Отчёт по лабораторной работе №2

Дисциплина: Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна, НПМмд-02-23

Содержание

# 1 Цель работы

Изучить шифры перестановки.

# 2 Задание

1. Реализовать маршрутное шифрование.
2. Реализовать шифрование с помощью решёток.
3. Реализовать шифрование таблицей Виженера.

# 3 Теоретическое введение

Шифры перестановки преобразуют открытый текст в криптограмму путем перестановки его символов. Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра. Важным требованием является равенство длин ключа и исходного текста.

Существует два широко распространенных метода перестановок:

1. **Маршрутное шифрование.**

Данный способ шифрования разработал французский математик Франсуа Виет. Открытый текст записывают в некоторую геометрическую фигуру (обычно прямоугольник) по некоторому пути, а затем, выписывая символы по другому пути, получают шифртекст. Пусть и - целые положительные числа, большие 1. Открытый текст разбивается на блоки равной длины, состоящие из числа символов, равному произведению . Если последний блок получится меньше остальных, то в него следует дописать требуемое количество произвольных символов. Составляется таблица размерности . Блоки вписывается построчно в таблицу. Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Ключом такой криптограммы является маршрут и числа и . Обычно буквы выписывают по столбцам, которые упорядочивают согласно паролю: внизу таблицы приписывается слово из неповторяющихся букв и столбцы нумеруются по алфавитному порядку букв пароля.

1. **Шифрование с помощью решеток.**

Данный способ шифрования предложил австрийский криптограф Эдуард Флейснер в 1881 году. Суть этого способа заключается в следующем. Выбирается натуральное число , строится квадрат размерности и построчно заполняется числами . Повернем его по часовой стрелке на 90° и присоединим к исходному квадрату справа. Проделаем еще дважды такую процедуру и припишем получившиеся квадраты снизу. Получился большой квадрат размерности .

Далее из большого квадрата вырезаются клетки, содержащие числа от 1 до . В каждой клетке должно быть только одно число. Получается своего рода решето. Шифрование осуществляется следующим образом. Решето накладывается на чистый квадрат 2k × 2k и в прорези вписываются буквы исходного текста по порядку их следования. Когда заполнятся все прорези, решето поворачивается на 90° и вписывание букв продолжается. После третьего поворота все клетки большого квадрата окажутся заполненными. Подобрав подходящий пароль (число букв пароля должно равняться и они не должны повторяться), выпишем буквы по столбцам. Очередность столбцов определяется алфавитным порядком букв пароля.

Важно отметить, что число к подбирается в соответствии с количеством букв исходного теста. В идеальном случае . Если такого равенства достичь невозможно, то можно либо дописать произвольную букву к последнему слову открытого текста, либо убрать ее.

1. **Таблица Виженера.**

В 1585 году французский криптограф Блез Виженер опубликовал свой метод шифрования в «Трактате о шифрах». Шифр считался нераскрываемым до 1863 года, когда австриец Фридрих Казиски взломал его.

Открытый текст разбивается на блоки длины . Ключ представляет собой последовательность из натуральных чисел: . Далее в каждом блоке первая буква циклически сдвигается вправо по алфавиту на позиций, вторая буква - на позиций, последняя - на позиций. Для лучшего запоминания в качестве ключа можно взять осмысленное слово, а алфавитные номера входящих в него букв использовать для осуществления сдвигов.

Более подробно см. в [1–6].

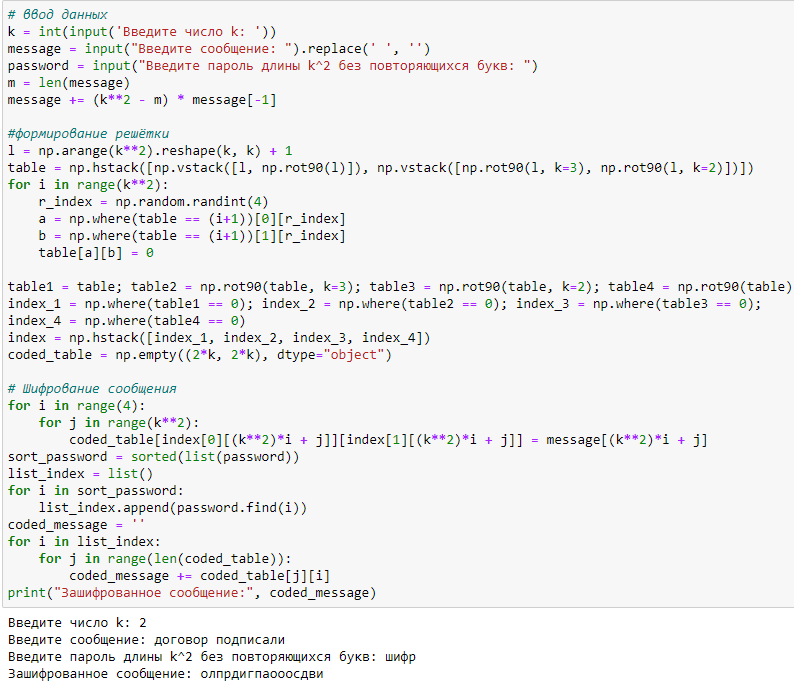
# 4 Выполнение лабораторной работы

1. Реализуем маршрутное шифрование (рис. ??).



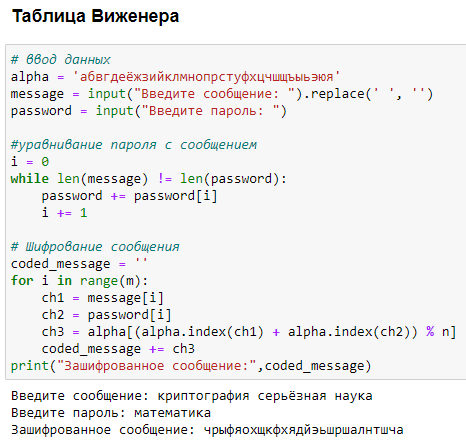
Код. Маршрутное шифрование

1. Реализуем шифрование с помощью решёток (рис. ??).



Код. Шифрование с помощью решёток

1. Реализуем шифрование таблицей Виженера (рис. ??).



Код. Шифрование таблицей Виженера

# 5 Выводы

Изучила шифры перестановки на примере маршрутного шифрования, шифрования с помощью решёток и шифрования таблицей Виженера.

# Список литературы

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016. URL: <https://www.gnu.org/software/bash/manual/>.

2. Newham C. [Learning the bash Shell: Unix Shell Programming](http://www.amazon.com/Learning-bash-Shell-Programming-Nutshell/dp/0596009658). O’Reilly Media, 2005. 354 с.

3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.

4. Robbins A. [Bash Pocket Reference](https://www.ncbi.nlm.nih.gov/pubmed/25246403). O’Reilly Media, 2016. 156 с.

5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.

6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.