Отчёт по лабораторной работе 7

Макухина Анастасия Вадимовна

Содержание

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!».
Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

- Определить вид шифротекста при известном ключе и известном открытом тексте.
- Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

1. Создадим код, генерирующий ключи.

Рисунок 1.

2. Создадим приложение, которое определяет

- вид шифротекста при известном ключе и известном открытом тексте;
- ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста

Рисунок 2.

3. Проведём проверки.

Рисунок 3.

Ответы на контрольные вопросы:

1. *Поясните смысл однократного гаммирования.*

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Однократное гаммирование – это когда каждый символ попарно с символом ключа складываются по модулю 2 (XOR).

2. *Перечислите недостатки однократного гаммирования.*

Размер ключевого материала должен совпадать с размером передаваемых сообщений. Также необходимо иметь эффективные процедуры для выработки случайных равновероятных двоичных последовательностей и специальную службу для развоза огромного количества ключей. А ещё, если одну и ту же гамму использовать дважды для разных сообщений, то шифр из совершенно стойкого превращается в «совершенно нестойкий» и допускает дешифрование практически вручную.

3. *Перечислите преимущества однократного гаммирования.*

С точки зрения теории криптоанализа метод шифрования случайной однократной равновероятной гаммой той же длины, что и открытый текст, является невскрываемым. Кроме того, даже раскрыв часть сообщения, дешифровщик не сможет хоть сколько-нибудь поправить положение - информация о вскрытом участке гаммы не дает информации об остальных ее частях. К достоинствам также можно отнести простоту реализации и удобство применения.

4. *Почему длина открытого текста должна совпадать с длиной ключа?*

Потому что каждый символ открытого текста должен складываться с символом ключа попарно.

5. *Какая операция используется в режиме однократного гаммирования, назовите её особенности?*

В режиме однократного гаммирования используется сложение по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Особенность заключается в том, что этот алгоритм шифрования является симметричным. Поскольку двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, шифрование и расшифрование выполняется одной и той же программой.

6. *Как по открытому тексту и ключу получить шифротекст?*

Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста сложения по модулю 2 (XOR). Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины.

7. *Как по открытому тексту и шифротексту получить ключ?*

Если известны шифротекст и открытый текст, то задача нахождения ключа решается также сложением по модулю 2.

8. *В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра?*

Необходимые и достаточные условия абсолютной стойкости шифра:

- Полная случайность ключа;
- Равенство длин ключа и открытого текста;
- Однократное использование ключа.

Выводы

В ходе выполнения лабораторной работы я изучила теорию и освоила на практике применение режима однократного гаммирования.