НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет информационных технологий

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) Программная инженерия и компьютерные науки

Предмет: Защита информации

Лабораторная работа № 2

Тема: **Криптографические методы защиты информации**

Выполнил, гр 20209 Княжев М.А.  
Преподаватель Перов А.А.

Новосибирск  
2023

**Содержание**

Оглавление

[Цель лабораторной работы 2](#_Toc148589629)

[Задание: 3](#_Toc148589630)

[Выполнение лабораторной работы: 4](#_Toc148589631)

[Пункт1 4](#_Toc148589632)

[Пункт 2 8](#_Toc148589633)

[Пункт 3 18](#_Toc148589634)

[Ссылка на архив с программами: 26](#_Toc148589635)

# 

# Цель лабораторной работы

Цель работы – ознакомиться с криптографическими методами защиты информации.

# Задание:

Княжев Михаил в группе 6 по списку.

1. Разработать поточный шифр для шифрования/расшифрования строки, введённой с клавиатуры. Шифр Вернама.

2. Разработать блочный шифр для шифрования/расшифрования файла. Skipjack.

3. Реализовать произвольную хеш-функцию (известную или на основе блочного шифра). MD5.

# Выполнение лабораторной работы:

Реализация пунктов было выполнено на языке java. Детальное описание будет в скриншотах после //.

Реализация шифра Вернама и Skipjack представлена в 3 классах: Main (ввод начальных данных), Encrypt (шифрование), Decrypt (дешифрование).

Реализация блочной хеш функции(MD5) взятой с википедии представлена в 2 классах: Main (ввод начальных данных), MD5 (реализация самой хеш функции).

## Пункт1

Алгоритм Вернама использует случайный ключ равный длине входящей строки. Шифрование происходит применением побитового исключающего или между ключем шифрования и входящим сообщением.

Класс Main представлен на рисунке 1.

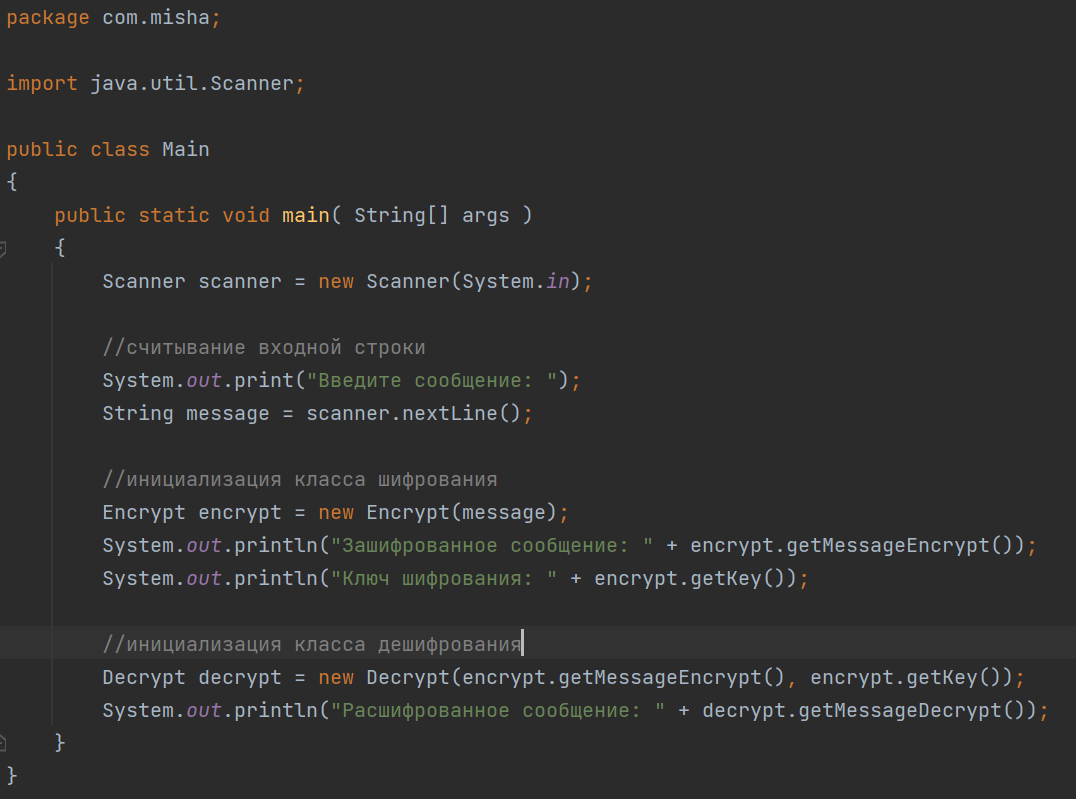


рисунок 1

Класс Encryt показан на рисунке 2.

