

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

Масолова Анна Олеговна, 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.

Реализовать алгоритм шифрования гаммированием конечной гаммой.

Выполнение лабораторной работы

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

$$k = k_1 k_2 \dots k_i \dots k_m,$$

а p - последовательность, которая является ключом:

$$p = p_1 p_2 \dots p_i \dots p_m,$$

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:

$$c = c_1 c_2 \dots c_i \dots c_m$$

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 → KEYKEYKE

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

Полученные результаты

Полученные результаты

Введите сообщение: информационная безопасность

Введите ключ (гамма): криптография

Преобразование КРИПТОГРАФИЯ -> КРИПТОГРАФИЯКРИПТОГРАФИЯКРИ

Ваше сообщение:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ([10, 15, 22, 16, 18, 14, 1, 24, 10, 16, 15, 15, 1, 33, 10022, 2, 6, 9, 16, 17, 1, 19, 15, 16, 19, 20, 30])

Ваша гамма:

КРИПТОГРАФИЯ ([12, 18, 10, 17, 20, 16, 4, 18, 1, 22, 10, 33, 12, 18, 10, 17, 20, 16, 4, 18, 1, 22, 10, 33, 12, 18, 10])

Зашифрованное сообщение:

ФЯЮЯДЬДЗЙДЧНЛР СЧТББЖЧОЭДЁ ([22, 0, 32, 0, 5, 30, 5, 9, 11, 5, 25, 15, 13, 18, 10022, 19, 26, 25, 20, 2, 2, 8, 25, 16, 31, 5, 7])

Figure 1: Результаты шифрования гаммированием

Выводы

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.