

Отчёт по лабораторной работе №8

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

Данилова Анастасия Сергеевна

Содержание

0.1	Цель лабораторной работы	1
1	Выполнение работы	1
1.1	Контрольные вопросы	2
2	Вывод	3

0.1 Цель лабораторной работы

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

1 Выполнение работы

Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

```

1 def encrypt(plaintext, key):
2     ciphertext = ''
3     key_idx = 0
4     for char in plaintext:
5         # Применяем однократное гаммирование
6         encrypted_char = chr(ord(char) ^ ord(key[key_idx]))
7         ciphertext += encrypted_char
8         # Увеличиваем индекс ключа с помощью циклического счетчика
9         key_idx = (key_idx + 1) % len(key)
10    return ciphertext
11
12 def decrypt(ciphertext, key):
13     plaintext = ''
14     key_idx = 0
15     for char in ciphertext:
16         # Применяем однократное гаммирование
17         decrypted_char = chr(ord(char) ^ ord(key[key_idx]))
18         plaintext += decrypted_char
19         # Увеличиваем индекс ключа с помощью циклического счетчика
20         key_idx = (key_idx + 1) % len(key)
21    return plaintext
22
23 P1 = "Первый текст"
24 P2 = "Еще один текст"
25 key = "секретныйключ"
26 C1 = encrypt(P1, key)
27 C2 = encrypt(P2, key)
28
29 print("Исходный текст P1:", P1)
30 print("Исходный текст P2:", P2)
31 print("Зашифрованный текст C1:", C1)
32 print("Зашифрованный текст C2:", C2)
33 D1 = decrypt(C1, key)
34 D2 = decrypt(C2, key)
35
36 print("Расшифрованный текст D1:", D1)
37 print("Расшифрованный текст D2:", D2)

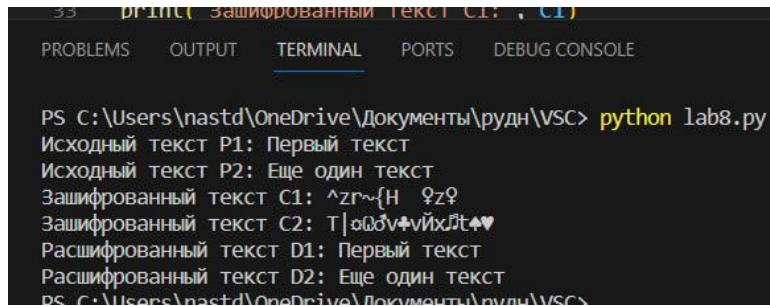
```

Код

```

33 print("Зашифрованный текст C1:", C1)

```



```

PS C:\Users\nastd\OneDrive\Документы\пудн\VSC> python lab8.py
Исходный текст P1: Первый текст
Исходный текст P2: Еще один текст
Зашифрованный текст C1: ^zг~{H 9z9
Зашифрованный текст C2: T|æðv+viXjt♠♥
Расшифрованный текст D1: Первый текст
Расшифрованный текст D2: Еще один текст
PS C:\Users\nastd\OneDrive\Документы\пудн\VSC>

```

Результат

1.1 Контрольные вопросы

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

Для определения другого текста без знания ключа можно использовать метод криптоанализа, который включает в себя анализ частотности букв, поиски общих слов или выражений, анализ повторяющихся блоков и другие методы. Однако, без ключа дешифрование текста может быть сложным и требовать большого количества времени и вычислительных ресурсов.

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

При повторном использовании ключа при шифровании текста возможно нарушение криптографической стойкости и приведение к возможности восстановления ключа или дешифрования текста без его использования. Поэтому рекомендуется использовать каждый ключ только один раз.

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

В режиме шифрования однократного гаммирования одним ключом двух открытых текстов каждый открытый текст сначала обрабатывается с помощью операции XOR с ключом, а затем происходит операция XOR между зашифрованными текстами. Таким образом, ключ применяется только один раз для шифрования каждого открытого текста.

4. Перечислите недостатки шифрования одним ключом двух открытых текстов.

Недостатки шифрования одним ключом двух открытых текстов включают возможность угадывания ключа или дешифрования текста, если злоумышленник имеет доступ к нескольким парам зашифрованных и открытых текстов. Кроме того, использование одного и того же ключа для нескольких текстов может привести к компрометации стойкости шифрования или к “слабым” ключам.

5. Перечислите преимущества шифрования одним ключом двух открытых текстов.

Преимущества шифрования одним ключом двух открытых текстов включают уменьшение объема ключевого материала, что упрощает его хранение и управление. Это также может сэкономить вычислительные ресурсы и время, поскольку для шифрования и расшифрования двух текстов требуется всего одно применение ключа. Если ключ надежен и хорошо защищен, шифрование одним ключом двух текстов может быть безопасным и эффективным методом шифрования.

2 Вывод

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