****

**Московский авиационный институт**

**(Национальный исследовательский университет)**

**Институт № 3**

**Кафедра 311**

**Информационная безопасность**

**Лабораторная работа № 1**

**«Шифр Цезаря»**

**Выполнил студент  
Максимов Евгений Викторович**

**Группа М3З-302-БК**

**Дата 11.05.2022 г.**

**Принял преподаватель  
Кос Оксана Игоревна**

Оглавление

[Цель лабораторной работы 3](#_Toc103680448)

[Глава 1. Принцип Шифра Цезаря. 4](#_Toc103680449)

[Глава 2. Шифрование с помощью Шифра Цезаря. 5](#_Toc103680450)

[Глава 3. Расшифровка текста 7](#_Toc103680451)

[Глава 4. Взлом Шифра Цезаря 9](#_Toc103680452)

[Итоги лабораторной работы 11](#_Toc103680453)

[Список литературы 12](#_Toc103680454)

# Цель лабораторной работы

Изучить:

* 1. Принцип Шифра Цезаря;
  2. Зашифровать текст с помощью Шифра Цезаря, используя русский, английский алфавит и спецсимволы;
  3. Расшифровать зашифрованный текст;
  4. Взломать зашифрованный текст.

# Глава 1. Принцип Шифра Цезаря.

Шифр Цезаря (шифр сдвига, код Цезаря или сдвиг Цезаря) — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, «А» была бы заменена на «Г», «Б» станет «Д», и так далее.

Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и всё ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.

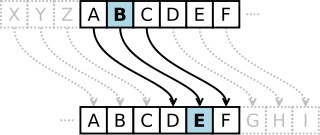


Рисунок 1.1. Шифр Цезаря

# Глава 2. Шифрование с помощью Шифра Цезаря.

**Задача**: зашифровать исходный текст Шифром Цезаря. Для шифрования точек, запятых и пробелов использовать случайный символ из списка: ['!', '@', '#', '$', '%'].

**Дано**:

*Исходный текст*: "По легенде Великий Северный Воин, прознал о великане, который жил в озере с лотосами, поедавшего любого, кто подходил близко к озеру и поклялся его убить. Воин нанес татау на своё тело, взяв силу из земли мёртвых. Затем он собрался и пошёл по тропе к озеру с лотосами, воин победил великана и отсёк ему голову своим кинжалом, которая упала на землю и стала островом. Потомки воина стали называться ракьят и заселили остров. Позднее остров был открыт и частично заселён переселенцами из Европы. Ракьят жили в содружестве с колонистами, переняли их язык, научились пользоваться их технологиями, хотя сами не развивались, как и предыдущие несколько тысяч лет. In a hole in the ground there lived a hobbit. Not a nasty, dirty, wet hole, filled with the ends of worms and an oozy smell, nor yet a dry, bare, sandy hole with nothing in it to sit down on or to eat: it was a hobbit-hole, and that means comfort."

*Ключ шифра*: 5

**Результат**:

«Фу!ркиктйк#Зкрнпно@ЦкзкхтAо%Зунт#$фхумтер%у$зкрнпетк$$пучухAо#лнр%з@умкхк!ц$ручуцесн%#фукйезэкиу#рDжуиу$#пчу#фуйъуйнр$жрнмпу$п!умкхш!н%фупрEрцE$киу$шжнчB$#Зунт@теткц$чечеш!те!цзуE!чкру@$змEз@цнрш!нм@мксрн%сEхчзAъ@!Мечкс!ут#цужхерцE@н!фуэEр!фу@чхуфк$п$умкхш#ц!ручуцесн$%зунт$фужкйнр!зкрнпете!н!учцEп@ксш@иурузш#цзунс!пнтлерус$@пучухеE@шфере@те$мксрD#н%цчере!уцчхузус%%Фучуспн#зунте!цчерн%темAзечBцE%хепBEч%н!мецкрнрн@уцчхуз!$Фумйткк%уцчхуз#жAр$учпхAч%н%ьецчньту@мецкрEт#фкхкцкрктыесн@нм@КзхуфA$#ХепBEч@лнрн!з#цуйхшлкцчзк#ц@пурутнцчесн%%фкхктEрн$нъ!EмAп!%тешьнрнцB!фурBмузечBцE$нъ!чкътуруинEсн%$ъучE#цесн%тк%хемзнзернцB$$пеп#н!фхкйAйшюнк%ткцпурBпу@чAцEь$ркч@$Ns%f$mtqj!ns!ymj$lwtzsi#ymjwj!qnАji%f#mtggny$@Sty@f$sfxyГ#%inwyГ!@Бjy%mtqj@!knqqji$Бnym%ymj!jsix#tk!Бtwrx!fsi$fs%ttДГ$xrjqq!#stw#Гjy$f!iwГ@@gfwj%$xfsiГ!mtqj$Бnym@stymnsl!ns!ny@yt%xny!itБs!ts$tw%yt@jfyE$ny@Бfx@f$mtggnyEmtqj$@fsi@ymfy%rjfsx$htrktwy@»

