

Отчёт по лабораторной работе №8

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

Ханина Ирина Владимировна, НБИбд-02-18

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	11
	Список литературы	12

List of Tables

List of Figures

3.1	Рис 1. Общая схема шифрования двух различных текстов одним ключом	8
4.1	Рис 2. Код приложения	9
4.2	Рис 3. Формула нахождения текста P2 при известных обеих шифровках C1 и C2 и открытом тексте P1	10

1 Цель работы

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

2 Задание

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

3 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]

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой (рис. 1):

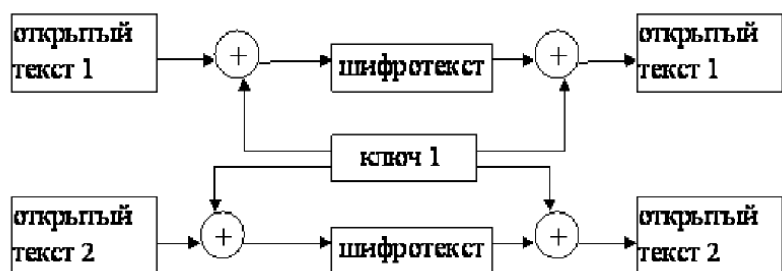


Figure 3.1: Рис 1. Общая схема шифрования двух различных текстов одним ключом

4 Выполнение лабораторной работы

Исходные данные:

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

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

```
In [19]: from operator import xor

string1 = 'НаВашисходящийот1204'
string2 = 'ВСеверныйфилиалБанка'
key = 'Хп68ПОдвык92Иторн08s'

def gamming(x, y):
    text = []
    for x, y in zip(x, y):
        text.append(chr(xor(ord(x), ord(y))))
    t = ''.join(text)
    return t

s1 = gamming(string1, key)
print("Зашифрованное послание 1: ", bytes(s1, "UTF-8").hex())
s2 = gamming(string2, key)
print("Зашифрованное послание 2: ", bytes(s2, "UTF-8").hex())
s = gamming(s1, s2)
print("Сложение 2 шифров: ", bytes(s, "UTF-8").hex())
print("Открытый текст 1: ", gamming(s, string2))
print("Открытый текст 2: ", gamming(s, string1))

Зашифрованное послание 1: 389fd0a4d08857267577750ed1bb207b0002d08c020847
Зашифрованное послание 2: 371ed083d08a225e0e979727ed081d089207205510dd08dd082d183
Сложение 2 шифров: 0f1127027d787c0e07707720009053d081d08fd08ad084
Открытый текст 1: НаВашисходящийот1204
Открытый текст 2: ВСеверныйфилиалБанка
```

Figure 4.1: 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) с подстановкой вместо P_1 полученных на предыдущем шаге новых символов сообщения P_2 . И так далее. Действуя подобным образом, злоумышленник даже если не прочитает оба сообщения, то значительно уменьшит пространство их поиска.

$$C_1 \oplus C_2 \oplus P_1 = P_1 \oplus P_2 \oplus P_1 = P_2.$$

Figure 4.2: Рис 3. Формула нахождения текста P_2 при известных обеих шифровок C_1 и C_2 и открытом тексте P_1

5 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