Лабораторная работа № 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Аксёнова Алина Владимировна

Содержание

List of Figures

List of Tables

Цель работы

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

Задание

Прочитать оба текста, не зная ключа и не стремясь его определить

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).

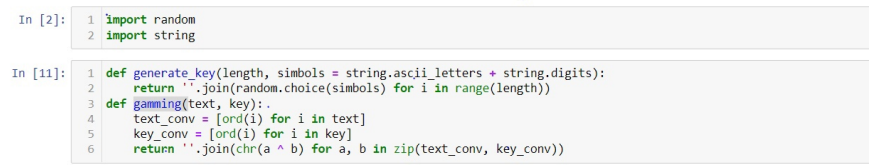

Figure 0.1: Импорт библиотек и написание функций

2. Генерируем случайный ключ, а затем определяем вид шифротекстов C1 и C2 при известном ключе и известном открытом тексте. (Рис. 0.2).

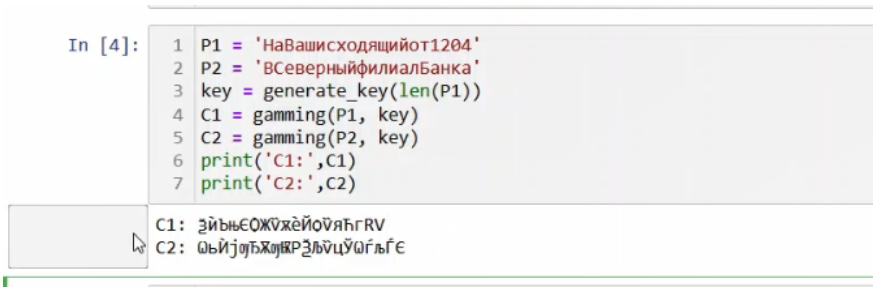

Figure 0.2: Шифрование открытого текста

3. Применяем функцию “gamming” к полученным шифрам, а затем еще и к одному из открытых текстов, чтобы получить другой, неизвестный открырй текст (Рис. 0.3).

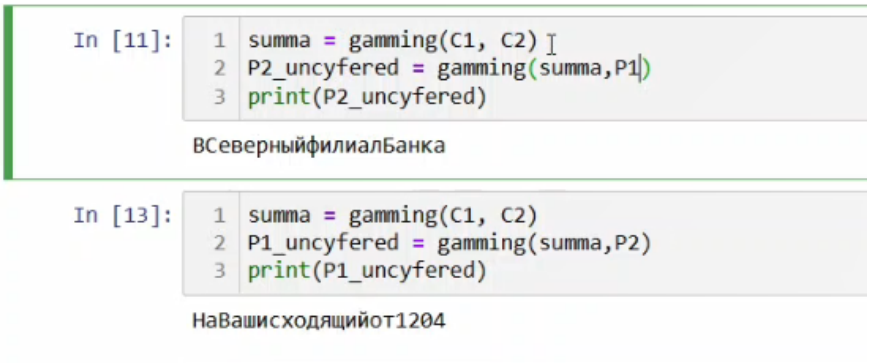

Figure 0.3: Определение открытых текстов

Ответы на котнрольные вопросы

1. Необходимо прогаммировать один шифротекст вторым, а после прогаммировать результат одним из исходных текстов. Таким образом мы получим другой исходный текст.

2. Мы из шифрованного текста обратно получим исходный нешифрованный..

3. Поочередно гаммируем каждый текст одним ключом.

4. Подверженность взлому, шифр становится абсолютно вскрываемым. При утечке же хотя бы части одного из исходных текстов злоумышленник сможет расшифровать все тексты.

5. Можно сократить издержки по доставке ключей сторонам, либо вообще исключить их, если ключ использовать все время.

Выводы

В результате выполнения данной работы было освоено на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом

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.