пМинистерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Информационных технологий и управления

Кафедра Интеллектуальных информационных технологий

**ОТЧЁТ**

по дисциплине «Средства и методы защиты информации в интеллектуальных системах»

Лабораторная работа №2

Вариант 2

Выполнил: Робилко Т. М.

гр. 221701

Проверил: В. В. Захаров

Минск 2024

**Задание:**

1) Реализовать в виде программы шифр (зашифрование и расшифрование)

в соответствии с вариантом (вариант 2: шифр Виженера). Язык исходного текста русский или английский по выбору исполнителя.

2) Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.

3) Оценить криптографическую стойкость реализованного шифра.

4) Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма.

**Ход работы:**

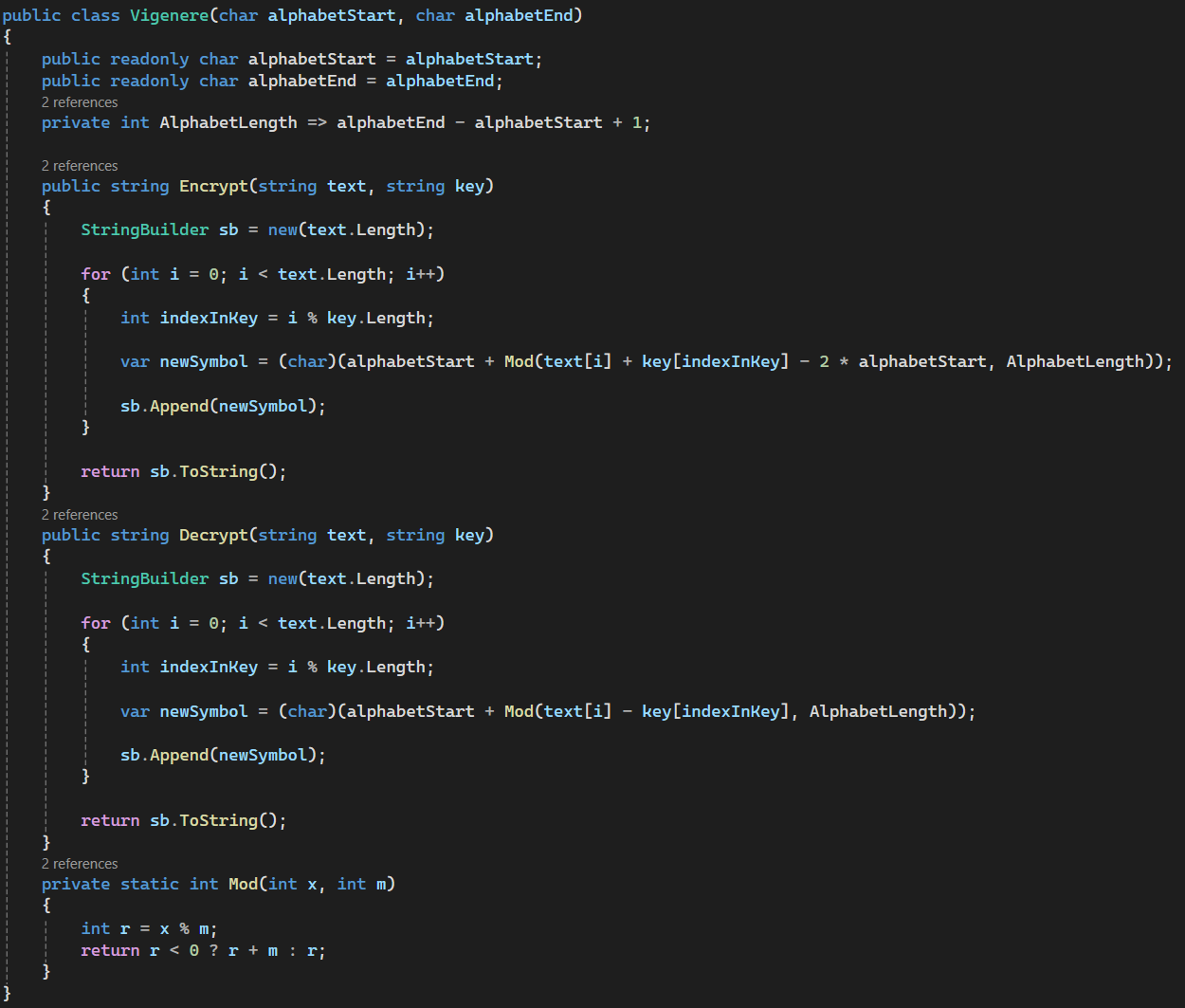
1. Описание алгоритма зашифрования:
   * Инициализировать алфавит для генерации посредством передачи списка символов в конструктор генератора;
   * Передать в метод зашифрования исходное сообщение и ключ;
   * Повторить ключ, пока его длина не станет больше или равна длине исходного текста;
   * Для каждого символа исходного текста применить формулу нахождения символа зашифрованного текста,

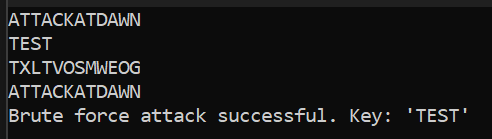
где kj – символ строки-ключа

1. Описание алгоритма расшифрования
   * Инициализировать алфавит для генерации посредством передачи списка символов в конструктор генератора;
   * Передать в метод зашифрования зашифрованное сообщение и ключ;
   * Повторить ключ, пока его длина не станет больше или равна длине исходного текста;
   * Для каждого символа зашифрованного текста применить формулу нахождения символа исходного текста,

где kj – символ строки-ключа

1. Класс Vigenere, реализующий алгоритм зашифрования и расшифрования



1. Вывод программы, включающий исходное сообщение, ключ для шифрования и расшифрованное сообщение. Также выводится полученный путём полного перебора ключ для шифрования.

**Выводы и описание криптографической стойкости использованного шифра**

Главный недостаток шифра Виженера состоит в том, что его ключ повторяется. Поэтому криптоанализ шифра может быть построен в два этапа:

1. Поиск длины ключа. Можно анализировать распределение частотностей в зашифрованном тексте с различным прореживанием. То есть брать текст, включающий каждую 2-ю букву зашифрованного текста, потом каждую 3-ю и т. д. Как только распределение частотностей букв будет сильно отличаться от равномерного (например, по энтропии), то можно говорить о найденной длине ключа.
2. Криптоанализ. Совокупность l шифров Цезаря (где l — найденная длина ключа), которые по отдельности легко взламываются.

Длину ключа возможно определить с помощью теста Касиски, основанном на нахождении индекса совпадения отдельных символов.

Нахождение ключа методом прямого перебора, как и в случае с подбором пароля, имеет экспоненциальное время, поэтому становится неэффективным с увеличением длины ключа.

**Способы улучшения криптостойкости шифра Виженера:**

1. Известно, что в качестве ключа для шифрования часто использовались короткие и осмысленные фразы. Как следует из проведенных в ходе лабораторной работе опытов и теоретической оценки времени дешифрования методом полного перебора, короткие кодовые фразы являются неэффективными. Осмысленность же может упростить ручной перебор на основе некоторых предположений, сделанных на основании знаний о получателе/отправителе сообщений.
2. Использование нестандартной таблицы для шифрования. Стандартный вариант таблицы – множество алфавитов, формирующих шифры цезаря, которые более подвержены дешифрованию. Использование произвольного порядка символов усложнит дешифрование.