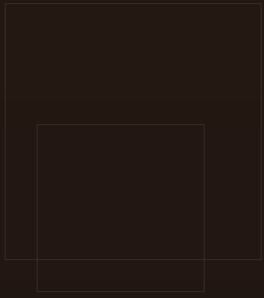


Шифры перестановки: Маршрутная перестановка, Решётка Кардано, Шифр Виженера

Хамза Хуссен

Лабораторная работа №2



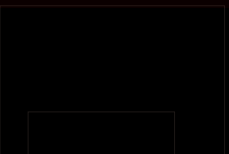
Ц е л ь р а б о т ы

Изучение трёх базовых технологий шифрования:

Маршрутная перестановка символов.

Решётка Кардано.

Шифр Виженера (полиалфавитный метод).



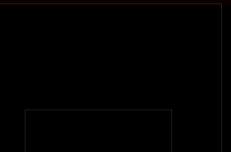


Ш и ф р м а р ш р у т н о й п е р е с т а н о в к и

Основан на геометрических фигурах (таблицах).

Текст записывается по одному маршруту, считывается по другому.

Пример: заполнение таблицы по горизонтали, чтение по вертикали.



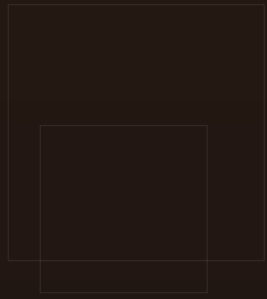
Реализация маршрутной перестановки (Python)

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

Заполнение таблицы символами текста.

Использование пароля для перестановки столбцов.

Пример вывода: "ВНаарааанаатТаасВааеаеа"



Ш и ф р К а р д а н о (р е ш ё т к а)

Инструмент для кодирования/декодирования с помощью карточки с прорезями.

Таблица поворачивается 4 раза для полного заполнения.

Предложен Джероламо Кардано (1550 год).

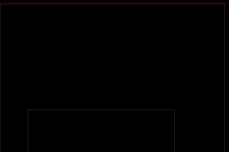
Слайд 6: Реализация решётки Кардано (Python)

Генерация вращающейся матрицы размером $k \times k$.

Заполнение прорезей символами сообщения.

Использование пароля для шифрования.

Пример вывода: "oooоддвоспги"





Ш и ф р К а р д а н о (р е ш ё т к а)

Инструмент для кодирования/декодирования с помощью карточки с прорезями.

Таблица поворачивается 4 раза для полного заполнения.

Предложен Джероламо Кардано (1550 год).

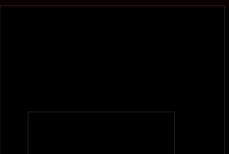
Слайд 6: Реализация решётки Кардано (Python)

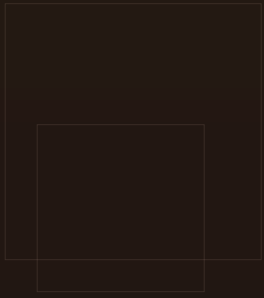
Генерация вращающейся матрицы размером $k \times k$.

Заполнение прорезей символами сообщения.

Использование пароля для шифрования.

Пример вывода: "oooоддвоспги"





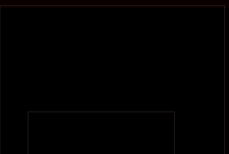
Реализация решётки Кардано (Python)

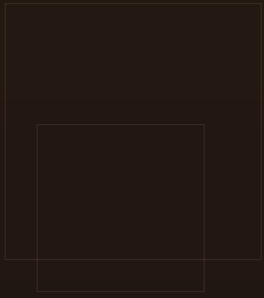
Генерация вращающейся матрицы размером $k \times k$.

Заполнение прорезей символами сообщения.

Использование пароля для шифрования.

Пример вывода: "oooоддвоспги"





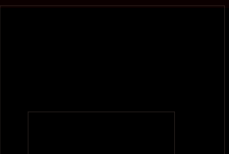
Ш и ф р В и ж е н е р а

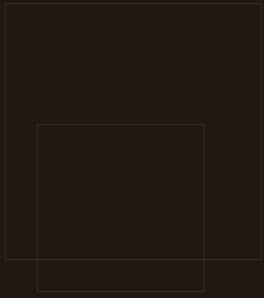
Полиалфавитный шифр с использованием ключевого слова.

Использует таблицу Tabula Recta (26 алфавитов).

Устойчив к частотному анализу.

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





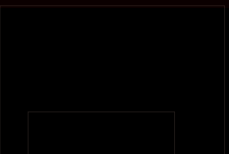
В ы в о д ы р а б о т ы

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!

