

Шифр гаммирования

Джафер Идрисов

29 апреля, 2025, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

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

Выполнение лабораторной работы

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$$C_1 = P_1 \oplus K$$

$$C_2 = P_2 \oplus K$$

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR получаем:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2$$

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар $C_1 \oplus C_2$ (известен вид обеих шифровок). Тогда зная P_1 имеем:

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2$$

Схема работы алгоритма



Рис. 1: Работа алгоритма гаммирования

Пример работы программы

```
13
14 def vzlom(P1, P2):
15     code = []
16     for i in range(len(P1)):
17         code.append(liters[(liters.index(P1[i]) + liters.index(P2[i])) % len(liters)])
18     print(code)
19     pr = "".join(code)
20     print(pr)
```

In [11]: 1 len(P1)

Out[11]: 13

In [12]: 1 len(P2)

Out[12]: 13

In [13]: 1 vzlom(P1, P2)

['х', 'у', 'л', 'ь', 'з', 'а', 'ж', 'б', 'ю', 'с', 'щ', 'ь', 'щ']
хульЗаЖбЮсЩьщ

Рис. 2: Работа алгоритма взлома ключа

In [24]: 1 P1 = "КодофаяФраза1"
2 gamma = "хульЗаЖбЮсЩьщ"

In [25]: 1 shifr(P1, gamma)

Исходный текст: [44, 16, 5, 16, 22, 1, 32, 54, 18, 1, 0, 1, 66]

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения лабораторной работы было разработано приложение, позволяющее шифровать тексты в режиме однократного гаммирования.