Информационная безопасность. Отчет по лабораторной работе № 8

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

Горбунова Ярослава Михайловна

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом [1].

# 2 Указание к работе

Исходные данные. Две телеграммы Центра:

P1 = НаВашисходящийот1204 P2 = ВСеверныйфилиалБанка

Ключ Центра длиной 20 байт:

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

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой, приведённой на fig. 1.

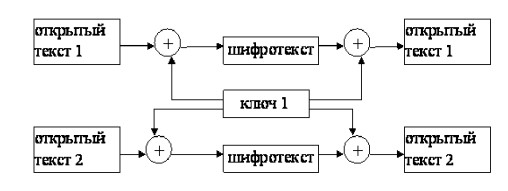


Figure 1: Общая схема шифрования двух различных текстов одним ключом

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

C1 = P1 ⊕ K, C2 = P2 ⊕ K. (8.1)

Открытый текст можно найти в соответствии с (8.1), зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства (8.1) складываются по модулю 2. Тогда с учётом свойства операции XOR

1⊕1 = 0, 1⊕0 = 1 (8.2)

получаем:

C1 ⊕C2 = P1 ⊕K ⊕P2 ⊕K = P1 ⊕P2.

Предположим, что одна из телеграмм является шаблоном — т.е. имеет текст фиксированный формат, в который вписываются значения полей. Допустим, что злоумышленнику этот формат известен. Тогда он получает достаточно много пар C1 ⊕C2 (известен вид обеих шифровок). Тогда зная P1 и учитывая (8.2), имеем:

C1 ⊕C2 ⊕P1 = P1 ⊕P2 ⊕P1 = P2. (8.3)

Таким образом, злоумышленник получает возможность определить те символы сообщения P2, которые находятся на позициях известного шаблона сообщения P1. В соответствии с логикой сообщения P2, злоумышленник имеет реальный шанс узнать ещё некоторое количество символов сообщения P2. Затем вновь используется (8.3) с подстановкой вместо P1 полученных на предыдущем шаге новых символов сообщения P2. И так далее. Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит пространство их поиска.

# 3 Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Для выполнения работы была написана программа (fig. 2 - fig. 6) с помощью языка программирования С++, которая получает на вход два открытых текста “NaVasishodysiyot1204”, “VSevernyifilialBanka” и ключ “05 0C 17 7F 0E 4E 37 D2 94 10 09 2E 22 57 FF C8 0B B2 70 54”, затем шифрует открытые тексты методом однократного гаммирования и получает два шифротекста. После этого предполагаем два случая. В первом неизвестен открытый текст 2, во втором - открытый текст 1. Методом сложения по модулю 2, однократного гаммирования, определяется открытый текст 2 и текст 1 для случаев соответственно. Определение открытых текстов происходит без ключа, не осуществляются попытки его определения.



Figure 2: Программа (1)



Figure 3: Программа (2)



Figure 4: Программа (3)

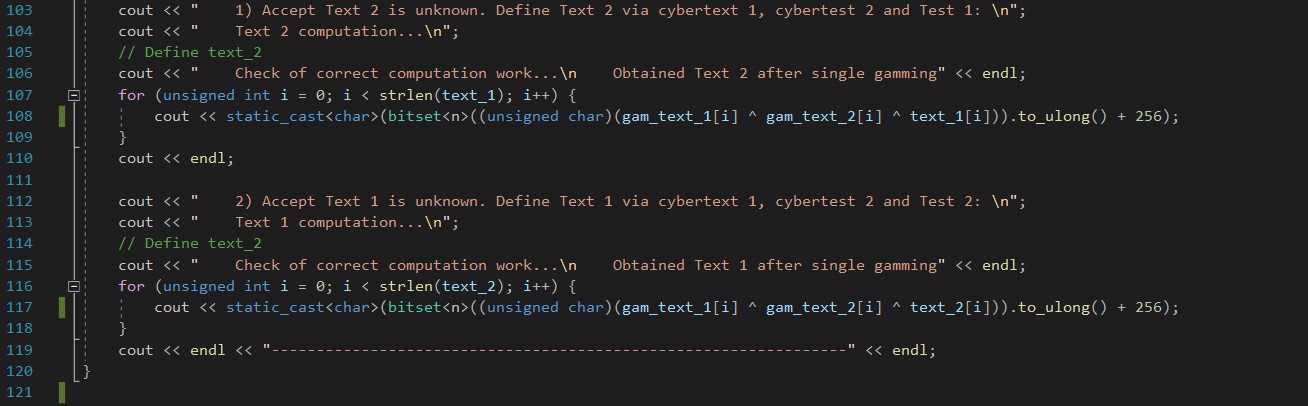


Figure 5: Программа (4)

