Автор:

Завгородний Станислав Дмитриевич

студент

ФГАОУ ВО «Самарский национальный исследовательский

университет им. академика С.П. Королева»

г. Самара, Самарская область

РЕШЕТКА КАРДАНО

Аннотация: *в статье рассматриваются общие принципы шифрования и дешифрования с помощью решетки Кардано. В основе работы лежат понятия о шифровании и дешифровании, а также реализуется программа генерация квадратной решетки Кардано.*

Ключевые слова: *шифрование, дешифрование.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. Шифрование – обратимое преобразование информации в целях сокрытия информации от посторонних лиц, а также предоставлении информации лицам, имеющим к ней доступ. Главной задачей шифрования информации является соблюдение конфиденциальности, целостности и идентифицируемости передаваемой информации.

Определение 2. Дешифрование – процесс получения открытых данных по зашифрованным, в тех случаях, когда алгоритм расшифрования и его параметры не известны и расшифрование не может быть осуществлено обычным путем. Одной из главных задач криптографии является дешифрование текстов.

Введение

Джероламо Кардано в 1550 году предложил метод шифрования сообщений на основе простой решетки. Планировалось маскировать сообщения под видом обычного послания, чтобы они были не похожи на шифрованные. Зашифрованное таким способом сообщение считается примером стеганографии. Одной из

самых популярных разновидностей решетки Кардано является вращающаяся сетка, в основе которой лежит шахматная доска.

Шифрование с добавлением «мусора»

Для шифрования таким образом используется квадратная решетка размерностью N x N, в которой вырезаны только некоторые клетки, в которые в последствии будут помещены буквы, при этом не должно произойти такой ситуации, при которой две разные клетки при повороте решетки совпали. Шифрование осуществляется следующим образом: на листок бумаги устанавливается решетка, через ее пустые клетки записывается текст сообщения слева направо и сверху вниз, затем решетка 3 раза поворачивается на 90 градусов, и после каждого поворота заноситься текст сообщения. В конце алгоритма во все пустые клетки записываются случайные буквы или цифры, ненесущие полезной информации.

Шифрование без добавления «мусора»

Этот алгоритм отличается от предыдущего тем, что при его использовании вырезаются клетки так, что при ее поворотах в каждое место на бумаге можно было бы записать по одной букве. Такая решетка должна быть с четным количеством клеток в строке или столбце. С увеличение размера решетки, увеличивается количество генерируемых решеток. Их количество определяется следующим образом: C = 4^(N^2/4), где N количество клеток в стороне решетки.

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

Рис. 1. Конструктор квадратных решеток Кардано размерностью 8 * 8

*Реализация генератора решеток Кардано размерностью 8 * 8*

Программа генерирования решеток Кардано была реализована языке программирования C++ в среде разработок C++ Builder. Код генерации решетки Кардано:

```
{   for (int i = 1; i < 9; i++) {
for (int j = 1; j < 9; j++) {
Kardano[i][j]=0;}}
Memo1->Text="";
randomize();
for (int i = 1; i < 5; i++) {
for (int j = 1; j < 5; j++)
{int c = (rand()) % 4 +1;
if (c==1) {Kardano[i][j]=1;}
if (c==2) {Kardano[j][9-i]=1;}
if (c==3) {Kardano[9-i][9-j]=1;}
if (c==4) {Kardano[9-j][i]=1;}}}
for (int i = 1; i < 9; i++) {
for (int j = 1; j < 9; j++)
{ if (Kardano[i][j]==0) Memo1->Text=(Memo1->Text)+0;
if (Kardano[i][j]==1) Memo1->Text=(Memo1->Text)+1;}
Memo1->Lines->Text=(Memo1->Lines->Text)+'\n';}}
```

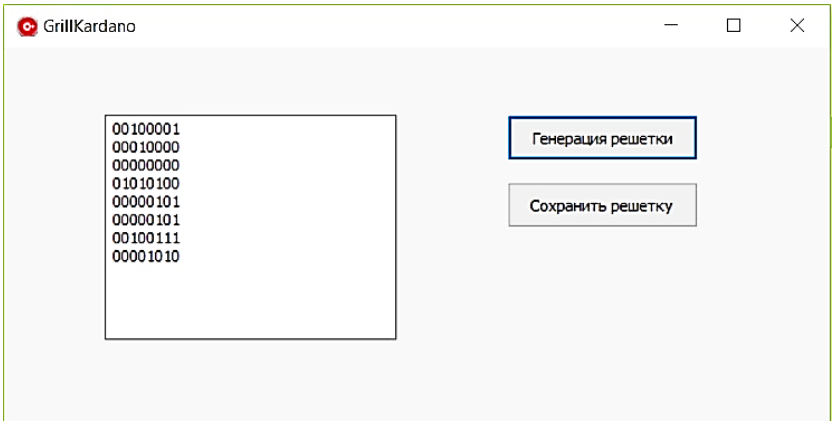

Рис. 2. Пример реализованного генератора решеток Кардано

Список литературы

1. Саломаа А. Криптография с открытым ключом / Пер. с англ. – М.: Мир, 1995.

2. Алферов А.П. Основы криптографии: Учеб. пособ. / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин [и др.]. – 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002.