Элементы криптографии. Шифрование различных исходных текстов одним ключом

Ханина Ирина Владимировна НБИбд-02-18

17 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

Теоретическое введение

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

Теоретическое введение

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется в соответствии со схемой:

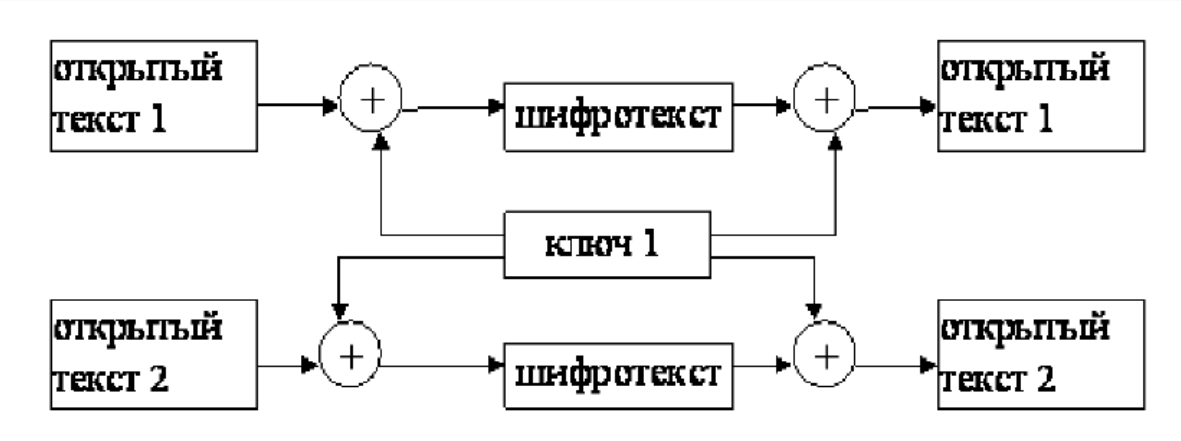

Figure 1: Рис 1. Общая схема шифрования двух различных текстов одним ключом

Цель лабораторной работы

Цель - освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Задачи 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.

Результаты выполнения лабораторной работы

Я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом. Код программы:

```
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:  380fd0a4d08857267577750ed1b6d1bb207b0002d08c020847
Зашифрованное послание 2:  371ed083d08a2a5e0979727ed081d089207205510dd08dd082d183
Сложение 2 шифров:  0f1127027d787c0e0770777200090553d081d08fd08ad084
Открытый текст 1:  НаВашисходящийот1204
Открытый текст 2:  ВСеверныйфилиалБанка
```

Figure 2: Рис 2. Код приложения