Отчёт по лабораторной работе

Лаб 7

Аристид Жан Лоэнс Аристобуль

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования1

# 2 Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# 3 Выполнение лабораторной работы

Здесь мы представляем открытый текст на шестнадцатеричном представлении (рис. 1).

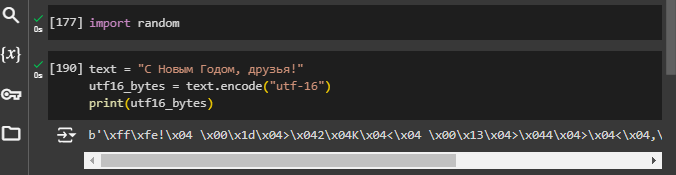


Рис. 1: шестнадцатеричное представление

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

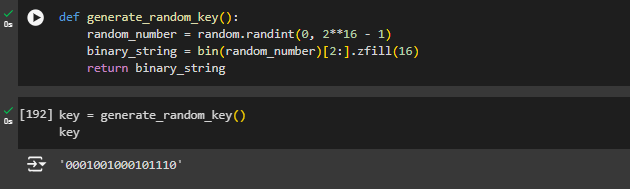


Рис. 2: Random Key

Здесь мы представляем открытый текст двойчном представлении (рис. 3).

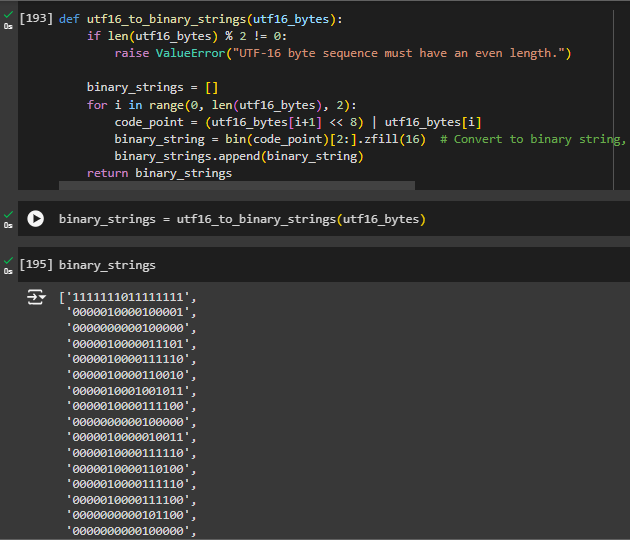


Рис. 3: Двойчное представление

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

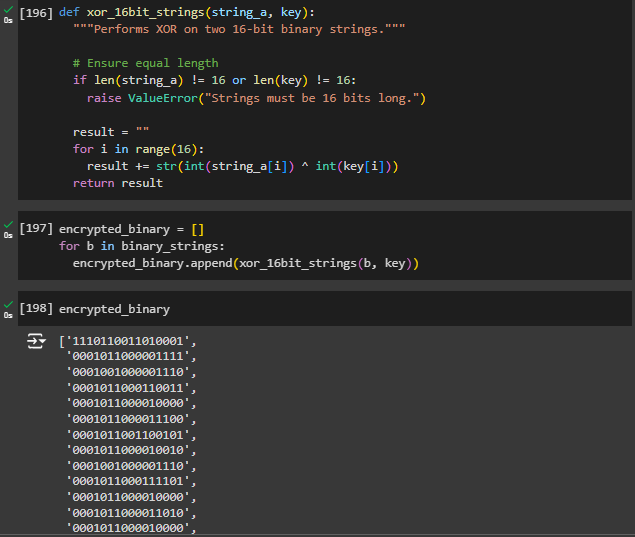


Рис. 4: Зашифрованный текст

Здесь у нас дешифрованный текст в двойчном представлении. (рис. 5).

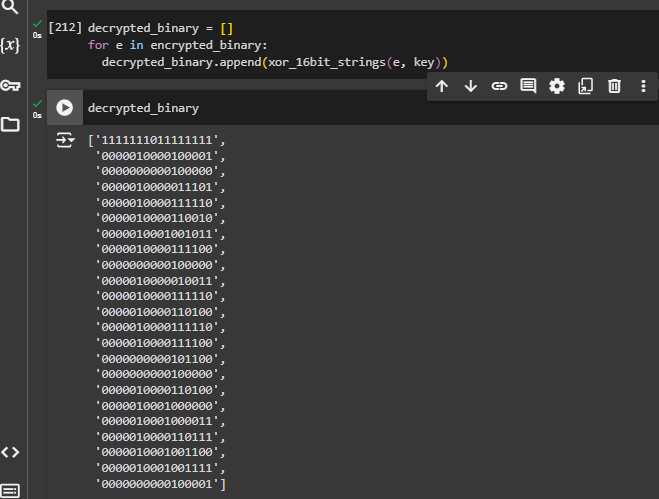


Рис. 5: Дешифрованный текст в двойчом представлении

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

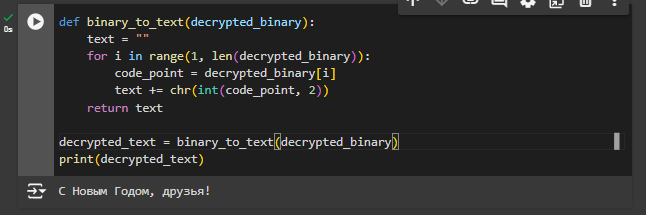


Рис. 6: дешифрованный текст

Мы исползуем другой ключ для дешифрования (рис. 7).

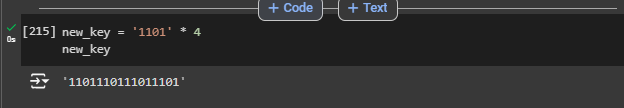


Рис. 7: Новый Ключ

Здесь мы получили неправилное сообщение исползуя другой ключ для дешифрования (рис. 8).

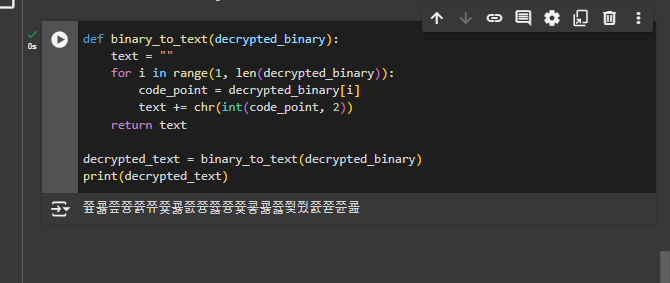


Рис. 8: Неправилное сообщение

# 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.