рисунок 2

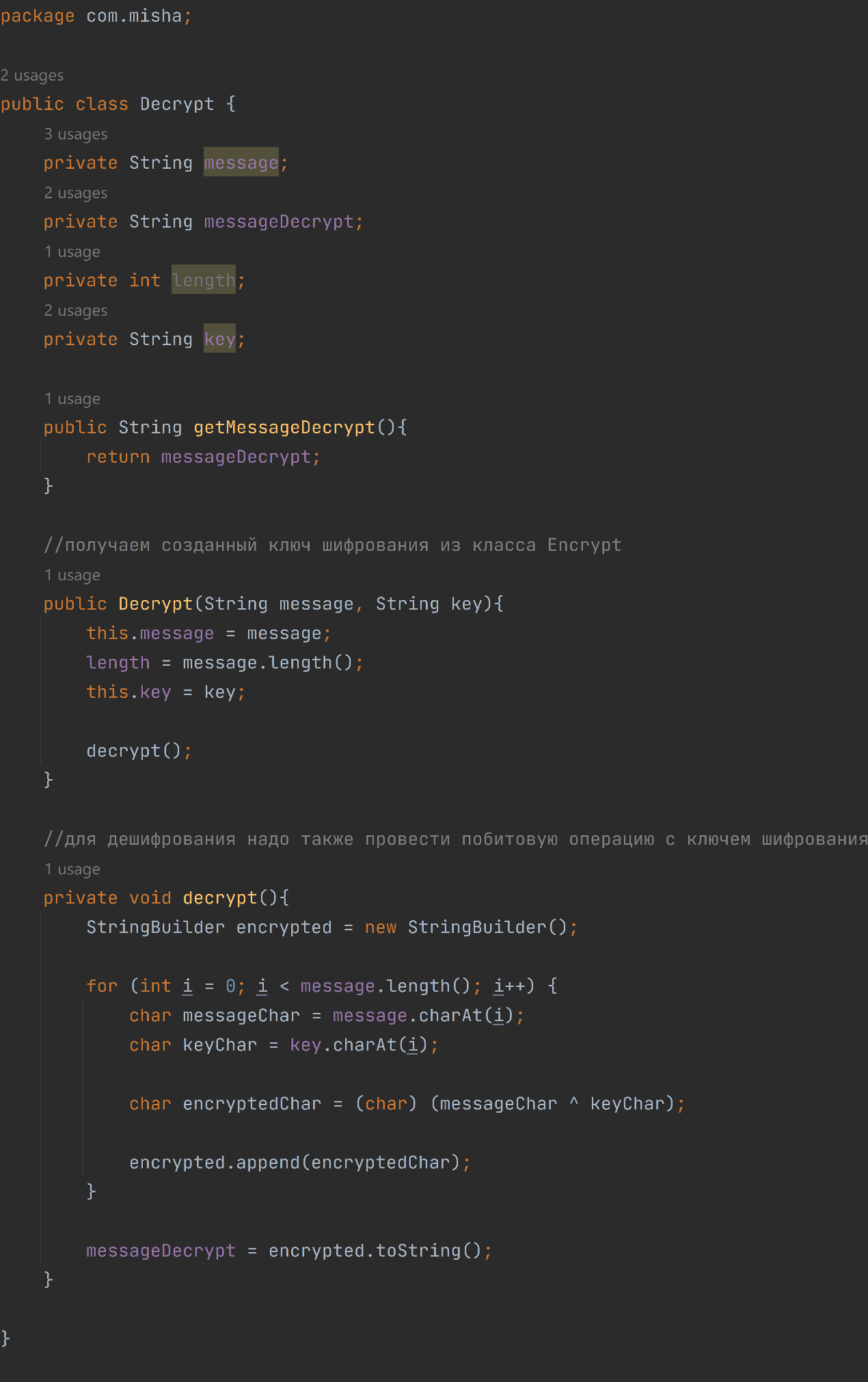
Класс шифрования, он же Encryt показан на рисунке 3.

рисунок 3

Тестирование программы представлена на рисунках 4, 5.

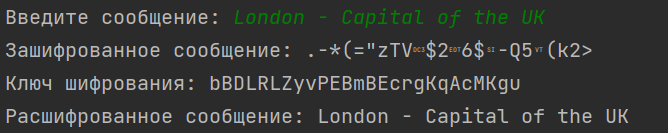


рисунок 4

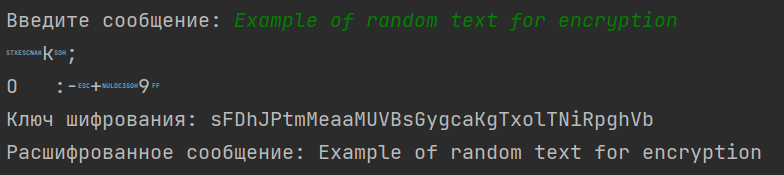


рисунок 5

Как можно заметить, программа корректно шифрует и расшифровывает фразы, введенные с клавиатуры. Также можно заметить, что вышли два совершенно различных зашифрованных сообщения.

## Пункт 2

Алгоритм Skipjack требует разбиения блоков сообщения на 8 байт, то есть главная задача считать файл, а потом разделить на 8 символов и применить библиотеку шифрования. Также необходимо проделать такую же манипуляцию с зашифрованным файлом, считать 8 байт для расшифровки сообщения. Важным уточнением является что шифрованный файл представлен в виде последовательности байтов, а также что класс дешифрования не начнет дешифровку пока не найдет в начале ключевое слово key с самим ключем.

Класс Main представлен на рисунке 6.

