**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.**

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

**Введение** Java – это один из самых популярных языков программирования, разработанный компанией Sun Microsystems (ныне Oracle). Его главными преимуществами являются кроссплатформенность, надежность и удобство работы. Благодаря виртуальной машине Java (JVM) код можно запускать на разных операционных системах без изменений. Этот язык широко используется в веб-разработке, создании мобильных приложений, корпоративного программного обеспечения и других областях.

**Основные принципы программирования в Java** Программирование в Java базируется на нескольких ключевых концепциях:

1. **Объектно-ориентированное программирование (ООП)** – код организуется в классы и объекты, что упрощает его поддержку и расширение.
2. **Кроссплатформенность** – компиляция в байт-код позволяет выполнять программы на разных устройствах без изменений исходного кода.
3. **Автоматическое управление памятью** – благодаря механизму «сборки мусора» освобождение памяти происходит автоматически.
4. **Безопасность и надежность** – встроенные механизмы безопасности позволяют предотвращать выполнение вредоносного кода.

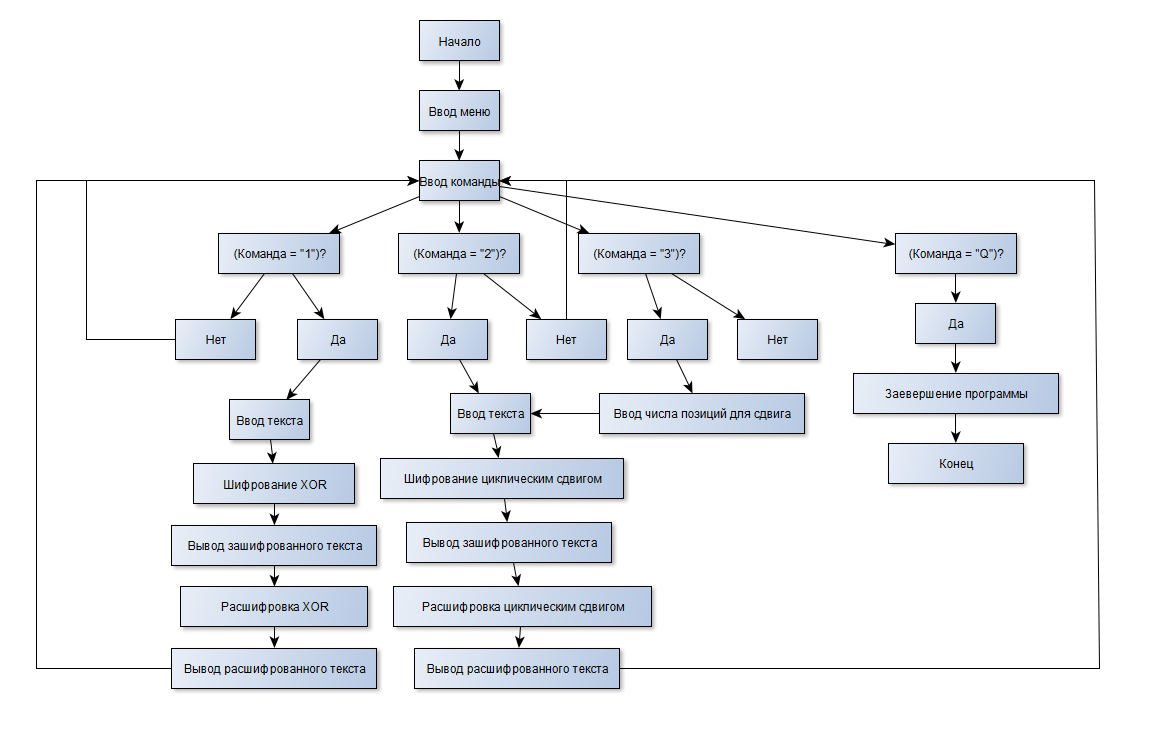
**Шифрование текста с помощью побитовых операций** Побитовые операции – это эффективный способ обработки данных на уровне отдельных битов. В криптографии такие операции применяются для простых методов шифрования, включая шифрование на основе логической операции XOR (исключающее ИЛИ).

Принцип работы XOR-шифрования заключается в том, что каждый бит входных данных изменяется в зависимости от соответствующего бита ключа. Если бит ключа равен 1, бит изменяется на противоположный, если 0 – остается неизменным. Такой метод позволяет зашифровать данные, а затем, применяя ту же операцию с тем же ключом, выполнить расшифровку.

**Заключение** Использование побитовых операций, таких как XOR, является эффективным методом простого симметричного шифрования. Java предоставляет удобные инструменты для работы с такими операциями, что делает возможным реализацию надежных алгоритмов защиты данных. Данный подход используется в различных областях, включая базовое шифрование, цифровую обработку сигналов и сетевую безопасность.

