**Шифр**

**гаммирования**

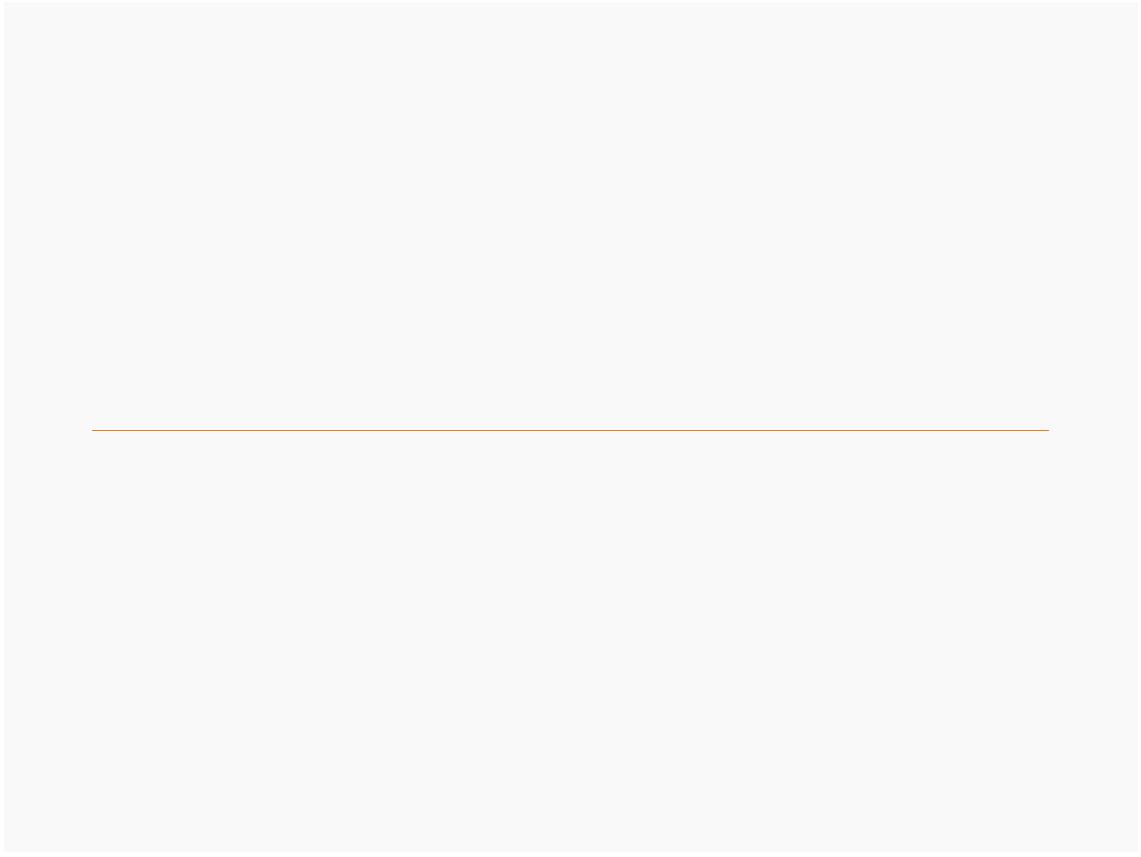
Кузьмин Артем

2

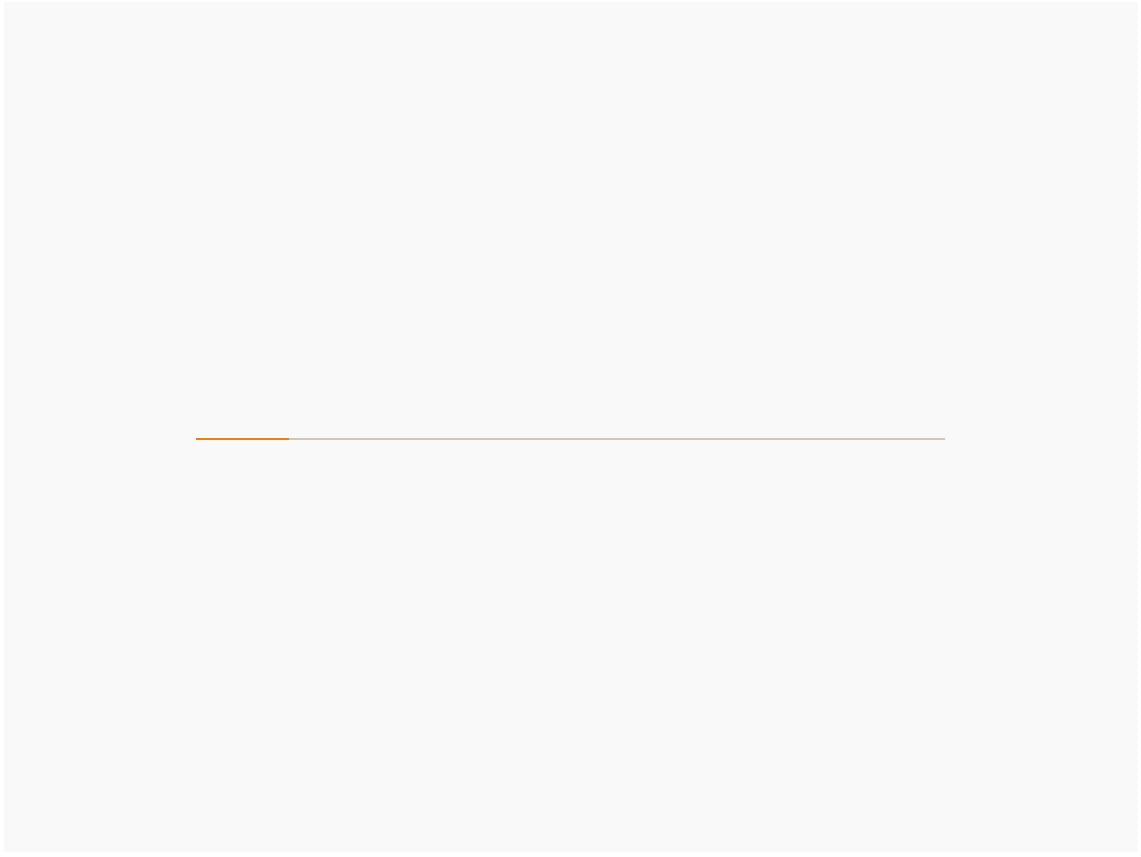
9 мая, 2025, Москва, Россия

