Шифр гаммирования

Егор Судаков НБИ-01-20

18 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

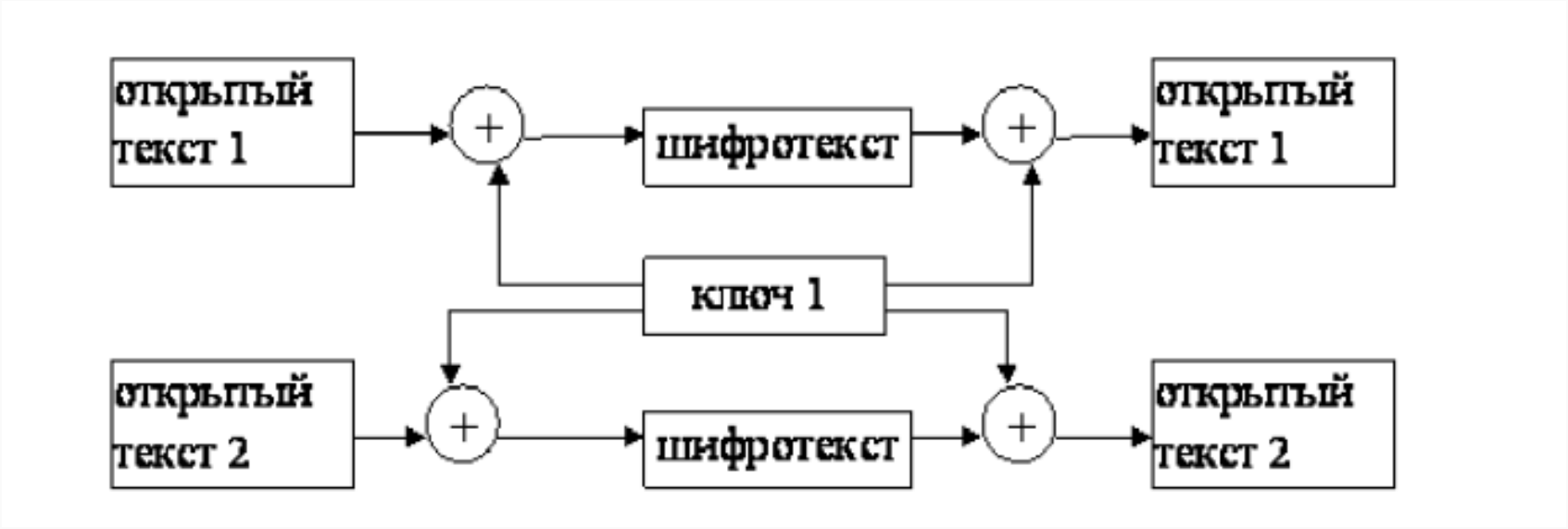

Figure 1: Работа алгоритма гаммирования

Пример работы программы

```
In [8]:  1 P1="СекретноеСлово"

In [9]:  1 P2="ОтветНаВопрос1"

In [10]: 1 len(P1)
Out[10]: 14

In [11]: 1 len(P2)
Out[11]: 14

In [12]: 1 vzlom(P1, P2)
['9', 'ч', 'м', 'х', 'ч', 'Я', 'н', 'Р', 'у', 'а', 'ы', 'ь', 'у', 'Е']
9чмхчЯнРуаыьуЕ
```

Figure 2: Работа алгоритма взлома ключа

```
In [14]: 1 gamma = "9чмхчЯнРуаыьуЕ"

In [15]: 1 gamma_shifr(P1, gamma)
Числа текста  [51, 6, 12, 18, 6, 20, 15, 16, 6, 51, 13, 16, 3, 16]
```

Выводы

Результаты выполнения лабораторной работы

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