Отчёт по лабораторной работе №8

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

Волков Тимофей Евгеньевич

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить (fig. 2).

Функции (fig. 1):  
hex\_ — перевод в шестнадцатиричную систему.  
gen\_key — генерирует рандомный ключ.  
encrypt — шифрует текст.  
decrypt — дешифрует тескт.

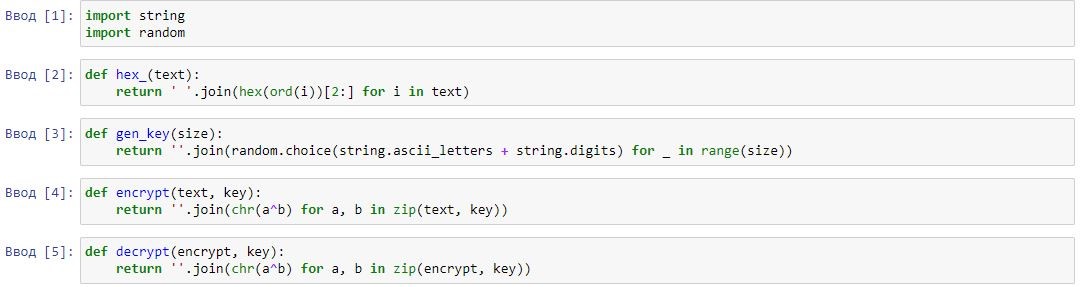


Figure 1: Функции

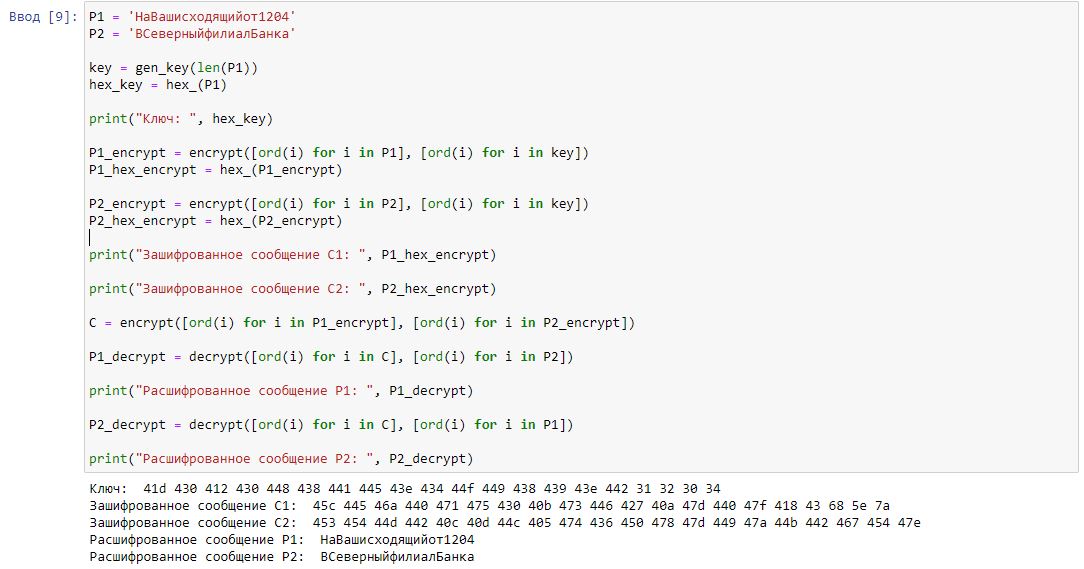


Figure 2: Вывод результата

# Выводы

Освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?  
   Сложить по модулю 2 оба шифротекста и декодировать первый текст используя полученное значение и известный второй текст.
2. Что будет при повторном использовании ключа при шифровании текста?  
   Оба текста, шифрованные одним ключем будут подвержены риску взлома.
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?  
   Шифруем оба текста одним ключем.
4. Перечислите недостатки шифрования одним ключом двух открытых текстов.  
   Подверженость риску взлома.
5. Перечислите преимущества шифрования одним ключом двух открытых текстов.  
   Используется меньше ключей.