Российский Университет Дружбы Народов

1/8



**[Цели и задачи](#br2)**



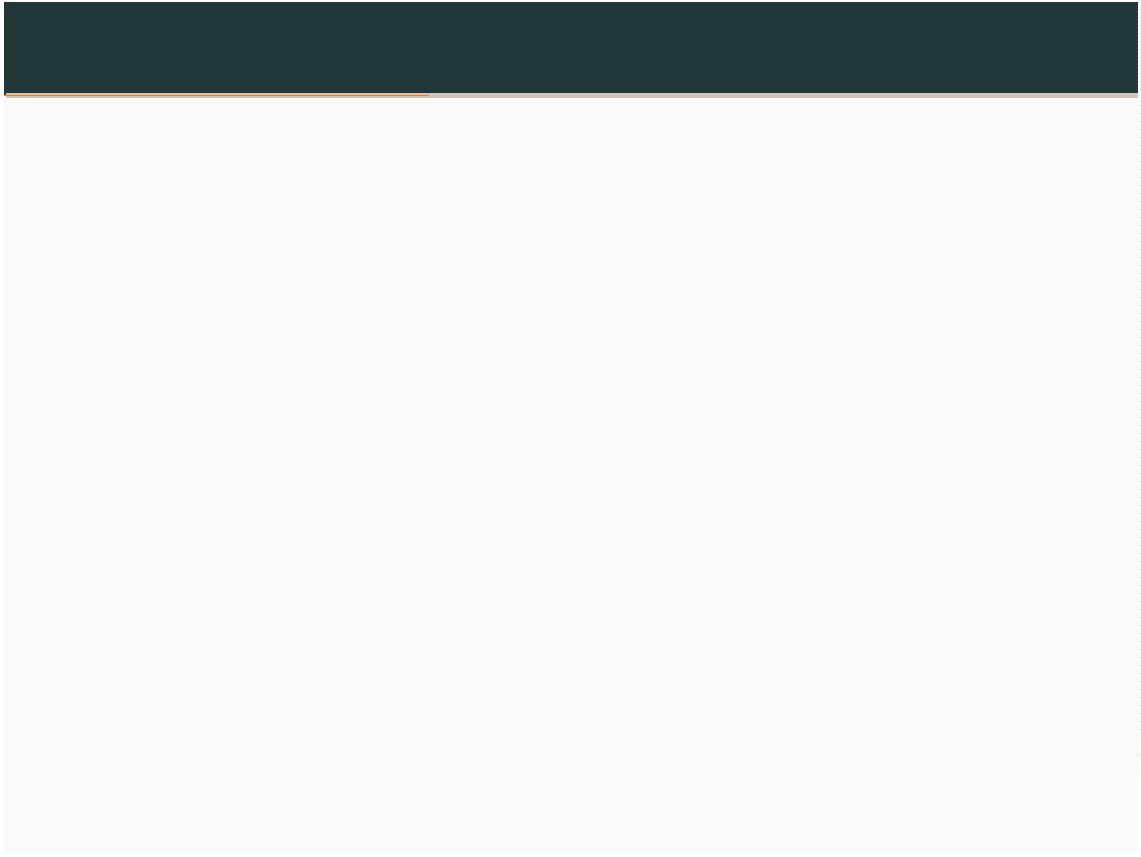
**Цель лабораторной работы**

•Освоить на практике применение

