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		М.Н. Исаева
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ

ИСТОРИЧЕСКИЕ ШИФРЫ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. 5912		С.В.Льдокова
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2021

1. Цель

Вариант 16. Реализовать алгоритм книжного шифрования. Провести его частотный анализ. Реализация системы должна работать в двух режимах: шифрования и дешифрования, позволять вводить ключ вручную и генерировать его автоматически.

2. Описание алгоритма

Книжный шифр

Ключом шифрования при использовании книжного шифра является страница текста (например, из книги), содержащая все символы алфавита. Для шифрования каждого символа открытого текста находится соответствующий символ на странице (произвольный, если таких символов на странице несколько), и в качестве шифртекста выписываются номер строки найденного символа и его порядковый номер в данной строке.

3. Описание реализации

На входе программа получает ключ шифрования, хранящийся в файле, и начинает считывать его построчно. Составляются списки, которые содержат в себе информацию о положении каждой буквы алфавита (номер строки и номер символа в данной строке). То есть для каждого символа существует свой список позиций. Затем программа шифрует/дешифрует его, в зависимости от того, в каком режиме она работает на данный момент. После этого, программа выводит шифрованный/дешифрованный текст.

В режиме шифрования программа вычисляет в какой ячейке листа лежит нужный символ и из общего количества подлистиков вытаскивает рандомную пару, хранящую номер строки и номер позиции искомого символа.

В режиме дешифрования при считывании файла создается лист из строк. Чтобы расшифровать символ достаточно обратиться по номеру строки и извлечь порядковый номер символа.

4. Примеры

Ключ шифрования представлен стихотворением, находящимся в файле text.txt. Зашифруем строку «Two wrongs don not make a right», используя данный ключ.

Вывод программы: 15.15 21.17 3.4 11.14 7.15 16.5 4.11 4.8 16.21 8.11 11.25 23.24 8.24 14.10 15.18 22.23 18.7 11.12 9.20 11.5 1.5 9.28 8.3 18.3 4.14 9.5 18.11 4.2 19.22 12.8 6.10

Частотный анализ (рис. 1):

```
" " – 6
"T" – 1
"a" – 2
"d" – 1
"e" – 1
"g" – 2
"h" – 1
"i" – 1
"k" – 1
"m" – 1
"n" – 3
"o" – 4
"r" – 2
"s" – 1
"t" – 2
"w" – 2
```

Рисунок 1 - Частота встречаемости символов в строке

Расшифруем полученный шифртекст по ключу text.txt.

Вывод программы: Two wrongs don not make a right

Таким образом, программа выдала ожидаемые результаты, следовательно, сработала корректно.

5. Вывод

Заметным преимуществом книжного шифра является отсутствие проблем, связанных с подготовкой и передачей секретного ключа, ведь кодовый текст сразу существует в нескольких экземплярах. Однако этот шифр, так же, как и другие подвержен всем обычным средствам криптоанализа. И эти средства позволяют криптоаналитику угадать кодовые слова, а иногда и полностью взломать код, путём выявления ключевого текста.

Уильям Фридман и его жена Элизабет Фридман смогли взломать книжный шифр и без книги, так как корреспонденты иногда использовали для одной буквы одно и то же обозначение страниц и строк несколько раз. Фридманам удалось прочесть переписку индийских националистов, славших разведывательные данные, используя книжный шифр на базе старого немецко-английского словаря. К моменту суда им удалось достать и окончательное доказательство — сам словарь.

Если использовать шифр более осторожно, то надежность его заметно увеличится, так как он

будет действовать как гомофонный шифр с чрезвычайно большим количеством эквивалентов. Однако это будет организовано за счет очень большого расширения зашифрованного текста.

6. Список литературы

[1] А. А. Овчинников, Основы информационной безопасности. Исторические шифры, Санкт-Петербург : Редакционно-издательский центр ГУАП, 2018.

[2] Р. Чёрчхаус, Коды и шифры. Юлий Цезарь, "Энигма" и Интернет, Весь мир, 2005.