Отчет по лабораторной работе №8

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

Бармина Ольга Константиновна

2022 Sep 21th

Содержание

# 1 Цель работы

Целью данной работы является освоение на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом. [1]

# 2 Выполнение лабораторной работы

1. Подгрузила необходимые библиотеки, задала функцию для генерации ключа, преобразованию ключа в шестнадцатеричное предстваление, и для шифрования текста.

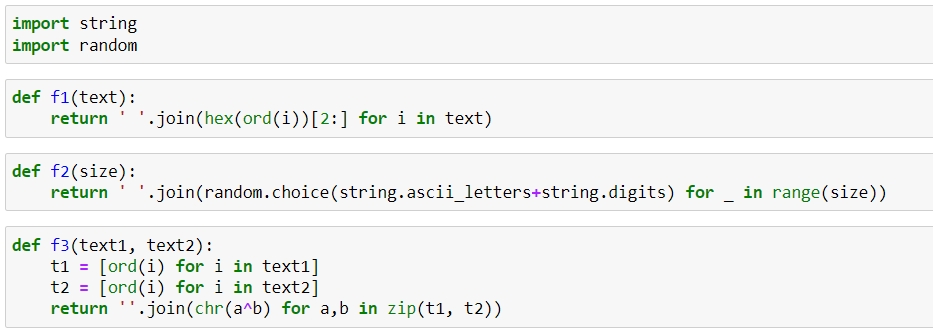


рис 1. функции

1. Задала 2 текста, создала ключ, преобразовала его в шестнадцатеричное представление.

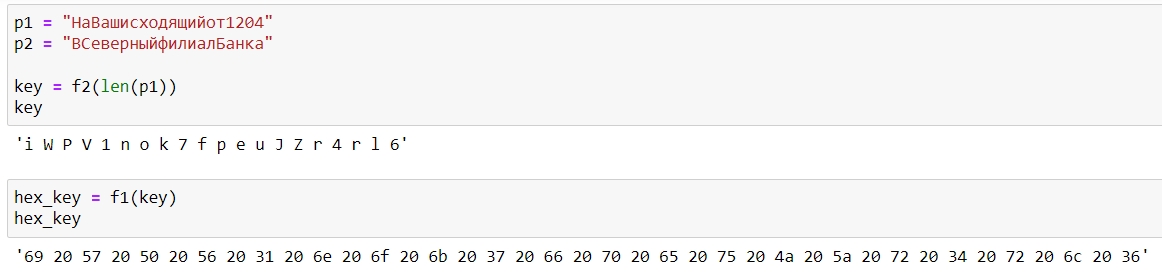


рис 2. создание ключа

1. Закодировала оба сообщения с помощью ключа. Создала декриптор, использующий оба сообщения. Раскодировала сообщения при помощи него.



рис 3. шифрование

# 3 Контрольные вопросы

1. Чтобы определить один из текстов, зная другой, необходимо вопсользоваться следующей формулой: , где и - шифротексты. Т.е. ключ в данной формуле не используется.
2. При повторном использовании ключа при шифровании текста получим исходное сообщение.
3. Режим шифрования однократного гаммирования одним ключом двух открытых текстов реализуется по следующей формуле:
4. где - шифротексты, - открытые тексты, - единый ключ шифровки
5. Недостатки шифрования одним ключом двух открытых текстов: Во-первых, имея на руках одно из сообщений в открытом виде и оба шифротекста, злоумышленник способен расшифровать каждое сообщение, не зная ключа. Во-вторых, зная шаблон сообщений, злоумышленник получает возможность определить те символы сообщения , которые находятся на позициях известного шаблона сообщения .
6. Преимущества шифрования одним ключом двух открытых текстов: Такой подход помогает упростить процесс шифрования и дешифровки. Также, при отправке сообщений между 2-я компьютерами, удобнее пользоваться одним общим ключом для передаваемых данных

# 4 Выводы

В ходе работы мы освоили на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 5 Список литературы

1. Методические материалы курса