Отчёт по лабораторной работе №7. Элементы криптографии. Однократное гаммирование.

Предмет: информационная безопасность

Александр Сергеевич Баклашов

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования. [1]

# 2 Теоретическое введение

Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

# 3 Выполнение лабораторной работы

1. Создадим функции для перевода в 16-ричный вид, шифрования и дешифрования, а также импортируем необх. библиотеки. (рис. [1](#fig:001))

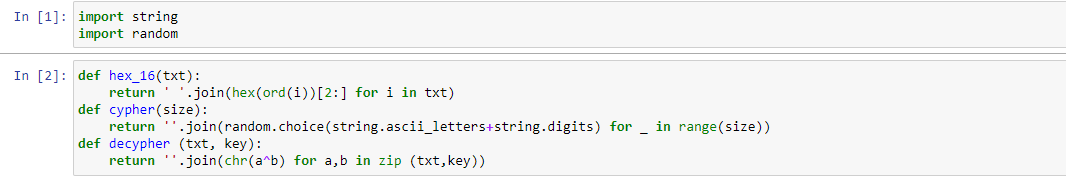


Figure 1: Функции

1. Создадим код для получения шифротекста. (рис. [2](#fig:002))

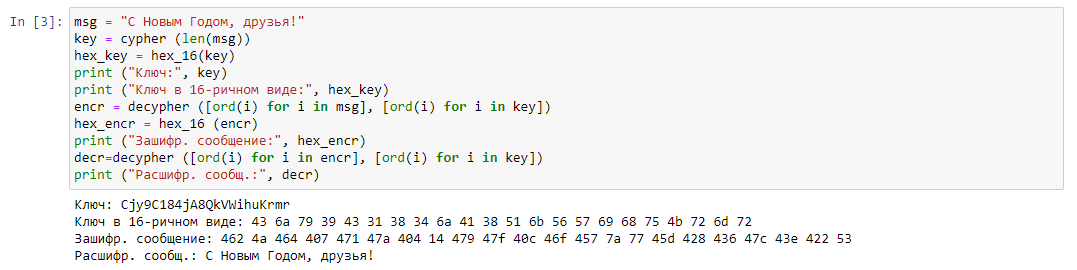


Figure 2: Шифротекст

1. Создадим код для получения варианта прочтения открытого текста. (рис. [3](#fig:003))

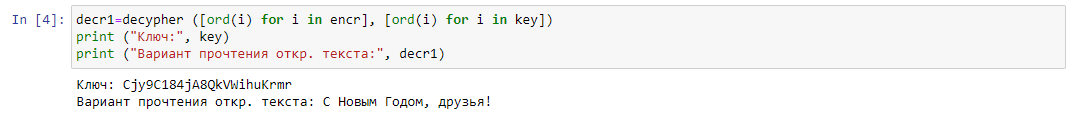


Figure 3: Открытый текст

# 4 Вывод

В результате выполнения работы я освоил на практике применение режима однократного гаммирования.

# 5 Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование - выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. 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.

1. Перечислите недостатки однократного гаммирования.

Абсолютная стойкость шифра доказана только в случае, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения.

1. Перечислите преимущества однократного гаммирования.

Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой. Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P.

1. Почему длина открытого текста должна совпадать с длиной ключа?

Если ключ длиннее текста - появится неоднозначность декодирования, а если короче - операция XOR будет применена не ко всем элементам.

1. Какая операция используется в режиме однократного гаммирования, назовите её особенности?

Используется операция XOR, которая является симметричной.

1. 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: Ci = Pi (+) Ki где Ci — i-й символ получившегося зашифрованного послания, Pi — i-й символ открытого текста, Ki — i-й символ ключа, i = 1, m.

1. Как по открытому тексту и шифротексту получить ключ?

Если известны шифротекст и открытый текст, то обе части равенства необходимо сложить по модулю 2 с Pi: Ci (+) Pi = Pi (+) Ki (+) Pi = Ki, Ki = Ci (+) Pi.

1. 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.

# 6 Библиография

1. Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование. - 3 с. [Электронный ресурс]. М. URL: [Лабораторная работа №6](file:///C:/Users/bakla/Labs%20IAD/Lab6/007-lab_crypto-gamma.pdf) (Дата обращения: 18.10.2022).