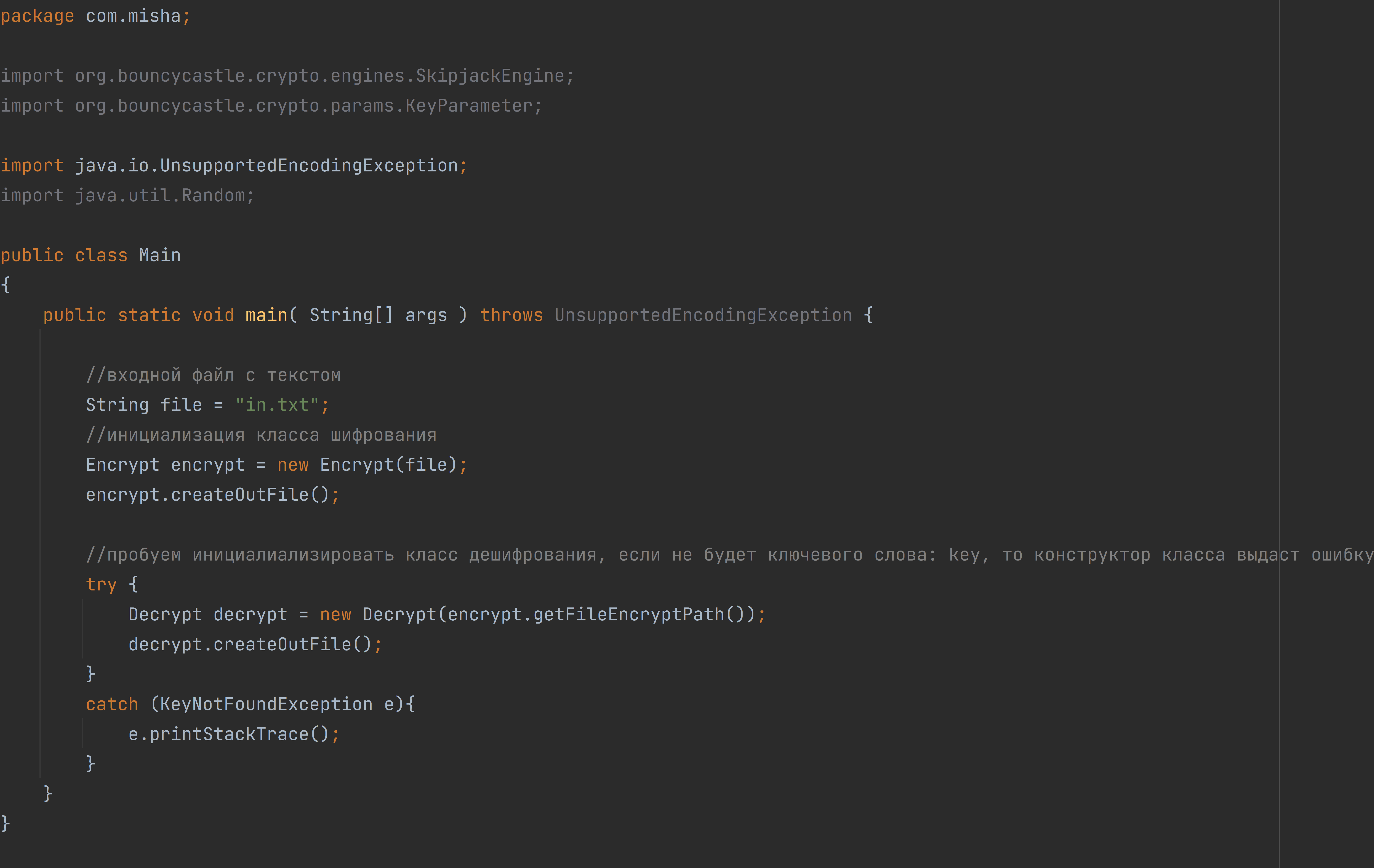


рисунок 6

Класс Encrypt представлен на рисунках 7, 8, 9.

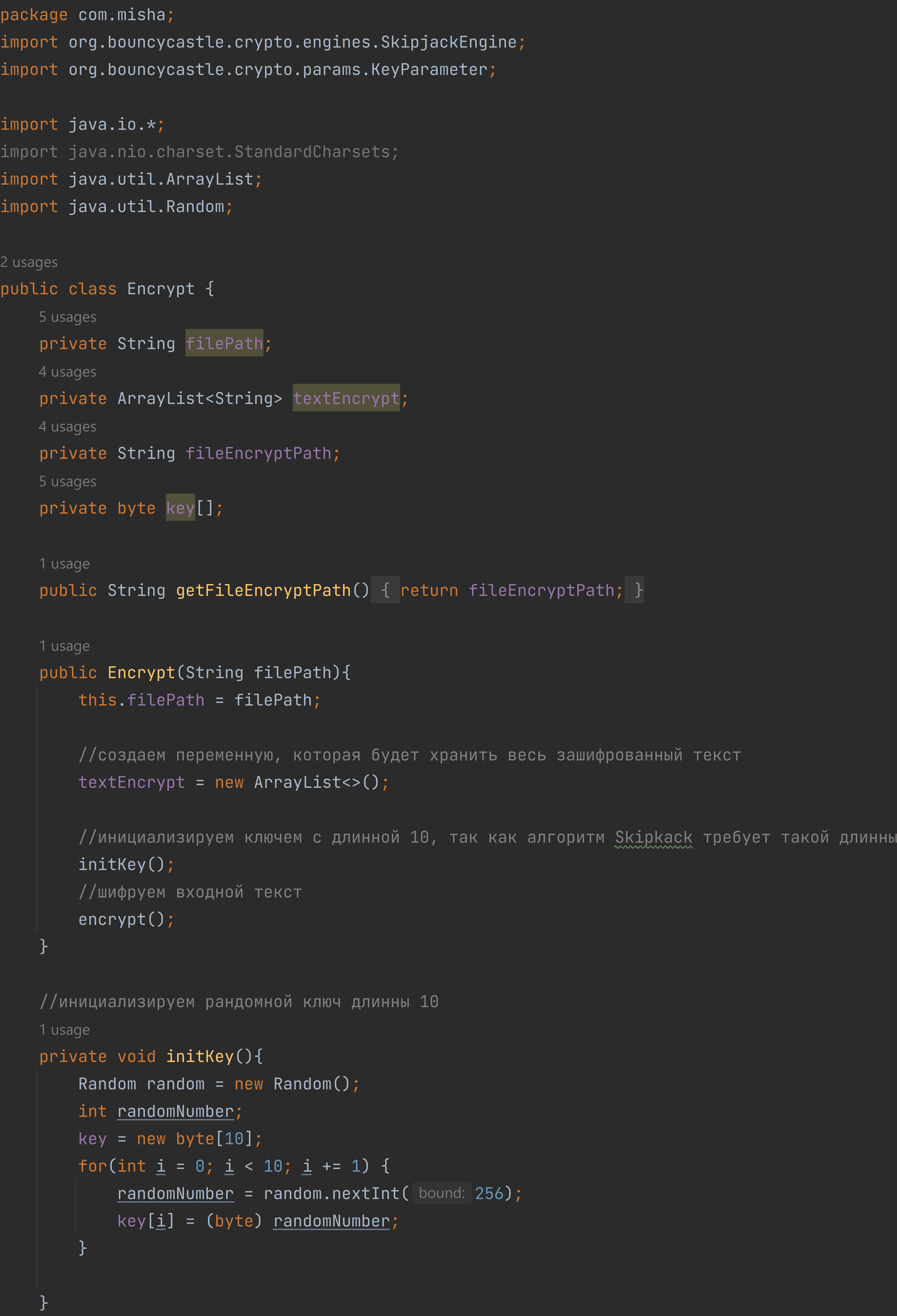
рисунок 7



рисунок 8



рисунок 9

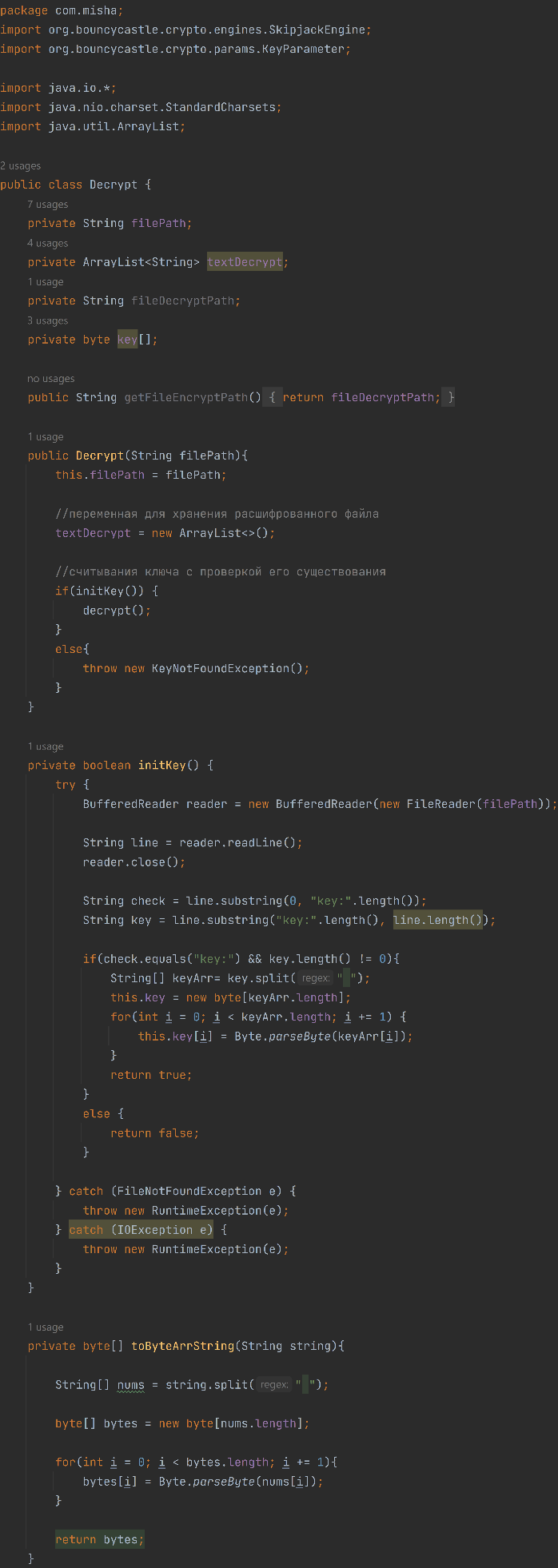
Класс Decrypt представлен на рисунках 10, 11, 12.

