Отчёт по лабораторной работе №8
Дисциплина: Информационная безопасность
Тема: Элементы криптографии. Шифрование различных исходных текстов одним ключом

Студент: Олейников Артём Игоревич
Группа: НБИбд-01-23

Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Описание процесса выполнения задания

Этап 1. Реализация однократного гаммирования

Описание действия:
Создано приложение на Python, реализующее шифрование и дешифрование с помощью операции XOR (гаммирования) между текстом и ключом.

Используемая команда:

python otp_lab8.py

Результат выполнения (вывод в консоль):

```
perl
P1: НаВашисходящийот1204
P2: ВСеверныйфилиалБанка
Key (hex): 050C177F0E4E37D29410092E2257FFC80BB27054

Ciphertext C1 (hex): 9D 8F 9E DC 6E 2B 24 BB FE 64 7E 5D 42
63 D1 A0 90 84 14 20
Ciphertext C2 (hex): BF A9 B3 BA 59 49 57 DD 8A 44 77 75 66
34 B6 89 EB 82 3B 74

C1 XOR C2 (P1 ⊕ P2) (hex): 22 26 2D 66 37 62 73 66 74 20 09
28 24 57 67 29 7B 06 2F 54
P1 XOR P2 (ASCII): "&#-f7bsft \t($Wg){./T
```

Примечание: Расшифровка возможна при знании одной из исходных строк. Предполагается, что P1 может быть известным шаблоном, что позволяет частично восстановить P2.

Выводы

В ходе лабораторной работы были реализованы основные принципы однократного гаммирования. На практике показано, что при использовании одного ключа для двух

различных сообщений возможно частичное восстановление второго текста без знания ключа. Это подтверждает теоретическую уязвимость метода при нарушении условия однократности использования ключа. Метод однократного гаммирования обеспечивает абсолютную стойкость только при строгом соблюдении условий: случайный ключ, равная длина и однократное использование.