листинг разработанных программ с подробными комментариями;

4. Результаты работы программ;

5. Проверку правильности работы программ.

6. Выводы.