

Элементы криптографии. Однократное гаммирование

Венчаков Никита Юрьевич¹

17 октября, 2022

¹Российский университет дружбы народов, Москва, Россия

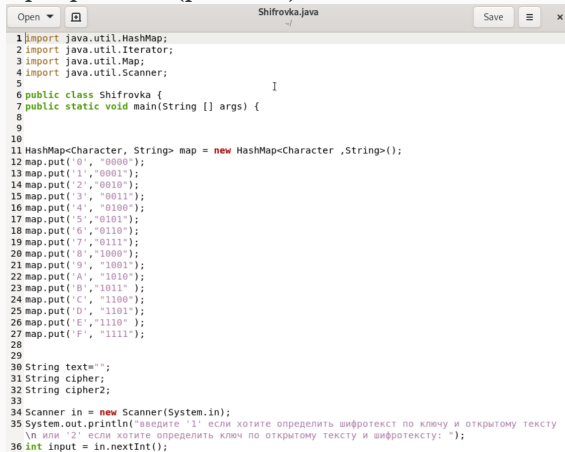
- Венчаков Никита Юрьевич
- студент 4 курса
- Студенческий билет: 1032196697
- группа НБИбд-01-19
- Российский университет дружбы народов
- venchakov2001@gmail.com

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

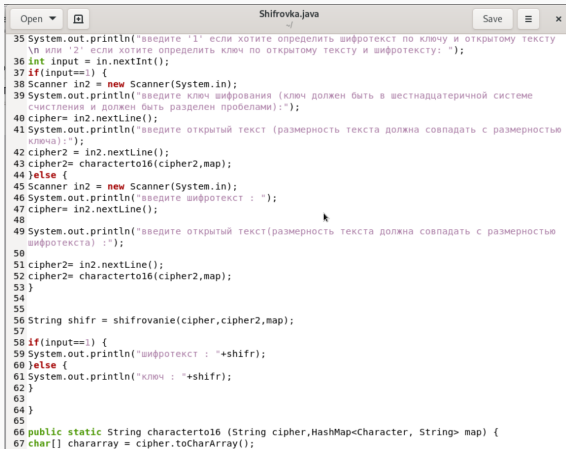
1. Создал программу на Java для гаммирования текста. Текст программы: (рис. N^о 1)



The screenshot shows a code editor window titled 'Shifrovka.java'. The code is as follows:

```
1 import java.util.HashMap;
2 import java.util.Iterator;
3 import java.util.Map;
4 import java.util.Scanner;
5
6 public class Shifrovka {
7     public static void main(String [] args) {
8
9
10
11     HashMap<Character, String> map = new HashMap<Character, String>();
12     map.put('0', "0000");
13     map.put('1', "0001");
14     map.put('2', "0010");
15     map.put('3', "0011");
16     map.put('4', "0100");
17     map.put('5', "0101");
18     map.put('6', "0110");
19     map.put('7', "0111");
20     map.put('8', "1000");
21     map.put('9', "1001");
22     map.put('A', "1010");
23     map.put('B', "1011");
24     map.put('C', "1100");
25     map.put('D', "1101");
26     map.put('E', "1110");
27     map.put('F', "1111");
28
29
30     String text="";
31     String cipher;
32     String cipher2;
33
34     Scanner in = new Scanner(System.in);
35     System.out.println("введите '1' если хотите определить шифротекст по ключу и открытому тексту
36     \n или '2' если хотите определить ключ по открытому тексту и шифротексту: ");
37     int input = in.nextInt();
```

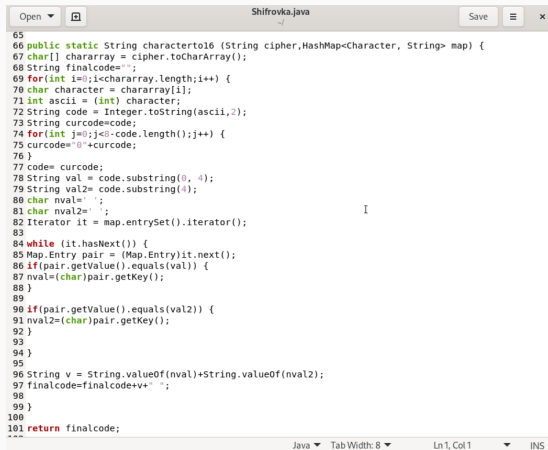
Часть программы №2



```
35 System.out.println("введите '1' если хотите определить шифротекст по ключу и открытому тексту  
  \n или '2' если хотите определить ключ по открытому тексту и шифротексту: ");  
36 int input = in.nextInt();  
37 if(input==1) {  
38 Scanner in2 = new Scanner(System.in);  
39 System.out.println("введите ключ шифрования (ключ должен быть в шестнадцатеричной системе  
  счисления и должен быть разделен пробелами):");  
40 cipher= in2.nextLine();  
41 System.out.println("введите открытый текст (размерность текста должна совпадать с размерностью  
  ключа):");  
42 cipher2 = in2.nextLine();  
43 cipher2= caracterto16(cipher2,map);  
44 }else {  
45 Scanner in2 = new Scanner(System.in);  
46 System.out.println("введите шифротекст : ");  
47 cipher= in2.nextLine();  
48  
49 System.out.println("введите открытый текст(размерность текста должна совпадать с размерностью  
  шифротекста) :");  
50  
51 cipher2= in2.nextLine();  
52 cipher2= caracterto16(cipher2,map);  
53 }  
54  
55  
56 String shifr = shifrovanie(cipher,cipher2,map);  
57  
58 if(input==1) {  
59 System.out.println("шифротекст : "+shifr);  
60 }else {  
61 System.out.println("ключ : "+shifr);  
62 }  
63  
64 }  
65  
66 public static String caracterto16 (String cipher,HashMap<Character, String> map) {  
67 char[] chararray = cipher.toCharArray();
```

