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

Ким Реачна

24 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

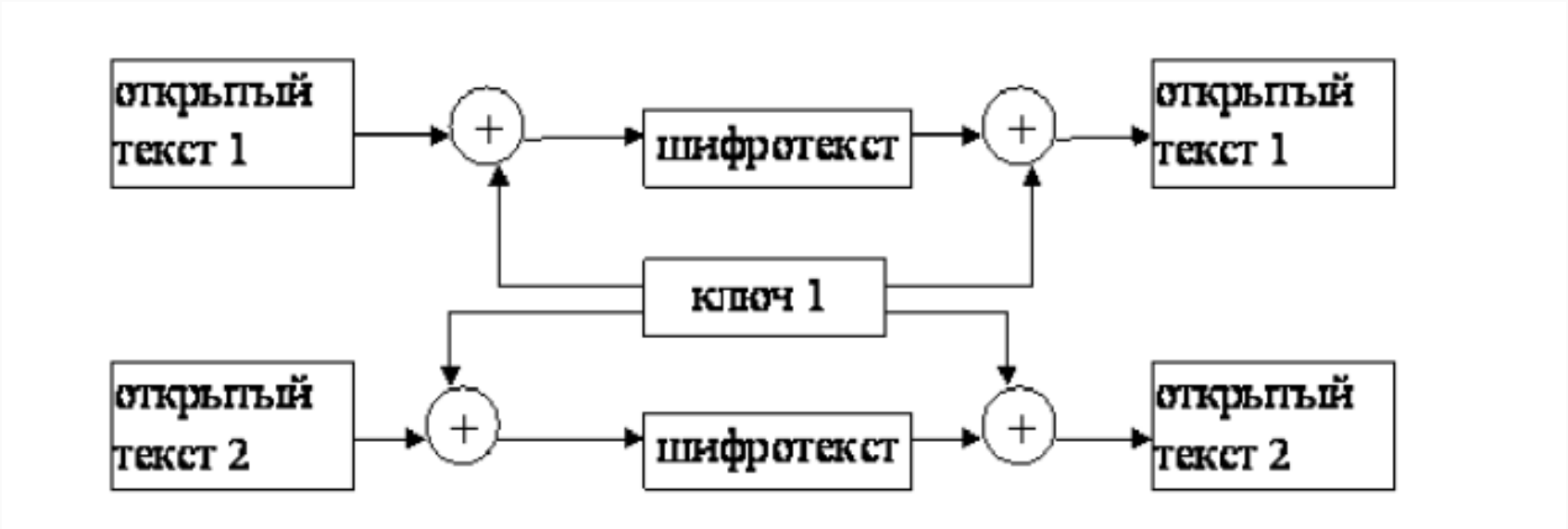

Рис. 1: Работа алгоритма гаммирования

Пример работы программы

```
14 def vzlom(P1, P2):
15     code = []
16     for i in range(len(P1)):
17         code.append(liters[(liters.index(P1[i]) + liters.index(P2[i])) % len(liters)])
18     print(code)
19     pr = "".join(code)
20     print(pr)
```

```
[2]  1 len(P1)
```

```
13
```

```
[3]  1 len(P2)
```

```
13
```

```
[4]  1 vzlom(P1, P2)
```

```
['х', 'У', 'Л', 'Ь', 'г', 'А', 'р', 'Б', 'Ю', 'С', 'Щ', 'Ь', 'Щ']
хУЛЬгАрБЮСЩЬЩ
```

Рис. 2: Работа алгоритма взлома ключа

Пример работы программы

```
[26]  1 P1 = "КодофаяФраза1"
      2 gamma = "хУЛьгАрБЮСЩЬЩ"
```

```
[27]  1 shifr(P1, gamma)
```

```
Числа текста  [44, 16, 5, 16, 22, 1, 32, 54, 18, 1, 9, 1, 66]
Числа гаммы  [23, 53, 45, 62, 4, 33, 18, 34, 64, 51, 59, 62, 59]
3
13
7
50
Числа шифротекста  [67, 69, 50, 3, 26, 34, 50, 13, 7, 52, 68, 63, 50]
Шифротекст  24РвшБРлёТ3ЭР
Расшифрованный текст:  КодофаяФраза1
```

Рис. 3: Работа алгоритма шифрования и дешивровки

Выводы

Результаты выполнения лабораторной работы

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