Отчёт по лабораторной работе

Лабораторная работа 8

Дзугаева Лилия Владиславовна

Table of Contents

## Цель работы

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

## Выполнение лабораторной работы

1. Генерируем случайный ключ, соответствующий длине текста, который мы хотим кодировать. Вводим два сообщения. Применяя алгоритм, указанный в условии лабораторной работы, получаем, что можем расшифровать сообщения. Т.е. если злоумышленник знает одно из закодированных сообщений по одному ключу, то он сможет расшифровать и (уменьшить область поиска) другие сообщения, закодированные по тому же ключу.



рис. 1.

1. Ответы на контрольные вопросы:
   1. *Как, зная один из текстов, определить другой, не зная при этом ключа?* С помощью формул режима однократного гаммирования получим шифротексты обеих телеграмм: C\_1 = P\_1 ⊕ К C\_2 = P\_2 ⊕ К. Задача нахождения открытого текста по известному шифротексту двух телеграмм, зашифрованных одним ключом, может быть решена. Складываем по модулю 2 (XOR) (обозначается знаком ) оба равенства и получаем: C\_1 ⊕ C\_2 = P\_1 ⊕ К ⊕ P\_2 ⊕ К = P\_1 ⊕ P\_2. Если один из текстов известен — т.е. имеет фиксированный формат, в который вписываются значения полей, и нам известен этот формат, то тогда получим достаточно много пар C\_1 ⊕ C\_2 (известен вид обеих шифровок). Далее зная P\_1 и учитывая свойство операции XOR, имеем: C\_1 ⊕ C\_2 ⊕ P\_1 = P\_1 ⊕ P\_2 ⊕ P\_1 = P\_2. Таким образом, получаем возможность определить те символы сообщения P\_2, которые находятся на позициях известного шаблона сообщения P\_1. В соответствии с логикой сообщения P\_2, у нас есть реальный шанс узнать ещё некоторое количество символов сообщения P\_2. Затем вновь используем предыдущее равенство с подстановкой вместо P\_1 полученных на предыдущем шаге новых символов сообщения P\_2. И так далее. Действуя подобным образом, даже если не прочитаем оба сообщения, то значительно уменьшим пространство их поиска.
   2. *Что будет при повторном использовании ключа при шифровании текста?* Если на сообщение наложить ключ дважды, мы получим исходное сообщение.
   3. *Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?* Один ключ накладываем на оба открытых текста и получаем два зашифрованных одним ключом шифротекста.
   4. *Перечислите недостатки шифрования одним ключом двух открытых текстов.* При условии, что злоумышленник знает о том, что ключ шифрования един и он получил одну из пар текстов (зашифрованный текст и открытый), то он может найти ключ (см. вопрос 1) и расшифровать остальные тексты.
   5. *Перечислите преимущества шифрования одним ключом двух открытых текстов.* Это позволяет упростить разработку шифровальных и дешифровальных систем. Если мы реализуем обмен, например, между двумя компьютерами, то удобно использовать единый ключ для всех данных.

## Выводы

В ходе выполнения лабораторной работы я изучил теорию и освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы