Отчет по лаборатной работе №7

по предмету Информационная безопасность

Алхимова Дарья Сергеевна

Содержание

[Цель работы 1](#__RefHeading___Toc298_394501025)

[Задание 1](#__RefHeading___Toc300_394501025)

[Теоретическое введение 1](#__RefHeading___Toc302_394501025)

[Выполнение лабораторной работы 2](#__RefHeading___Toc304_394501025)

[Выводы 9](#__RefHeading___Toc306_394501025)

[Список литературы 9](#__RefHeading___Toc308_394501025)

# Цель работы

Освоить на практике применение режима однократного гаммирования.

# Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:  
1. Определить вид шифротекста при известном ключе и известном открытом тексте.  
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# Теоретическое введение

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком +) между элементами гаммы и элементами подлежащего сокрытию текста. Напомним, как работает операция XOR над битами: 0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 0. Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, вос- пользовавшись таблицей ASCII-кодов.

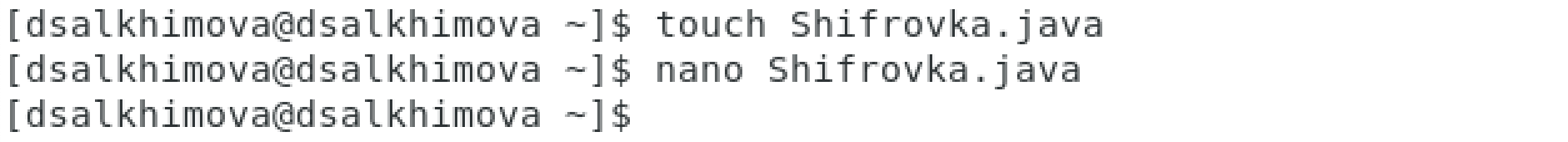
Необходимые и достаточные условия абсолютной стойкости шифра:  
+ полная случайность ключа;  
+ равенство длин ключа и открытого текста;  
+ однократное использование ключа.

Метод гаммирования становится бессильным, если известен фрагмент исход- ного текста и соответствующая ему шифрограмма. В этом случае простым вычи- танием по модулю 2 получается отрезок псевдослучайной последовательности и по нему восстанавливается вся эта последовательность.

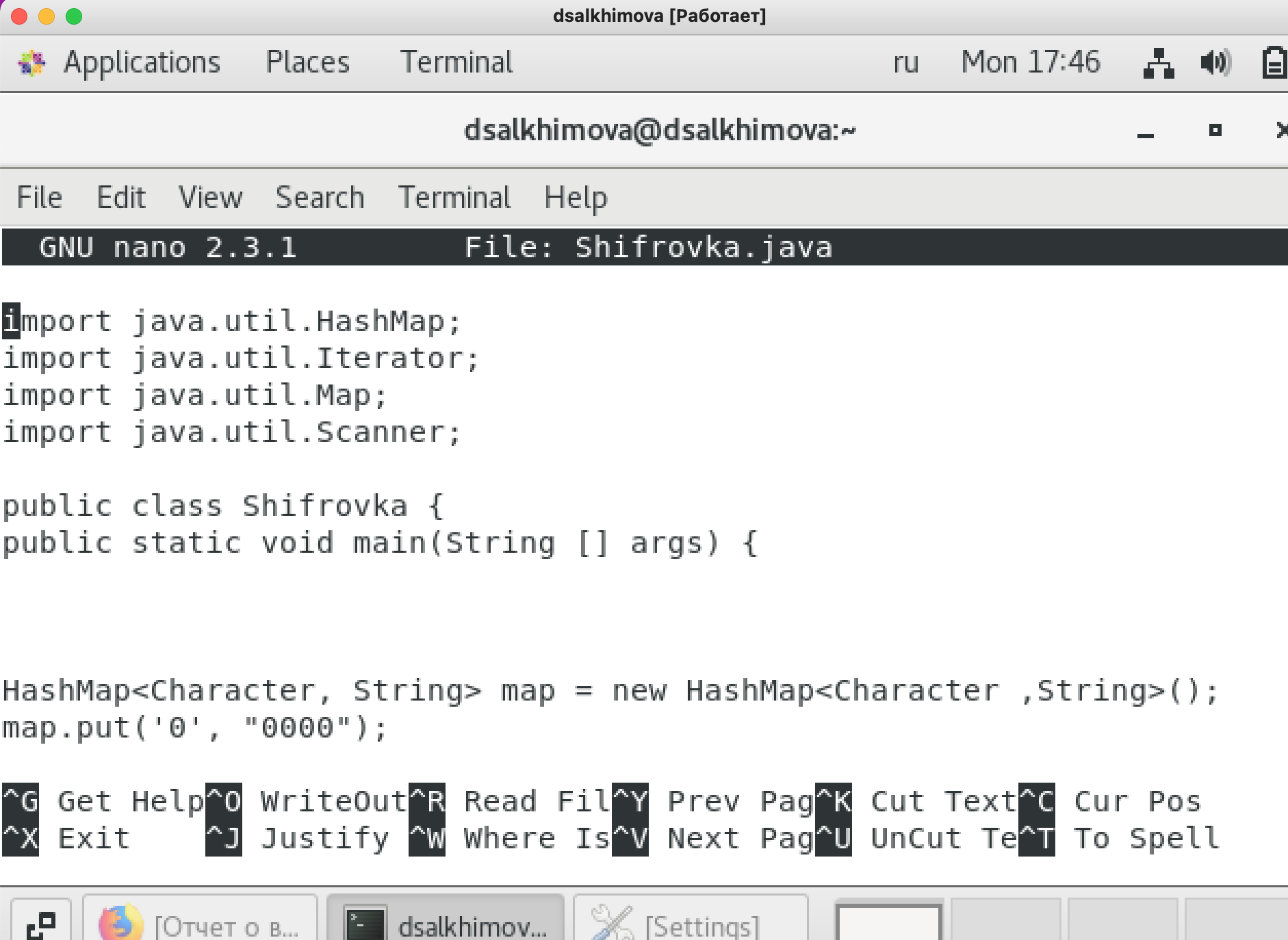
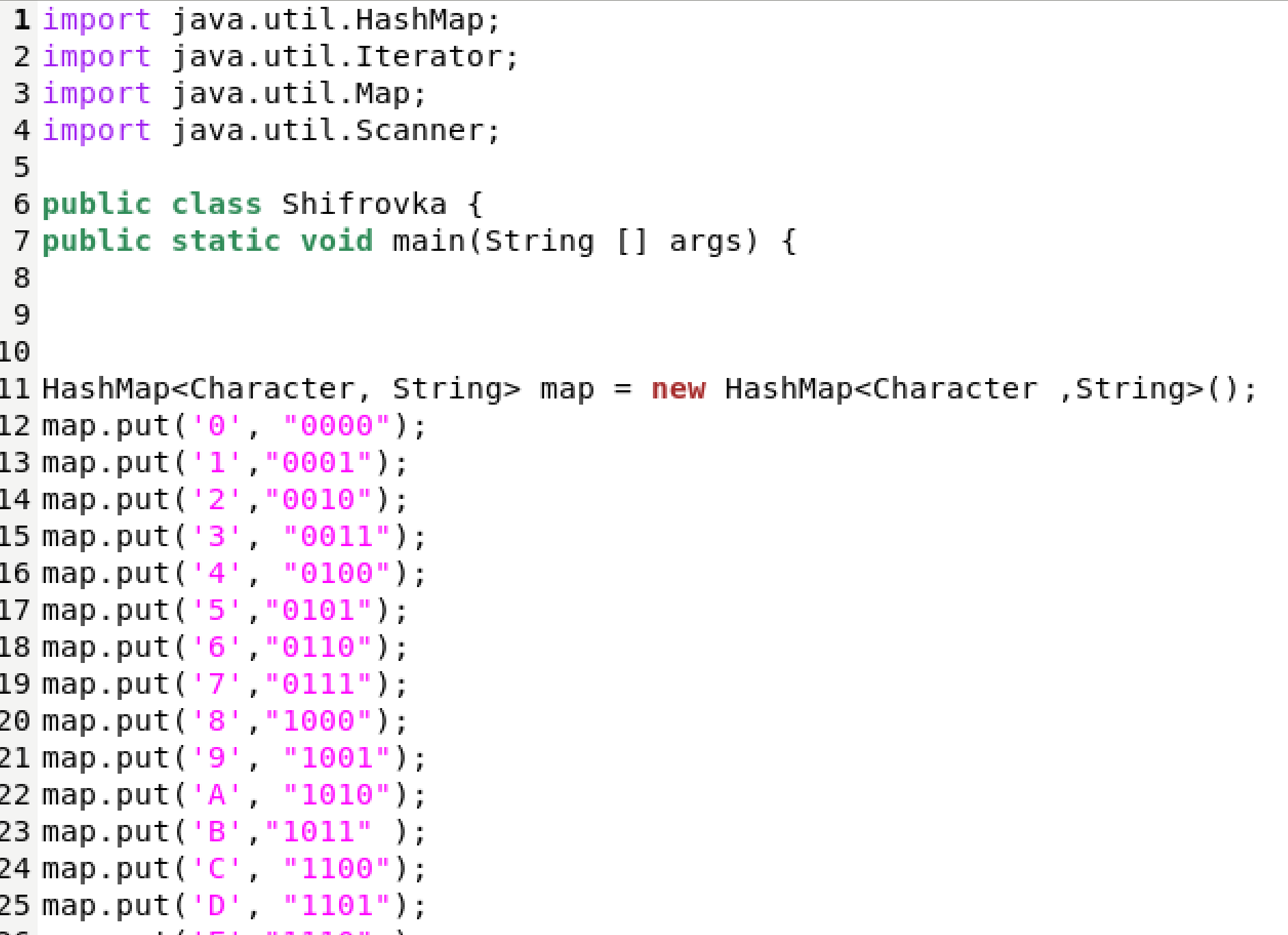
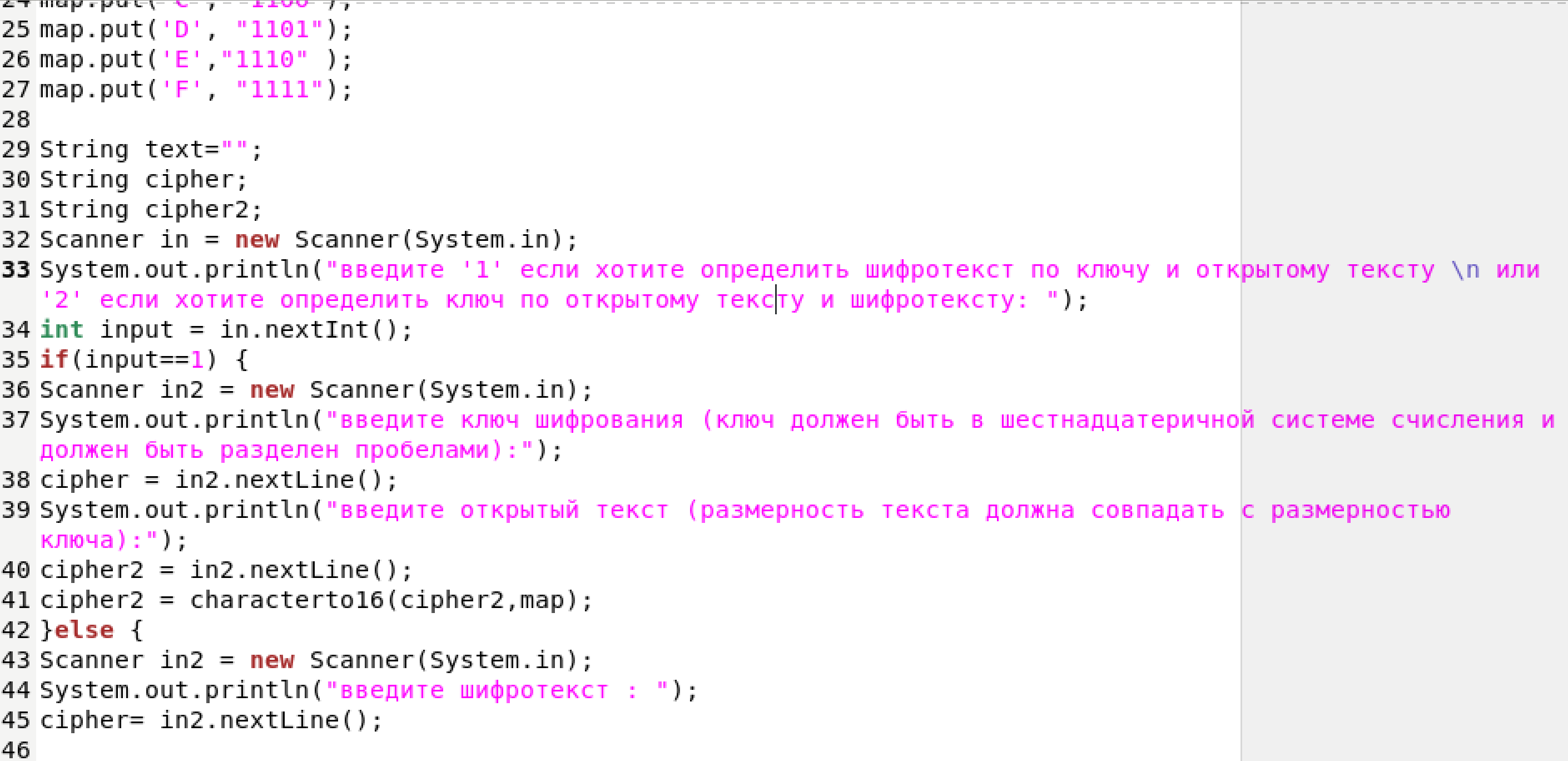
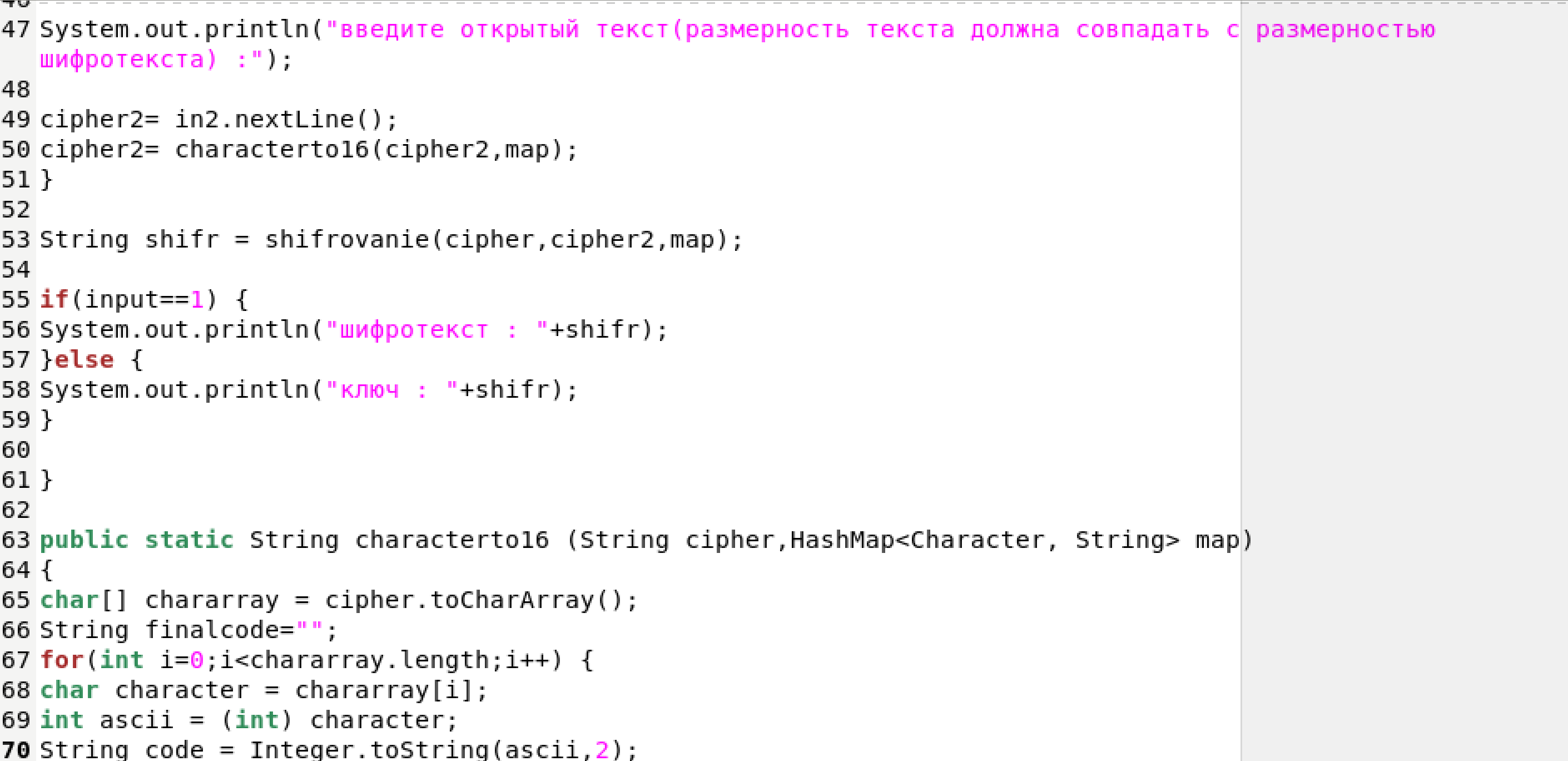