Рисунок 10

рисунок 11

рисунок 12

Тестирование программы предоставлено в виде текста, файлы будут приложены в архиве к программам.

Входящий файл: There are a number of traditions for weddings that have survived into the 21st century.

It is still traditional for the bride and groom to have their own parties the night before getting married.

The groom's party is called a 'Stag party', while the bride's is known as a 'Hen party'.

On the morning of the wedding, the groom should not see the bride. If he does, this is bad luck.

The bride puts on her special wedding dress, which is usually white. She also needs to wear 'something old,

something new, something borrowed and something blue'.

At the church, or registry office, the bride and groom exchange rings before walking together back down the aisle.

When they get outside, the bride throws her bouquet in the air. Tradition says that whoever catches it will be the next person to get married.

But it's not only the bride who throws something. All the people at the wedding throw confetti and rice over the happy couple.

Finally, after the reception, the bride and groom drive off to have their honeymoon.

Зашифрованный файл: key:-52 50 -67 105 -71 -11 -12 97 98 -122

-118 10 -113 69 -65 32 -87 20 -40 -69 -73 110 98 109 100 126 -96 -35 42 -44 -84 -38 80 -87 -98 -8 -51 -21 -19 1 13 -68 10 -120 -38 -106 -25 -62 22 -22 -72 12 -42 88 81 118 50 -116 19 -58 -30 -56 114 -88 118 70 -72 103 -119 -1 -22 114 97 84 -101 -55 3 -103 3 81 -10 38 12 -100 -90 103 96 -31 43 84 103 35 70 -121 127 -110 -17 -45

-61 -99 -107 -100 -84 -92 -61 0 -6 -34 -2 -85 -68 21 -127 23 46 -88 41 6 61 -17 93 80 10 72 109 113 -27 53 -51 -59 72 -69 96 -42 -13 74 -82 97 -109 91 69 97 -61 83 91 -117 101 -88 43 -37 2 -12 -15 21 -114 -55 111 100 -72 -76 99 95 87 86 45 73 -125 -41 -22 -63 -58 -87 62 -17 117 83 102 -114 -12 28 117 -104 101 -16 4 -33 29 122 -10 15 89 69 106 39 74 83 -32 -71 73 23 20 106 2 115 29 -18 127 -73 71 -95

85 57 -47 92 -88 -15 -24 110 127 66 37 -32 -25 97 -54 56 -21 109 59 23 69 -69 -79 14 54 -10 97 -72 60 -116 -93 71 -78 -90 113 -75 -21 102 -10 82 80 41 -100 116 -103 -109 -106 55 -36 -126 97 -83 23 33 -30 -121 51 -57 13 -91 -104 47 32 -109 -32 -106 -32 72 12 -37 -127 -72 -111 -36 88 -46 -89 -37 -93 100 -44 46 -84 -117 96 47 -97 105

28 89 45 -35 125 -114 -14 123 76 -73 -27 -75 26 -84 -51 90 -94 81 77 -6 -68 16 52 -82 29 91 23 7 -109 -60 104 -44 8 40 79 -14 -107 0 109 49 123 34 -86 10 -64 -76 -38 -2 -76 76 24 94 49 -57 -113 23 -22 31 -16 92 -27 -75 -2 -23 -57 124 -2 7 72 -23 -34 13 53 -62 -11 -73 58 -119 20 123 124 107 -81 111 6 57 -92 -65 -11 77 -81 83 -96 106 23 -75

45 82 25 43 47 -127 -121 -48 -29 -126 -46 85 48 -4 65 -116 125 103 -71 -59 -110 25 -29 -64 58 25 7 -63 104 -118 108 0 56 -114 110 -115 5 67 -26 -120 -79 -14 53 57 117 96 6 -117 123 64 70 115 110 -103 -39 102 -7 118 47 21 85 26 120 -121 -71 -7 79 62 -91 -40 -96 113 112 -30 19 -70 -22 -98 65 -90 41 107 14 49 69 -92 6 42 -68 84 32 -107 -70 -25 -117 -18 -97 15 14 -124 -28 37 -52 74 124 -102 27 41 50 -3 -10 120

-108 87 44 -103 52 -73 7 50 -8 -11 115 -98 39 19 -64 83 -79 -24 -101 -45 -93 -64 -8 53 10 6 -47 9 22 50 104 -80 81 -78 -127 -108 23 -109 -53 -26 21 -19 -50 44 -7 -116 -58 48 -54 79 -44 -63 -98 92 7 -39

46 -52 4 111 -3 5 -1 -117 46 24 -53 126 109 -99 -23 -89 34 -107 108 -81 122 97 -25 -57 38 36 75 92 -72 -107 -68 8 -35 35 53 77 -57 44 60 10 108 -21 38 -31 61 100 -126 -25 94 47 116 -81 95 18 47 93 23 28 -107 -37 -88 -9 -58 69 -88 36 -22 -13 81 33 -27 -42 86 -76 -47 33 97 63 -89 -127 -46 -26 119 -104 104 -73 -84 10 36 8 -80 82 -78 -103 70 0 19 40 121 36 -44 -27 -87 58 -64 -119 65 -102 125 -82 127 -110 108 -99 -123 59 -58 -74 -110 -73

