

## Лабораторная работа №2

Математические основы защиты информации и информационной безопасности

---

Мануэл Марсия Педру

2026

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

## Докладчик

---

- Мануэл Марсия Педру
- Студент группы НФИмд-02-25
- Студ. билет 1032255503
- Российский университет дружбы народов имени Патриса Лумумбы



## Цель работы

---

## Цель работы

---

Изучить шифры простой замены и научиться их реализовывать.

## Выполнение лабораторной работы

---

## Выполнение лабораторной работы

---

Реализация маршрутного шифрования  
Данный способ шифрования разработал  
французский математик Франсуа Виет.  
Открытый текст записывают в некоторую  
геометрическую фигуру (обычно прямоугольник)  
по некоторому пути, а затем, выписывая  
символы по другому пути, получают шифртекст.

## Реализация шифрования с помощью решеток

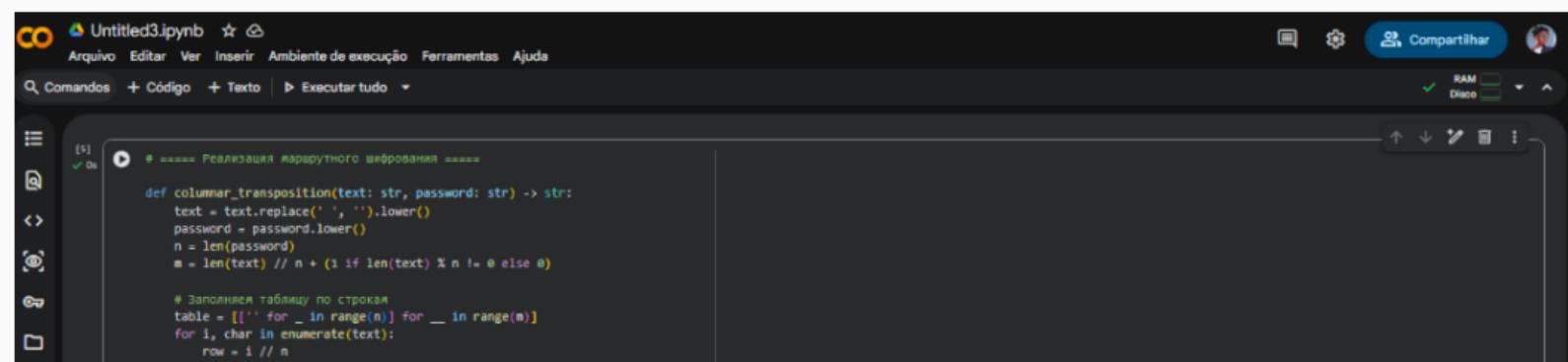
---

## Реализация шифрования с помощью решеток

Данный способ шифрования предложил австрийский криптограф Эдуард Флейснер в 1881 году. Суть этого способа заключается в следующем. Выбирается натуральное число  $n > 1$ , строится квадрат размерности  $n \times n$  и построчно заполняется числами 1, 2, ...,  $n^2$ .

#Реализация таблицы Виженера В 1585 году французский криптограф Блез Виженер опубликовал свой метод шифрования в «Трактате о шифрах». Шифр считался нераскрываемым до 1863 года, когда австриец Фридрих Казиски взломал его.

Выполним реализацию этого алгоритма на языке Python (рис. (fig:001?)):



The screenshot shows a Jupyter Notebook interface with the following details:

- Title Bar:** Untitled3.ipynb
- Toolbar:** Arquivo, Editar, Ver, Inserir, Ambiente de execução, Ferramentas, Ajuda
- Search Bar:** Comandos, Código, Texto, Executar tudo
- Code Cell:** [4] # ===== Реализация маршрутного шифрования =====

```
def columnar_transposition(text: str, password: str) -> str:  
    text = text.replace(' ', '').lower()  
    password = password.lower()  
    n = len(password)  
    m = len(text) // n + (1 if len(text) % n != 0 else 0)  
  
    # Заполняем таблицу по строкам  
    table = [['' for _ in range(n)] for __ in range(m)]  
    for i, char in enumerate(text):  
        row = i // n
```
- Runtime Status:** RAM Discos
- Page Number:** 5/7

## Вывод

---

- В ходе выполнения лабораторной работы были изучены шифры простой замены, а также написаны их алгоритмы на языке Python.

## Список литературы

---

## Список литературы

---

::: {#refs}