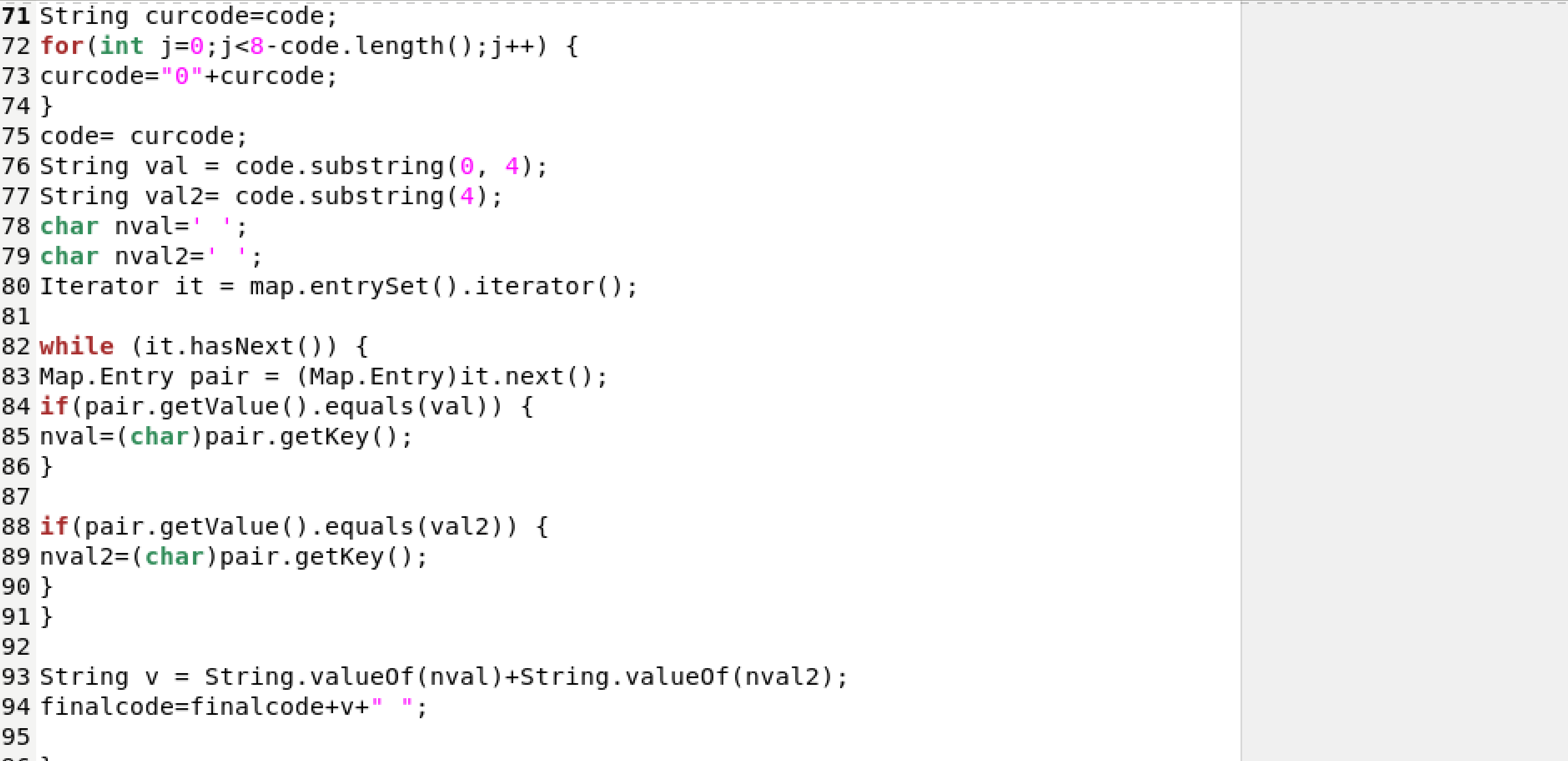
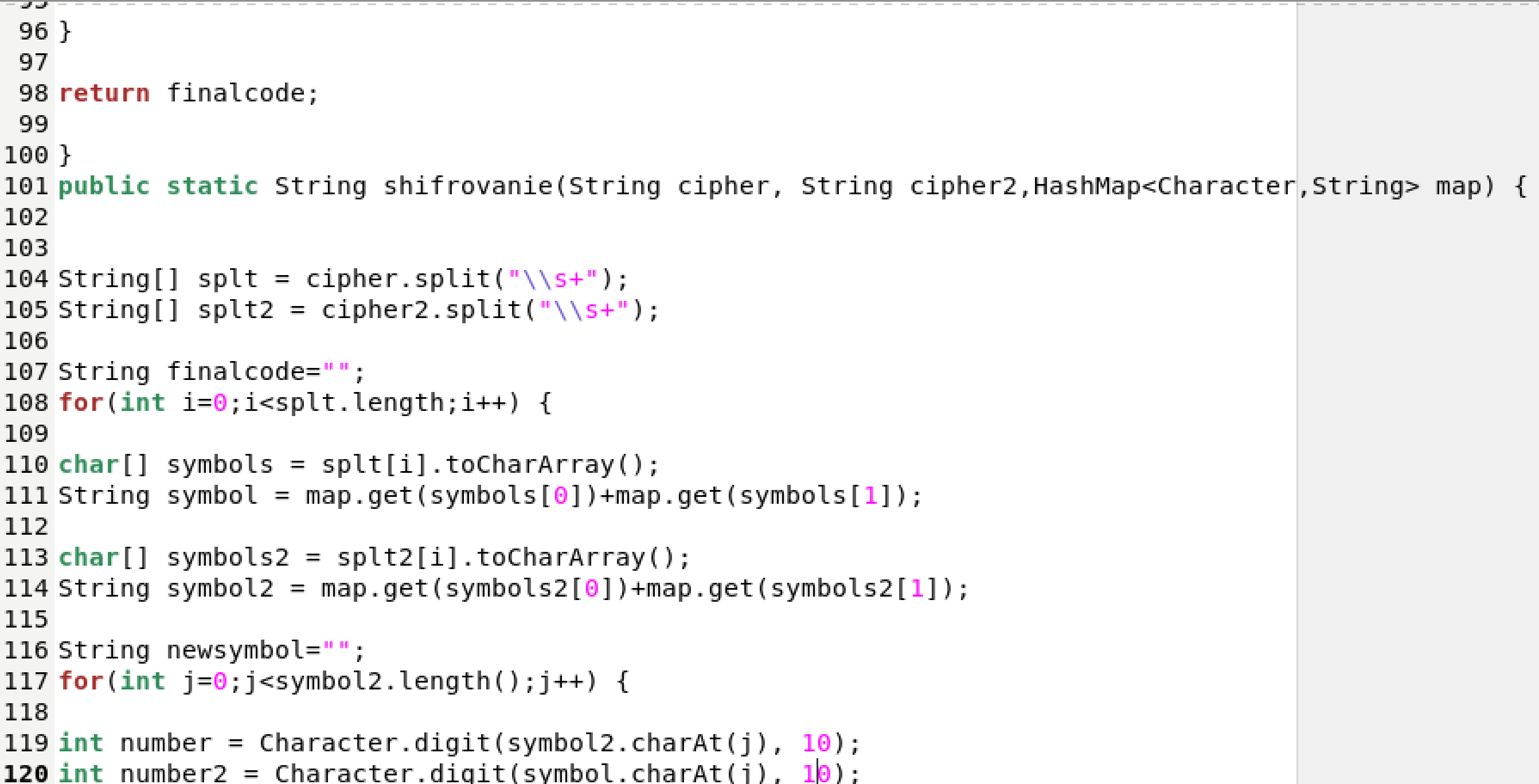
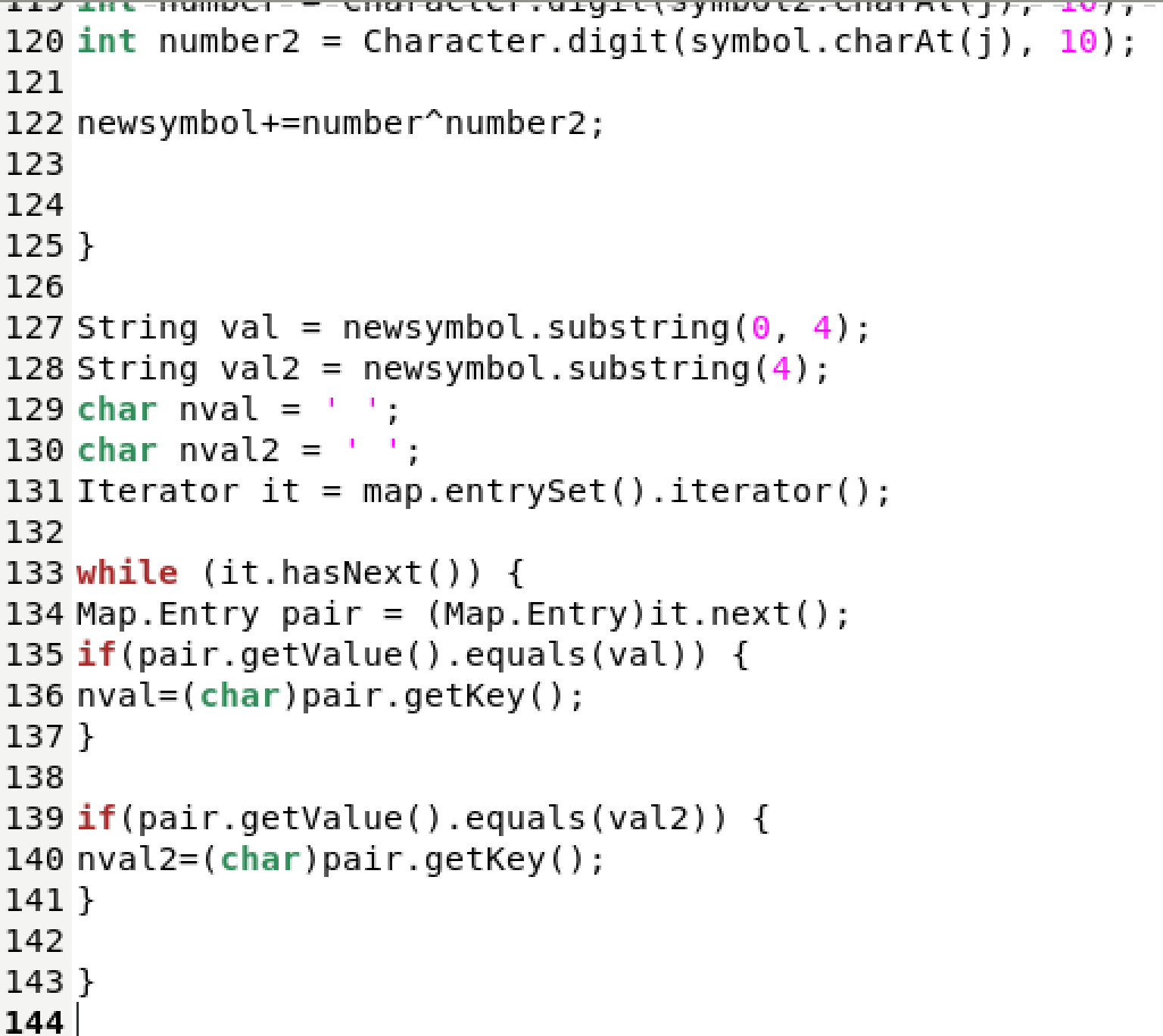