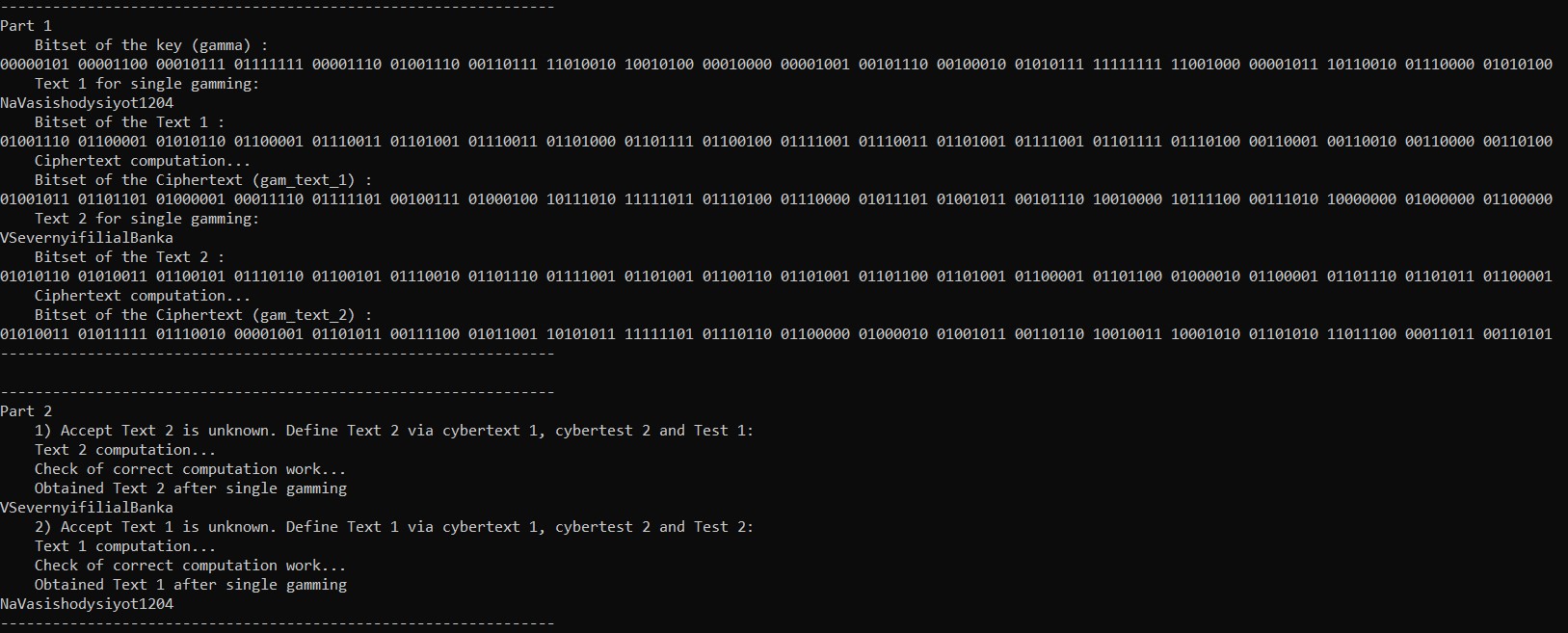


Figure 6: Вывод работы программы

## 3.1 Контрольные вопросы

1. Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа? – По формулам: C1 ⊕ C2 ⊕ P1 = P2, C1 ⊕C2 ⊕ P2 = P1.
2. Что будет при повторном использовании ключа при шифровании текста? – Расшифровка текста.
3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов? – Ключ применяется к каждому из текстов в отдельности, получаются два различных шифротекста.
4. Перечислите недостатки шифрования одним ключом двух открытых текстов. – При наличии минимум двух шифротекстов и хотябы одного открытого текста можно получить другой открытый текст даже не имея ключа.
5. Перечислите преимущества шифрования одним ключом двух открытых текстов. – Нет необходимости в хранении двух последовательностей символов ключа.

# 4 Выводы

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

# 5 Список литературы

1. Методические материалы курса