

Шифры перестановки: Маршрутная перестановка, Решётка Кардано, Шифр Виженера

Хамза Хуссен

Лабораторная работа №2

Ц е л ь р а б о т ы

Изучение трёх базовых технологий шифрования:

Маршрутная перестановка символов.

Решётка Кардано.

Шифр Виженера (полиалфавитный метод).

Шифр маршрутной перестановки

Основан на геометрических фигурах (таблицах).

Текст записывается по одному маршруту, считывается по другому.

Пример: заполнение таблицы по горизонтали, чтение по вертикали.

Реализация маршрутной перестановки (Python)

Ввод текста, параметров таблицы (n , m) и пароля.

Заполнение таблицы символами текста.

Использование пароля для перестановки столбцов.

Пример вывода: "ВНаарааанаамТаасВааеаеа"

Шифр Кардано (решётка)

Инструмент для кодирования/декодирования с помощью карточки с прорезями.

Таблица поворачивается 4 раза для полного заполнения.

Предложен Джероламо Кардано (1550 год).

Слайд 6: Реализация решётки Кардано (Python)

Генерация вращающейся матрицы размером $k \times k$.

Заполнение прорезей символами сообщения.

Использование пароля для шифрования.

Пример вывода: "ооооддвоcпги"

Шифр Кардано (решётка)

Инструмент для кодирования/декодирования с помощью карточки с прорезями.

Таблица поворачивается 4 раза для полного заполнения.

Предложен Джероламо Кардано (1550 год).

Слайд 6: Реализация решётки Кардано (Python)

Генерация вращающейся матрицы размером $k \times k$.

Заполнение прорезей символами сообщения.

Использование пароля для шифрования.

Пример вывода: "ооооддвоcпги"

Реализация решётки Кардано (Python)

Генерация вращающейся матрицы размером $k \times k$.

Заполнение прорезей символами сообщения.

Использование пароля для шифрования.

Пример вывода: "ооооддвооспги"

Ш и ф р В и ж е н е р а

Полиалфавитный шифр с использованием ключевого слова.

Использует таблицу Tabula Recta (26 алфавитов).

Устойчив к частотному анализу.

Описан Джован Баттиста Беллазо (1553), известен по имени Блеза Виженера.

Выводы работы

Шифры перестановки — классические методы изменения порядка символов.

Маршрутная перестановка демонстрирует использование таблиц.

Решётка Кардано — метод многоэтапного вращающегося шифрования.

Шифр Виженера — переход к полиалфавитным системам, повышающий стойкость.

Вопросы и заключение

Криптографические методы остаются актуальными для изучения основ защиты информации.

Реализация на Python позволяет наглядно понять алгоритмы.

Спасибо за внимание!