Информационная безопасность. Отчет по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Горбунова Ярослава Михайловна

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования [1].

# 2 Указание к работе

Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» (fig. 1) является простой, но надёжной схемой шифрования данных. Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования. В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊕) между элементами гаммы и элементами подлежащего сокрытию текста. Напомним, как работает операция XOR над битами: 0⊕0 = 0, 0⊕1 = 1, 1⊕0 = 1, 1⊕1 = 0. Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное

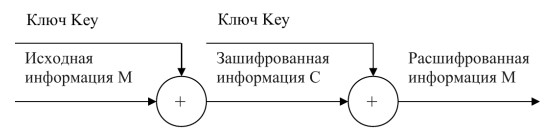


Figure 1: Схема однократного использования Вернама

значение, а шифрование и расшифрование выполняется одной и той же программой. Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста следующего правила (fig. 2):

Figure 2: Формула 7.1

Figure 2: Формула 7.1

где C\_i — i-й символ получившегося зашифрованного послания, P\_i — i-й символ открытого текста, K\_i — i-й символ ключа, i = 1, m. Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины. Если известны шифротекст и открытый текст, то задача нахождения ключа решается также в соответствии с (fig. 2), а именно, обе части равенства необходимо сложить по модулю 2 с P\_i (fig. 3):

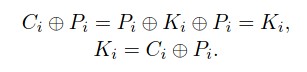


Figure 3: Формула 7.2

Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, воспользовавшись таблицей ASCII-кодов.

К. Шеннон доказал абсолютную стойкость шифра в случае, когда однократно используемый ключ, длиной, равной длине исходного сообщения, является фрагментом истинно случайной двоичной последовательности с равномерным законом распределения. Криптоалгоритм не даёт никакой информации об открытом тексте: при известном зашифрованном сообщении C все различные ключевые последовательности K возможны и равновероятны, а значит, возможны и любые сообщения P .

Необходимые и достаточные условия абсолютной стойкости шифра: – полная случайность ключа; – равенство длин ключа и открытого текста; – однократное использование ключа.

Рассмотрим пример.

Ключ Центра:

05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54

Сообщение Центра:

Штирлиц – Вы Герой!!

D8 F2 E8 F0 EB E8 F6 20 2D 20 C2 FB 20 C3 E5 F0 EE E9 21 21

Зашифрованный текст, находящийся у Мюллера:

DD FE FF 8F E5 A6 C1 F2 B9 30 CB D5 02 94 1A 38 E5 5B 51 75

Дешифровальщики попробовали ключ:

05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 55 F4 D3 07 BB BC 54

и получили текст:

D8 F2 E8 F0 EB E8 F6 20 2D 20 C2 FB 20 C1 EE EB E2 E0 ED 21

Штирлиц - Вы Болван!

Другие ключи дадут лишь новые фразы, пословицы, стихотворные строфы, словом, всевозможные тексты заданной длины.

# 3 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: 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.

Для выполнения работы была написана программа (fig. 4 - fig. 7) с помощью языка программирования С++, которая получает на вход открытый текст “Stirlis - Vy Geroy!!” и ключ “05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54”, затем шифрует открытый текст методом однократного гаммирования и получает шифротекст. После этого методом сложения по модулю 2 или дешифровки методом однократного гаммирования определяет ключ, с помощью которого из полученного шифротекста можно получить целевой фрагмент текста, указанный в задании, “S Novym Godom drysya” (в данном сообщении были убраны запятая и восклицательный знак, чтобы добиться одинаковой размерности открытого и целевого текста, также сообщения транскрипированы на латиницу).

