Лабораторная работа №7

Лукьянова Ирина Владимировна, НФИбд-02-19

Содержание

# 1 **Цель работы**

Освоить на практике применение режима однократного гаммирования.[[1]](#footnote-20)

# 2 **Теоретические сведения**

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

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преоб- разован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# 3 **Выполнение лабораторной работы**

Добавляем необходимые библиотеки и создаем функцию генерации ключа.(рис. 1)

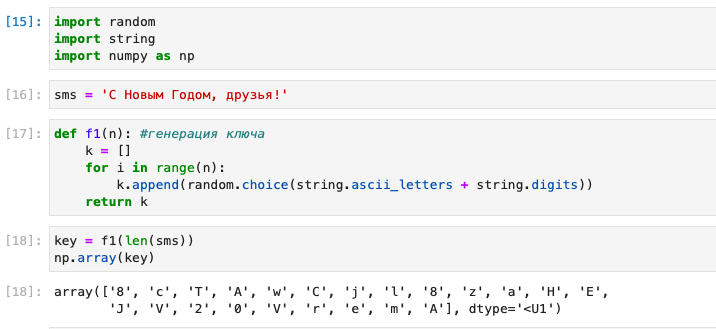


Figure 1: Код

Создаем функцию перевода в 16 строку и переводим ключ, с помощью этой функции.(рис. 2)

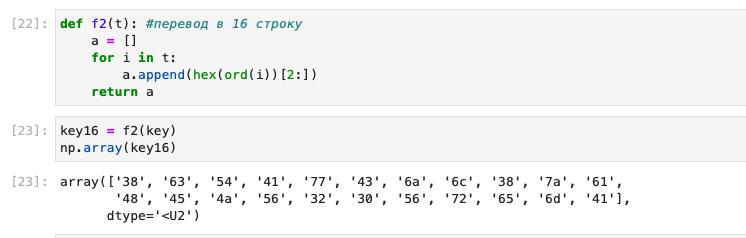


Figure 2: Код 2

Создаем функцию сложения по модулю 2 (XOR) для нее нам нужна еще одна функция, которая переводит наши символы в числа. (рис. 3)



Figure 3: Функции

В итоге получаем следующие данные: (рис. 4)

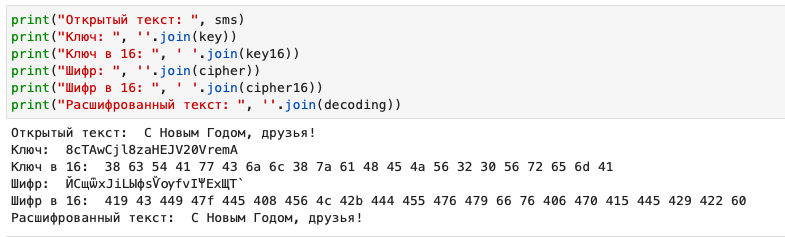


Figure 4: Вывод данных

После мы создаем новый ключ, используя открытый текст и шифр и расшифровываем сообщение с новым ключом: (рис. 5)



Figure 5: Проверяем работу сервиса

В завершении сравниваем ключи и убеждаемся в правильности найденного нового ключа.

# 4 **Контрольные вопросы**

1. Поясните смысл однократного гаммирования. Гаммирование — это наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.
2. Перечислите недостатки однократного гаммирования. Ключ одного размера с сообщением, что является уязвимостью.
3. Перечислите преимущества однократного гаммирования. Стойкость и легкость в использоавании.
4. Почему длина открытого текста должна совпадать с длиной ключа? Каждый символ текста попарно складывается с символом ключа. Следовательно шифротекст получится той же длины.
5. Какая операция используется в режиме однократного гаммирования,назовите её особенности? Сложение по модулю 2 (ХOR). Каждая пара двоичных знаков заменяется одним двоичным знаком шифрованного текста в соответствии с принятым алгоритмом;
6. Как по открытому тексту и ключу получить шифротекст? Сложить по модулю 2 символы открытого текста и ключа.
7. Как по открытому тексту и шифротексту получить ключ? Сложить по модулю 2 символы открытого текста и шифротекста.
8. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? полная случайность ключа; равенство длин ключа и открытого текста; однократное использование ключа.

# 5 Выводы

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.

# 6 Список литературы

1. [Элементы криптографии. Однократное гаммирование. / Кулябов Д. С., Королькова А. В., Геворкян М. Н. - Москва: - 7 с.](https://esystem.rudn.ru/pluginfile.php/1651893/mod_resource/content/2/007-lab_crypto-gamma.pdf)
2. [Руководство по оформлению Markdown.](https://gist.github.com/Jekins/2bf2d0638163f1294637)

1. Элементы криптографии. Однократное гаммирование. [↑](#footnote-ref-20)