Отчёта по лабораторной работе №8

дисциплина: Информационная безопасность

Кашкин Иван Евгеньевич

Содержание

[Цель работы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202532)

[Задание](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202533)

[Теоретическое введение](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202534)

[Выполнение лабораторной работы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202535)

[Выводы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202536)

[Список литературы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab5\report.docx#_Toc177202537)

# Цель работы

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

# Теоретические сведения

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.

Метод гаммирования с обратной связью заключается в том, что для получения сегмента гаммы используется контрольная сумма определенного участка шифруемых данных.

Например, если рассматривать гамму шифра как объединение непересекающихся множеств H(j)

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

C1 = P1 ⊕ K C2 = P2 ⊕ K

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:

C1 ⊕ C2 = P1 ⊕ K ⊕ P2 ⊕ K = P1 ⊕ P2

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 C1 ⊕ C2 (известен вид обеих шифровок). Тогда зная P1 имеем:

C1 ⊕ C2 ⊕ P1 = P1 ⊕ P2 ⊕ P1 = P2

Таким образом, злоумышленник получает возможность определить те символы сообщения P2, которые находятся на позициях известного шаблона сообщения P1.

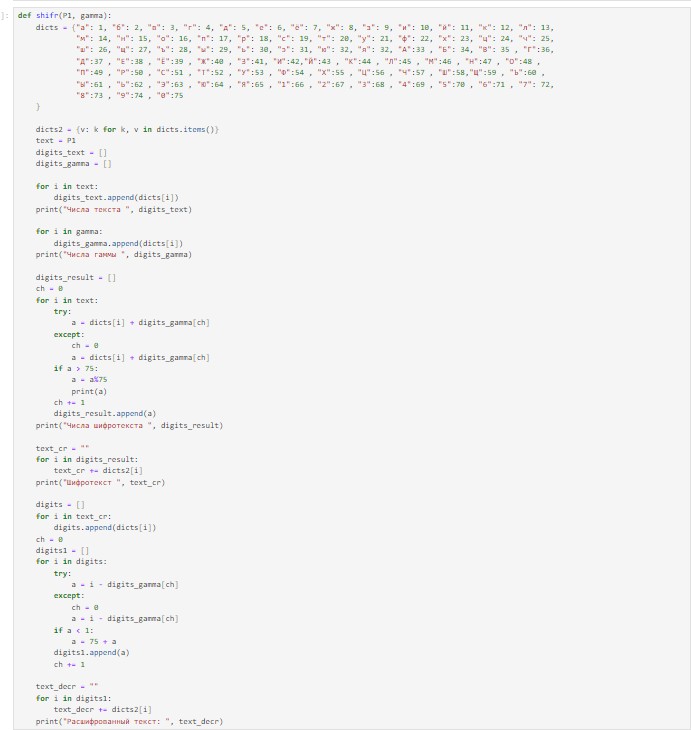
В соответствии с логикой сообщения P2, злоумышленник имеет реальный шанс узнать

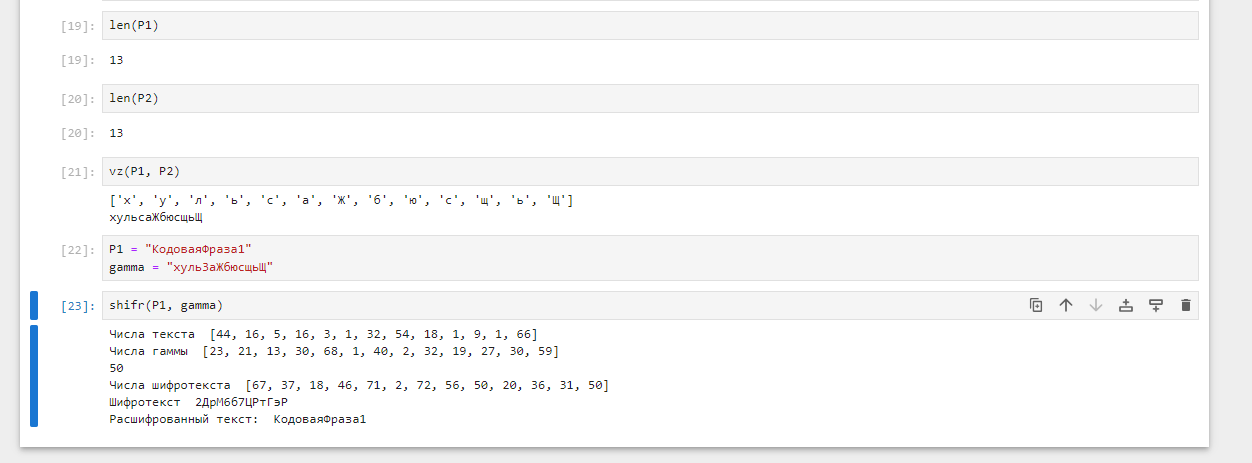
ещё некоторое количество символов сообщения P2.

Затем вновь используется равенство с подстановкой вместо P1 полученных на предыдущем шаге новых символов сообщения P2.

# Выполнение работы







**Выводы**

В ходе выполнения лабораторной работы было разработано приложение, позволяющее шифровать тексты в режиме однократного гаммирования.

# Список литературы{.unnumbered}

1. [Шифрование методом гаммирования](http://altaev-aa.narod.ru/security/XOR.html)
2. [Режим гаммирования в блочном алгоритме шифрования](https://kabinfo.ucoz.ru/index/shifr_reshetka_kardano/0-374)