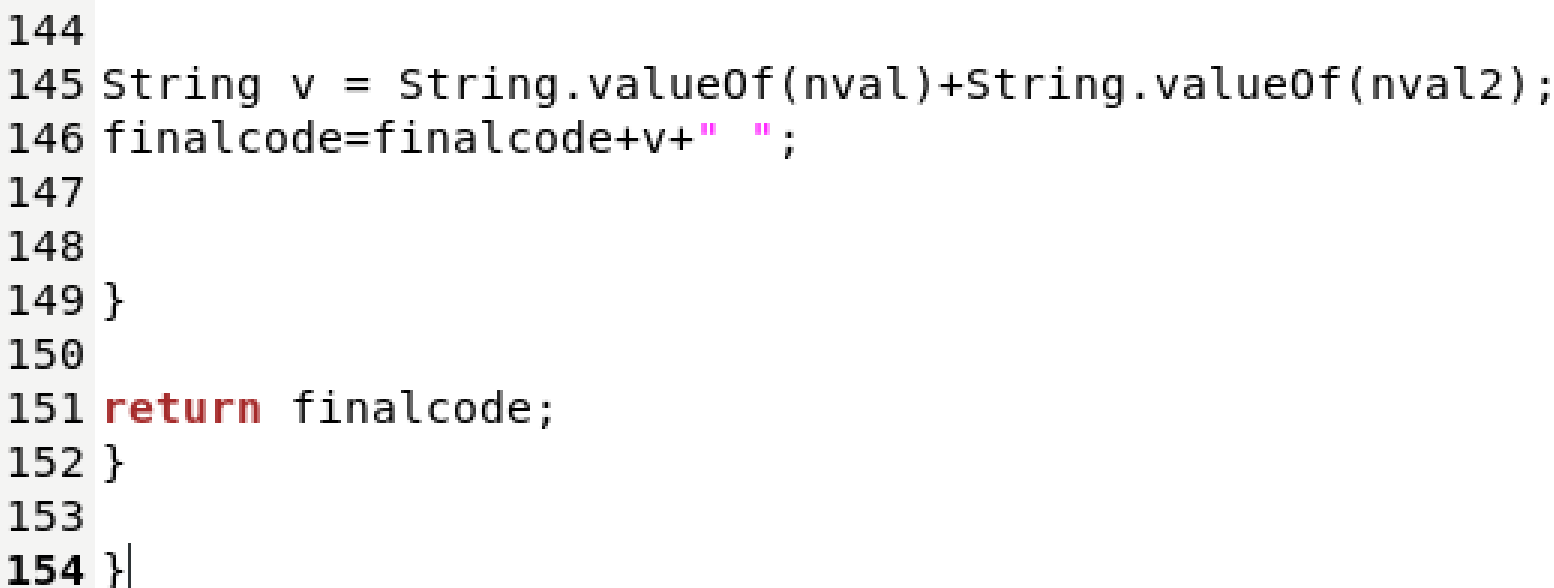
Алгоритм гаммирования:  
1. Генерация сегмента гаммы H(1) и наложение его на соответствующий участок шифруемых данных.  
2. Подсчет контрольной суммы участка, соответствующего сегменту гаммы H(1).  
3. Генерация с учетом контрольной суммы уже зашифрованного участка данных следующего сегмента гамм H(2).  
4. Подсчет контрольной суммы участка данных, соответствующего сегменту данных H(2) и т.д.

