****

**Московский авиационный институт**

**(Национальный исследовательский университет)**

**Институт № 3**

**Кафедра 311**

**Информационная безопасность**

**Лабораторная работа № 5**

**«Шифр Гаммированием»**

**Выполнил студент  
Максимов Евгений Викторович**

**Группа М3З-302-БК**

**Дата 26.04.2022 г.**

**Принял преподаватель  
Кос Оксана Игоревна**

Оглавление

[Цель лабораторной работы 3](#_Toc103199368)

[Глава 1. Принцип Шифра Гаммированием (XOR). 4](#_Toc103199369)

[Глава 2. Шифрование XOR. 5](#_Toc103199370)

[Глава 3. Расшифровка текста 6](#_Toc103199371)

[Глава 3. Листинг программы 7](#_Toc103199372)

[*Метод обработки строоки* 7](#_Toc103199373)

[Итоги лабораторной работы 8](#_Toc103199374)

[Список литературы 9](#_Toc103199375)

# Цель лабораторной работы

Изучить:

* 1. Принцип шифрования Гаммированием;
  2. Зашировать текст Гаммирование;
  3. Расшифрованить текст.

# Глава 1. Принцип Шифра Гаммированием (XOR).

Гамми́рование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных.

# Глава 2. Шифрование XOR.

**Задача**: *з*ашифровать исходный текст с помощью ключа.

**Ключ:** «LEMON»

**Исходный текст:** «As no objection was made to the young people's engagement with their aunt, and all Mr. Collins's scruples of leaving Mr. and Mrs. Bennet for a single evening during his visit were most steadily resisted, the coach conveyed him and his five cousins at a suitable hour to Meryton; and the girls had the pleasure of hearing, as they entered the drawing-room, that Mr. Wickham had accepted their uncle's invitation, and was then in the house.»

**Зашифрованный текст:** «6m!!l\*/%+/1$ l2,<n!$)\*n8\*m;&)e4 ;""m?+#5!\*i?e(!)-"("+"1m8'8-m;&),?o/9+9cn-+)o/ )m<be " ,#<i?e>,<95!\*=l\*+o")$;& +e»

# Глава 3. Расшифровка текста

**Задача:** расшифровать текст зная ключ

**Ключ:** «LEMON»

**Расшифрованный текст:** «As no objection was made to the young people's engagement with their aunt, and all Mr. Collins's scruples of leaving Mr. and Mrs. Bennet for a single evening during his visit were most steadily resisted, the coach conveyed him and his five cousins at a suitable hour to Meryton; and the girls had the pleasure of hearing, as they entered the drawing-room, that Mr. Wickham had accepted their uncle's invitation, and was then in the house.»

# Глава 3. Листинг программы

# *Метод обработки строоки*

private static String processStinrg(String sourceString, String key, Mode mode) {  
 StringBuilder sb = new StringBuilder();  
 // Если расшифровываем, то надо раскодировать строку из Base64  
 char[] sourceChars = Mode.*ENCRYPT*.equals(mode)  
 ? sourceString.toCharArray()  
 : new String(Base64.*getDecoder*().decode(sourceString.getBytes(*UTF\_8*)), *UTF\_8*).toCharArray();  
 for (int i = 0; i < sourceChars.length; i++) {  
 sb.append((char) (sourceChars[i] ^ key.charAt(i % key.length())));  
 }  
  
 // Если шифруем, то шифруем байты в Base64 для удобства восприятия  
 if (Mode.*ENCRYPT*.equals(mode)) {  
 return Base64.*getEncoder*().encodeToString(sb.toString().getBytes(*UTF\_8*));  
 }  
  
 return sb.toString();  
}

# Итоги лабораторной работы

Мы научились шифровать и расшифровывать текст методом Гаммирования.

# Список литературы

1. [[Wikipedia.org](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F)] – Гаммирование;