

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

Шемякин Алексей НФИбд-02-18

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:

$$C_1 = P_1 \oplus K$$

$$C_2 = P_2 \oplus K$$

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



Figure 1: Работа алгоритма гаммирования

Пример работы программы

```
"C:\Program Files\Java\jdk-11.0.11\bin\java.exe" "-javaagent:C:\Program Files\JetBrains\IntelliJ IDEA 2020.  
Введите:  
'1' если хотите определить шифротекст по ключу и открытому тексту  
'2' если хотите определить ключ по открытому тексту и 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:  
HappyNewYearMyFriends  
открытый текст второго сообщения: Vb0&0&
```

Figure 2: Работа алгоритма взлома ключа

Выводы

Результаты выполнения лабораторной работы

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