

«Практическая работа: *Лабораторная работа №1. Шифрование данных методами подстановки, перестановки и полиалфавитными шифрами»*

Выполнили:

студент группы 1ИСП11-18

Белякова А.А.

Ищенко Т.С.

Проверил:

Возвахов Д.А.

Москва

2022

**Цель работы:** Приобретение навыков шифрования информации с использованием простейших методов шифрования.

**Исходные данные:**

10

Hello World

**Алгоритм работы программы:**

1. Шаг для дешифровки
2. Текс для дешифровки
3. Количество букв в английском алфавите
4. Делаем цикл в длину текста
5. Получаем код из таблицы Unicode со смешением
6. Если номер вышел за нижнюю границу строчных латинских букв
7. Возвращаем его в границы строчных латинских букв
8. Выводим букву, соответствующую искомому номеру

**Текст программы:**

n = int(input())

s = input()

abc = 26

for i in range(len(s)):

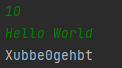
word = ord(s[i]) - n

if word < 97:

word += abc

print(chr(word), end='')

**Результат работы программы:**



**Анализ результата:**

Программа отработала успешно.

**Вывод:**

Программа выстра в шифровке, но является не сильно надёжной, так как зашифрованный текст имеет те же самые статистические характеристики, что и исходный, поэтому зная стандартные частоты появления символов в том языке, на котором написано сообщение, и подбирая по частотам появления символы в зашифрованном сообщении, можно восстановить таблицу замены.

Контрольные вопросы

1. Почему метод подстановки имеет слабую надежность?

Так как зашифрованный текст имеет те же самые статистические характеристики, что и исходный, поэтому зная стандартные частоты появления символов в том языке, на котором написано сообщение, и подбирая по частотам появления символы в зашифрованном сообщении, можно восстановить таблицу замены.

1. Что такое частотный анализ?

Частотный анализ — один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей, как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.

1. Что является криптографическим ключом в методе перестановки?

Шифры перестановки основаны на том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов. Ключом такого шифра является используемая при шифровании перестановочная матрица или вектор, указывающий правило перестановки.

1. Как связаны метод подстановки и многоалфавитные шифры?

Методы шифрования заменой (подстановкой) основаны на том, что символы исходного текста, обычно разделенные на блоки и записанные в одном алфавите, заменяются одним или несколькими символами другого алфавита в соответствии с принятым правилом преобразования.

1. В чем отличие криптографии от криптоанализа?

Криптография — это наука о том, как обеспечить секретность сообщения.

Криптоанализ — это наука о том, как вскрыть шифрованное сообщение, то есть как извлечь открытый текст не зная ключа.

1. По какому признаку шифры делят на симметричные и асимметричные?

Алгоритмы шифрования часто делятся на две категории, известные как симметричное и асимметричное шифрование. Принципиальное различие между этими двумя методами заключается в том, что алгоритмы симметричного шифрования используют один ключ, в то время как асимметричные используют два разных, но связанных между собой ключа.