Шифр гаммирования

Кашкин Иван Евгеньевич

26 октября, 2024, 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

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:

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

Пример работы программы

```
[17]: a = ord("а")
liters = [chr(i) for i in range(a, a + 32)]
a = ord("0")
for i in range(a, a+10):
    liters.append(chr(i))

a = ord("А")
for i in range(1040, 1072):
    liters.append(chr(i))

P1 = "КодоваяФраза1"
P2 = "Безопасность2"

def vz(P1, P2):
    code = []
    for i in range(len(P1)):
        code.append(liters[(liters.index(P1[i]) + liters.index(P2[i])) % len(liters)])
    print(code)
    pr = "".join(code)
    print(pr)
```

Figure 2: Работа алгоритма взлома ключа

```
[19]: len(P1)

[19]: 13

[20]: len(P2)

[20]: 13

[21]: vz(P1, P2)

['х', 'у', 'л', 'ь', 'с', 'а', 'Ж', 'б', 'ю', 'с', 'щ', 'ь', 'Щ']
хульсаЖбюсщьЩ

[22]: P1 = "КодоваяФраза1"
gamma = "хульЗаЖбюсщьЩ"

[23]: shifr(P1, gamma)

Числа текста  [44, 16, 5, 16, 3, 1, 32, 54, 18, 1, 9, 1, 66]
Числа гаммы  [23, 21, 13, 30, 68, 1, 40, 2, 32, 19, 27, 30, 59]
```

Выводы

Результаты выполнения лабораторной работы

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