Шифр гаммирования

Альсид Мона НФИбд-03-18[1]

18 декабря 2021 г. Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

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

Выполнения 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:

$$C1 = P1 \oplus K$$
$$C2 = P2 \oplus$$

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:

$$C1 \oplus C2 = P1 \oplus K \oplus P2 \oplus K = P1 \oplus P2$$

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 $C1 \oplus C2$ (известен вид обеих шифровок). Тогда зная $P1$ имеем:

$$C1 \oplus C2 \oplus P1 = P1 \oplus P2 \oplus P1 = P2$$

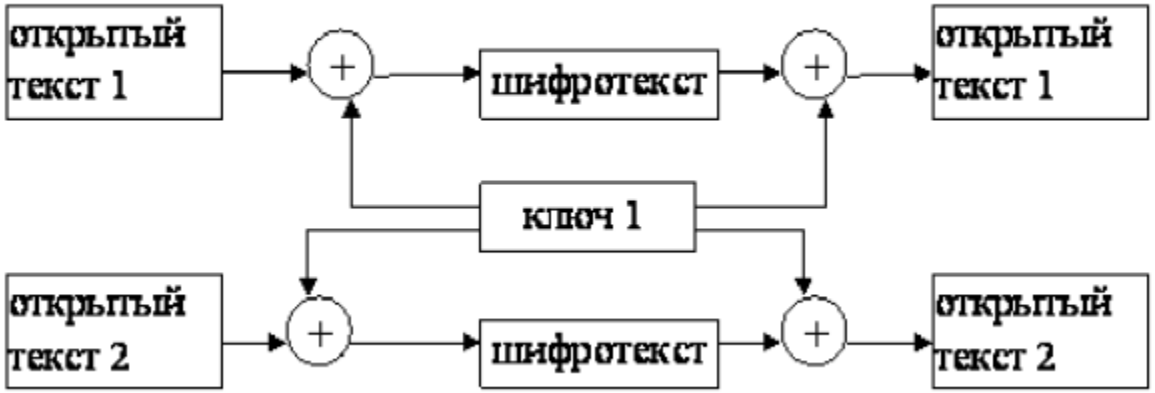

Figure 1: Работа алгоритма гаммирования

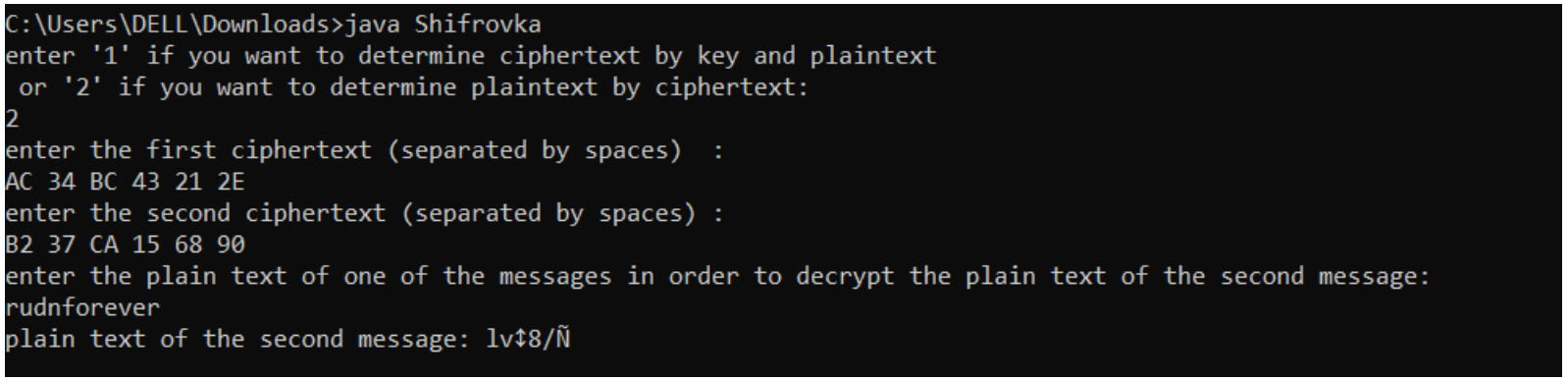

Figure 2: Работа алгоритма взлома ключа

Выводы

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