Отчёт по лабораторной работе 8

Макухина Анастасия Вадимовна

Содержание

Цель работы

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

Выполнение лабораторной работы

Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе.

1. Создадим код, генерирующий ключи.

Рисунок 1.

2. Создадим приложение

Рисунок 2.

3. Проведём проверки.

Рисунок 3.

4. Определим и выразим аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

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 ⊕ C2 (известен вид обеих шифровок). Тогда зная P1 и учитывая (8.2), имеем:

C1 ⊕ C2 ⊕ P1 = P1 ⊕ P2 ⊕ P1 = P2. (8.3)

Таким образом, злоумышленник получает возможность определить те символы сообщения P2, которые находятся на позициях известного шаблона сообщения P1. В

соответствии с логикой сообщения P2, злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения P2. Затем вновь используется (8.3) с подстановкой вместо P1 полученных на предыдущем шаге новых символов сообщения P2. И так далее. Действуя подобным образом, злоумышленник даже если не прочитает обасообщения, то значительно уменьшит пространство их поиска.

Ответы на контрольные вопросы:

1. *Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?*

Надо сложить между собой по модулю 2 шифры и известный текст, то есть C1, C2 и P1 (допустим он известен).

2. *Что будет при повторном использовании ключа при шифровании текста?*

Риск расшифровки сообщений злоумышленником повысится.

3. *Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?.*

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

$C1 = P1 \oplus K$,

$C2 = P2 \oplus K$.

4. *Перечислите недостатки шифрования одним ключом двух открытых текстов.*

- снижение уровня защиты информации

5. *Перечислите преимущества шифрования одним ключом двух открытых текстов.*

- нужно хранить меньше ключей

Выводы

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