режима однократного гаммирования

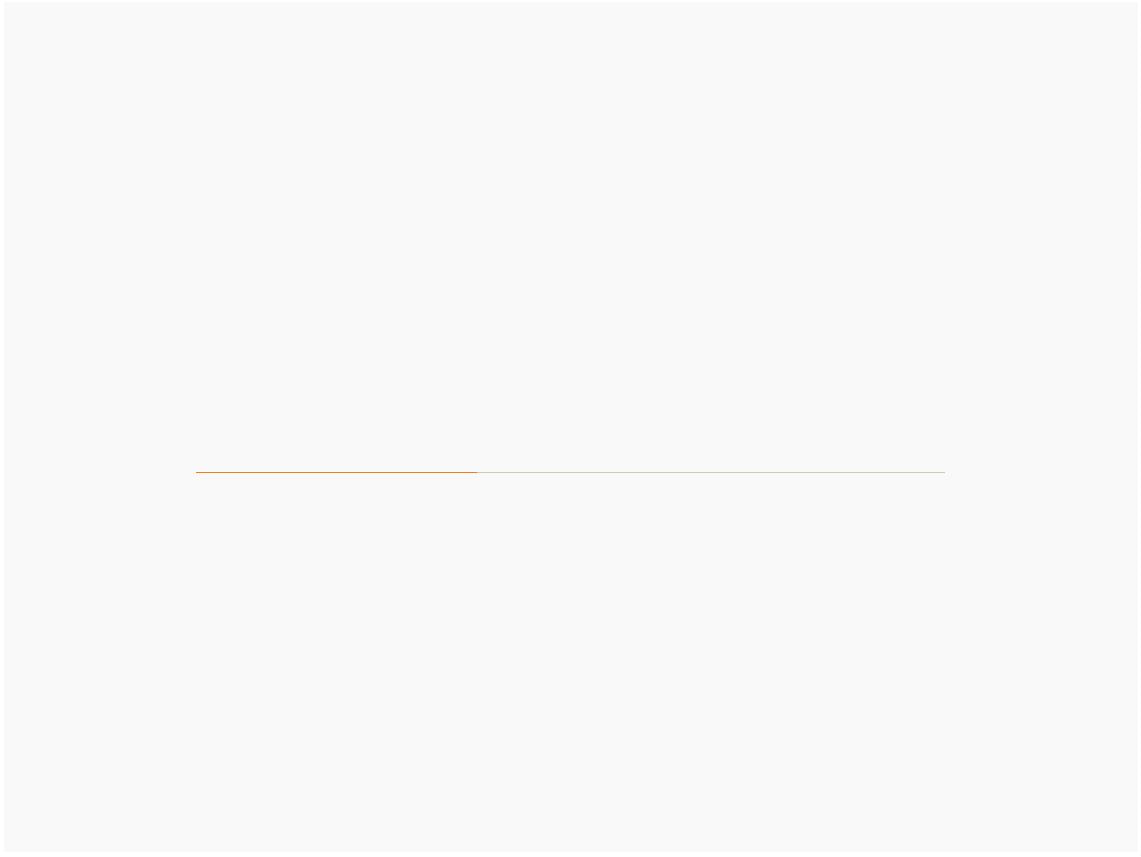
на примере кодирования различных

исходных текстов одним ключом.



