Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Аскеров Александр Эдуардович

Содержание

Список иллюстраций

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 Теоретическое введение

2.1 Шифр гаммирования

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

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы шифра на открытые данные обратимым образом (например, используя операцию сложения по модулю 2). Процесс дешифрования сводится к повторной генерации гаммы шифра при известном ключе и наложении такой же гаммы на зашифрованные данные. Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей и изменяется случайным образом для каждого шифруемого слова. Если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (подбором ключа). В этом случае криптостойкость определяется размером ключа.

Метод гаммирования становится бессильным, если известен фрагмент исходного текста и соответствующая ему шифрограмма. В этом случае простым вычитанием по модулю 2 получается отрезок псевдослучайной последовательности и по нему восстанавливается вся эта последовательность.

Метод гаммирования с обратной связью заключается в том, что для получения сегмента гаммы используется контрольная сумма определенного участка шифруемых данных. Например, если рассматривать гамму шифра как объединение непересекающихся множеств H(j), то процесс шифрования можно пердставить следующими шагами:

- Генерация сегмента гаммы H(1) и наложение его на соответствующий участок шифруемых данных.
- Подсчет контрольной суммы участка, соответствующего сегменту гаммы H(1).
- Генерация с учетом контрольной суммы уже зашифрованного участка данных следующего сегмента гамм H(2).
- Подсчет контрольной суммы участка данных, соответствующего сегменту данных H(2) и т.д.

3 Выполнение лабораторной работы

Приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования:

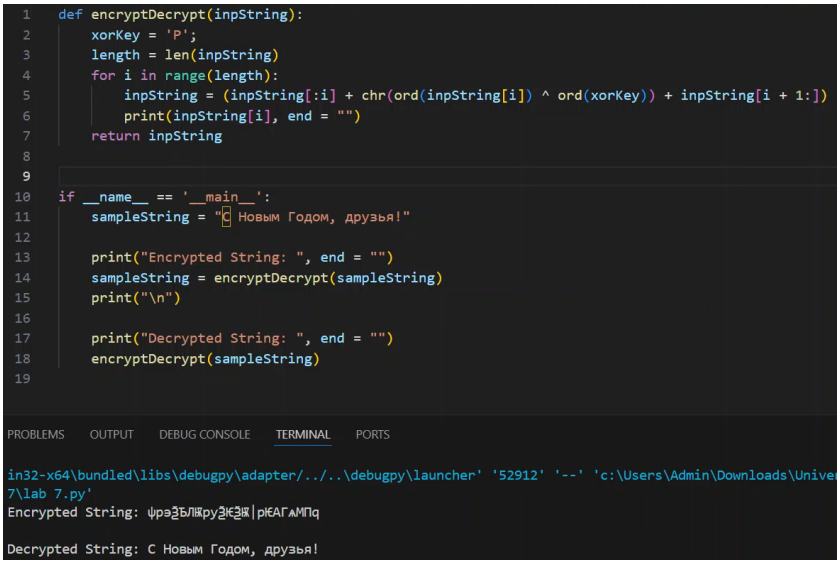

Рис. 3.1: Программа

4 Выводы

Применение режима однократного гаммирования освоено на практике.

5 Контрольные вопросы

1. Однократное гаммирование – это метод шифрования, при котором каждый символ открытого текста комбинируется с соответствующим символом ключа только один раз.

2. Недостатки однократного гаммирования:

- Уязвимость к атакам частотного анализа из-за повторяющихся шифротекстов.
- Необходимость генерации случайного ключа такой же длины, что и открытый текст.
- Один и тот же ключ не может использоваться повторно для шифрования других сообщений.

3. Преимущества однократного гаммирования:

- При правильной реализации обеспечивает абсолютную стойкость.
- Шифротекст не подвержен атакам, основанным на статистическом анализе.

4. Длина открытого текста должна совпадать с длиной ключа в однократном гаммировании, чтобы каждый символ открытого текста мог быть комбинирован с соответствующим символом ключа.

5. В режиме однократного гаммирования используется операция XOR (исключающее ИЛИ), которая комбинирует каждый бит открытого текста с соответствующим битом ключа. Особенностью XOR является то, что результат равен 1 только в случае, если входные биты различны.

6. Для получения шифротекста по открытому тексту и ключу необходимо применить операцию XOR между каждым символом открытого текста и соответствующим символом ключа.

7. Получение ключа по открытому тексту и шифротексту в случае однократного гаммирования невозможно без знания исходного ключа, так как операция XOR необратима.

8. Необходимые и достаточные условия абсолютной стойкости шифра включают в себя:

- Ключ должен быть случайным, длинным и использоваться только один раз.
- Ключ должен быть такой же длины, что и открытый текст.
- Ключ должен быть известен только отправителю и получателю сообщения.

Список литературы

1. XOR cypher