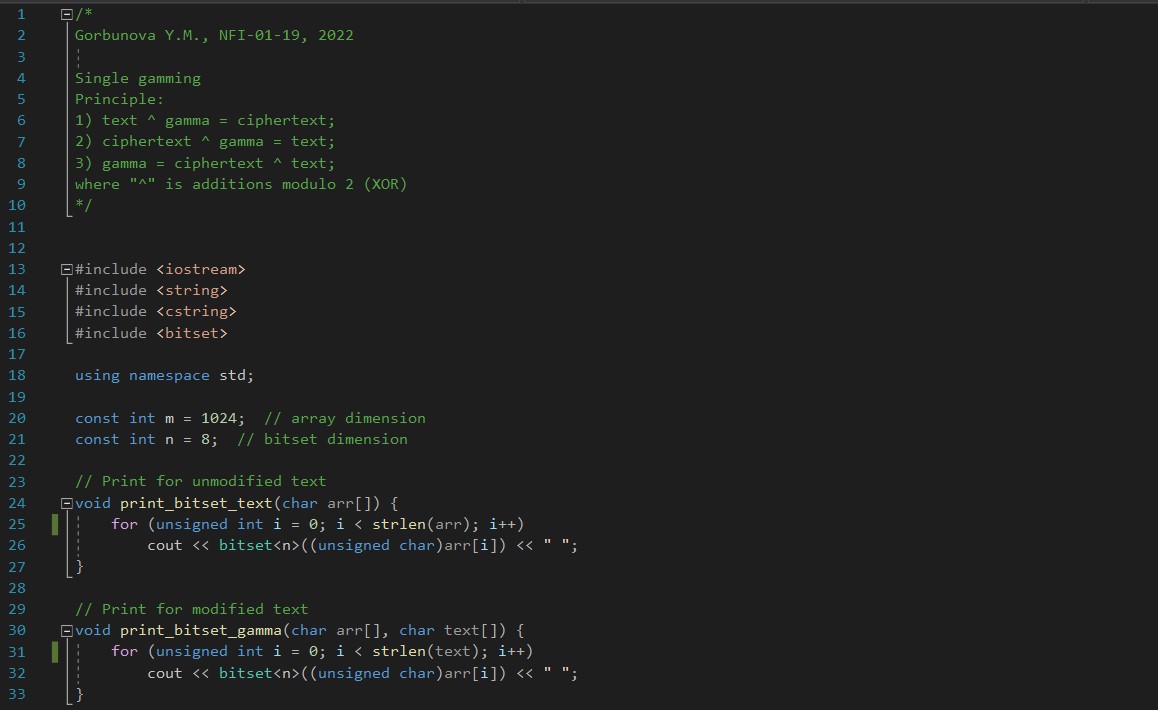


Figure 4: Программа (1)