-82 31 -7 18 32 99 -39 96 -19 82 -15 79 -26 37 99 56 -105 96 -46 81 114 95 36 86 -20 16 99 89 119 56 43 112 60 -7 13 88 3 126 -74 -32 31 -123 105 97 53 -76 -21 -36 -55 -53 -92 105 3 -35 -63 -6 99 20 34 3 73 -90 125 126 -61 21 -77 -71 -50 20 -10 -80 -11 20 55 62 -49 62 -26 94 108 121 -44 63 63 -30 -127 -73 124 120 -6 -27 11 114 -70 63 -2 60 -6 -42 -50 -104 84 -95 -28 -12 62 14 91 21 115 -52 62 79 92 112 -28 27 -54 14 122 -127 46 -86 -54 -75 -115 101 -49 67 99 -44 -58 104 98 -34 -19 74 35 58 -37 -115 -95 -101

80 -4 -42 -56 62 -116 -32 64 -78 -53 96 102 -96 26 -75 -110 115 22 64 -107 39 31 9 -86 -3 80 68 119 59 -85 -34 100 -128 -111 0 80 -26 115 -126 79 -79 -24 -101 -45 -93 -64 -8 53 -29 70 -125 38 94 -15 -123 -37 -106 12 -68 -126 108 111 5 -25 112 99 74 -86 109 113 -77 86 -40 52 -92 116 -56 -120 45 -89 86 12 83 127 -75 -38 17 -116 -89 -105 -67 45 -64 1 -66 -8 -7 -72 114 118 -93 -109 -49 -19 -93 18 0 -111 -113 -58 -13 122 25 -70 -103 -84 -27 -56 -22 -57 -88 115 -109 -78 -48 -110 -26 -8

-5 -127 -123 -99 -59 86 17 -73 48 -122 62 32 -39 -75 -21 -19 -115 -98 106 20 47 104 125 24 -48 120 -9 43 27 62 127 50 -85 -19 61 50 -52 -31 -84 84 -39 -68 -51 56 103 -41 -113 11 -35 -24 -59 32 77 52 -85 27 124 -41 94 -99 29 25 5 49 -86 -19 9 34 -2 113 -89 70 -44 -79 55 -29 34 64 101 -96 5 -64 21 -17 74 -121 -22 108

Расшифрованный файл: There are a number of traditions for weddings that have survived into the 21st century.

It is still traditional for the bride and groom to have their own parties the night before getting married.

The groom's party is called a 'Stag party', while the bride's is known as a 'Hen party'.

On the morning of the wedding, the groom should not see the bride. If he does, this is bad luck.

The bride puts on her special wedding dress, which is usually white. She also needs to wear 'something old,

something new, something borrowed and something blue'.

At the church, or registry office, the bride and groom exchange rings before walking together back down the aisle.

When they get outside, the bride throws her bouquet in the air. Tradition says that whoever catches it will be the next person to get married.

But it's not only the bride who throws something. All the people at the wedding throw confetti and rice over the happy couple.

Finally, after the reception, the bride and groom drive off to have their honeymoon.

Как можно видеть программа корректно расшифровала файл.

## Пункт 3

Алгоритм взят с сайта: <https://ru.wikipedia.org/wiki/MD5>.

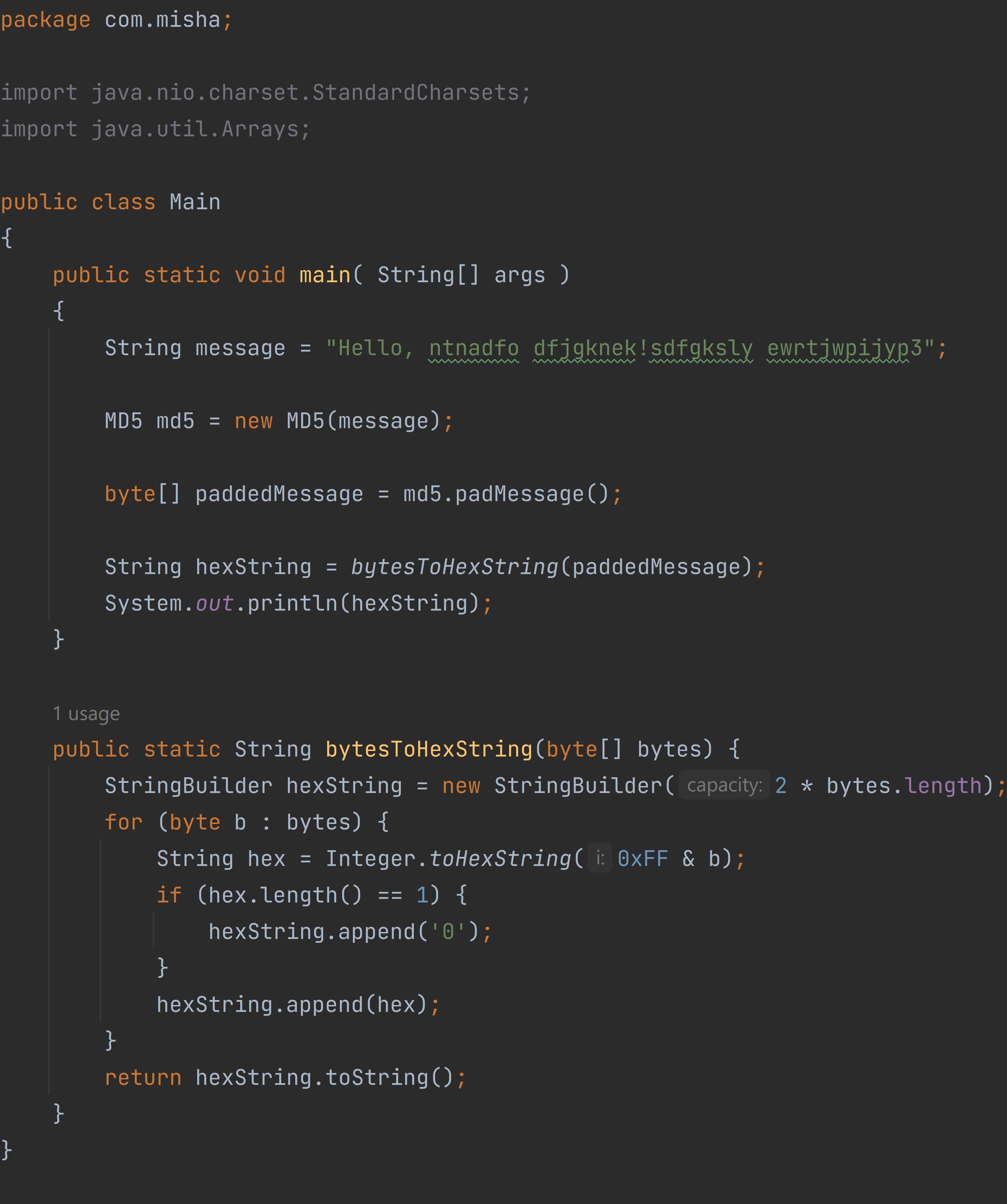
Класс Main показан на рисунке 14: 

