Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Кекишева Анастасия Дмитриевна

Содержание

# 1 Цель работы

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

# 2 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.

# 3 Теоретическое введение

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней. Главным образом, шифрование служит для соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма .

Как мы узнали ранее, гаммирование — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле [1].

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование)той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста следующего правила: > Ci = Pi Ki,

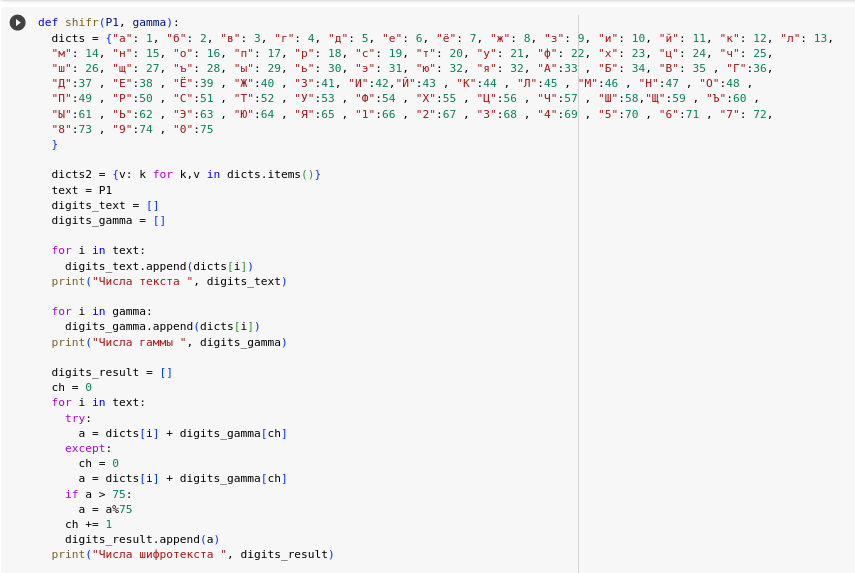
где Ci — i-й символ получившегося зашифрованного послания, Pi — i-й cимвол открытого текста, Ki — i-й символ ключа, i = 1, m. Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины.

Если известны шифротекст и открытый текст, то задача нахождения ключа решается через формулу, а именно, обе части равенства необходимо сложить по модулю 2 с Pi: > Ci Pi = Pi Ki Pi = Ki, > Ki = Ci Pi.

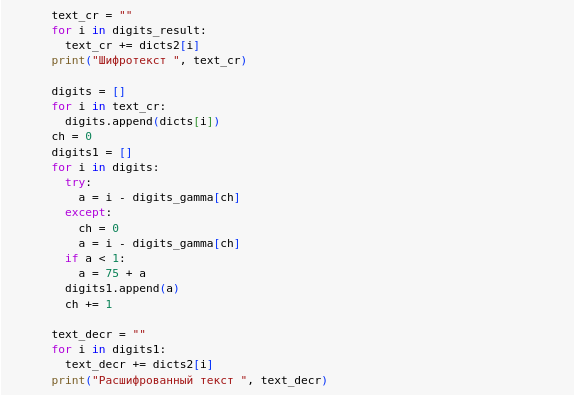
Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, воспользовавшись таблицей ASCII-кодов [2].

# 4 Выполнение лабораторной работы

1. Написала приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования (рис. ??, ??).  
   Она определяет вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе;

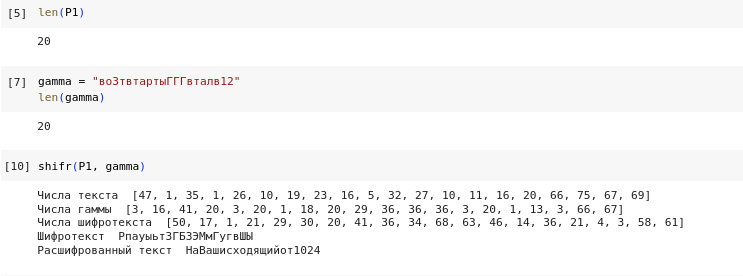


Первая часть программы

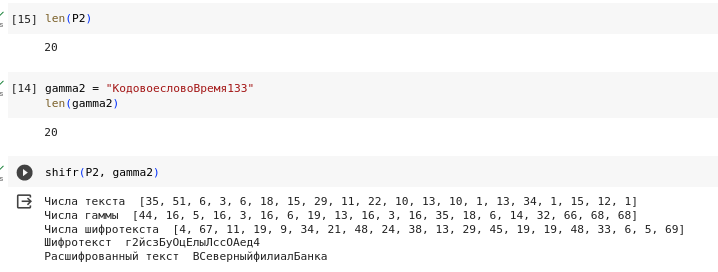


Вторая часть программы

1. Придумала гамму и запустила программу - результаты представлены на ?? для Р1 и на ?? для Р2.



Результат выполнения для Р1



Результат выполнения для Р2

1. Определила и выразила аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить (рис. ??).



Вариант взлома

# 5 Выводы

1. Освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.
2. Написала приложение, позволяющее шифровать и дешифровать тексты в режиме однократного гаммирования и определять вид шифротекстов при известном ключе.

# Список литературы

1. Однократное гаммирование [Электронный ресурс]. URL: <https://studfile.net/preview/272674/page:7/>.

2. Лабораторная работа No 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом [Электронный ресурс]. URL: <https://esystem.rudn.ru/pluginfile.php/2090423/mod_resource/content/2/008-lab_crypto-key.pdf>.