Отчёт по лабораторной работе №8 Информационная безопасность

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

Выполнила: Данзанова Саяна, НПИбд-01-21, 1032217624

Содержание

# Цель работы

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

# Теоретическое введение

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 c так называемой «схемой 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)

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 полченных 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.

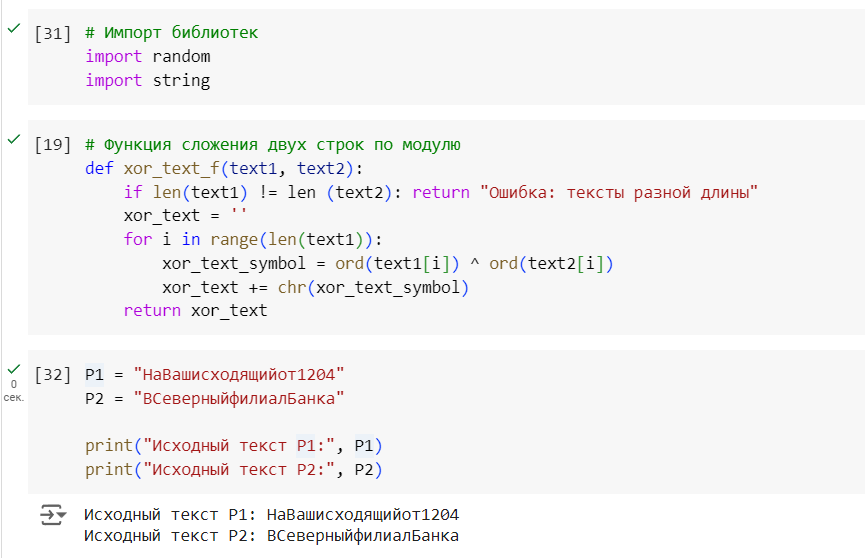
# Выполнение лабораторной работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста.

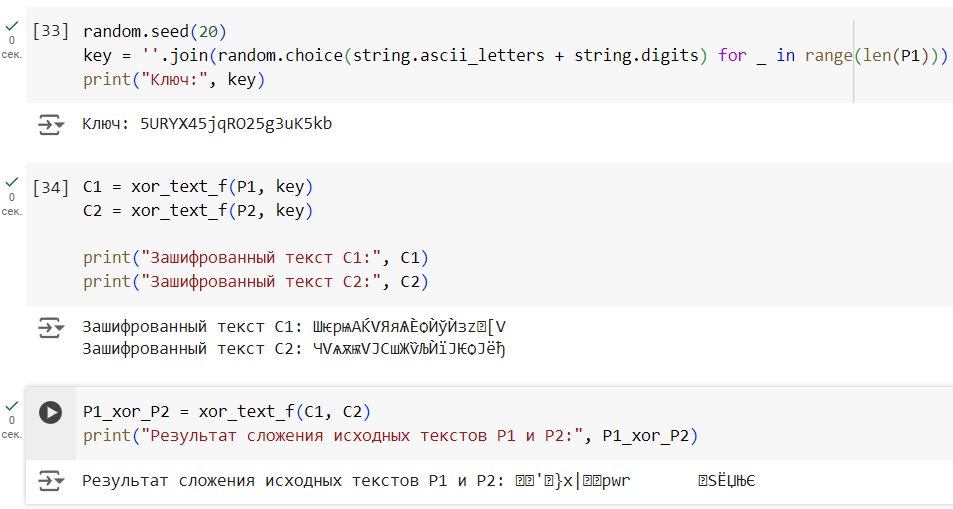
Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе;

Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

Для решения задачи написан программный код:



(Программный код приложения, реализующего режим однократного гаммирования)



(Программный код приложения, реализующего режим однократного гаммирования)

# Вывод

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

# Список литературы. Библиография

[0] Методические материалы курса