рисунок 14

Класс MD5 показан на рисунке 15, 16, 17, 18, 19, 20:

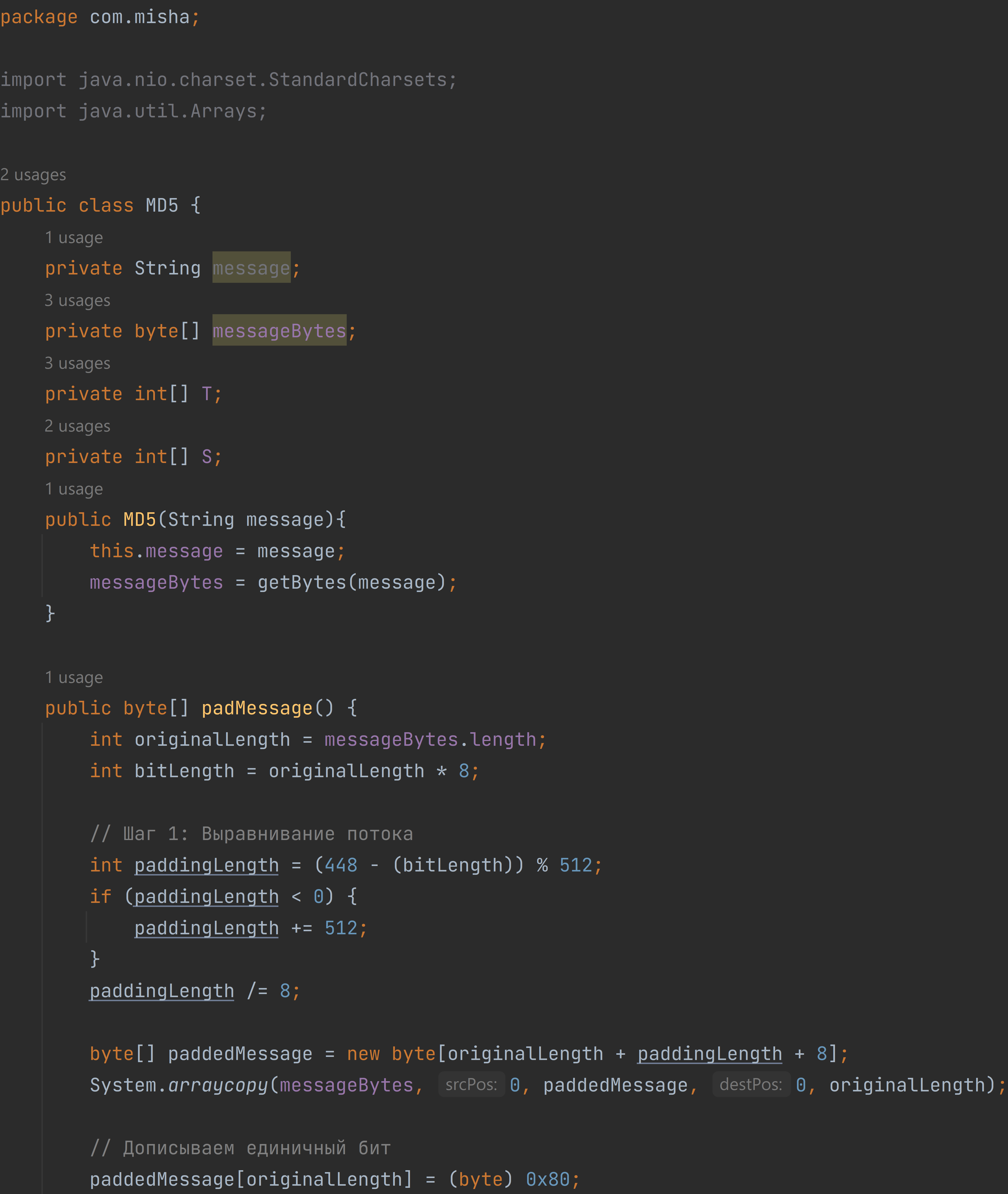