2. (рис.№2)

Часть программы №3



```
65
66 public static String caractertol6 (String cipher,HashMap<Character, String> map) {
67 char[] chararray = cipher.toCharArray();
68 String finalcode="";
69 for(int i=0;i<chararray.length;i++) {
70 char character = chararray[i];
71 int ascii = (int) character;
72 String code = Integer.toString(ascii,2);
73 String curcode=code;
74 for(int j=0;j<8-code.length();j++) {
75 curcode="0"+curcode;
76 }
77 code= curcode;
78 String val = code.substring(0, 4);
79 String val2= code.substring(4);
80 char nval=' ';
81 char nval2=' ';
82 Iterator it = map.entrySet().iterator();
83
84 while (it.hasNext()) {
85 Map.Entry pair = (Map.Entry)it.next();
86 if(pair.getValue().equals(val)) {
87 nval=(char)pair.getKey();
88 }
89
90 if(pair.getValue().equals(val2)) {
91 nval2=(char)pair.getKey();
92 }
93
94 }
95
96 String v = String.valueOf(nval)+String.valueOf(nval2);
97 finalcode=finalcode+v+" ";
98
99 }
100
101 return finalcode;
102 }
```

3. (рис.№3)

Часть программы №4



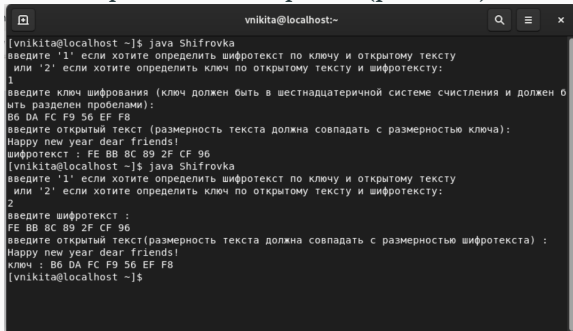
```
118
119 String newSymbol="";
120 for(int j=0;j<symbol2.length();j++) {
121
122 int number= Character.digit(symbol2.charAt(j), 10);
123 int number2 = Character.digit(symbol.charAt(j), 10);
124
125 newSymbol+=number^number2;
126
127 }
128
129
130 String val = newSymbol.substring(0, 4);
131 String val2= newSymbol.substring(4);
132 char nval=' ';
133 char nval2=' ';
134 Iterator it = map.entrySet().iterator();
135
136 while (it.hasNext()) {
137 Map.Entry pair = (Map.Entry)it.next();
138 if(pair.getValue().equals(val)) {
139 nval=(char)pair.getKey();
140 }
141
142 if(pair.getValue().equals(val2)) {
143 nval2=(char)pair.getKey();
144 }
145
146 }
147
148 String v = String.valueOf(nval)+String.valueOf(nval2);
149 finalcode=finalcode+v+" ";
150
151
152 }
153
154 return finalcode;
155 }
```

4. (рис.№4)

Скомпилировал программу с помощью команды `javac Shifrovka.java` и Запустил её с помощью команды `java Shifrovka`

5. Просмотр итогов выполнения

Написал ключ для кодирования: B6 DA FC F9 56 EF F8 Затем текст, который этот ключ должен кодировать: Happy new year dear friends! Получил такой вывод: FE BB 8C 89 2F CF 96 Проверив обратный механизм работы программы, убедился, что все работает исправно(рис.Nº5)



```
vnikita@localhost:~  
[vnikita@localhost ~]$ java Shifrovka  
введите '1' если хотите определить шифротекст по ключу и открытому тексту  
или '2' если хотите определить ключ по открытому тексту и шифротексту:  
1  
введите ключ шифрования (ключ должен быть в шестнадцатеричной системе счисления и должен быть разделен пробелами):  
B6 DA FC F9 56 EF F8  
введите открытый текст (размерность текста должна совпадать с размерностью ключа):  
Happy new year dear friends!  
шифротекст : FE BB 8C 89 2F CF 96  
[vnikita@localhost ~]$ java Shifrovka  
введите '1' если хотите определить шифротекст по ключу и открытому тексту  
или '2' если хотите определить ключ по открытому тексту и шифротексту:  
2  
введите шифротекст :  
FE BB 8C 89 2F CF 96  
введите открытый текст(размерность текста должна совпадать с размерностью шифротекста) :  
Happy new year dear friends!  
ключ : B6 DA FC F9 56 EF F8  
[vnikita@localhost ~]$
```

Освоил на практике применение режима однократного гаммирования.