Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Аксёнова Алина Владимировна

Содержание

List of Figures

List of Tables

Цель работы

Освоить на практике применение режима однократного гаммирования

Задание

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

Теоретическое введение

С точки зрения теории криптоанализа, метод шифрования однократной случайной равновероятной гаммой той же длины, что и открытый текст, является невскрываемым (далее для краткости авторы будут употреблять термин “однократное гаммирование”, держа в уме все вышесказанное). Обоснование, которое привел Шеннон, основываясь на введенном им же понятии информации, не дает возможности усомниться в этом - из-за равных априорных вероятностей криптоаналитик не может сказать о дешифровке, верна она или нет. 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.

Ход работы

1. Импортируем все необходимые библиотеки и пишем функцию генерирования ключа, а также функцию гаммирования. (Рис. 0.1).

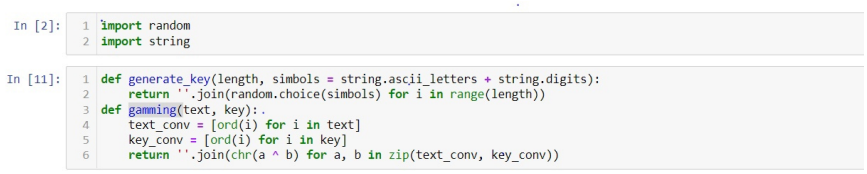

Figure 0.1: Импорт библиотек и написание функций

2. Определяем вид шифротекста при известном ключе и известном открытом тексте. (Рис. 0.2).

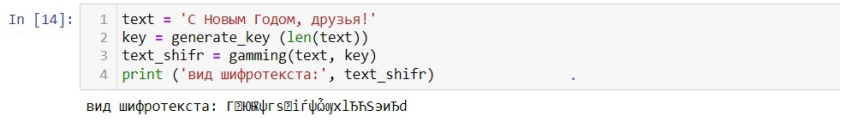

Figure 0.2: Шифрование открытого текста

3. Применяем функцию “gamming” к полученному шифру и ключу, чтобы провериьь правильность работы программы. В результате снова получаем исходный текст (Рис. 0.3).

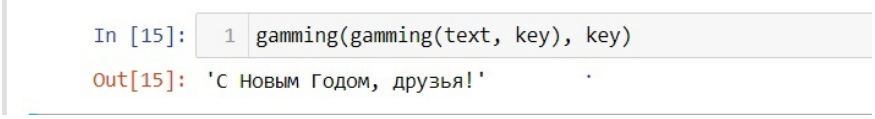

Figure 0.3: Проверка правильности работы кода

4. Определяем ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. (Рис. 0.4).

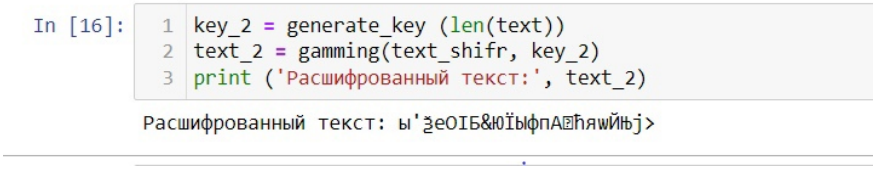

Figure 0.4: Расшифровка зашифрованного текста новым ключом

Ответы на котнрольные вопросы

1. 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) (обозначается знаком $\oplus$).

2. Недостатки: Размер ключевого материала должен совпадать с размером передаваемых сообщений. Кроме того, 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. Преимущества: 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. Потому что каждый символ открытого текста должен складываться с символом ключа попарно.

5. 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. Сложить по модулю 2 каждый символ открытого текста и ключа

7. Сложить по модулю 2 каждый символ открытого текста и шифротекста.

8. Необходимые и достаточные условия абсолютной стойкости шифра: Полная случайность ключа; Равенство длин ключа и открытого текста; Однократное использование ключа.

Выводы

В результате выполнения данной работы было освоено на практике применение режима однократного гаммирования

Библиографический список

1. Острейковский В. А. Информатика: учеб. для вузов / В. А. Острейковский. - 4-е изд., стер. - М.: Высш. шк., 2007. - 511 с.

2. Алексеев, М. Е. Шифрование методом гаммирования / М. Е. Алексеев // 70-я научно-техническая конференция учащихся, студентов и магистрантов, 15-20 апреля 2019 г., Минск : сборник научных работ : в 4 ч. Ч. 4. - Минск : БГТУ, 2019. - С. 398-401.

3. Прикладные задачи шифрования [Электронный ресурс]. – Режим доступа : http://citforum.ru/internet/securities/cryptobook07.shtml, свободный. – Загл. с экрана.

4. Шифры гаммирования [Электронный ресурс]. – Режим доступа : https://bstudy.net/825827/tehnika/shifry_gammirovaniya, свободный. – Загл. с экрана.