

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ
ПРЕПОДАВАТЕЛЬ

ассистент

должность, уч. степень, звание

подпись, дата

М.Н. Исаева

инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

ИСТОРИЧЕСКИЕ ШИФРЫ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ
ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. №

5911

подпись, дата

А.А. Бенцлер

инициалы, фамилия

Санкт-Петербург 2021

Цель работы

Реализовать алгоритм шифрования при помощи решётки Кардано. Провести анализ с помощью полного перебора. Реализация каждой системы должна работать в двух режимах: шифрования и дешифрования, позволять вводить ключ вручную и генерировать его автоматически.

1. Алгоритм

Выбирается число k . Строим квадрат со стороной длины k и заполняем его клетки числами от 1 до k^2 :

| | |
|---|---|
| 1 | 2 |
| 3 | 4 |

Рисунок 1 «шаг 1»

Поворачиваем квадрат на 90 градус по часовой стрелке и приписываем справа от исходного квадрата

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 1 |
| 3 | 4 | 4 | 2 |

Рисунок 2 «шаг 2»

Поворачивая на 90 градусов по часовой стрелки и добавляя полученный квадрат сначала снизу, а затем слева от предыдущего, получим следующий квадрат со стороной $2k$:

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 1 |
| 3 | 4 | 4 | 2 |
| 2 | 4 | 4 | 3 |
| 1 | 3 | 2 | 1 |

Рисунок 3 «шаг 3»

В этом квадрате закрасим произвольным образом все цифры, причем каждая цифра может быть закрашена только один раз.

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 1 |
| 3 | 4 | 4 | 2 |
| 2 | 4 | 4 | 3 |
| 1 | 3 | 2 | 1 |

Рисунок 4 «шаг 4»

Мы получили решетку для шифрования. Код для шифрования представляет последовательность k цифр от 1 до 4, i -тая цифра обозначает в каком подквадрате (нумеруются в порядке создания) закрашивать число i (например, для этой таблицы код решетки имеет вид: 1224). Асимптотическая сложность шифра - 4^k . Решетка накладывается на пустой лист бумаги, закрашиваемые клетки вырезаются. Для первой подстроки ее i -ый символ записывается в вырезанное i -ое число решетки. Повторяем процесс еще 3 раза, поворачивая перед этим решетку на 90 градусов по часовой стрелке. В результате получаем таблицу, составляющую из символов открытого текста. Криптограмма из этой таблицы получается путем построчного выписывания символов.

Пример:

Воспользуемся приведённым выше квадратом для шифрования слова «ВОЗДУХОПЛАВАТЕЛЬ». Шаги заполнения матрицы:

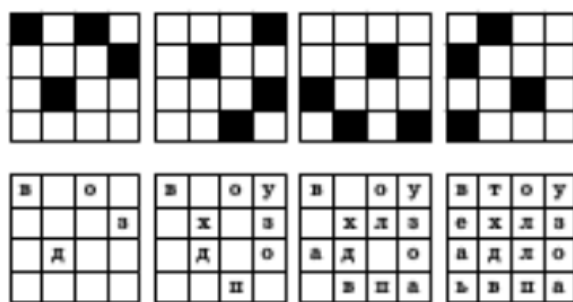


Рисунок 5 «шаги заполнения матрицы»

Выписав строки получившейся заполненной матрицы, получим шифртекст :

ВТОУЕХЛЗАДЛОБВПА

При заявленных ограничениях (каждая ячейка матрицы должна при четырёхкратном наложении маски-квадрата использоваться ровно один раз) размерность матрицы m должна быть

кратна 4. Кроме того, количество прорезанных ячеек в маске должно составлять четверть от общего количества ячеек, т.е. $m^2/4$.

Если уменьшить количество вырезанных ячеек, каждая ячейка матрицы будет использоваться не ровно один раз, а не более одного раза, т.е. появится некоторое количество неиспользуемых ячеек. Заполняя эти ячейки случайными символами, можно таким образом внести некоторый избыточный «шум» в сообщение, несколько затруднив статистический анализ шифртекста.

2. Криптографический анализ

В ходе работы был программно проведен анализ стойкости алгоритма с помощью полного перебора.

k – количество символов, составляющих ключ.

При $k = 4$, полным перебором был найден ключ и расшифровано сообщение за 0 секунд.

При $k = 16$, скорость нахождения ключа зависит от позиций соответствующих цифр.

Таким образом, если ключ = 1111111112314, время подбора составляет ~ 14 секунд.

