Шифр гаммирования

Яна Башкирова НБИ-01-20

15 октября, 2023, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

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

Выполнение лабораторной работы

Гаммирование

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Алгоритм взлома

Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

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

Алгоритм взлома

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства складываются по модулю 2. Тогда с учётом свойства операции XOR получаем:

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

Алгоритм взлома

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 $C_1 \oplus C_2$ (известен вид обеих шифровок). Тогда зная P_1 имеем:

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

Схема работы алгоритма

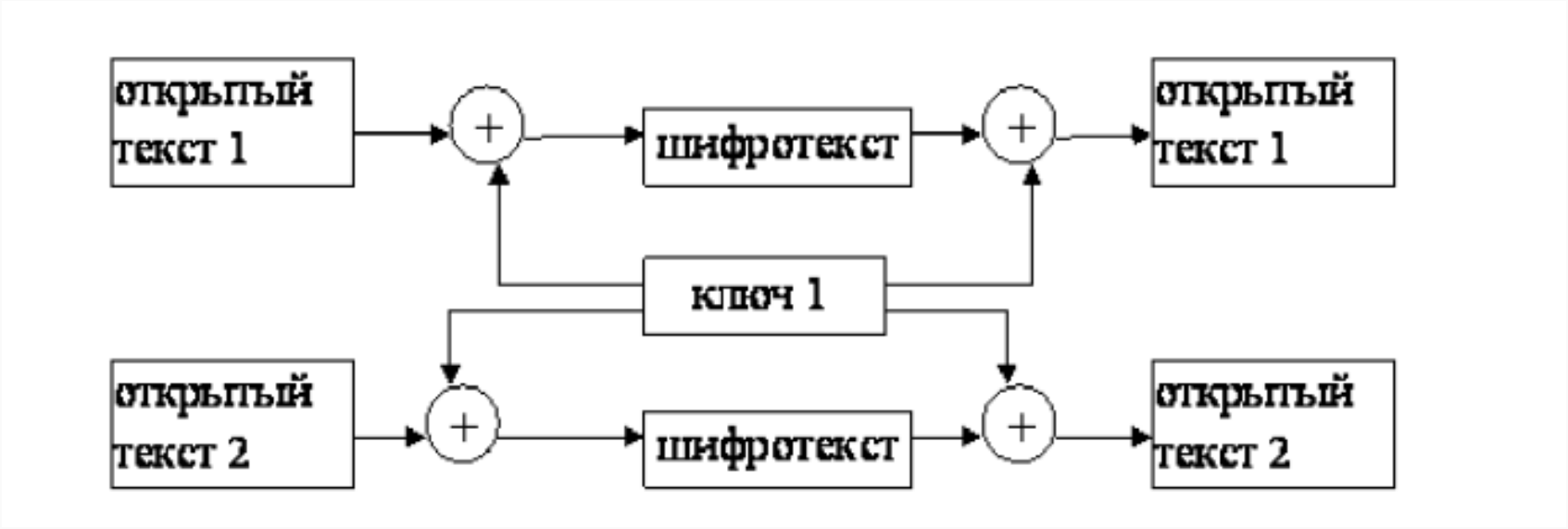

Figure 1: Работа алгоритма гаммирования

Пример работы программы

```
In [2]:
def vzlom(P1, P2):
    code = []
    for i in range(20):
        code.append(alph[(alph.index(P1[i]) + alph.index(P2[i])) %len(alph) ])
    print(code)
    p3 = "".join(code)
    print(p3)
```

```
In [3]:
vzlom(P1, P2)
```

```
['щ', 'С', 'З', 'в', 'э', 'Ш', 'ю', 'Ж', 'ч', 'Ш', '7', '4', 'р', 'й', 'щ', 'У', '1', 'Е', 'А', '4']
щСЗвэШюЖчШ74рйщУ1ЕА4
```

Figure 2: Работа алгоритма взлома ключа

```
In [13]:
shifr(P1, gamma)
```

```
числа текста  [47, 1, 35, 1, 26, 42, 19, 23, 16, 5, 32, 27, 10, 11, 16, 20, 66, 67, 75, 69]
Числа гаммы  [27, 51, 41, 3, 31, 58, 32, 40, 25, 58, 72, 69, 18, 11, 27, 53, 66, 38, 33, 69]
1
25
29
21
57
30
33
63
Числа шифра:  [74, 52, 1, 4, 57, 25, 51, 63, 41, 63, 29, 21, 28, 22, 43, 73, 57, 30, 33, 63]
шифровка 9ТагЧчСЭЭЭыуъфЙ8ЧьАЭ
```

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения лабораторной работы было разработано приложение, позволяющее шифровать тексты в режиме однократного гаммирования.