Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом.

Алхимова Дарья Сергеевна НБИ-01-19[1]

25 октября, 2022

[1]Российский Университет Дружбы Народов

Информация

Докладчик

- Алхимова Дарья Сергеевна
- студентка 4 курса
- группы НБИбд-01-19
- Российский университет дружбы народов
- 1032191645@rudn.ru

Цель работы

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

Теоретическое введение

Определение гаммирования

Гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, вос- пользовавшись таблицей ASCII-кодов.

Алгоритм взлома

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:

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

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:

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

Таким образом, злоумышленник получает возможность определить те символы сообщения P_2, которые находятся на позициях известного шаблона сообщения P_1.

Выполнение лабораторной работы

Запуск программы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе.

```
[dsalkhimova@dsalkhimova ~]$ javac lab8.java
[dsalkhimova@dsalkhimova ~]$ java lab8
введите '1' если хотите определить шифротекст по ключу и открытому тексту
 или '3' если хотите определить открытый текст по шифротексту:
3
введите первый шифротекст(через пробелы) :
AA BB CC
введите второй шифротекст(через пробелы) :
12 34 56
введите открытый текст одного из сообщений для расшифровки открытого текста второго сообщения:
Hello, I'm Dasha!
открытый текст второго сообщения: ðêö
[dsalkhimova@dsalkhimova ~]$
```

Рис. 1: Запуск программы

Вывод

В процессе выполнения данной лабораторной работы я приобрела навыки применения режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.