# Выполнение лабораторной работы

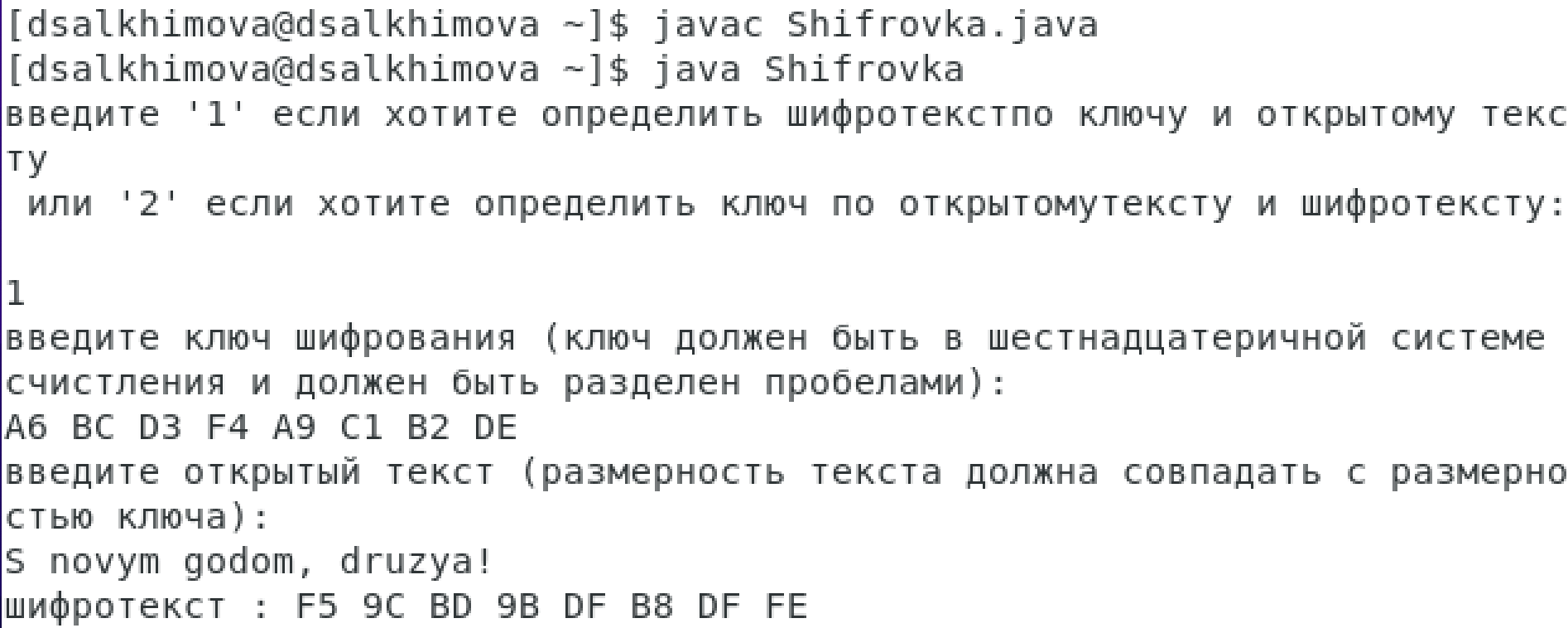
1. Создала файл программы и открыла его для заполнения кодом. ([рис. 1](images7/1.png)).

