Лабораторная работа № 8

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

Казакова Виктория Алексеевна

Содержание

# 1 Цель работы

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

# 2 Задание

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.

# 3 Ход работы

1. Создала функцию шифрования (рис. [1](#fig:001)). Данная функция шифрования получает на вход два текста. Функция ord выдает код символа. Return перебирает символы. Для пары символов взяли zip.

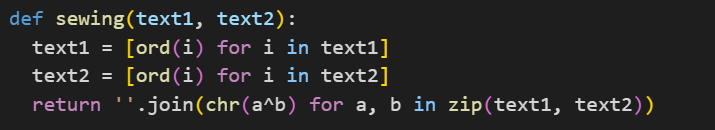


Figure 1: Функция шифрования

1. Ввела данные из условия. Зашифровала текст с помощью ключа К, вывела данные. (рис. [2](#fig:002)).

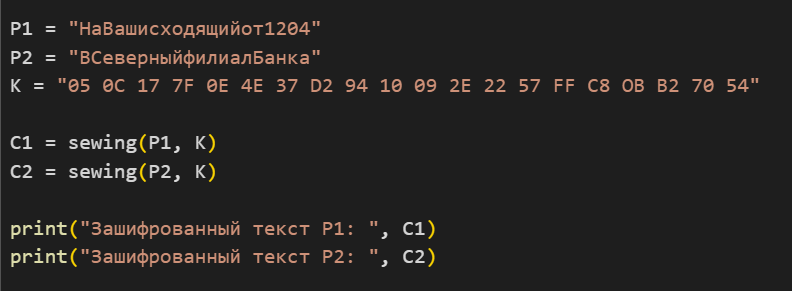


Figure 2: Шифрование текста

1. Создала последовательность, с помощью которой происходит расшифровка текста. Расшифроваю при помощи нее текст и вывожу их в дополнительные переменные.(рис.@fig:003).

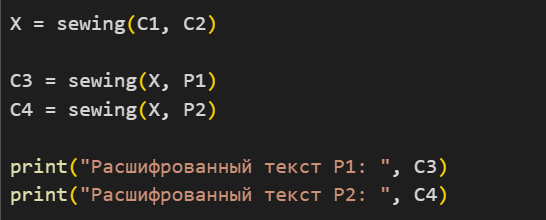


Figure 3: Перешифровка текста

1. Запустила программу и получила результат. (рис. [4](#fig:004)).

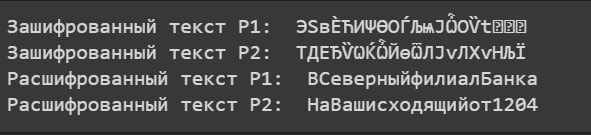


Figure 4: Результат

# 4 Вывод

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

# 5 Список литературы

1. [Методический материал 1] [https://esystem.rudn.ru/pluginfile.php/2090284/mod\_resource/content/2/007-lab\_crypto-gamma.pdf]
2. [Методический материал 2] [https://esystem.rudn.ru/pluginfile.php/2090286/mod\_resource/content/2/008-lab\_crypto-key.pdf]
3. [Google Colab] [https://colab.research.google.com/?hl=ru]