Отчёт по лабораторной работе

Лабораторная работа 8

Дзугаева Лилия Владславовна

Цель работы:

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

Ход работы:

1. Генерируем случайный ключ, соответствующий длине текста, который мы хотим кодировать.
2. Вводим два сообщения. Применяя алгоритм, указанный в условии лабораторной работы, получаем, что можем расшифровать сообщения. Т.е. если злоумышленник знает одно из закодированных сообщений по одному ключу, то он сможет расшифровать и (уменьшить область поиска) другие сообщения, закодированные по тому же ключу.

In [16]:
```
key = [int('0x' + i, 16) for i in input("Введите ключ: ").split(' ')]
```
```
Введите ключ: b2 c3 3d f4 e2 c7 a5 7e d2 3a 4f d2 2b c6 1e
```

In [17]:
```
len_text = len(key)
```

In [18]:
```
text = [ord(c) for c in input("Введите первый текст: ")]
if len(text) != len_text:
    print('Длины ключа и текста не совпадают!')
```
```
Введите первый текст: Будьте здоровы!
```

In [19]:
```
text2 = [ord(c) for c in input("Введите второй текст: ")]
if len(text2) != len_text:
    print('Длины ключа и текста не совпадают!')
```
```
Введите второй текст: Счастья и тепла
```

In [20]:
```
a1 = [key[c] ^ text[c] for c in range(len_text)]
a2 = [key[c] ^ text2[c] for c in range(len_text)]
otv = [a1[c] ^ a2[c] for c in range(len_text)]
p1 = [otv[c] ^ text[c] for c in range(len_text)]
p2 = [otv[c] ^ text2[c] for c in range(len_text)]
```

In [21]:
```
print(' '.join([chr(p1[i]) for i in range(len_text)]))
print(' '.join([chr(p2[i]) for i in range(len_text)]))
```
```
С ч а с т ь я   и   т е п л а
Б у д ь т е   з д о р о в ы !
```

Заключение:

В ходе выполнения лабораторной работы я изучил теорию и освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Ответы на контрольные вопросы:

1. Как, зная один из текстов (P_1 или P_2), определить другой, не зная при этом ключа?

С помощью формул режима однократного гаммирования получим шифротексты обеих телеграмм:

$$C_1 = P_1 \oplus К,$$
$$C_2 = P_2 \oplus К.$$

Задача нахождения открытого текста по известному шифротексту двух телеграмм, зашифрованных одним ключом, может быть решена. Складываем по модулю 2 (XOR) (обозначается знаком $\oplus$) оба равенства и получаем:

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

Если один из текстов известен — т.е. имеет фиксированный формат, в который вписываются значения полей, и нам известен этот формат, то тогда получим достаточно много пар $C_1 \oplus C_2$ (известен вид обеих шифровок). Далее зная P_1 и учитывая свойство операции XOR, имеем:

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

Таким образом, получаем возможность определить те символы сообщения P_2, которые находятся на позициях известного шаблона сообщения P_1. В соответствии с логикой сообщения P_2, у нас есть реальный шанс узнать ещё некоторое количество символов сообщения P_2. Затем вновь используем предыдущее равенство с подстановкой вместо P_1 полученных на предыдущем шаге новых символов сообщения P_2. И так далее. Действуя подобным образом, даже если не прочитаем оба сообщения, то значительно уменьшим пространство их поиска.

2. Что будет при повторном использовании ключа при шифровании текста?

Если на сообщение наложить ключ дважды, мы получим исходное сообщение.

3. Как реализуется режим шифрования однократного гаммирования одним ключом двух открытых текстов?

Один ключ накладываем на оба открытых текста и получаем два зашифрованных одним ключом шифротекста.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

При условии, что злоумышленник знает о том, что ключ шифрования един и он получил одну из пар текстов (зашифрованный текст и открытый), то он может найти ключ (см. вопрос 1) и расшифровать остальные тексты.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Это позволяет упростить разработку шифровальных и дешифровальных систем. Если мы реализуем обмен, например, между двумя компьютерами, то удобно использовать единый ключ для всех данных.