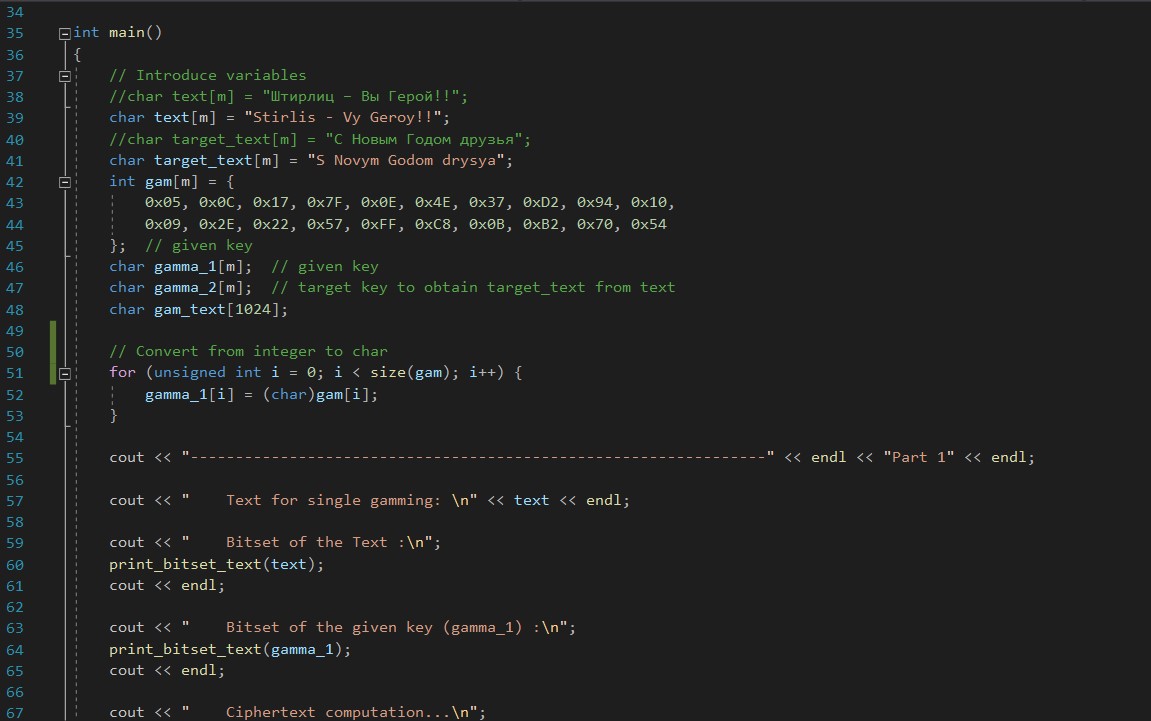


Figure 5: Программа (2)

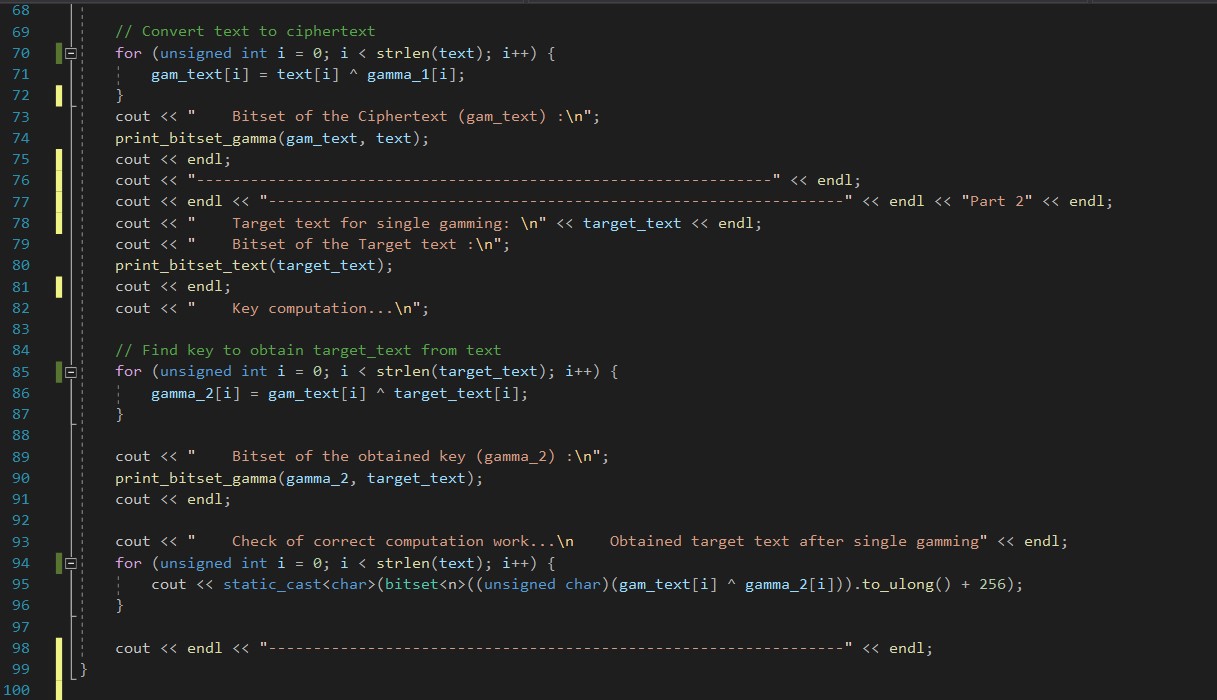


Figure 6: Программа (3)