**[Выполнение лабораторной](#br4)**

**[работы](#br4)**



Гаммирование

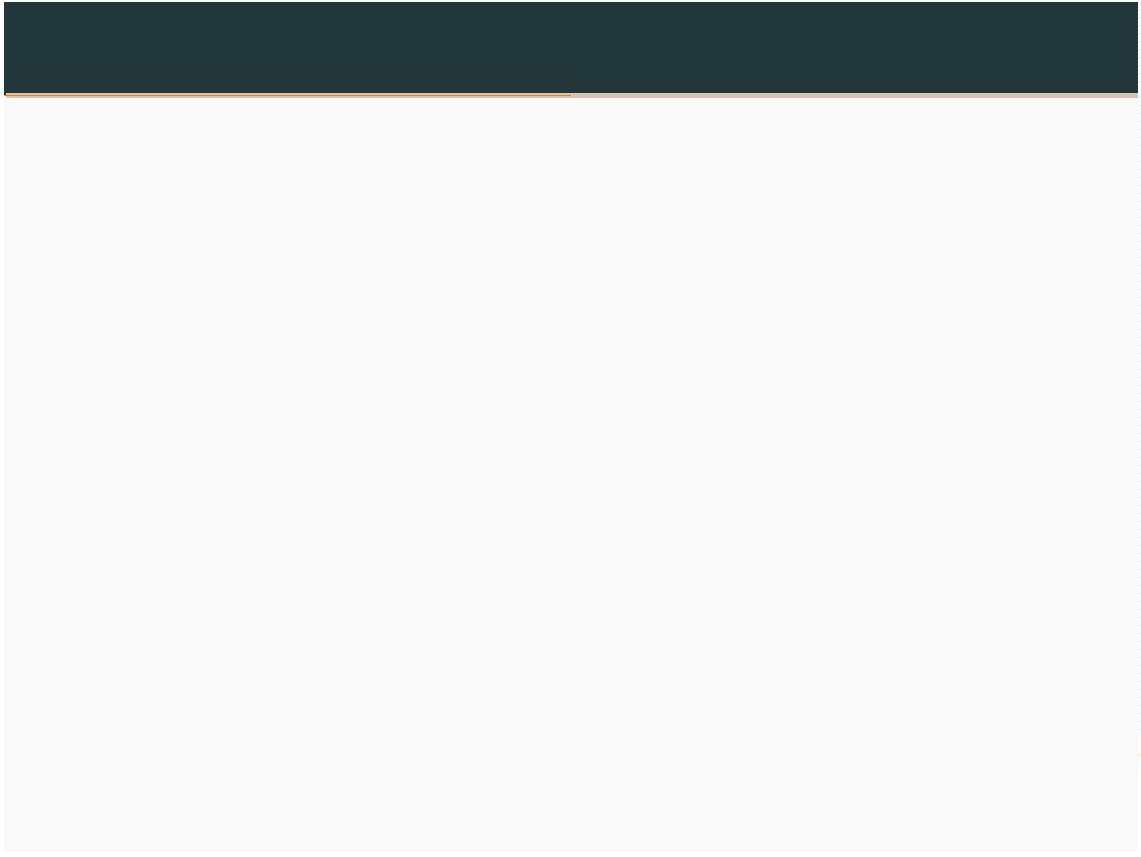
Гаммирование – это наложение (снятие) на открытые

(зашифрованные) данные криптографической гаммы, т.е.

последовательности элементов данных, вырабатываемых

с помощью некоторого криптографического алгоритма,

для получения зашифрованных (открытых) данных.