Если ключ = 4213241324133213, время подбора >30 минут.

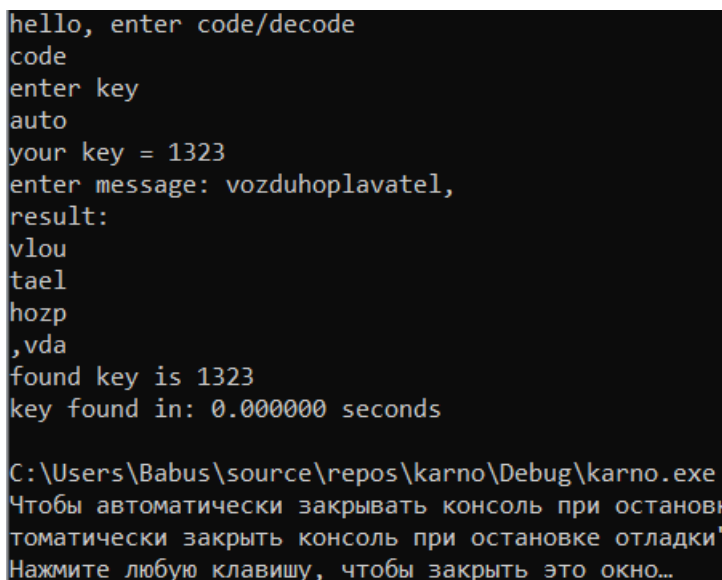
3. Описание программы

Программа состоит из класса Kardano:

- void result() – результат зашифрованного сообщения
- void initial_lattice(string key) - инициализация решетки кодирования
- void code() – метод кодирования
- void decode() – метод декодирования
- void BruteForce(int n, int k, int t) – рекурсивная функция анализа полным перебором

Существует возможность как кодирования сообщения с помощью заданного ключа, так и с помощью случайно сгенерированного ключа.

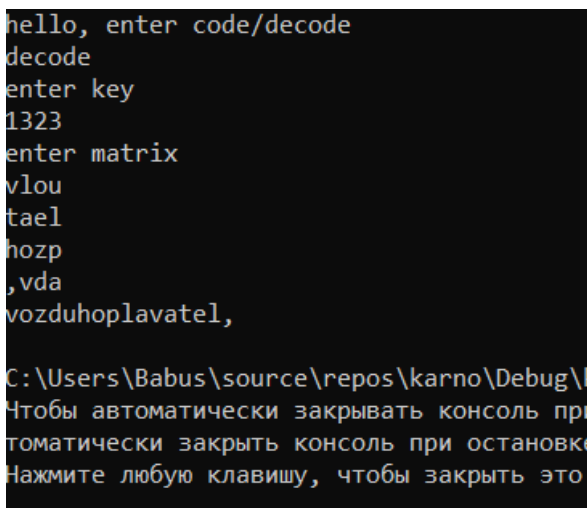
4. Пример работы программы:



```
hello, enter code/decode
code
enter key
auto
your key = 1323
enter message: vozduhoplavatel,
result:
vlou
tael
hozp
,vda
found key is 1323
key found in: 0.000000 seconds

C:\Users\Babus\source\repos\karno\Debug\karno.exe
Чтобы автоматически закрывать консоль при остановке отладки,
нажмите любую клавишу, чтобы закрыть это окно...
```

Рисунок 6 «результат работы программы кодирования»



```
hello, enter code/decode
decode
enter key
1323
enter matrix
vlou
tael
hozp
,vda
vozduhoplavatel,
```

Рисунок 7 «результат работы программы декодирования»

5. Вывод

В ходе данной лабораторной работы был программно воспроизведен шифр с помощью решетки Кардано, а так же проведен анализ с помощью полного перебора. Можно сделать следующие выводы о проделанной работе:

Шифр Кардано не требует ничего, кроме времени. Но при этом он невероятно сложен для дешифровки. Не зная как выглядела решетка, практически невозможно восстановить исходный текст. Количество вариантов растет вместе с размерностью квадрата. Единственный шанс для дешифровки, если известно часть послания или слова, что используются там, но даже в этом случае на дешифровку придётся потратить много времени. Следует отметить, что чем больше послание, тем надежнее оно зашифровано.

6. Список источников

1. [А.А. Овчинников “Исторические шифры”](#)
2. [А.Л. Чмора "Современная прикладная криптография"](#)
3. [Черчхаус. Коды и шифры](#)