Шифргаммирования

Назармамадов Умед Джамшедович

29 апреля, 2025, Москва, Россия

РоссийскийУниверситетДружбы Народов

Целиизадачи

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

Выполнениелабораторной работы

Алгоритмвзлома

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.
Шифротексты обеих телеграмм можно получить по формулам режима однократного гаммирования:

Алгоритмвзлома

$$C_1 = P_1 \oplus K$$

$$C_2 = P_2 \oplus K$$

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:

Алгоритмвзлома

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

Алгоритмвзлома

Предположим, что одна из телеграмм является шаблоном — т.е. имееттекст 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:

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

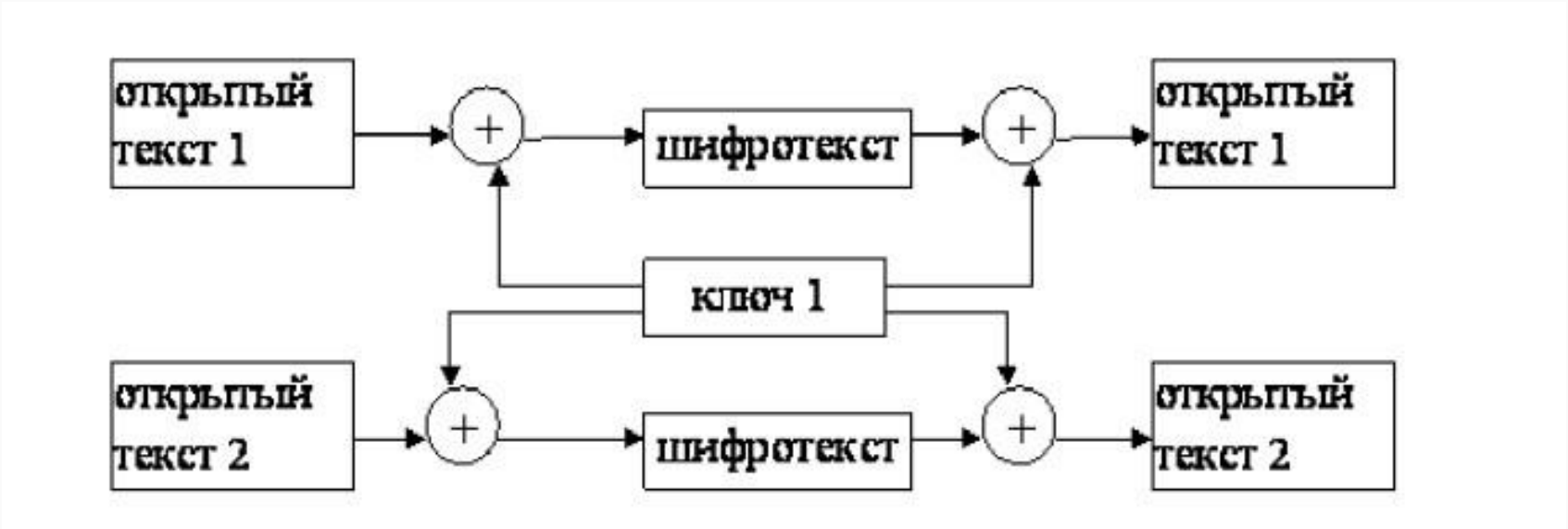

Рис. 1: Работа алгоритма гаммирования

```
13
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)
```

In [11]:
```
1 len(P1)
```

Out[11]: 13

In [12]:
```
1 len(P2)
```

Out[12]: 13

In [13]:
```
1 vzlom(P1, P2)
```

```
['х', 'у', 'л', 'ь', 'З', 'а', 'Ж', 'б', 'ю', 'с', 'щ', 'ь', 'Щ']
хульЗаЖбюсщьЩ
```

In [24]:
```
1 P1 = "КодофаяФраза1"
2 gamma = "хульЗаЖбюсщьЩ"
```

In [25]:
```
1 shifr(P1, gamma)
```

Рис. 2: Работа алгоритма взлома ключа

Выводы

Результатывыполнениялабораторнойработы

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