**Лабораторная работа №2**

КЛАССИЧЕСКИЕ ШИФРЫ ПЕРЕСТАНОВКИ

Цель работы: изучение классических криптографических шифров перестановки и криптоанализа классических шифров перестановки на основе атак зашифрованного текста.

Краткие теоретические сведения

Шифры перестановки

Шифры перестановки основываются на изменении месторасположения символов в исходном тексте. Данные шифры не изменяют частоту букв, а это значит, что они уязвимы к частотному анализу отдельного символа.

*Шифры перестановки без использования ключа*

Простые шифры перестановки не используют ключа. Применяется два подхода для реализации безключевого шифра перестановки.

Первый подход состоит в том, что текст записывается в таблицу столбец за столбцом, а передается по строкам. Второй способ – тест записывается в таблицу построчно, а передача производиться по столбцам.

Криптоанализ шифров перестановки без ключа

Если криптоаналитику известен способ передачи и количество строк или столбцов в таблице перестановки, то можно легко расшифровать сообщение.

*Ключевые шифры перестановки*

Исходный текст делиться на группы определенного размера. Перестановка символов в каждой группе осуществляется по ключу.



Зашифрованное сообщение: а лхегкеар рзееч кеур .

Дешифрация сообщения производится использованием ключа в обратном порядке.

*Комбинированные шифры перестановки*

Комбинированные шифры перестановки включают в себя объединения двух выше рассмотренных методов. Такое сочетание позволяет достигнуть большего скремблирования (перемешивания символов).

Процесс шифрования и дешифрования состоит из следующих шагов:

1) текст пишется строка за строкой

2) делается перестановка, изменяющая порядок следования столбцов;

3) столбец за столбцом передается новая таблица.

Процесс дешифрования проходит в обратном порядке.

*Шифры с двойной перестановкой*

В шифровании дважды реализуется алгоритм перестановки. Позволяет уменьшить возможную регулярность повторения символов и заметно усложнить применение статистических методов для криптоанализа.

**Задание**

1. Записать контрольный пример (минимум 20 символов)

2. Создать программу, реализующую процесс шифрования/дешифрования текста по изученным шифрам перестановки. Разрабатываемая подпрограмма использует только алфавит:

а бв г д е ё ж з и й к л м н оп р с т у ф хц ч ш щ ъ ьы э ю я \_ , .

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц ЧШ Щ Э Ю Я

При использовании шифра перестановки с ключом длина ключа и сам ключ должны задаваться пользователем.

Длина исходного текста должна быть не менее 1000 символов.

Подсчет количества символов должен быть осуществлен программой и выведен на экран.

3. Оформить отчет

|  |  |
| --- | --- |
| Вариант | Шифр |
| 1, 4, 7, 10, 13, 16, 19, 22, 25, 28 | Перестановка запись по столбцам |
| 2, 5, 8, 11, 14, 17, 20, 23, 26, 29 | Перестановка запись по строкам |
| 3, 6, 9, 12, 15, 18, 21, 24, 27, 30 | Ключевая перестановка |