Алгоритм взлома

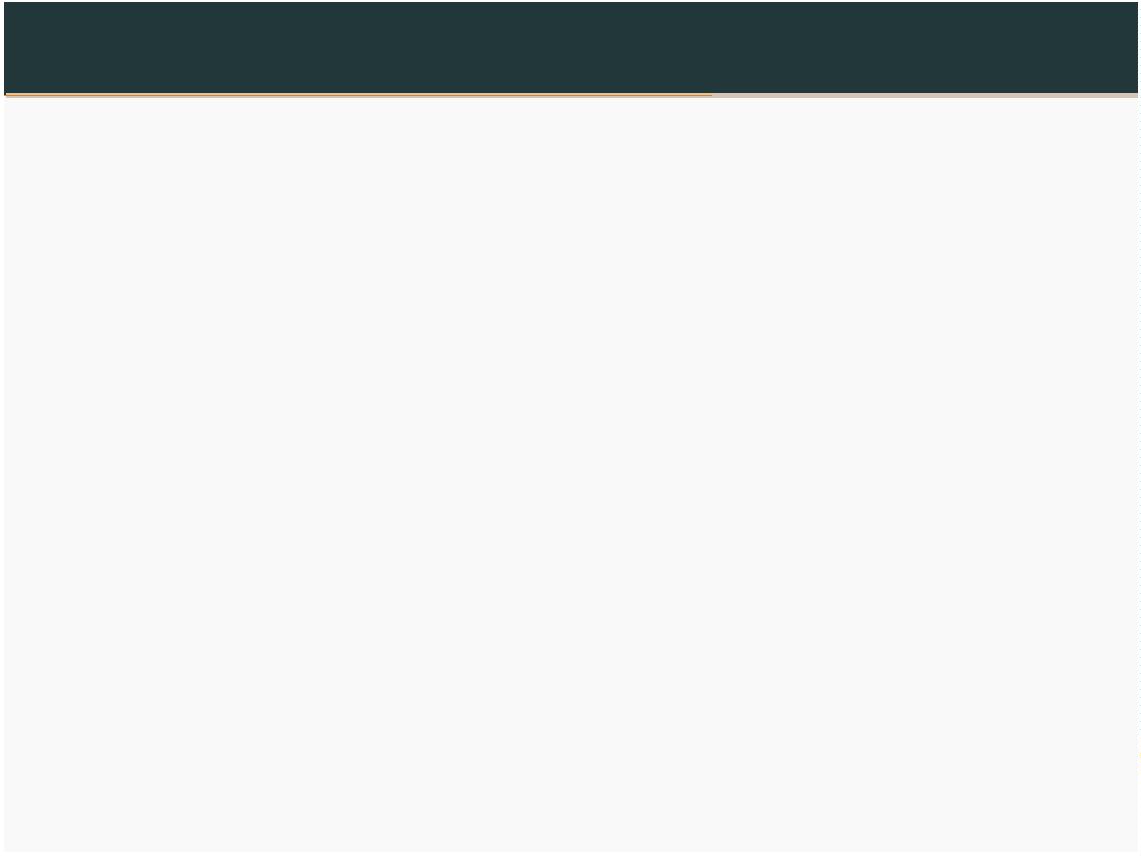
Шифротексты обеих телеграмм можно

получить по формулам режима

однократного гаммирования:

퐶1 = 푃1 ⊕ 퐾 퐶2 =

푃2 ⊕ 퐾



Алгоритм взлома

Открытый текст можно найти, зная

шифротекст двух телеграмм,

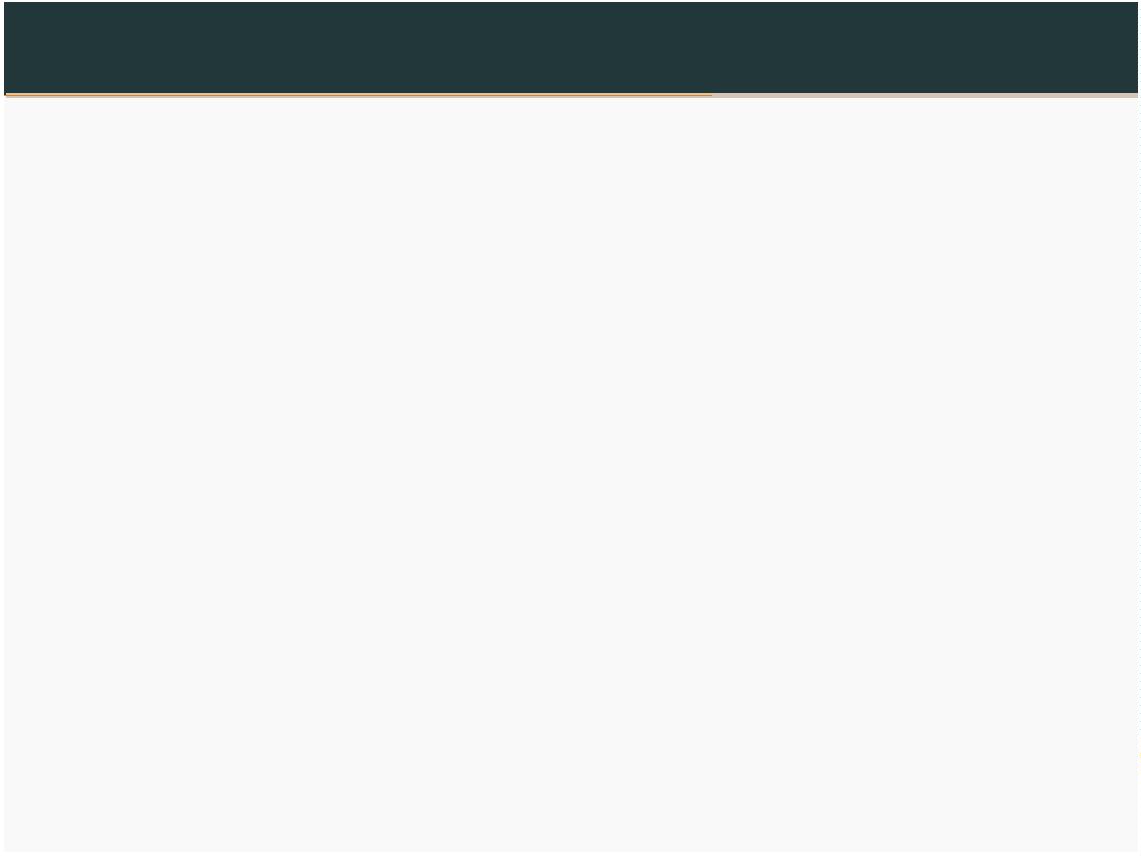
зашифрованных одним ключом. Для

это оба равенства складываются по

модулю 2. Тогда с учётом свойства

операции XOR получаем:

퐶1 ⊕ 퐶2 = 푃1 ⊕ 퐾 ⊕ 푃2 ⊕ 퐾 = 푃1 ⊕ 푃2



Алгоритм взлома

Предположим, что одна из телеграмм

является шаблоном — т.е. имеет текст

фиксированный формат, в который

вписываются значения полей.

