Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Гурбангельдиев Мухаммет НФИбд-03-18

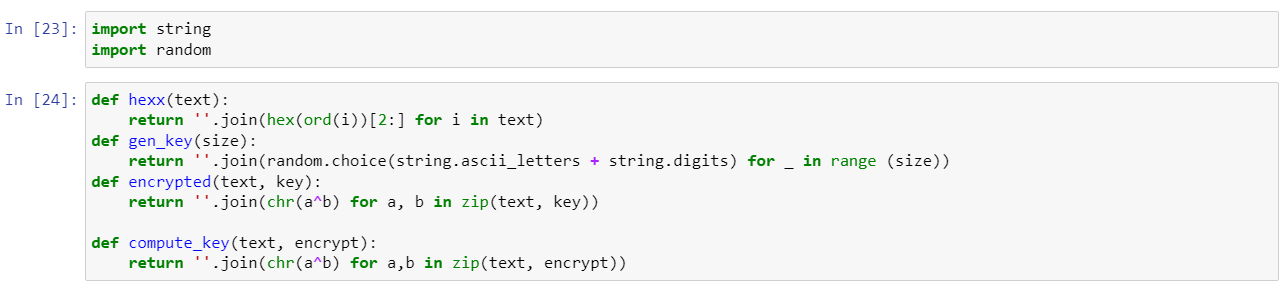
Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования

# Последовательность выполнения работы

1. Блок функции для расчетов. (рис. -@fig:001)



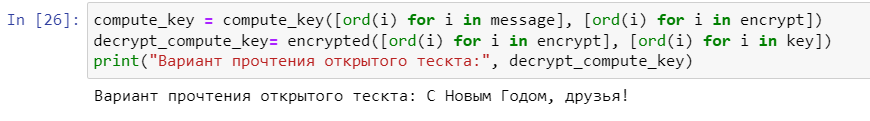
Блок функции для расчетов

1. Определил вид шифротекста при известном ключе и известном открытом тексте. (рис. -@fig:002)



Получение шифротекста

1. Определил ключ,с помощью которого шифротекст может быть преобразо- ван в некоторый фрагменттекста,представляющий собой один из возмож- ных вариантов прочтения открытого текста. (рис. -@fig:003)



Прочтение открытого текста

# Контрольные вопросы

1. Поясните смысл однократного гаммирования.

Гаммирование—метод симметричного шифрования,заключающийся в «нало- жении» последовательности,состоящей из случайных чисел,на открытый текст. Последовательность случайных чисел называется гаммапоследовательностью и используется для зашифровывания и расшифровывания данных.

1. Перечислите недостатки однократного гаммирования.

Ключ одного размера с сообщением,на один ключ используется только один текст.

1. Перечислите преимущества однократного гаммирования.

Простота и криптостойкость.

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

Каждый символ текста попарно складывается с символом ключа.

1. Какая операция используется в режиме однократного гаммирования,назо- вите её особенности?

Сложение по модулю 2.Особенность в симметричности–оерация при повтор- ном применении дает исходний результат.

1. Как по открытому тексту и ключу получить шифротекст?

Сложить по модулю 2 каждый символ открытого текста и ключа.

1. Как по открытому тексту и шифротексту получить ключ?

Сложить по модулю 2 каждый символ открытого текста и шифротекста.

1. В чем заключаются необходимые и достаточные условия абсолютной стой- кости шифра?

* полная случайность ключа;
* равенство длин ключа и открытого текста;
* однократное использование ключа.

# Выводы

Освоил на практике применение режима однократного гаммирования.