Отчёт по лабораторной работе №8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом.

Предмет: информационная безопасность

Александр Сергеевич Баклашов

Содержание

1 Цель работы **4**

2 Теоретическое введение **5**

3 Выполнение лабораторной работы **6**

4 Вывод **7**

5 Контрольные вопросы **8**

6 Библиография **9**

List of Figures

3.1 Функция 6
3.2 Код 6

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом. [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 функцию для шифрования и дешифрования, а также импортируем необх. библиотеки. (рис. 3.1)

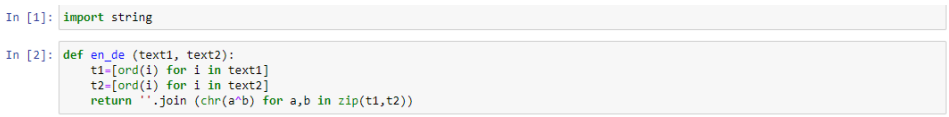

Figure 3.1: Функция

2. Создадим код для выполнения поставленной задачи. (рис. 3.2)

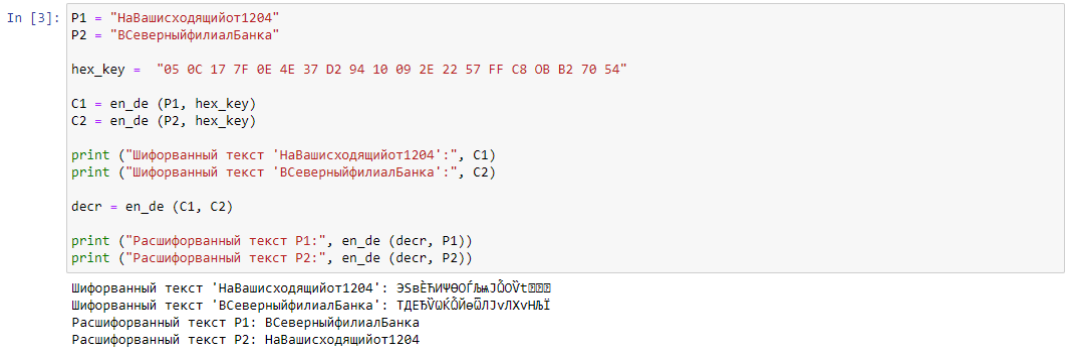

Figure 3.2: Код

4 Вывод

В результате выполнения работы я освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

5 Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Воспользуемся формулой:
C1 (+) C2 (+) P1 = P1 (+) P2 (+) P1 = P2.
C1 и C2 - шифрованные тексты, P1 и P2 - исходные тексты. Ключа K в формуле нет.

2. Что будет при повторном использовании ключа при шифровании текста?

Мы получим исходное сообщение.

3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

Шифротексты обеих текстов можно получить по формулам режима однократного гаммирования: C1 = P1 (+) K, C2 = P2 (+) K.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Можно расшифровать одно из сообщений, зная другое сообщение в открытом виде.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Упрощает дешифровку. Удобен в локальных сетях.

6 Библиография

1. Лабораторная работа № 8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом. - 3 с. [Электронный ресурс]. М. URL: Лабораторная работа №8 (Дата обращения: 29.10.2022).