Математические основы защиты информации и информационной безопасности. Лабораторная работа №3. Шифрование гаммированием

Лесков Данила Валерьевич, учебная группа: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич

20 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Ознакомиться с шифрованием гаммированием на примере гаммирования конечной гаммой.

Задачи лабораторной работы

Реализовать алгоритм шифрования гаммированием конечной гаммой.

Выполнение лабораторной работы

Гаммирование

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст.

Шифрование гаммированием

При шифровании гаммированием формируется `m` - разрядная случайная последовательность. Пусть `k` - передаваемое сообщение

$$k = k_1 k_2 ... k_i ... k_m,$$

а `p` - последовательность, которая является ключом:

$$p = p_1 p_2 ... p_i ... p_m,$$

тогда `i`-ый символ криптограммы будет равен:

$$c_i = p_i \oplus k_i,$$

где $\oplus$ - операция побитового сложения XOR. В результате криптограмму можно записать следующим образом:

$$c = c_1 c_2 ... c_i ... c_m$$

Описание реализации метода шифрования

Для того, чтобы применить операцию побитового сложения, необходимо, чтобы ключ и исходное сообщение были одной длины. Для достижения данной цели, ключ растягивается до тех пор, пока не сравняется длиной с исходным сообщением следующим образом: пусть сообщение будет

$$SECURITY,$$

длина ‘m’ которого равна 12, тогда ключ растягивается следующим образом:

$$KEY \rightarrow KEYKEYKE$$

Таким образом, к сообщению и ключу одинаковой длины можно применить операцию побитового сложения XOR.

Полученные результаты

Полученные результаты

```
Введите сообщение: шифрование гаммированием
Введите ключ (гамма): безопасность

Преобразование БЕЗОПАСНОСТЬ -> БЕЗОПАСНОСТЬБЕЗОПАСНОСТЬ

Ваше сообщение:
ШИФРОВАНИЕ ГАММИРОВАНИЕМ ([26, 10, 22, 18, 16, 3, 1, 15, 10, 6, 10020, 4, 1, 14, 14, 10, 18, 16, 3, 1, 15, 10, 6, 14])

Ваша гамма:
БЕЗОПАСНОСТЬ ([2, 6, 9, 16, 17, 1, 19, 15, 16, 19, 20, 30, 2, 6, 9, 16, 17, 1, 19, 15, 16, 19, 20, 30])

Зашифрованное сообщение:
ЪОЭАЯГТЬШЧ АВТКШБПФОЭЫШЙ ([28, 16, 31, 1, 0, 4, 20, 30, 26, 25, 10020, 1, 3, 20, 23, 26, 2, 17, 22, 16, 31, 29, 26, 11])

Process finished with exit code 0
```

Figure 1: Результаты шифрования гаммированием

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения данной лабораторной работы было выполнено ознакомление с шифрованием гаммированием на примере шифрования гаммированием с конечной гаммой.
В результате был программно реализован этот метод шифрования.