

# **Элементы криптографии. Шифрование (кодирование) различных исходных текстов ОДНИМ КЛЮЧОМ**

---

Максимова Ксения НБИбд-02-18<sup>1</sup>

18 декабря, 2021, Москва, Россия

<sup>1</sup>Российский Университет Дружбы Народов

# Цель лабораторной работы

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

Смысл однократного гаммирования заключается в наложении гаммы, то есть в сложении элементов некоторой строки с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

# Преимущества однократного гаммирования

1. Абсолютная стойкость шифра в случае, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.
2. Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении все различные ключевые последовательности возможны и равновероятны

При проведении процедуры однократного гаммирования необходимо хранить огромные объемы данных, которые можно было бы использовать в качестве гаммы.

# Необходимые и достаточные условия абсолютной стойкости шифра

---

1. полная случайность ключа;
2. равенство длин ключа и открытого текста;
3. однократное использование ключа

Разработано приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования с использованием одного ключа.