Отчёт по лабораторной работе №8

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

Ханина Ирина Владимировна, НБИбд-02-18

Содержание

[Цель работы 1](#_Toc90564760)

[Задание 1](#_Toc90564761)

[Теоретическое введение 1](#_Toc90564762)

[Выполнение лабораторной работы 2](#_Toc90564763)

[Выводы 3](#_Toc90564764)

[Список литературы 3](#_Toc90564765)

# Цель работы

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

# Задание

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.

# Теоретическое введение

Гаммирование или Шифр XOR - это наложение или снятие на открытые или зашифрованные данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных или открытых данных. С точки зрения теории криптоанализа метод однократного гаммирования той же длины, что и открытый текст, является невскрываемым. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Данный метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Необходимые и достаточные условия абсолютной стойкости шифра:

* полная случайность ключа;
* равенство длин ключа и открытого текста;
* однократное использование ключа. [[1]](https://referatbank.ru/referat/preview/7337/metodichka-programmnye-sredstva-zaschity-informacii.html)

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой ([рис. 1](image/3.png)):

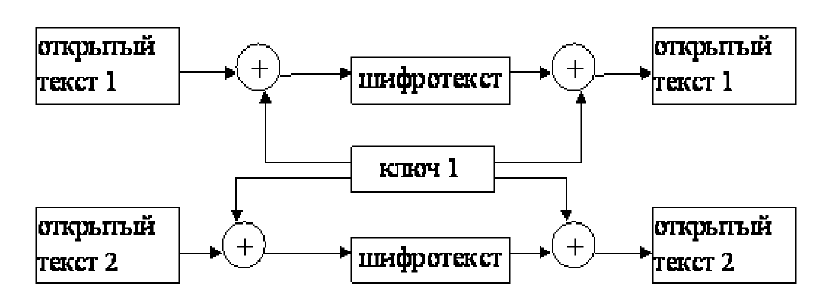


Рис 1. Общая схема шифрования двух различных текстов одним ключом

# Выполнение лабораторной работы

Исходные данные:

* P1 = НаВашисходящийот1204
* P2 = ВСеверныйфилиалБанка
* К = “Хп68ПОдвык92Иторн08s”. Ключ был подобран случайно. Длина ключа и открытых текстов равны.

Я разработала приложение на языке Python ([рис. 2](image/1.png)). Запуск программы производился в Jupiter Notepad. Для операции сложения по модулю 2 я использовала функцию xor() из модуля operator.



Рис 2. Код приложения

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 ([рис. 3](image/4.png)) 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.

Рис 3. Формула нахождения текста Р2 при известных обеих шифровок С1 и С2 и открытом тексте Р1

Рис 3. Формула нахождения текста Р2 при известных обеих шифровок С1 и С2 и открытом тексте Р1

# Выводы

В результате выполнения лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы

1. [Программные средства защиты информации](https://referatbank.ru/referat/preview/7337/metodichka-programmnye-sredstva-zaschity-informacii.html)