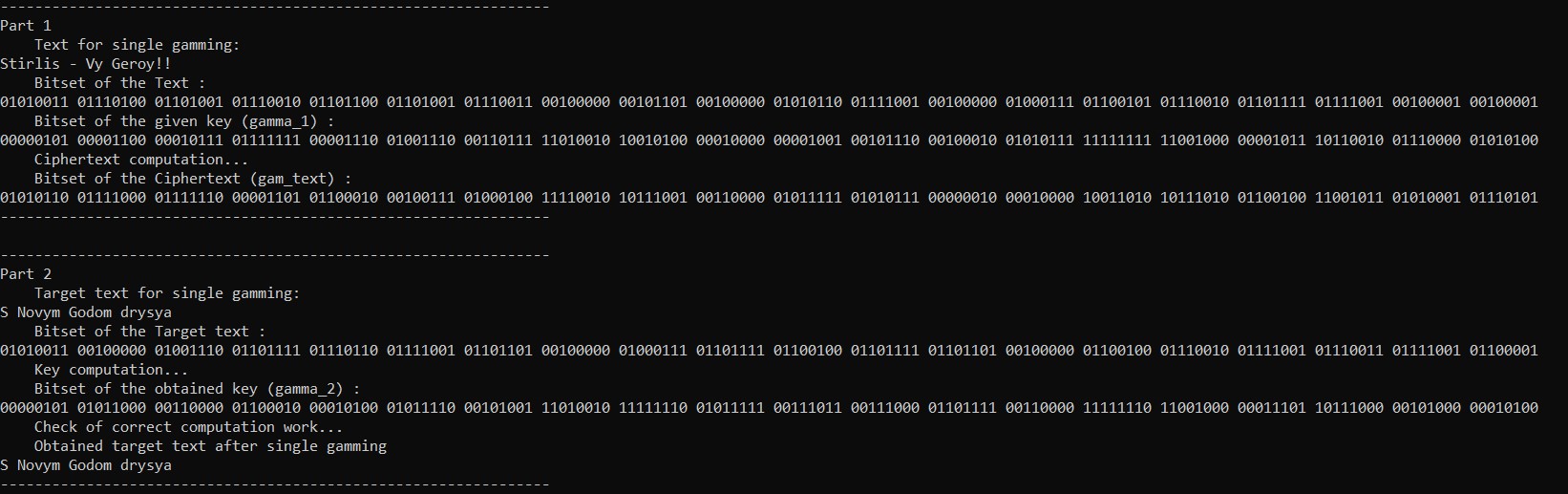


Figure 7: Вывод работы программы

## 3.1 Контрольные вопросы

1. Поясните смысл однократного гаммирования. – Дан открытый текст и ключ для шифрования открытого текста, с помощью клуча можно как шифровать открытый текст для получения шифротекста, так и дешифровать шифротекст для получения открытого текста.
2. Перечислите недостатки однократного гаммирования. – Необходимость иметь огромные объемы данных, которые можно было бы использовать в качестве гаммы.
3. Перечислите преимущества однократного гаммирования. – В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.
4. Почему длина открытого текста должна совпадать с длиной ключа? – Потому что в данном методе для каждого символа открытого текста предполагается символ ключа, наложение которорого приводит к шифровке символа открытого текста.
5. Какая операция используется в режиме однократного гаммирования, назовите её особенности? – Сложения по модулю 2 (XOR). Метод шифрования является симметричным, так как двойное при- бавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.
6. Как по открытому тексту и ключу получить шифротекст? – Шифротекст = открытый текст XOR ключ.
7. Как по открытому тексту и шифротексту получить ключ? – Ключ = открытый текст XOR шифротекст.
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.

# 4 Выводы

Освоено на практике применение режима однократного гаммирования.

# 5 Список литературы

1. Методические материалы курса