**Листинг программы**:

*Метод шифрования входящей строки:*

private static String encryptText(String inputText, int key) {

StringBuilder sb = new StringBuilder();

for (int i = 0; i < inputText.length(); i++) {

char sourceChar = inputText.charAt(i);

int charIdx;

if (CYPHER\_ALPHABET\_FOR\_SPEC\_SYMBOLS.contains(sourceChar)) {

sb.append(SPEC\_SYMBOLS.get(new Random().nextInt(SPEC\_SYMBOLS.size())));

} else {

charIdx = CYPHER\_ALPHABET.indexOf(sourceChar);

sb.append(encryptLetter(charIdx, key, CYPHER\_ALPHABET));

}

}

resultText = sb.toString();

return resultText;

}

*Метод шифрования входящей буквы:*

private static char encryptLetter(int sourceCharIdx, int key, List<Character> alphabet) {  
 return alphabet.get(abs(sourceCharIdx + key) % alphabet.size());  
}

# Глава 3. Расшифровка текста

**Задача**: расшифровать зашифрованный текст.

**Дано**:

*Зашифрованный текст:* «Фу!ркиктйк#Зкрнпно@ЦкзкхтAо%Зунт#$фхумтер%у$зкрнпетк$$пучухAо#лнр%з@умкхк!ц$ручуцесн%#фукйезэкиу#рDжуиу$#пчу#фуйъуйнр$жрнмпу$п!умкхш!н%фупрEрцE$киу$шжнчB$#Зунт@теткц$чечеш!те!цзуE!чкру@$змEз@цнрш!нм@мксрн%сEхчзAъ@!Мечкс!ут#цужхерцE@н!фуэEр!фу@чхуфк$п$умкхш#ц!ручуцесн$%зунт$фужкйнр!зкрнпете!н!учцEп@ксш@иурузш#цзунс!пнтлерус$@пучухеE@шфере@те$мксрD#н%цчере!уцчхузус%%Фучуспн#зунте!цчерн%темAзечBцE%хепBEч%н!мецкрнрн@уцчхуз!$Фумйткк%уцчхуз#жAр$учпхAч%н%ьецчньту@мецкрEт#фкхкцкрктыесн@нм@КзхуфA$#ХепBEч@лнрн!з#цуйхшлкцчзк#ц@пурутнцчесн%%фкхктEрн$нъ!EмAп!%тешьнрнцB!фурBмузечBцE$нъ!чкътуруинEсн%$ъучE#цесн%тк%хемзнзернцB$$пеп#н!фхкйAйшюнк%ткцпурBпу@чAцEь$ркч@$Ns%f$mtqj!ns!ymj$lwtzsi#ymjwj!qnАji%f#mtggny$@Sty@f$sfxyГ#%inwyГ!@Бjy%mtqj@!knqqji$Бnym%ymj!jsix#tk!Бtwrx!fsi$fs%ttДГ$xrjqq!#stw#Гjy$f!iwГ@@gfwj%$xfsiГ!mtqj$Бnym@stymnsl!ns!ny@yt%xny!itБs!ts$tw%yt@jfyE$ny@Бfx@f$mtggnyEmtqj$@fsi@ymfy%rjfsx$htrktwy@»

*Ключ шифрования:* 5

**Результат:**

«По легенде Великий Северный Воин прознал о великане который жил в озере с лотосами поедавшего любого кто подходил близко к озеру и поклялся его убить Воин нанес татау на своя тело взяв силу из земли мяртвых Затем он собрался и пошял по тропе к озеру с лотосами воин победил великана и отсяк ему голову своим кинжалом которая упала на землю и стала островом Потомки воина стали называться ракьят и заселили остров Позднее остров был открыт и частично заселян переселенцами из Европы Ракьят жили в содружестве с колонистами переняли их язык научились пользоваться их технологиями хотя сами не развивались как и предыдущие несколько тысяч лет In a hole in the ground there lived a hobbit Not a nasty dirty wet hole filled with the ends of worms and an oozy smell nor yet a dry bare sandy hole with nothing in it to sit down on or to eatя it was a hobbitяhole and that means comfort»

**Листинг программы:**

*Метод расшифровки текста:*

private static String decryptText(String inputText) {

StringBuilder sb = new StringBuilder();

for (int i = 0; i < inputText.length(); i++) {

char sourceChar = inputText.charAt(i);

int charIdx;

if (SPEC\_SYMBOLS.contains(sourceChar)) {

sb.append(' ');

} else {

charIdx = CYPHER\_ALPHABET.indexOf(sourceChar);

sb.append(decryptLetter(charIdx, key, CYPHER\_ALPHABET));

