Шифр гаммирования

Ласурия Данил

29 октября, 2022, 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

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.

Алгоритм взлома

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

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

Алгоритм взлома

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:

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

Алгоритм взлома

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:

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

Пример работы программы

```
vzlom(P1, P2)

['9', 'р', 'я', 'т', 'Ъ', 'р', 'Й', 'н', 'к', 'е']
9рятЪрЙнке
```

Figure 1: Работа алгоритма взлома ключа

```
Введите гамму 9рятЪрЙнке
Числа текста [46, 6, 4, 1, 44, 18, 10, 15, 4, 6]
числа гаммы [74, 18, 32, 20, 60, 18, 43, 15, 12, 6]
45
29
Числа зашифрованного текста [45, 24, 36, 21, 29, 36, 53, 30, 16, 12]
Зашифрованный текст:  ЛцГуыГУьок
Расшифрованный текст МегаКринге
```

Figure 2: Работа алгоритма шифрования и дешивровки

Выводы

Результаты выполнения лабораторной работы

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