рисунок 15

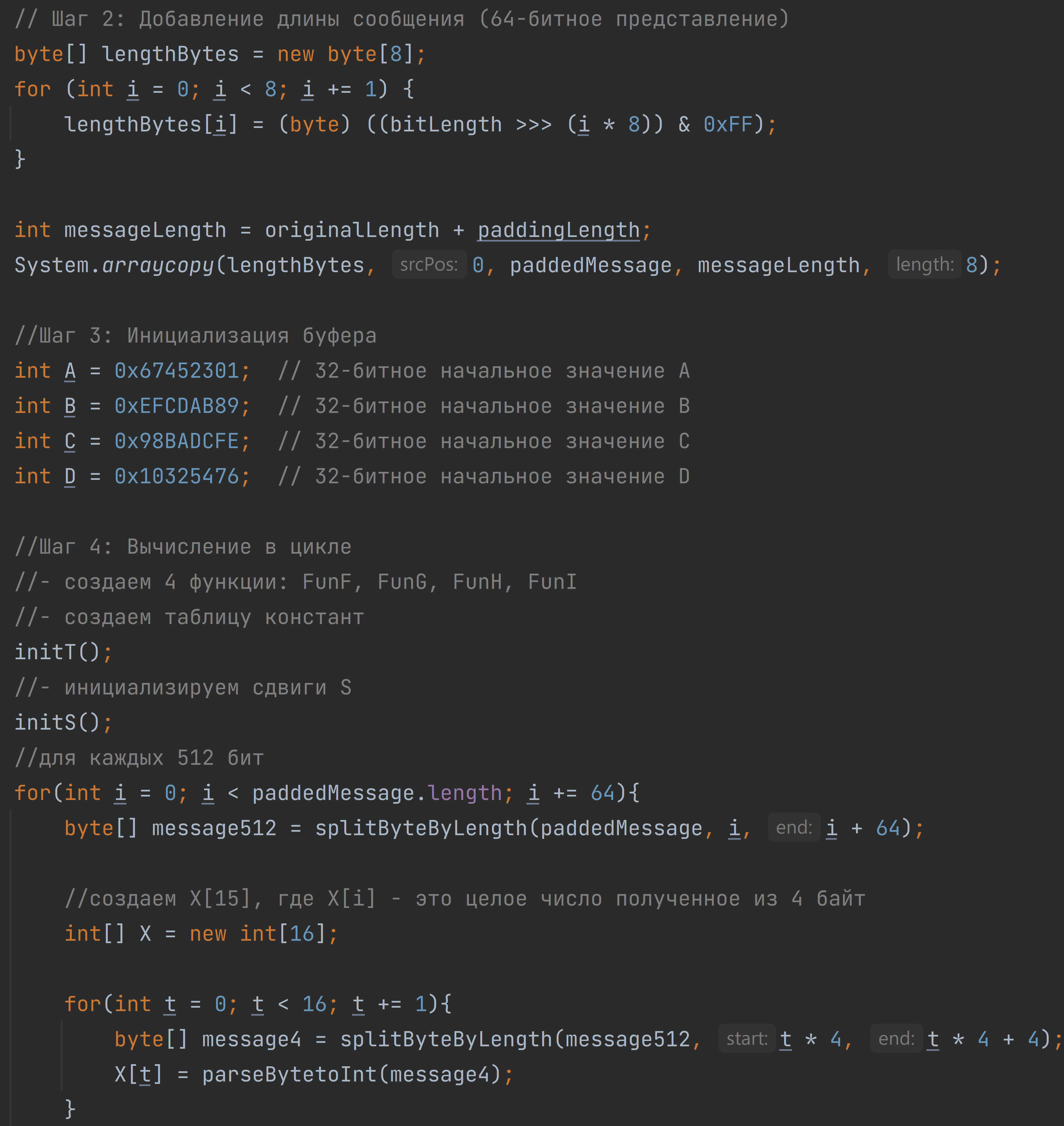
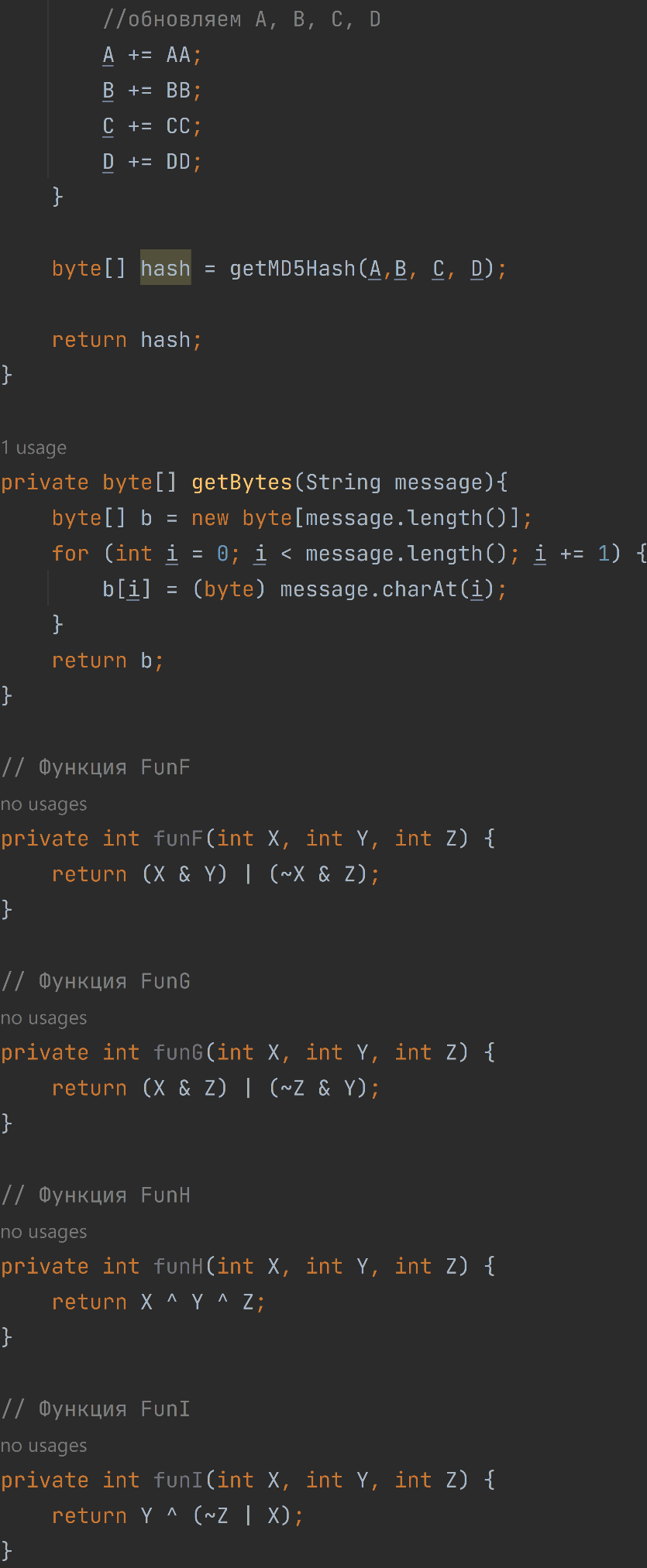


