

# Элементы криптографии. Однократное гаммирование.

---

Алхимова Дарья Сергеевна НБИ-01-19<sup>1</sup>

18 октября, 2022

<sup>1</sup>Российский Университет Дружбы Народов

## Докладчик

- Алхимова Дарья Сергеевна
- студентка 4 курса
- группы НБИбд-01-19
- Российский университет дружбы народов
- 1032191645@rudn.ru

Освоить на практике применение режима однократного гаммирования.

## Определение гаммирования

Гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

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

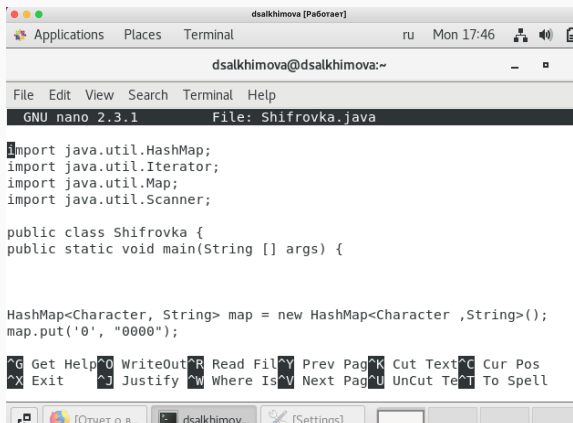
## Алгоритм гаммирования

1. Сгенерировать сегмент гаммы  $H(1)$  и наложить его на соответствующий участок шифруемых данных.
2. Подсчитать контрольную сумму участка, соответствующего сегменту гаммы  $H(1)$ .
3. Сгенерировать следующий сегмент гамм  $H(2)$  с учетом контрольной суммы уже зашифрованного участка данных.
4. Подсчитать контрольную сумму участка данных, соответствующего сегменту данных  $H(2)$  и т.д.

# Выполнение лабораторной работы

## Создала файл программы

Заполнила файл кодом программы гаммирования.



```
dsalkhimova [Работаer]
Applications Places Terminal ru Mon 17:46
dsalkhimova@dsalkhimova:~
File Edit View Search Terminal Help
GNU nano 2.3.1 File: Shifrovka.java

import java.util.HashMap;
import java.util.Iterator;
import java.util.Map;
import java.util.Scanner;

public class Shifrovka {
public static void main(String [] args) {

HashMap<Character, String> map = new HashMap<Character ,String>();
map.put('0', "0000");

^G Get Help ^O WriteOut ^R Read Fil ^Y Prev Pag ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Pag ^U UnCut Te ^T To Spell

[Отчет о в... dsalkhimov... [Settings]
```

Рис. 1: Фрагмент программы гаммирования

## Проверила правильность выполнения программы

Сначала по первому сценарию:

необходимо определить вид шифротекста при известном ключе и известном открытом тексте.

```
[dsalkhimova@dsalkhimova ~]$ javac Shifrovka.java
[dsalkhimova@dsalkhimova ~]$ 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):
A6 BC D3 F4 A9 C1 B2 DE
введите открытый текст (размерность текста должна совпадать с размерно
стью ключа):
S novym godom, druzya!
шифротекст : F5 9C BD 9B DF B8 DF FE
```

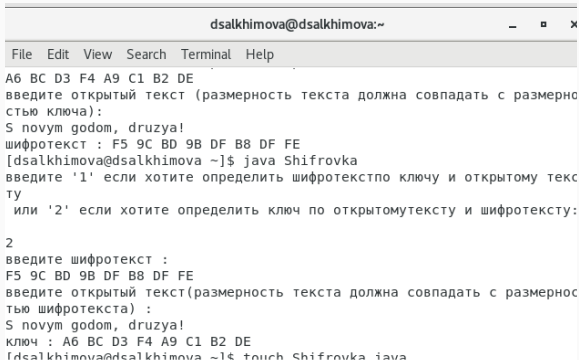
**Рис. 2:** Запуск программы по сценарию 1

# Выполнение лабораторной работы

## Проверила правильность выполнения программы

Затем по второму сценарию:

необходимо определить ключ, по которому шифротекст может быть преобразован во фрагмент текста (один из возможных вариантов прочтения открытого текста).



```
dsalkhimova@dsalkhimova:~  
File Edit View Search Terminal Help  
A6 BC D3 F4 A9 C1 B2 DE  
введите открытый текст (размерность текста должна совпадать с размерно  
стью ключа):  
S novym godom, druzya!  
шифротекст : F5 9C BD 9B DF B8 DF FE  
[dsalkhimova@dsalkhimova ~]$ java Shifrovka  
введите '1' если хотите определить шифротекстпо ключу и открытому текс  
ту  
или '2' если хотите определить ключ по открытому тексту и шифротексту:  
2  
введите шифротекст :  
F5 9C BD 9B DF B8 DF FE  
введите открытый текст(размерность текста должна совпадать с размернос  
тью шифротекста) :  
S novym godom, druzya!  
ключ : A6 BC D3 F4 A9 C1 B2 DE  
[dsalkhimova@dsalkhimova ~]$ touch Shifrovka.java
```

Рис. 3: Запуск программы по сценарию 2



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