**Презентацияполабораторнойработе№1**

Основыинформационнойбезопасности

Назармамадов У.ДЖ

16 сентября 2025

Российский университет дружбы народов, Москва, Россия

1/7

**Информация**

# Докладчик

* Назармамадов Умед Джамшедович
* студент группы НКАбд-03-23
* Российский университет дружбы народов

# Цель

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

# Задание

Два текста кодируются одним ключом (однократное гаммирование).

Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты 𝑃1 и 𝑃2 в режиме однократного гаммирования.

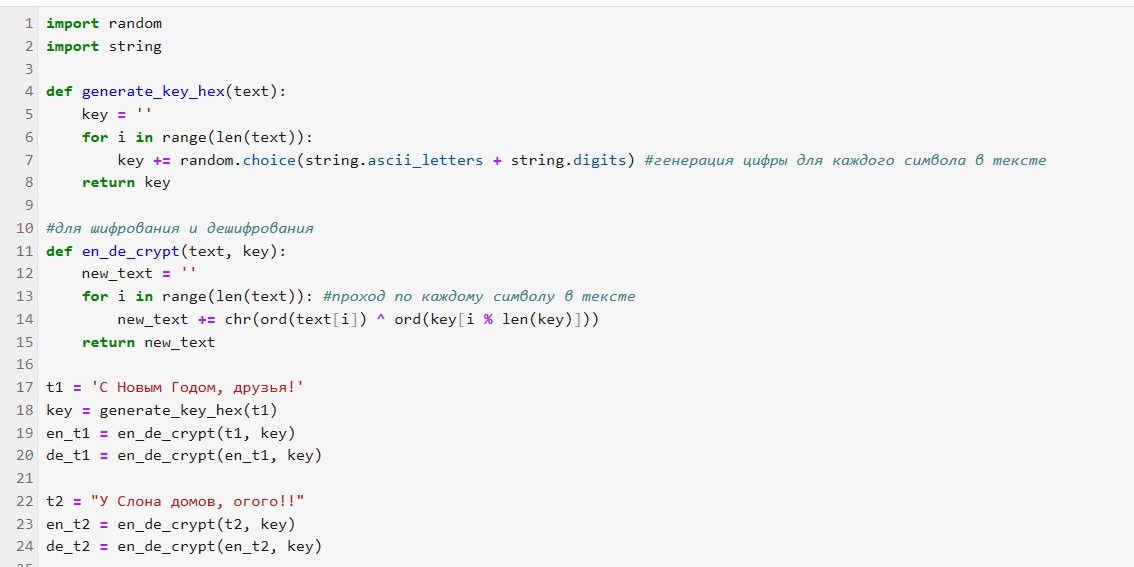
Приложение должно определить вид шифротекстов 𝐶1 и 𝐶2 обоих текстов 𝑃1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

# Выполнениелабораторнойработы

Я выполняла лабораторную работу на языке программирования Python, используя функции, реализованные в лабораторной работе №7.

# Выполнениелабораторнойработы

Используя функцию для генерации ключа, генерирую ключ, затем шифрую два разных текста одним и тем же ключом



**Рис. 1:** Шифрование двух текстов

# Вывод

В ходе лабораторной работы были освоины на практике навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

:::