рисунок 16



рисунок 17

рисунок 18

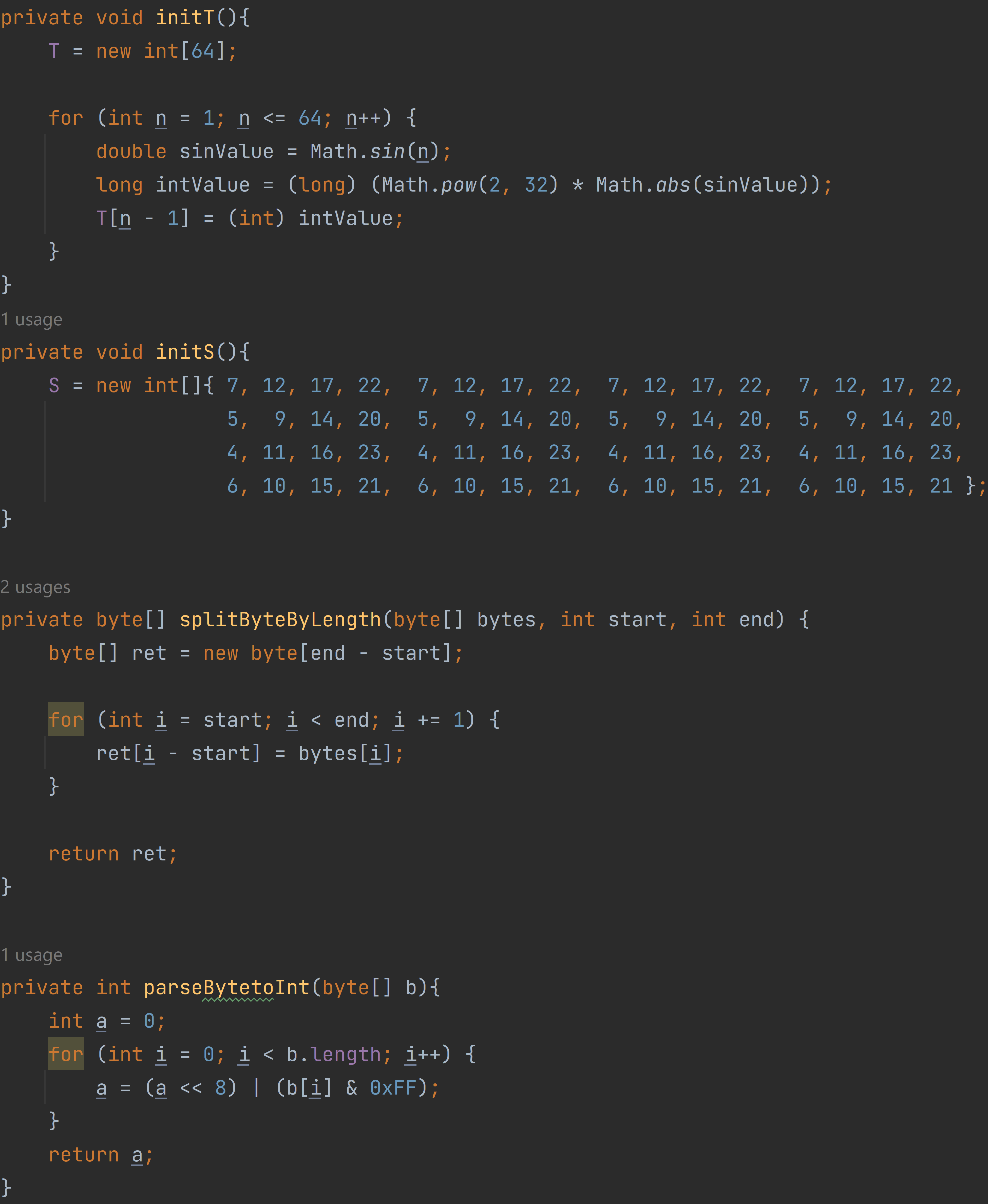


рисунок 19

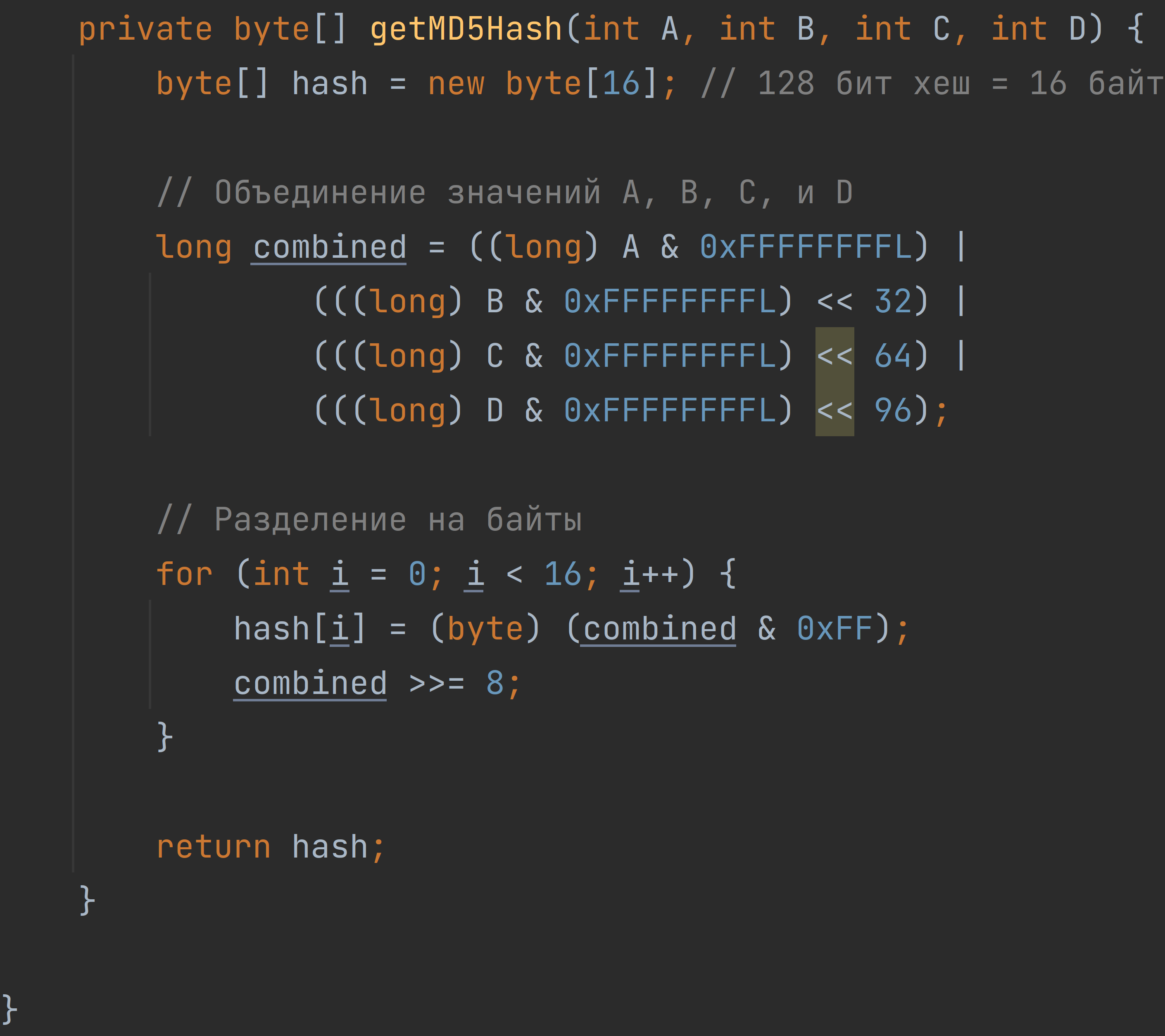


рисунок 20

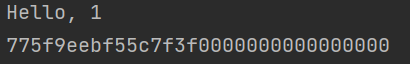
Тестирование показано на рисунках 21, 22:

рисунок 21



рисунок 22

Из картинок видно, что при незначительном изменение входных данных выходные данные значительно поменялись.

# Ссылка на архив с программами:

https://github.com/Knyazhev-Misha/data-protection-NSU.git