Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Татьяна Александровна Буллер

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Выполнение лабораторной работы

## 2.1 Определение кодировки шифротекста

Сообщение “D8 F2 E8 F0 EB E8 F6 20 2D 20 C2 FB 20 C3 E5 F0 EE E9 21 21” написано на русском языке, однако при переводе его из hex в текст стандартных кодировок ASCII/UTF-8 результат не совпадал с тем, какой был задан условием задания. Путем перебора кодировок было выяснено, что сообщение было написано в кодировке Windows-1251.

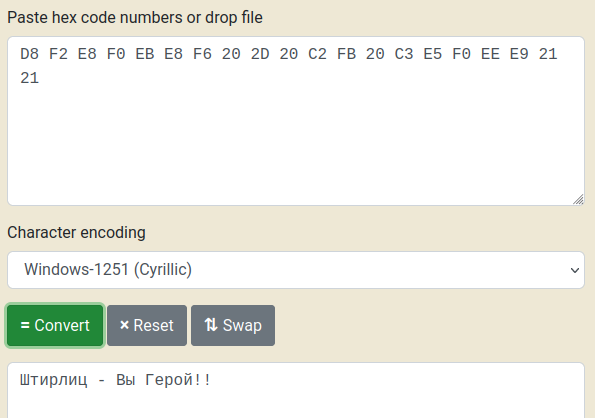


Рис. 1: Кодировка файла

## 2.2 Программа дешифрования по известному открытому тексту

Далее необходимо было написать код, с помощью которого можно было бы дешифровать сообщение. Метод шифрования XOR крайне уязвим к атакам по известному открытому тексту, поэтому, зная сообщение на выходе, мы без труда можем получить ключ, которым нужно было зашифровать строку, чтобы его получить. Для этого нужно обернуть операцию. Переведем известные нам строки шифра и открытого текста (“С Новым Годом, друзья!” в кодировке Windows-1251) в hex. Для того, чтобы далее провести с ними операции XOR, нужно перевести эти строки далее в бинарный формат. После сравним строки посимвольно и запишем результат: если символ в позиции n строки А совпадает с символом в той же позиции в строке Б, то в результат дописывается 0, иначе - 1. Необходимо отметить, что для корректной работы кода и получения полного ключа строки должны совпадать по длине. В случае, если какая-то из них короче другой, она повторяется до того, как длины совпадут.

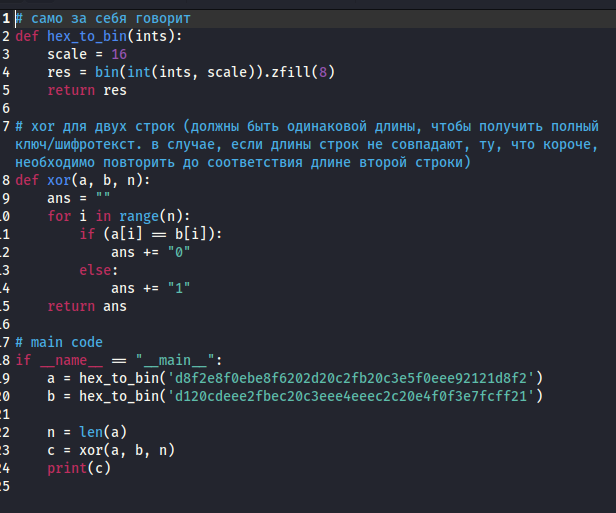


Рис. 2: Код программы

Программа выдает ключ в формате двоичного числа, который при необходимости далее можно перевести в шестнадцатиричный формат. Использовав полученный ключ вместо шифротекста, мы получим другой двоичный вывод. Переведя его в текст и расшифровав в кодировке Windows-1251 получим сообщение, ключ к которому и хотели найти, что говорит о том, что код сработал корректно.

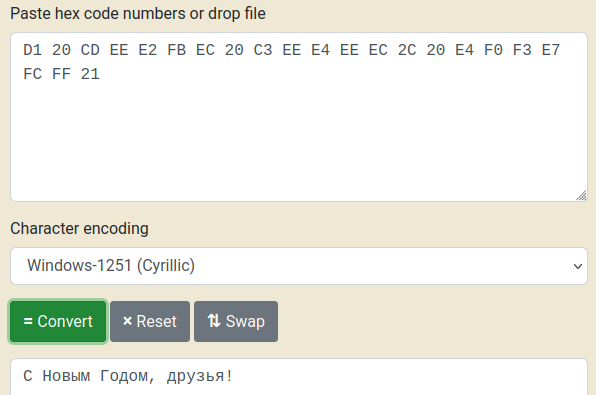


Рис. 3: Расшифровка полученного с новым ключом сообщения

# 3 Выводы

Было освоено на практике применение режима однократного гаммирования, написана программа, переводящая строки из шестнадцатиричного формата в двочиный и проводящая между ними XOR-операцию посимвольно.