Отчёт по лабораторной работе

Лаб 8

Аристид Жан Лоэнс Аристобуль

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 Выполнение лабораторной работы

Здесь мы представляем открытые тексты P1 и P2 на шестнадцатеричном представлении (рис. 1).

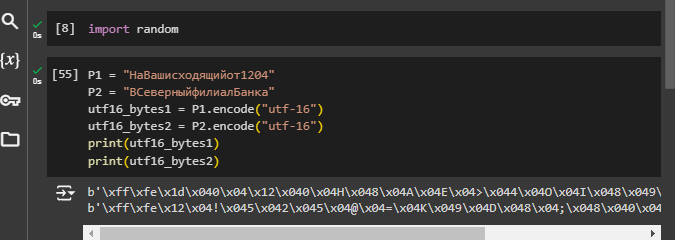


Рис. 1: шестнадцатеричное представление

Здесь генераваный ключ шифроврания случайным образом (рис. 2).

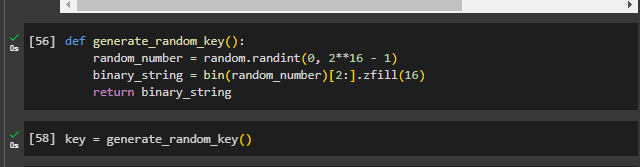


Рис. 2: Random Key

Здесь мы представляем открытыe тексты в двойчном представлении (рис. 3).

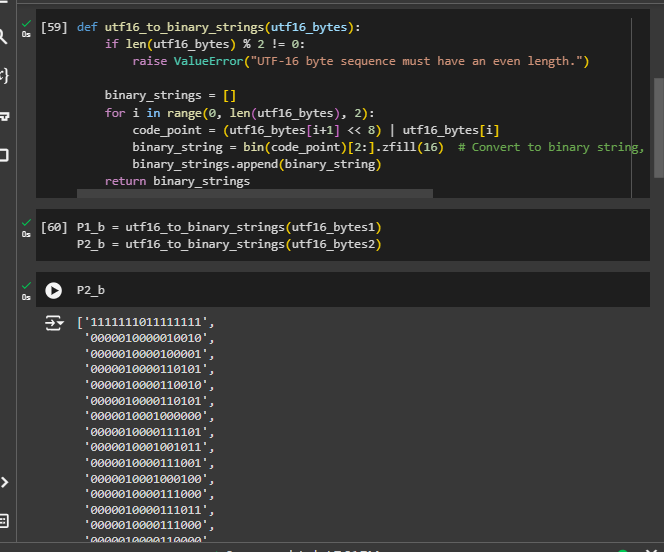


Рис. 3: Двойчное представление

Функция xor\_16bit\_strings() реализирует операция сложение по модулю 2 чтобы шифровать тексты. (рис. 4).

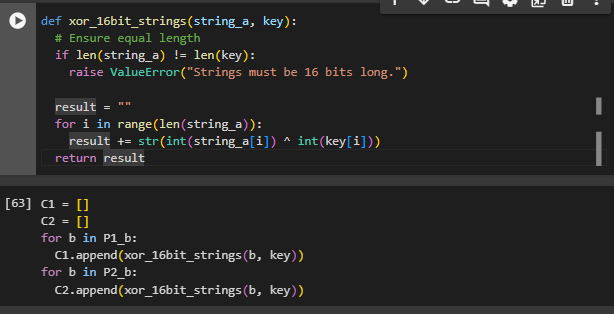


Рис. 4: Зашифрованный текст

Здесь у нас дешифрованные тексты в двойчном представлении. (рис. 5).

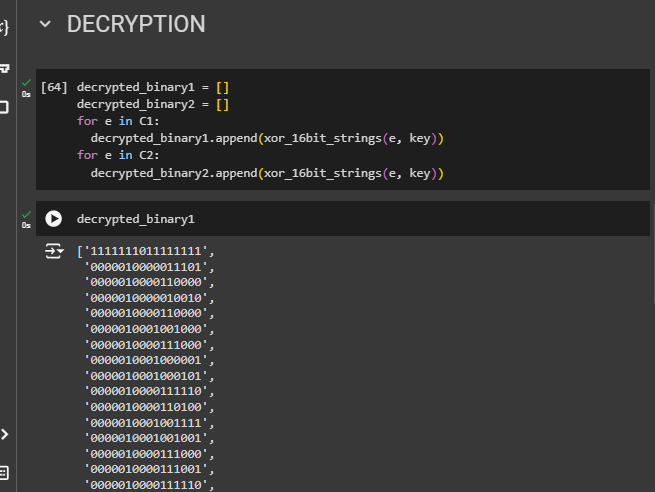


Рис. 5: Дешифрованный текст в двойчом представлении

Здесь Мы получили сообщение после дешифрования (рис. 6).

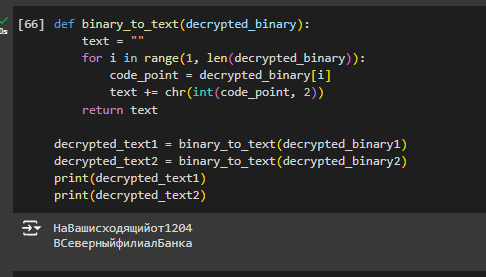


Рис. 6: дешифрованный текст

Мы исползуем другой метод без знания ключа что дешифровать. (рис. 7).

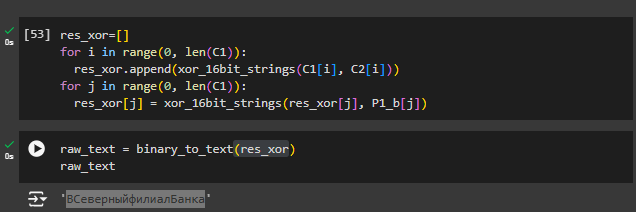


Рис. 7: Новый Ключ

# 4 Выводы

В ходе этой лабораторной работы мы изучили хороший метод криптографии для отправки сообщений, которые могут быть поняты только теми, у кого есть ключ дешифрования.