МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Факультет информационных технологий и робототехники

Кафедра программного обеспечения информационных систем и технологий

**Отчет**

**по лабораторной работе № 2**

**«Классические шифры»**

по дисциплине: «Основы информационной безопасности»

Вариант 15

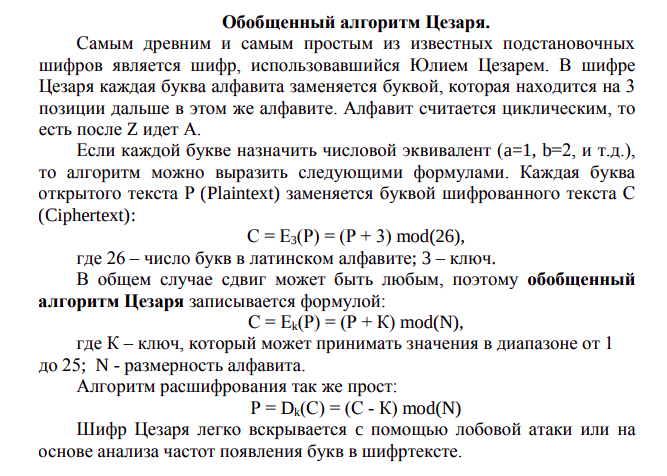
|  |  |
| --- | --- |
| Выполнили**:** | ст.гр. 10702122 |
|  | Тимощенко Н. В. |
|  |  |
|  |  |
| Приняла: | Белова С.В. |

Минск 2024

**Цель работы:**

Познакомиться с основными криптографическими терминами и моделью традиционного шифрования. Изучить типы криптосистем. Изучить особенности классических методов шифрования на примере конкретных алгоритмов

**Описание алгоритма шифрования и расшифрования:**



**Задания на лабораторную работу**

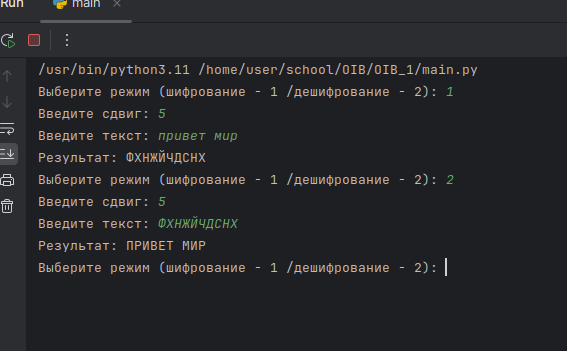
**Вариант**



1. Изучить теоретические основы (Лекция 3 и методические указания к лабораторной работе).
2. Описать алгоритмы шифрования и расшифрования на контрольном примере.
3. Написать независимые программные модули, реализующие алгоритм шифрования и алгоритм расшифрования в соответствии с вариантом задания, указанным преподавателем.

При шифровании: вводить с клавиатуры ключ и открытый текст, выводить на экран шифртекст. При расшифровании: вводить с клавиатуры ключ и шифртекст, выводить на экран открытый текст.

В коде программы задать алфавит согласно варианту задания. При вводе открытого текста проверять его принадлежность указанному алфавиту. При вводе ключа проверять его принадлежность пространству ключей. Криптосистему описать в виде класса. Алгоритмы шифрования и расшифрования реализовать как методы класса.



Результат выполнения задания

**Контрольные вопросы**

**Правило Керкхоффа**: Принцип Керкхоффа гласит, что безопасность криптосистемы должна зависеть только от секретности ключа, а не от секретности алгоритма.

**Основные термины**:

* 1. **Криптосистема**: Совокупность алгоритмов для шифрования и расшифрования данных.
  2. **Шифрование**: Процесс преобразования открытого текста в зашифрованный текст с использованием ключа.
  3. **Расшифрование**: Обратный процесс шифрования, преобразование зашифрованного текста обратно в открытый текст.
  4. **Алфавит**: Набор символов, используемых в шифровании.
  5. **Открытый текст**: Исходное сообщение до шифрования.
  6. **Пространство ключей**: Все возможные ключи, которые могут быть использованы в криптосистеме.

**Симметричные криптосистемы**: Это системы, в которых один и тот же ключ используется для шифрования и расшифрования. Модель, предложенная К. Шенноном, включает в себя:

* 1. **Шифрование**:
  2. **Расшифрование**:

**Классификация криптосистем**:

* 1. По типу ключа: симметричные и асимметричные.
  2. По типу алгоритма: блочные и потоковые.
  3. По применению: для шифрования данных, для цифровых подписей и т.д.

**Блочные и потоковые криптосистемы**:

* 1. **Блочные**: Шифруют данные блоками фиксированного размера (например, AES).
  2. **Потоковые**: Шифруют данные побитно или побайтово (например, RC4).

**Различие между расшифрованием и дешифрованием**:

* 1. **Расшифрование**: Процесс преобразования зашифрованного текста обратно в открытый текст с использованием ключа.
  2. **Дешифрование**: Процесс взлома шифра без знания ключа.

**Основные понятия**:

* 1. **Криптография**: Наука о методах обеспечения конфиденциальности и целостности информации.
  2. **Криптология**: Общее название для криптографии и криптоанализа.
  3. **Криптоанализ**: Наука о методах взлома шифров.
  4. **Стеганография**: Искусство скрытия факта передачи информации.

**Классические системы шифрования**: Это шифры, такие как Цезарь, Виженер и т.д. Они редко используются на практике из-за низкой криптостойкости, но их принципы лежат в основе современных симметричных криптосистем.

**Криптостойкость**: Способность шифра противостоять криптоанализу. Шифр называется абсолютно стойким, если невозможно расшифровать сообщение без ключа, даже имея бесконечное количество вычислительных ресурсов. Пример: одноразовый блокнот (One-Time Pad).

**Криптосистемы, защищенные по вычислениям**: Это системы, которые считаются безопасными, если взлом требует неприемлемо большого времени или ресурсов. Пример: RSA, AES.

**Листинг кода:**

class CaesarCipher:  
 def \_\_init\_\_(self, shift):  
 self.shift = shift  
 self.alphabet = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФ1ХЦЧШЩЪЫЬЭЮЯ '  
 self.alphabet\_size = len(self.alphabet)  
  
 def encrypt(self, text):  
 encrypted\_text = ''  
 for char in text.upper():  
 if char in self.alphabet:  
 new\_index = (self.alphabet.index(char) + self.shift) % self.alphabet\_size  
 encrypted\_text += self.alphabet[new\_index]  
 else:  
 encrypted\_text += char  
 return encrypted\_text  
  
 def decrypt(self, text):  
 decrypted\_text = ''  
 for char in text.upper():  
 if char in self.alphabet:  
 new\_index = (self.alphabet.index(char) - self.shift) % self.alphabet\_size  
 decrypted\_text += self.alphabet[new\_index]  
 else:  
 decrypted\_text += char  
 return decrypted\_text  
  
def main():  
 while True:  
 mode = input("Выберите режим (шифрование - 1 /дешифрование - 2): ").strip().lower()  
  
 if mode != '1' and mode != '2':  
 print("Неверный режим. Пожалуйста, выберите 'шифрование - 1' или 'дешифрование - 2'.")  
 continue  
  
 shift = int(input("Введите сдвиг: "))  
 text = input("Введите текст: ")  
  
 cipher = CaesarCipher(shift)  
  
 if mode == '1':  
 result = cipher.encrypt(text)  
 elif mode == '2':  
 result = cipher.decrypt(text)  
  
 print(f'Результат: {result}')  
  
  
if \_\_name\_\_ == "\_\_main\_\_":  
 main()