

# Лабораторная работа №7

---

Автор: Асеева Яна Олеговна

Группа: НКНбд-01-19

## Цель выполнения лабораторной работы

---

Освоить на практике применение режима однократного гаммирования.

## Что такое гаммирование?

---

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

## Результат работы приложения

---

```
: 1 shifr("СНовымГодомДрузья")
```

Введите гамму(Только символы из dict): яьзурДмодГывНС

Числа текста [51, 47, 16, 3, 29, 14, 36, 16, 5, 16, 14, 37, 18, 21, 9, 30, 32]

числа гаммы [32, 30, 9, 21, 18, 37, 14, 16, 5, 36, 29, 3, 47, 51]

8

2

Числа зашифрованного текста [8, 2, 25, 24, 47, 51, 50, 32, 10, 52, 43, 40, 65, 72, 41, 60, 41]

Зашифрованный текст: жбчцНСРяиТЙЖЯ7ЗЪЗ

Расшифрованный текст СНовымГодомДрузья

## Выводы

---

В ходе выполнения лабораторной работы я освоила на практике применение режима однократного гаммирования.