

Лабораторная работа №8. Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Дисциплина: Информационная безопасность

Манаева Варвара Евгеньевна.

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Изучение механизма шифрования гаммирование как простейшего варианта системы шифрования с закрытым ключом.

1. Рассмотреть особенности и особенности кодирования однократного гаммирования с использованием одного ключа.
2. Создать код, который будет показывать принцип работы нескольких шифротекстов с одним ключом и его взлом.
3. изучить способы взлома и декодирование шифротекста без ключа.

Код

```
def key_create(s, alf):  
    k = ''.join(random.choice(alf) for i in range(s))  
    return k
```

```
def hex_coder(cod):  
    return ' '.join(hex(ord(i))[2:] for i in cod)
```

```
def string_coder(text, k, i_num):  
    if i_num == 1:  
        return ''.join(chr(ord(c) ^ ord(k)) for c, k in zip(text, k))  
    else:  
        return [''.join(chr(ord(c) ^ ord(k)) for c, k in zip(t, k)) for t in
```



```
def find_key(cypher, texts, s):  
    possible_keys = []  
    for f in range(len(texts)):  
        for i in range(len(cypher[f]) - s + 1):  
            key = [chr(ord(c) ^ ord(k)) for c, k in zip(cypher[f][i:i + s], t  
            intact_plaintext = string_coder(cypher[f], key, 1)  
            if texts[f] in intact_plaintext:  
                possible_keys.append(''.join(key))  
    return possible_keys
```

```
6 print(f"Изначальное сообщение P1: {P1}\nИзначальное сообщение P2: {P2}")
7 print(f"Зашифрованное сообщение C1: {C1}\n", f"В 16 бит {hex_coder(C1)}\n", f"Зашифрованное сообщение C2: {C2}\n", f"В 16 бит {hex_coder(C2)}", sep="")
  Executed at 2023.10.21 15:16:38 in 14ms

  ▾ Изначальное сообщение P1: Literature is an interesting subject indeed
    Изначальное сообщение P2: ёццшо5блнгъшожабквеёцшбје1цхулонё82йggquvw
    Зашифрованное сообщение C1: фР00щы0ы0км0ъ8в8иц50у0щ0ч0н0м0п0а0и0ц  W00N0ыT0У0Т
    В 16 бит 477 50 1a 16 40 428 44b 13 44e 459 17 42a 42 466 42b 429 53 11 423 441 1 449 56 43d 4d 45d 43f 12 41 43d 3 426 9 42b 19 1 4e 0 42b 54 7 421 54
    Зашифрованное сообщение C2: jёёл]Схх0хё0"равтт00Rгх0JүүдЧце00сым\аТАбёх
    В 16 бит 6a 47f 451 43b 5d 47c 45d 1 44e 47b b 5e 70 430 77 442 442 7f 0 52 72 40d 6 408 45e 434 44 427 426 435 7f c 73 42b 4d 5c 450 422 41 42a 432 478

7 1 possible_keys = find_key([C1, C2], [P1, P2], size)
  2 print("Возможные ключи для шифротекста:", possible_keys)
    Executed at 2023.10.21 15:16:38 in 41ms

    Возможные ключи для шифротекста: ['л9ns2цпфмм7у1цьчхэедл3ё9дёуамvfсёзунix0бф0', 'л9ns2цпфмм7у1цьчхэедл3ё9дёуамvfсёзунix0бф0']

8 1 D1, D2 = string_coder([C1, C2], possible_keys[-1], 2)
  2 print(f"Расшифрованный текст:\n{C1}\n=>\n{D1}\n\n{C2}\n=>\n{D2}")
    Executed at 2023.10.21 15:16:38 in 31ms

  ▾ Расшифрованный текст:
    фР00щы0ы0км0ъ8в8иц50у0щ0ч0н0м0п0а0и0ц  W00N0ыT0У0Т
    =>
    Literature is an interesting subject indeed

    jёёл]Схх0хё0"равтт00Rгх0JүүдЧце00сым\аТАбёх
    =>
    ёццшо5блнгъшожабквеёцшбје1цхулонё82йggquvw
```

Рис. 1: Результат

Контрольные вопросы

Как, зная один из текстов (P1 или P2), определить другой, не зная при этом ключа?

Ответ: Это возможно сделать только в том случае если текст P1 и P2 одной длины и имеют общий ключ.

Что будет при повторном использовании ключа при шифровании текста?

Ответ: Из-за одинаковости способа кодирования и декодирования после повторного использования слова и ключа даст нам шифротекст.

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

Ответ: Фактически, следуя схеме 8.1 и принципу “шифра XOR”, мы просто имеем два параллельных кодирования и декодирования с использованием одного ключа.

Перечислите недостатки шифрования одним ключом двух открытых текстов.

Ответ: Если вспомнить требования для абсолютной стойкости шифра, рассмотренных в предыдущей лабораторной, можно сразу понять по первому же пункту, что если ключ не будет случайным и каждый раз новым для каждой строки, то, найдя пересечения или аналоги в шифротекстах, можно определить одинаковые символы, что может пошатнуть защиту текста даже если у вас нет ни одного исходного кода. При этом получается, что если есть исходный текст (хотя бы один образец), определить другие слова становится легко.

Перечислите преимущества шифрования одним ключом двух открытых текстов.

Ответ:

- требуется передать один ключ, что сделать проще и быстрее
- при передаче большого количества шифротекста нет шанса запутаться в их порядке сочетания с ключами.

Выводы по проделанной работе

В результате выполнения работы мы освоили на практике применение режима однократного гаммирования и возможных способах взлома при отсутствии ключа и наличие исходных текстов и шифротекстов.

Были записаны скринкасты выполнения и защиты лабораторной работы.