

Математические основы защиты информации и информационной безопасности. Лабораторная работа №2. Шифры перестановки

Лесков Данила Валерьевич, учебная группа: НФИМд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич

14 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Ознакомиться с шифрами перестановки на примере маршрутного шифрования, шифрования с помощью решеток и таблицы Виженера.

Задачи лабораторной работы

1. Реализовать маршрутное шифрование;
2. Реализовать шифрование с помощью решеток;
3. Реализовать шифрование с помощью таблицы Виженера.

Выполнение лабораторной работы

Шифр перестановки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее.

При шифровании в такую таблицу вписывают исходное сообщение по определенному маршруту, а выписывают (получают шифrogramму) – по другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом. В рамках работы данного алгоритма шифрования задаются две переменные: m - количество столбцов таблицы, которое равно длине ключа и n - количество строк в таблице.

Для случая, когда в сообщении недостаточно букв для того, чтобы заполнить всю таблицу, предусмотрено добавление случайных букв в конец сообщения.

Маршрутное шифрование

<i>н</i>	<i>е</i>	<i>л</i>	<i>ь</i>	<i>з</i>	<i>я</i>
<i>н</i>	<i>е</i>	<i>д</i>	<i>о</i>	<i>о</i>	<i>ц</i>
<i>е</i>	<i>н</i>	<i>и</i>	<i>в</i>	<i>а</i>	<i>т</i>
<i>ь</i>	<i>п</i>	<i>р</i>	<i>о</i>	<i>т</i>	<i>и</i>
<i>в</i>	<i>н</i>	<i>и</i>	<i>к</i>	<i>а</i>	<i>а</i>
<hr/>					
<i>п</i>	<i>а</i>	<i>р</i>	<i>о</i>	<i>л</i>	<i>ь</i>

Figure 1: Маршрутное шифрование

В результате обработки алгоритма возвращаются отсортированные столбцы таблицы по алфавитному порядку букв ключа. На рис. 1 ключом является пароль, соответственно в результирующее сообщение сначала записывается столбец под буквой а ключа, и заканчивается столбцом под ь.

Поворотная решетка — это прямоугольная или квадратная карточка с четным числом строк и столбцов $2k \times 2k$. В ней проделаны отверстия таким образом, что при последовательном отражении или поворачивании и заполнении открытых клеток карточки постепенно будут заполнены все клетки листа.

Карточку сначала отражают относительно вертикальной оси симметрии, затем - относительно горизонтальной оси, и снова - относительно вертикальной. На рис. 2 изображена последовательность поворота решетки для заполнения её буквами сообщения:

Шифрование с помощью решеток

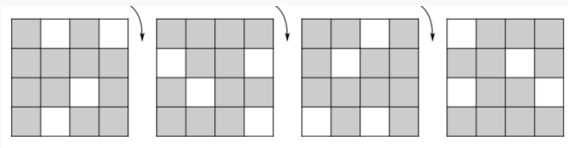


Figure 2: Шифрование с помощью решеток

По итогу, когда таблица заполнена, как и в предыдущем алгоритме столбцы решетки сортируются по алфавитному порядку букв ключа.

Таблица Виженера

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая *tabula recta* или таблица Виженера.

Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Например, предположим, что исходный текст имеет такой вид:

ATTACK AT DAWN

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE

Если n — количество букв в алфавите, m_j — номер буквы открытого текста, k_j — номер буквы ключа в алфавите, то шифрование Виженера можно записать следующим образом:

$$c_j = (m_j + k_j) \mod n$$

Пример таблицы виженера для латинского алфавита изображен на рис. 3:

Таблица Виженера

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Figure 3: Таблица Виженера

По итогу, когда таблица заполнена, как и в предыдущем алгоритме столбцы решетки сортируются по алфавитному порядку букв ключа.

Полученные результаты

Результаты маршрутного шифрования

```
Введите сообщение: это сообщение необходимо зашифровать  
Введите пароль: безопасность  
Зашифрованное сообщение:  
оовэнштейноофщителъмохоноыизмеав
```

Figure 4: Результаты маршрутного шифрования

Результаты шифрования с помощью решеток

```
Введите сообщение: информация. Безопасность
Сообщение с учетом добавления произвольных символов:
информационнаябезопасностьытктлхбь
Исходная матрица:
[1, 2, 3]
[4, 5, 6]
[7, 8, 9]
Образованная большая таблица k*2:
[1, 2, 3, 7, 4, 1]
[4, 5, 6, 8, 5, 2]
[7, 8, 9, 9, 6, 3]
[3, 6, 9, 9, 8, 7]
[2, 5, 8, 6, 5, 4]
[1, 4, 7, 3, 2, 1]
Зашифрованное сообщение в списковом представлении:
['o', 'k', 't', 'a', 'n', 'i']
['a', 'p', 'c', 'b', 'y', 'n']
['x', 'c', 'y', 'o', 'e', 'f']
['s', 'm', 't', 'i', 'z', 't']
['a', 'o', 'y', 'b', 'l', 'k']
['n', 'o', 'e', 'n', 'n', 'y']

Введите ключ (длина ключа = 6): ключик
Зашифрованное сообщение в виде словаря до сортировки:
{'t': ['o', 'k', 't', 'a', 'n', 'i'], 'e': ['a', 'p', 'c', 'b', 'y', 'n'], 'r': ['x', 'c']}
Зашифрованное сообщение в виде словаря после сортировки:
OrderedDict([('e', ['a', 'p', 'c', 'b', 'y', 'n']), ('m', ['s', 'm', 't', 'i', 'z', 't'])])

Зашифрованное сообщение:
арсбясмтизтаьблхцьефлюенныоктани
```

Figure 5: Результаты шифрования с помощью решеток

Результаты шифрования с помощью таблицы Виженера

Введите сообщение: **шифрование это безопасно**

Форматированное сообщение:

шифрование это безопасно

Введите пароль (не превышающий длину сообщения): **корм**

Дополненный ключ до длины сообщения:

кормкормкормкормкормко

Таблица:

абвгдежзийклмнопрстуфхцчшщъыьэюя

б в г д 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 а

вгдежзийклмнопрстуфхцчшщъыьэюяаб

эюяабвгдежзийклмнопрстуфхцчшщъыь

юяабвгдежзийклмнопрстуфхцчшщъыьэ

яабвгдежзийклмнопрстуфхцчшщъыьэю

Зашифрованное сообщение:

вцдъшррщтунюшпхушэрэчь

Figure 6: Результаты шифрования с помощью таблица Виженера

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения данной лабораторной работы было выполнено ознакомление с шифрами перестановки на примере маршрутного шифрования, шифрования с помощью решетов и таблицы Виженера.

В результате проделанной работы были программно реализованы эти методы шифрования.

Как итог, поставленные цели и задачи были успешно достигнуты.