Информационная безопасность. Отчет по лабораторной работе № 3

Шифрование гаммированием

Мухамеджанов Исматулло Иззатуллоевич

Содержание

# 1 Цель работы

Освоить на практике применение шифрование гаммирование [1].

# 2 Указание к работе

Шифрование Гаммированием

# 3 Выполнение лабораторной работы

1. Из всех схем шифрования простейшей и наиболее надежной является схема однократного использования (рис. 1). Формируется m- разрядная случайная двоичная последовательность — ключ шифра. Отправитесь производит побитовое сложение по модулю два (mod 2) ключа k - k1k2..ki…km и m- разрядной двоичной последовательности Р — P1P2..Pi…Рm соответствующей посылаемому сообщению:

сi = рi ⊕ ki;, i = 1, m, где р; — i-й бит исходного текста, k; — i-й бит ключа, — операция побитового сложения (XOR), с; — i-и 6m получившейся криптограммы с = c1c2 … сi … сm.

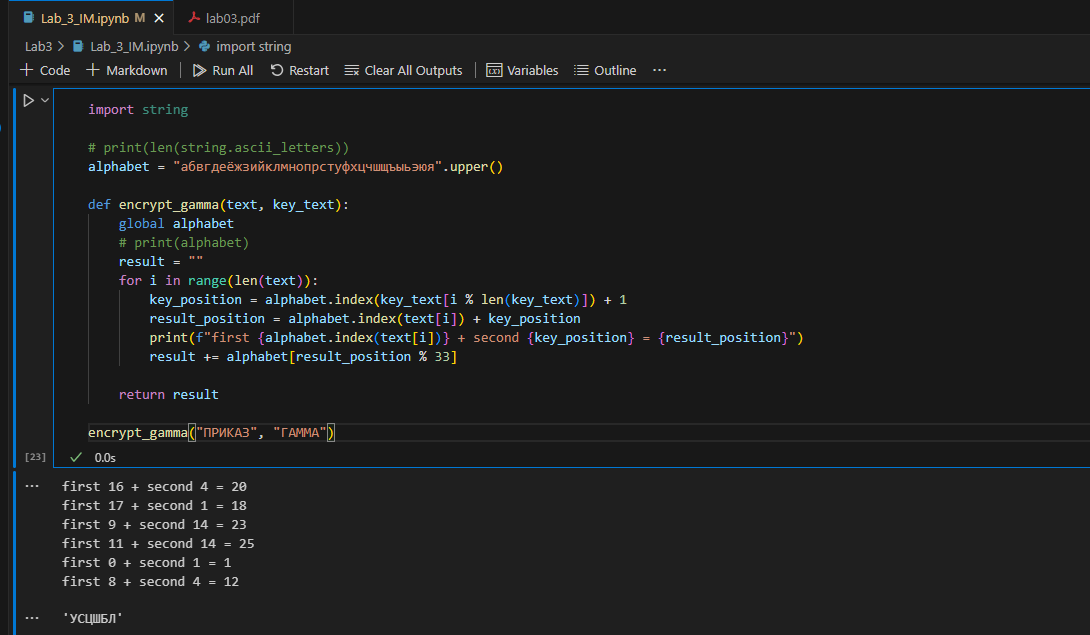


Figure 1: Программа (1)

# 4 Выводы

Освоены шифры методом гаммирования

# 5 Список литературы

1. Методические материалы курса