Допустим, что злоумышленнику этот

формат известен. Тогда он получает

достаточно много пар 퐶1 ⊕ 퐶2

(известен вид обеих шифровок). Тогда

зная 푃1 имеем:

퐶1 ⊕ 퐶2 ⊕ 푃1 = 푃1 ⊕ 푃2 ⊕ 푃1 = 푃2

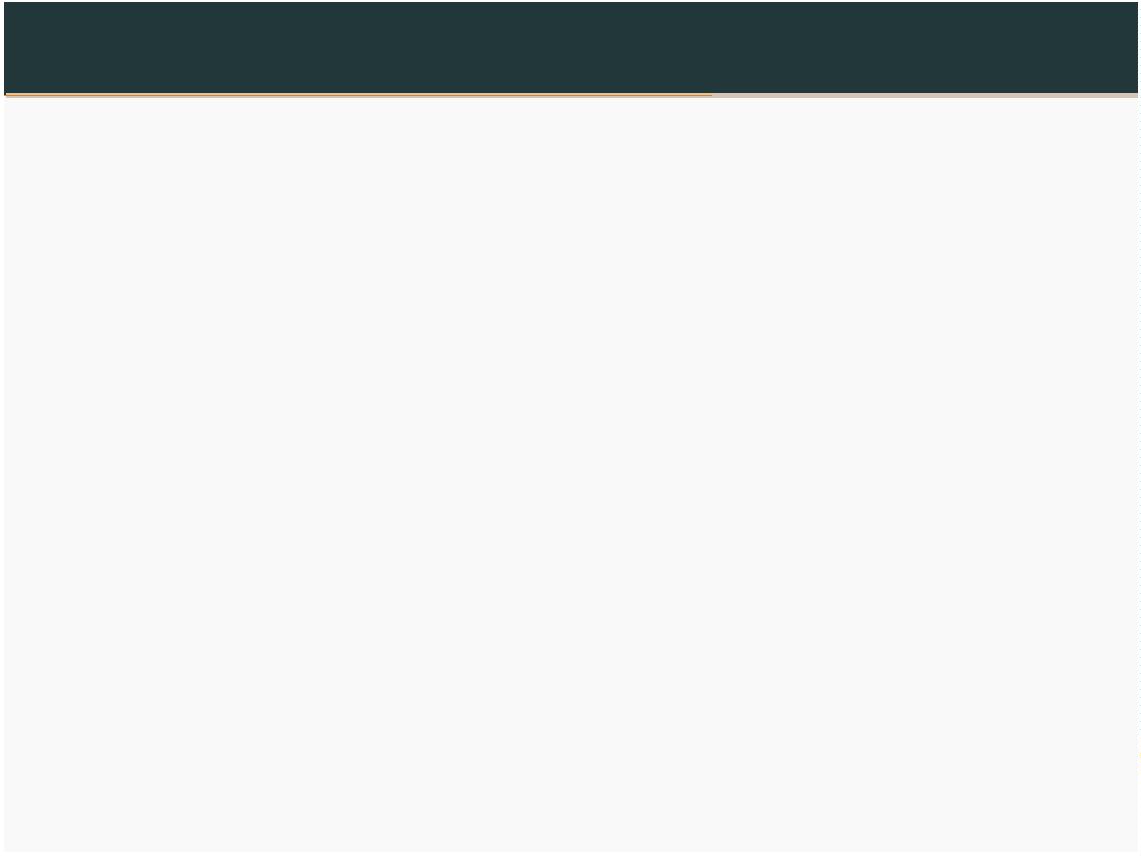
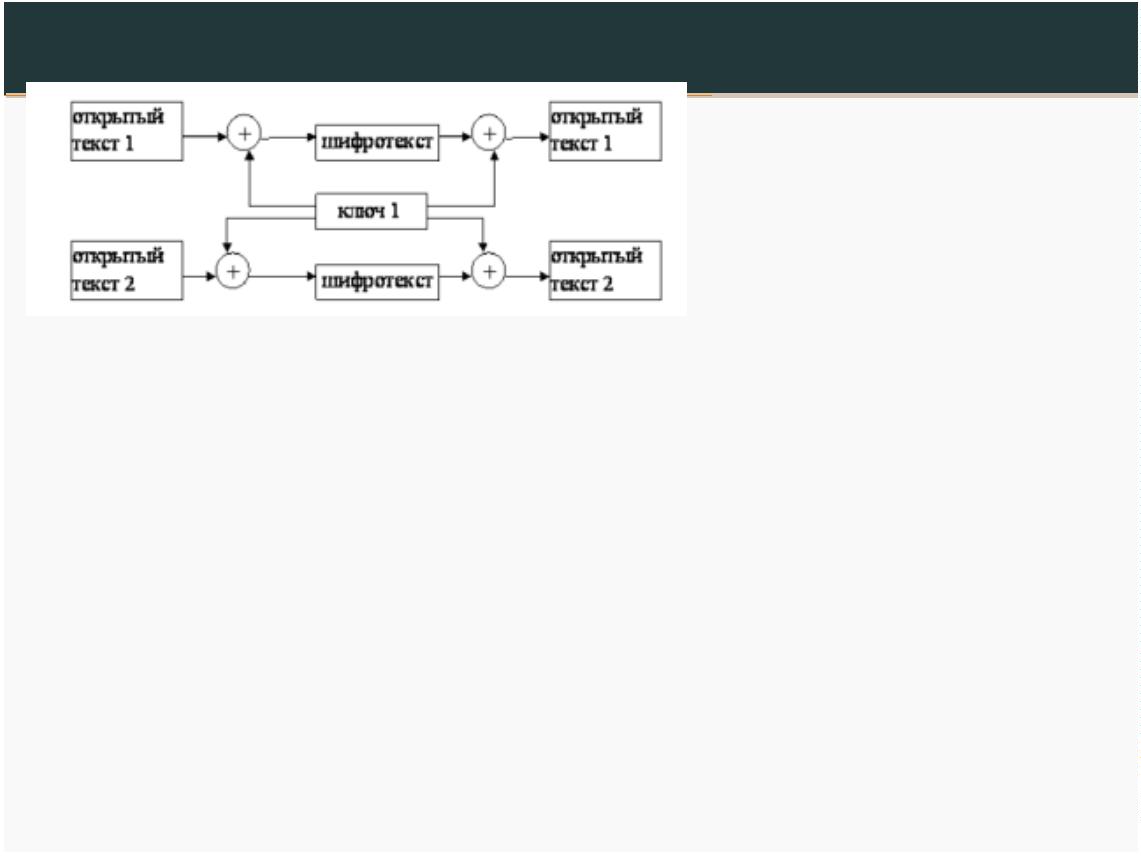


