**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет «Информационных технологий и программной инженерии»

Кафедра «Систем обработки данных»

|  |  |
| --- | --- |
| Направление подготовки: | 09.03.02 - Информационные системы и технологии |
| Направленность (профиль): | Технологии проектирования защищенных систем обработки данных |

**Лабораторная работа № 2**

по дисциплине:

|  |
| --- |
| Кроссплатформенное программирование |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Выполнили студенты группы ИСТ-321 | |  |
|  |  | Чаушьянц Р.В., Нариц А.А. | | |
|  |  | *Фамилия И. О.* | | |
|  |  | Руководитель | Заведующий кафедры СОД | |
| *оценка* |  |  | *уч. степень, уч. звание* | |
|  |  | Бородянский Юрий Михайлович | | |
| *дата, подпись* |  | *Фамилия И. О.* | | |

**Цель работы.**

Изучение общих принципов программирования в среде java. Написание приложения, осуществляющего «шифрование» текста путем преобразования символов с помощью побитовых операций.

**Задание.**

Необходимо создать консольное приложение, осуществляющее «шифрование» небольшого текста путем сложения по "XOR" числового кода каждого символа с ключом "sekret". Кроме сложения по "XOR", приложение должно поддерживать шифрование с помощью циклического сдвига вдоль кодовой таблицы (алфавита) на заданное число позиций. Текст для шифрования взять произвольно в количестве не менее трех строк. Приложение должно иметь текстовое меню со следующими пунктами:

1. Шифрование с помощью операции "XOR"
2. Шифрование с помощью циклического сдвига
3. Ввести число позиций для шифрования путем циклического сдвига

При выборе пунктов 1 и 2, приложение должно распечатывать исходный текст, зашифрованный текст и расшифрованный текст. При выборе пункта 3 приложение должно запросить у пользователя число, которое определяет величину сдвига, затем также распечатать исходный, зашифрованный и расшифрованный текст. Числовое значение буквы исходного текста брать по её порядковому номеру в алфавите. Так букве "А" соответствует число 1, букве "Б" соответствует число 2 и т.д. Регистр букв не учитывать.

**Теоретическая часть.**

**Введение** Java – это высокоуровневый объектно-ориентированный язык программирования, разработанный компанией Sun Microsystems (ныне Oracle). Он широко используется для создания веб-приложений, мобильных программ, десктопных и серверных систем. Основными преимуществами Java являются его кроссплатформенность, надежность, простота и мощная стандартная библиотека.

**Общие принципы программирования в Java** Программирование в Java основывается на нескольких ключевых принципах:

1. **Объектно-ориентированное программирование (ООП)** – Java поддерживает основные концепции ООП, такие как инкапсуляция, наследование и полиморфизм, что позволяет организовывать код в виде объектов и классов.
2. **Кроссплатформенность** – код Java компилируется в байт-код, который выполняется на Java Virtual Machine (JVM), что позволяет запускать программы на различных операционных системах без изменений.
3. **Автоматическое управление памятью** – Java использует механизм «сборки мусора» (Garbage Collection), который освобождает неиспользуемую память автоматически.
4. **Строгая типизация** – каждая переменная в Java должна иметь определенный тип данных, что помогает избежать многих ошибок на этапе компиляции.
5. **Безопасность** – Java имеет встроенные механизмы защиты, которые предотвращают выполнение вредоносного кода.

**Написание приложения для шифрования текста с помощью побитовых операций** Рассмотрим создание простого консольного приложения на Java, которое выполняет шифрование текста путем изменения битов символов.

1. **Создание основного класса** Напишем Java-программу, которая шифрует текст с использованием побитовой операции XOR.

import java.util.Scanner;

public class BitwiseEncryption {

public static String encryptDecrypt(String input, char key) {

StringBuilder output = new StringBuilder();

for (char c : input.toCharArray()) {

output.append((char) (c ^ key));

}

return output.toString();

}

public static void main(String[] args) {

Scanner scanner = new Scanner(System.in);

System.out.println("Введите текст для шифрования:");

String text = scanner.nextLine();

char key = 'K'; // Ключ для XOR-шифрования

String encrypted = encryptDecrypt(text, key);

System.out.println("Зашифрованный текст: " + encrypted);

String decrypted = encryptDecrypt(encrypted, key);

System.out.println("Расшифрованный текст: " + decrypted);

}

}

1. **Объяснение кода**

* encryptDecrypt – метод, выполняющий XOR-шифрование.
* main – основная функция, принимающая ввод пользователя и выполняющая шифрование и расшифровку.
* key – символ, который используется для XOR-преобразования.

1. **Компиляция и запуск** Сохраните код в файле BitwiseEncryption.java, затем выполните:

javac BitwiseEncryption.java

java BitwiseEncryption

После ввода текста программа зашифрует его, а затем расшифрует с использованием того же ключа.

**Заключение** Использование побитовых операций в Java позволяет реализовывать простые методы шифрования, такие как XOR-шифрование. Это демонстрирует работу с побитовыми операциями, управлением строками и взаимодействием с пользователем, что является важным аспектом программирования в Java.

**Ход работы.**

**Выводы.**