# Отчет по лабораторной работе № 8

## По дисциплине Информационная безопасность

### Выполнил: Максимов Алексей Александрович

### Группа: НПИ-бд-01-20

#### Российский Университет Дружбы Народов #### г. Москва

# Цель работы

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.

# Выполнение лабораторной работы

### Пишем программу для кодирования и декодирования сообщений

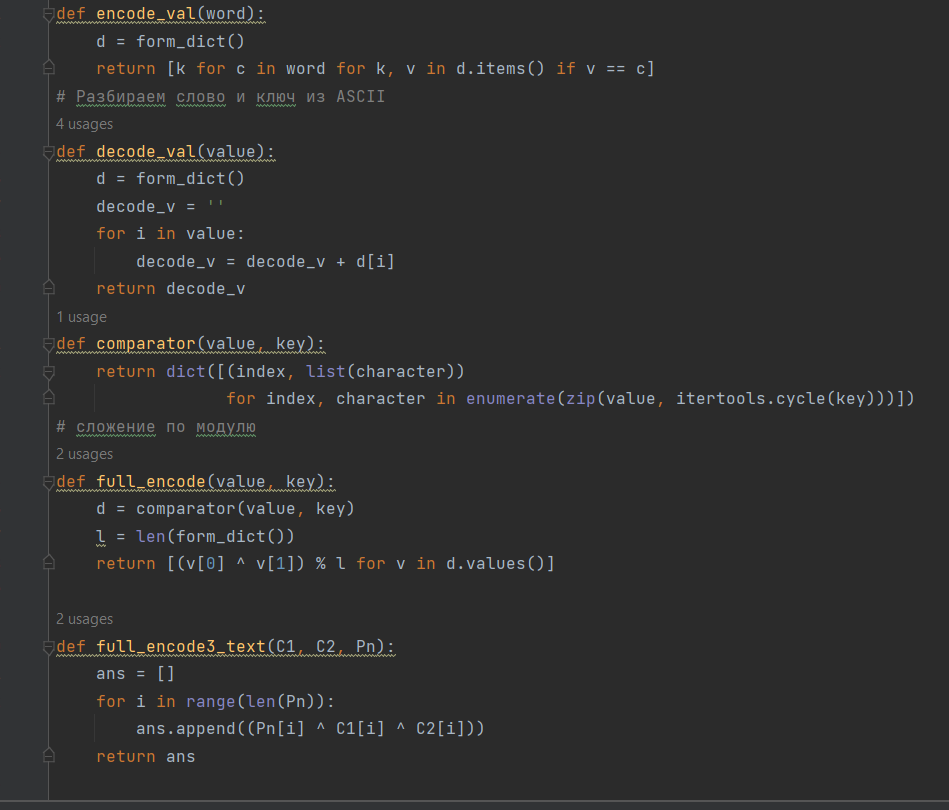


Image1

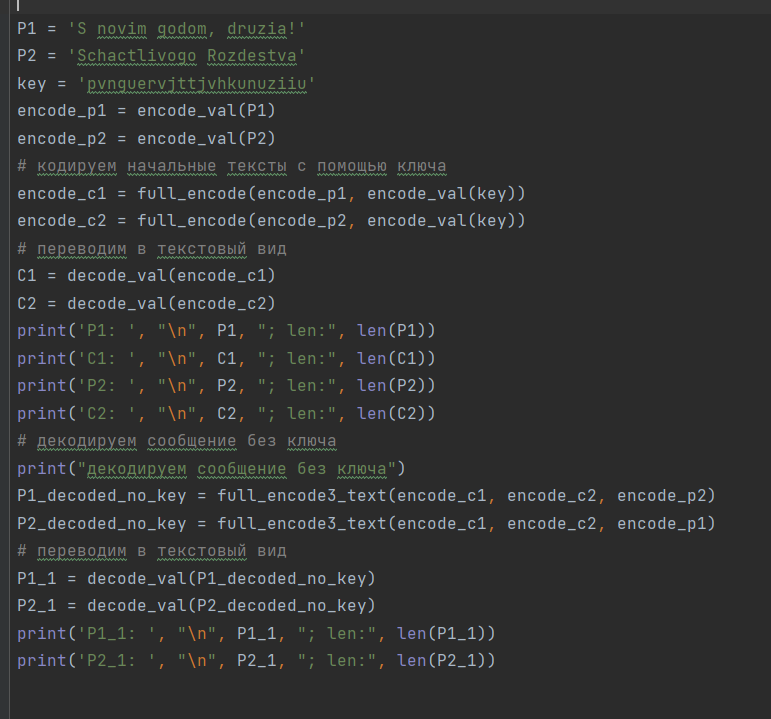


Image2

### Проверяем результат

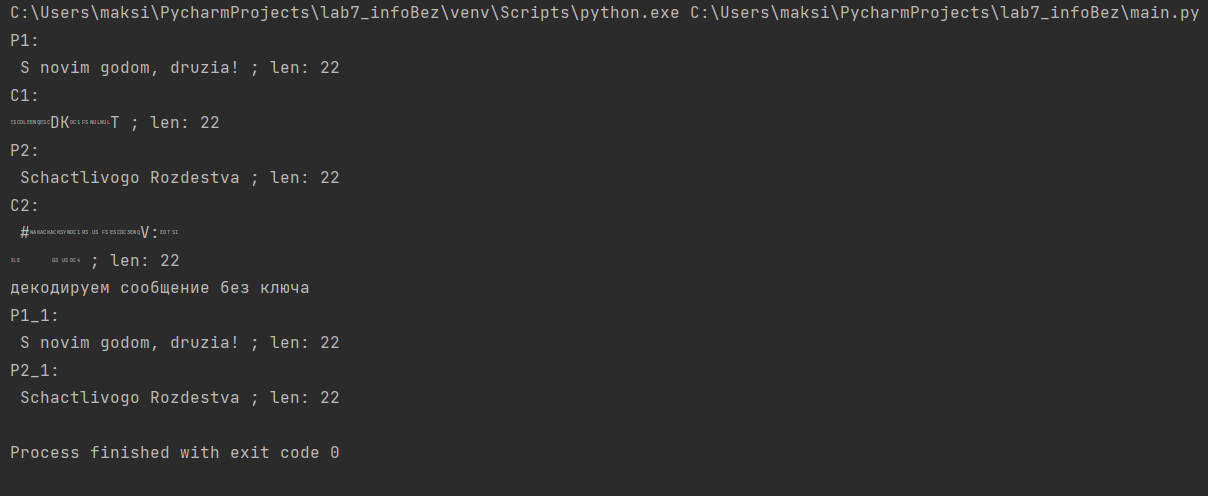


Image3

# Выводы

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