

Шифр гаммирования

Нгуен Чау Ки Ань НБИбд-01-18

18 декабря, 2021, 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:

$$1 = 1 \oplus$$

$$2 = 2 \oplus$$

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:

$$1 \oplus 2 = 1 \oplus \quad \oplus 2 \oplus = 1 \oplus 2$$

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 $1 \oplus 2$ (известен вид обеих шифровок). Тогда зная 1 имеем:

$$1 \oplus 2 \oplus 1 = 1 \oplus 2 \oplus 1 = 2$$

Схема работы алгоритма

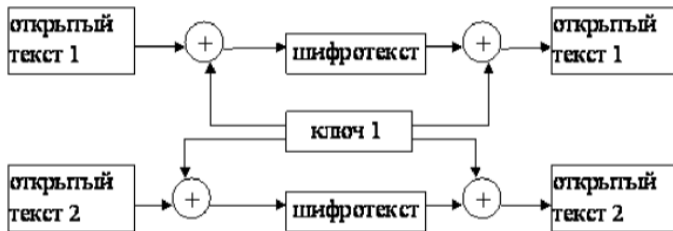


Figure 1: Работа алгоритма гаммирования

Пример работы программы

```
C:\>java Shifrovka
введите '1' если хотите определить шифротекст по ключу и открытому тексту
или '2' если хотите определить открытый текст по шифротексту:
2
введите первый шифротекст(через пробелы) :
AC 34 BC 43 21 2E
введите второй шифротекст(через пробелы) :
B2 37 CA 15 68 90
введите открытый текст одного из сообщений для того чтобы расшифровать открытый текст второго сообщения:
rudnforever
открытый текст второго сообщения: 1v08/?
```

Figure 2: Работа алгоритма взлома ключа

Выводы

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