* 
* Создание файла программы

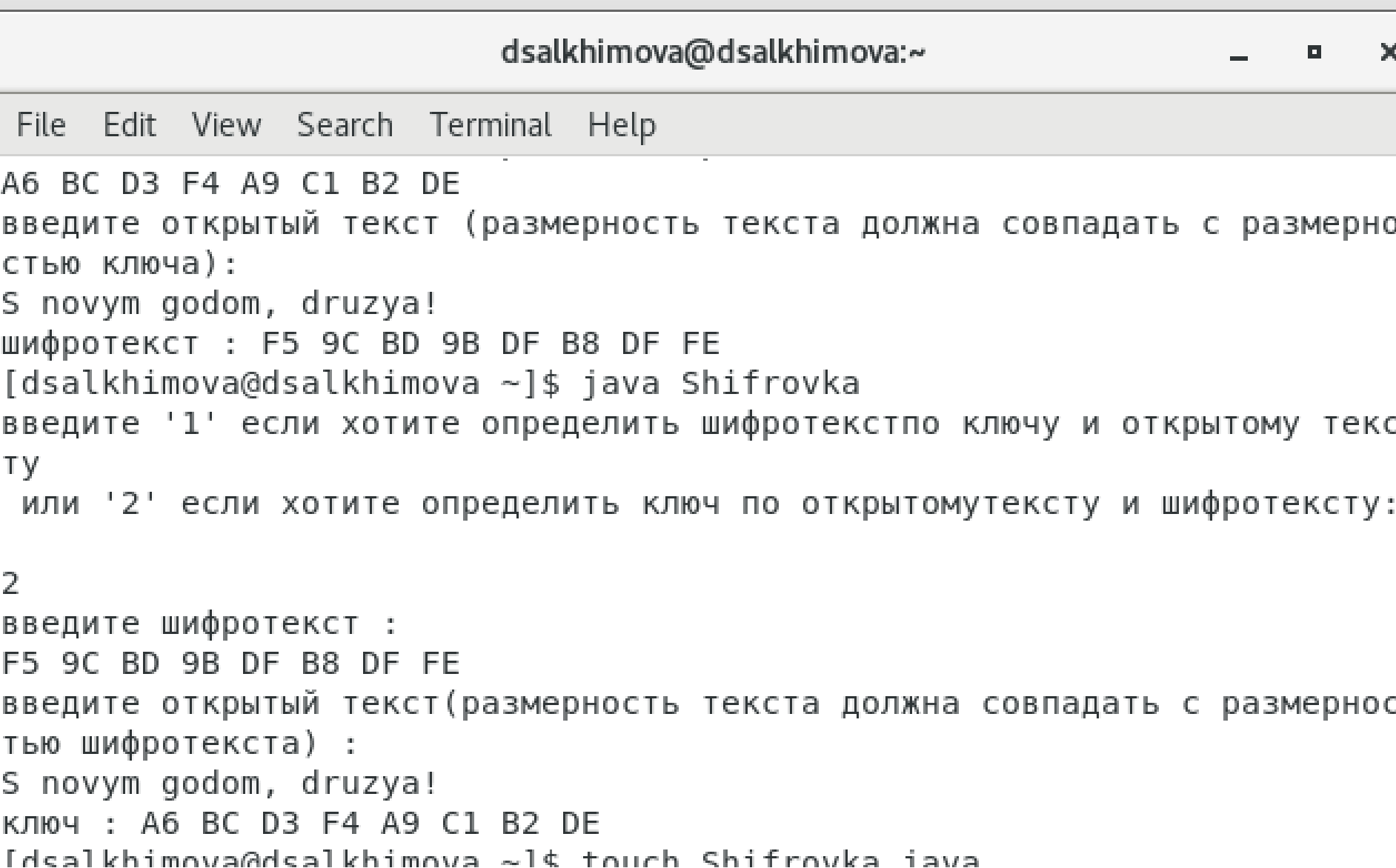
1. Заполнила файл кодом программы гаммирования ([рис. 2](images7/2.png)).

* 
* Фрагмент программы гаммирования
* Полный текст программы ([рис. 3](images7/3.png), [рис. 4](images7/4.png), [рис. 5](images7/5.png), [рис. 6](images7/6.png), [рис. 7](images7/7.png), [рис. 8](images7/8.png), [рис. 9](images7/9.png)):
* 
* Листинг программы 1/7
* 
* Листинг программы 2/7
* 
* Листинг программы 3/7
* 
* Листинг программы 4/7
* 
* Листинг программы 5/7
* 
* Листинг программы 6/7
* 
* Листинг программы 7/7

1. Проверила правильность выполнения программы гаммирования по первому сценарию (см. раздел Задание) ([рис. 10](images7/10.png)).

* 
* Запуск программы по сценарию 1

1. Проверила правильность выполнения программы гаммирования по второму сценарию (см. раздел Задание) ([рис. 11](images7/11.png)).

* 
* Запуск программы по сценарию 2

# Выводы

В процессе выполнения данной лабораторной работы я приобрела навыки применения режима однократного гаммирования.

# Список литературы

1. Описание лабораторной работы 7 - URL: <https://esystem.rudn.ru/pluginfile.php/1652175/mod_resource/content/2/007-lab_crypto-gamma.pdf>
2. Установка javac - URL: <https://stackoverflow.com/questions/5407703/javac-command-not-found>