Отчёт по лабораторной работе

Лабораторная работа 7

Дзугаева Лилия Владславовна

Table of Contents

[Цель работы 1](#_Toc90044986)

[Выполнение лабораторной работы 1](#_Toc90044987)

[Выводы 3](#_Toc90044988)

[Список литературы 3](#_Toc90044989)

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Выполнение лабораторной работы

1. Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования:



рис. 1.

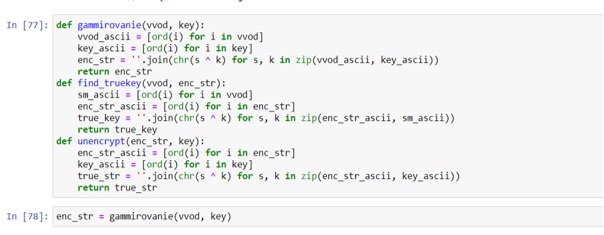


рис. 2.



рис. 3.

1. Ответы на контрольные вопросы:
   1. Поясните смысл однократного гаммирования. Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Однократное гаммирование – это когда каждый символ попарно с символом ключа складываются по модулю 2 (XOR).
2. Перечислите недостатки однократного гаммирования. Недостатки: Размер ключевого материала должен совпадать с размером передаваемых сообщений. Также необходимо иметь эффективные процедуры для выработки случайных равновероятных двоичных последовательностей и специальную службу для развоза огромного количества ключей. А ещё, если одну и ту же гамму использовать дважды для разных сообщений, то шифр из совершенно стойкого превращается в «совершенно нестойкий» и допускает дешифрование практически вручную.
3. Перечислите преимущества однократного гаммирования. Достоинства: С точки зрения теории криптоанализа метод шифрования случайной однократной равновероятной гаммой той же длины, что и открытый текст, является невскрываемым. Кроме того, даже раскрыв часть сообщения, дешифровщик не сможет хоть сколько-нибудь поправить положение - информация о вскрытом участке гаммы не дает информации об остальных ее частях. К достоинствам также можно отнести простоту реализации и удобство применения.
4. Почему длина открытого текста должна совпадать с длиной ключа? Потому что каждый символ открытого текста должен складываться с символом ключа попарно.
5. Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется сложение по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Особенность заключается в том, что этот алгоритм шифрования является симметричным. Поскольку двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, шифрование и расшифрование выполняется одной и той же программой.
6. Как по открытому тексту и ключу получить шифротекст? Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста следующего правила: C\_i = P\_i ⊕ K\_i, где C\_i — i-й символ получившегося зашифрованного послания, P\_i — i-й символ открытого текста, K\_i — i-й символ ключа, i = 1, m. Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины.
7. Как по открытому тексту и шифротексту получить ключ? Если известны шифротекст и открытый текст, то задача нахождения ключа решается также в соответствии с, а именно, обе части равенства необходимо сложить по модулю 2 с P\_i: C\_i ⊕ P\_i = P\_i ⊕ K\_i ⊕ P\_i = K\_i, K\_i = C\_i ⊕ P\_i.
8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра: Полная случайность ключа; Равенство длин ключа и открытого текста; Однократное использование ключа.

# Выводы

В ходе выполнения лабораторной работы я изучил теорию и освоил на практике применение режима однократного гаммирования.

# Список литературы