**Ход работы.**

В ходе работы была написана программа, реализующая следующие функции: iифрование с помощью операции "XOR", шифрование с помощью циклического сдвига.



import java.util.Scanner;

public class Main {

static final String KEY = "sekret";

static final String ALPHABET = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя?,. ";

static final Scanner scanner = new Scanner(System.in);

public static int shift = 0;

public static String xor\_cipher(String text) {

StringBuilder result = new StringBuilder();

for (int i = 0; i < text.length(); i++) {

result.append((char) (text.charAt(i) ^ KEY.charAt(i % KEY.length())));

}

return result.toString();

}

public static String cyclic\_shift(String text, boolean encode) {

StringBuilder result = new StringBuilder();

int position\_shift;

int index\_alfabet;

for (int i = 0; i < text.length(); i++) {

index\_alfabet = ALPHABET.indexOf(text.charAt(i));

position\_shift = encode ? (index\_alfabet + shift) : (index\_alfabet - shift);

position\_shift = (position\_shift + ALPHABET.length()) % ALPHABET.length();

result.append(ALPHABET.charAt(position\_shift));

}

return result.toString();

}

public static void command1() {

System.out.println("Введите текст:");

String original\_text = scanner.nextLine();

String encrypted\_text = xor\_cipher(original\_text.toLowerCase());

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

String decrypted\_text = xor\_cipher(encrypted\_text);

System.out.println("Расшифрованный текст: " + decrypted\_text + '\n');

}

public static void command2() {

System.out.println("Введите текст:");

String original\_text = scanner.nextLine();

String encrypted\_text = cyclic\_shift(original\_text.toLowerCase(), true);

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

String decrypted\_text = cyclic\_shift(encrypted\_text, false);

System.out.println("Расшифрованный текст: " + decrypted\_text + '\n');

}

public static void command3() {

System.out.println("Введите число позиций для сдвига:");

int old\_shift = shift;

shift = Integer.parseInt(scanner.nextLine());

System.out.printf("Число позиций для сдвига изменилось с %d на %d\n\n", old\_shift, shift);

}

public static void print\_menu() {

String text = """

1 - Шифрование с помощью операции XOR

2 - Шифрование с помощью циклического сдвига (Текущий сдвиг - %d)

3 - Ввести число позиций для шифрования путем циклического сдвига

Q - Выход из программы

""";

System.out.printf(text, shift);

}

public static void main(String[] args) {

String command;

do {

print\_menu();

command = scanner.nextLine();

switch (command) {

case "1":

command1();

break;

case "2":

command2();

break;

case "3":

command3();

break;

case "Q":

break;

default:

System.out.println("Команда не распознана!\n");

}

} while (!"Q".equals(command));

scanner.close();

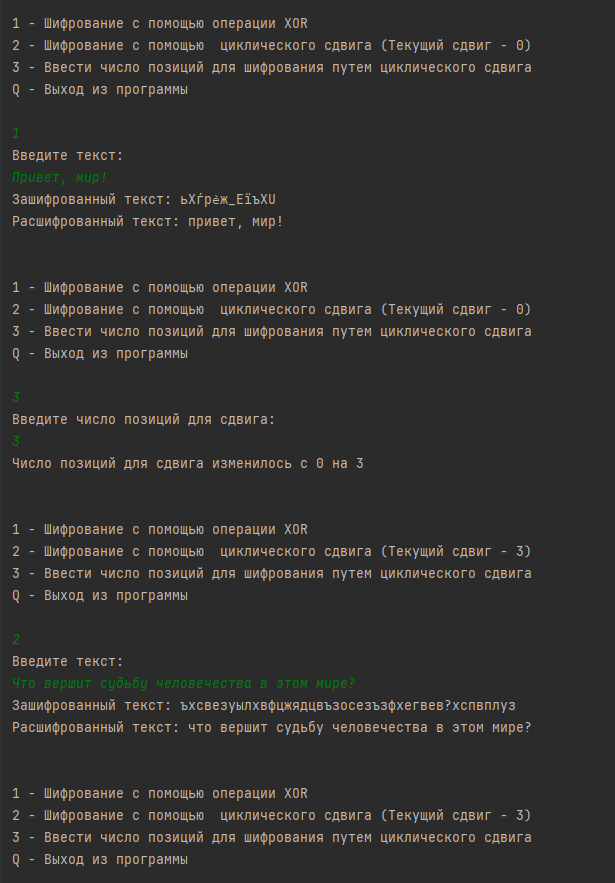
}

}

// Привет, мир!

// Что вершит судьбу человечества в этом мире?

// Эта строка включает все буквы русского алфавита.



**Выводы.**

Входе выполнения лабораторной работы, мы научились нескольким важным навыкам, которые пригодятся нам в будущем:

1. **Работа со строками и символами** – мы научились находить символы в алфавите, изменять их и обрабатывать текст, что полезно для программирования и работы с данными.
2. **Шифрование с использованием XOR** – этот метод важен в криптографии и защите данных, например, для шифрования сообщений.
3. **Циклический сдвиг** – помогает в обработке текста, создании шифров и работы с алгоритмами перестановок, что используется в защите информации и обработке данных.
4. **Работа с пользовательским вводом** – наш код умеет взаимодействовать с пользователем, считывать данные, обрабатывать их и выдавать результат, что важно при создании приложений и интерфейсов.
5. **Использование меню и обработка команд** – мы реализовали систему команд, которая делает программу удобной для пользователя, а это ключевой навык при разработке программного обеспечения.

Эти знания помогут нам создавать более сложные программы, понимать принципы шифрования и обработки данных, а также развивать навыки в программировании на Java.