Отчёт по лабораторной работе №2. Шифры перестановки

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Майорова О.А., 1032212322
Группа: НФИмд-02-21
Преподаватель: д.ф.-м.н., Кулябов Д. С.

Москва, 2021

Цель и задачи

Цель: Ознакомиться с шифрами перестановки на примере маршрутного шифрования, шифрования с помощью решёток и шифра Виженера.

Задачи:

- Рассмотреть и реализовать маршрутное шифрование.
- Рассмотреть и реализовать шифрование с помощью решёток.
- Рассмотреть и реализовать шифр Виженера.

Теоретическое введение

Шифр перестановки - элементы исходного открытого текста меняют местами по определённому правилу.

Маршрутное шифрование - открытый текст записывается в геом. фигуру по некот. траектории, и выписывается по другой.

Шифрование с помощью решёток - используется трафарет с прорезями-ячейками с определённой посл-тью его перемещений.

Шифр Виженера - последовательность нескольких шифров Цезаря с различными значениями сдвига.

Маршрутное шифрование

Пример: исходный

текст - “нельзя недооценивать пртивника”; пароль - “пароль”;

н	*е*	*л*	*ь*	*з*	*я*
н	*е*	*д*	*о*	*о*	*ц*
е	*н*	*и*	*в*	*а*	*т*
ь	*п*	*р*	*о*	*т*	*и*
в	*н*	*и*	*к*	*а*	*а*
п	*а*	*р*	*о*	*л*	*ь*

Результат работы функции:

```
1 route('нельзя недооценивать противника', 'пароль')
```

```
'еенпнзоатаьовокннеьвлдирияцтир'
```

Шифрование с помощью решёток

Пример: исходный текст - “договор подписали”; пароль - “шифр”;

Результат работы функции:

```
1 grid('договор подписали', 'шифр')
```

```
'сдроволиоагпдопи'
```

Каждый новый запуск функции будет генерировать новый шифротекст, так как задание “отверстий” в трафарете осуществляется на основе случайности.

```
1 grid('договор подписали', 'шифр')
```

```
'опргдлипдаоосвои'
```

Шифр Виженера

Пример: исходный текст - “криптография серьезная наука”;

пароль - “математика”;

м	а	т	е	м	а	т	и	к	а	м	а	т	е	м	а	т	и	к	а	м	а	т	е	м	а
к	р	и	п	т	о	г	р	а	ф	и	я	с	е	р	ь	е	з	н	а	я	н	а	у	к	а

Результат работы функции:

```
1 Vigenere('криптография серьезная наука', 'математика')
```

```
'цръфюохшкффявкььчпчакнтшца'
```

Заключение

Таким образом, была достигнута цель, поставленная в начале лабораторной работы.

- Было осуществлено знакомство с шифрами перестановки;
- Была получена реализация шифрования с помощью решёток для заданного пароля;
- Были получены реализации маршрутного шифрования и шифра Виженера для русского алфавита нижнего регистра.

Спасибо за внимание