Схема работы алгоритма

Рис. 1: Работа алгоритма

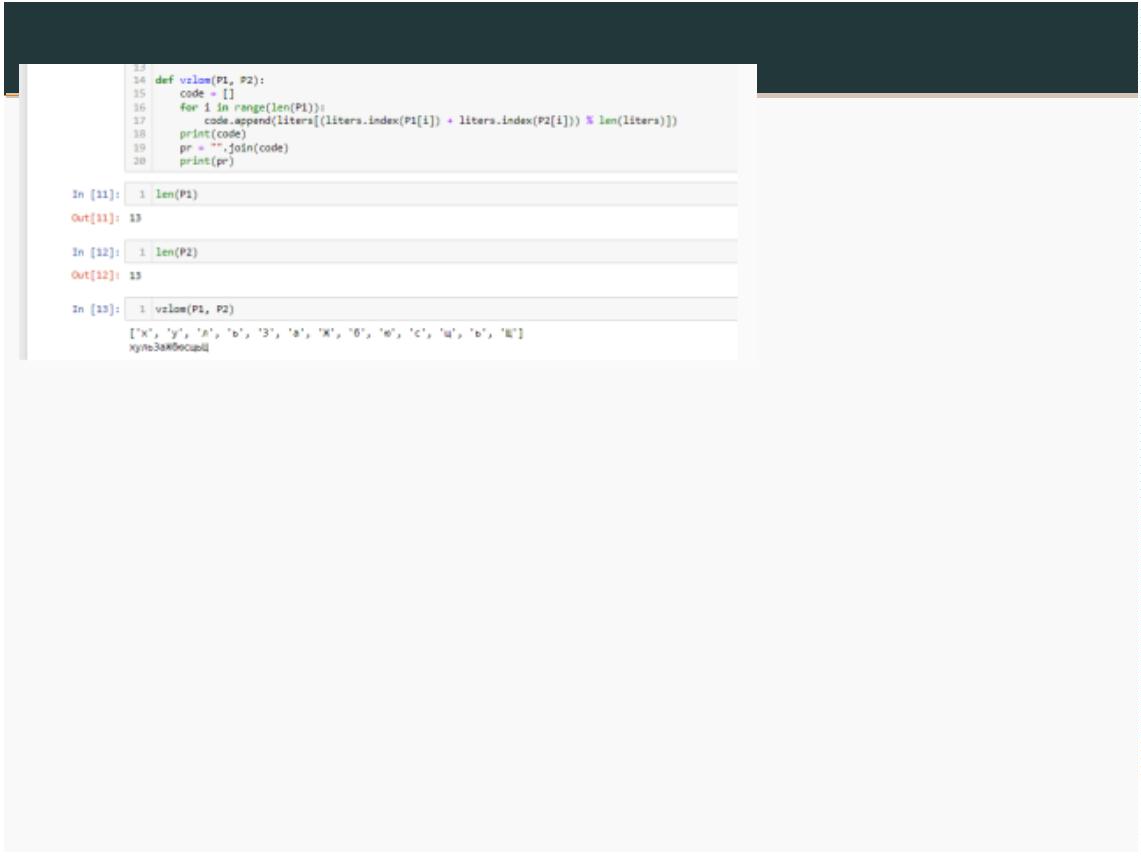
гаммирования



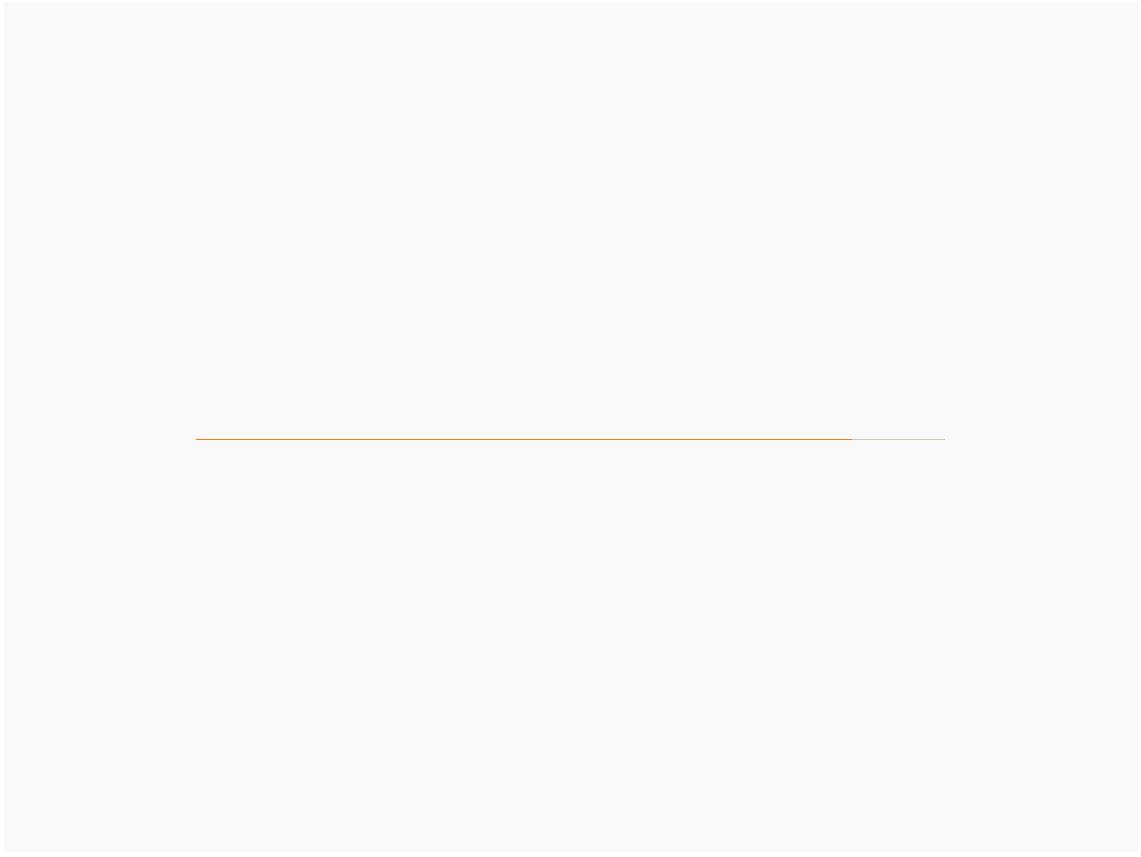
Пример работы программы

Рис. 2: Работа алгоритма взлома

ключа



**[Выводы](#br11)**



**Результаты выполнения лабораторной работы**

В ходе выполнения лабораторной

работы было разработано

приложение, позволяющее

шифровать тексты в режиме

однократного гаммирования.