}

}

return sb.toString();

}

*Метод расшифровки входящей буквы:*

private static char decryptLetter(int sourceCharIdx, int key, List<Character> alphabet) {

return sourceCharIdx - key < 0

? alphabet.get(alphabet.size() - abs(sourceCharIdx - key))

: alphabet.get(abs(sourceCharIdx - key) % alphabet.size());

}

# Глава 4. Взлом Шифра Цезаря

**Задача:** определить ключ шифрования и расшифровать текст. Вместо спецсимволов использовать пробел.

**Дано:**

*Зашифрованный текст:*

«Фу!ркиктйк#Зкрнпно@ЦкзкхтAо%Зунт#$фхумтер%у$зкрнпетк$$пучухAо#лнр%з@умкхк!ц$ручуцесн%#фукйезэкиу#рDжуиу$#пчу#фуйъуйнр$жрнмпу$п!умкхш!н%фупрEрцE$киу$шжнчB$#Зунт@теткц$чечеш!те!цзуE!чкру@$змEз@цнрш!нм@мксрн%сEхчзAъ@!Мечкс!ут#цужхерцE@н!фуэEр!фу@чхуфк$п$умкхш#ц!ручуцесн$%зунт$фужкйнр!зкрнпете!н!учцEп@ксш@иурузш#цзунс!пнтлерус$@пучухеE@шфере@те$мксрD#н%цчере!уцчхузус%%Фучуспн#зунте!цчерн%темAзечBцE%хепBEч%н!мецкрнрн@уцчхуз!$Фумйткк%уцчхуз#жAр$учпхAч%н%ьецчньту@мецкрEт#фкхкцкрктыесн@нм@КзхуфA$#ХепBEч@лнрн!з#цуйхшлкцчзк#ц@пурутнцчесн%%фкхктEрн$нъ!EмAп!%тешьнрнцB!фурBмузечBцE$нъ!чкътуруинEсн%$ъучE#цесн%тк%хемзнзернцB$$пеп#н!фхкйAйшюнк%ткцпурBпу@чAцEь$ркч@$Ns%f$mtqj!ns!ymj$lwtzsi#ymjwj!qnАji%f#mtggny$@Sty@f$sfxyГ#%inwyГ!@Бjy%mtqj@!knqqji$Бnym%ymj!jsix#tk!Бtwrx!fsi$fs%ttДГ$xrjqq!#stw#Гjy$f!iwГ@@gfwj%$xfsiГ!mtqj$Бnym@stymnsl!ns!ny@yt%xny!itБs!ts$tw%yt@jfyE$ny@Бfx@f$mtggnyEmtqj$@fsi@ymfy%rjfsx$htrktwy@»

**Решение:** с помощью частотного анализа определено, что наиболее часто встречающаяся буква английского алфавита: «Е», а русского – «О». Зная это, находим наиболее часто встречающуюся букву в зашифрованном тексте, определяем её принадлежность к русскому или английскому алфавиту и считаем расстояние между ней и наиболее частой буквой алфавита.

**Результат:**

«На краю дороги стоял дуб Вероятно в десять раз старше берез составлявших «По легенде Великий Северный Воин прознал о великане который жил в озере с лотосами поедавшего любого кто подходил близко к озеру и поклялся его убить Воин нанес татау на своя тело взяв силу из земли мяртвых Затем он собрался и пошял по тропе к озеру с лотосами воин победил великана и отсяк ему голову своим кинжалом которая упала на землю и стала островом Потомки воина стали называться ракьят и заселили остров Позднее остров был открыт и частично заселян переселенцами из Европы Ракьят жили в содружестве с колонистами переняли их язык научились пользоваться их технологиями хотя сами не развивались как и предыдущие несколько тысяч лет In a hole in the ground there lived a hobbit Not a nasty dirty wet hole filled with the ends of worms and an oozy smell nor yet a dry bare sandy hole with nothing in it to sit down on or to eatя it was a hobbitяhole and that means comfort»

**Листинг программы:**

*Метод поиска ключа шифра:*

private static int findKey(String encryptedString) {  
 Map<Character, Integer> letter2count = countLetters(encryptedString);  
 Character mostOccuredLetter = getMostOccuredCharacter(letter2count);  
 Character mostFrequencyEnLetter = 'e';  
 Character mostFrequencyRuLetter = 'о';  
 int mostOccuredLetterIdx = CYPHER\_ALPHABET.indexOf(toLowerCase(mostOccuredLetter));  
 int mostOccuredEnLetterIdx = CYPHER\_ALPHABET.indexOf(mostFrequencyEnLetter);  
 int mostOccuredRuLetterIdx = CYPHER\_ALPHABET.indexOf(mostFrequencyRuLetter);  
 int key = mostOccuredLetterIdx - mostOccuredEnLetterIdx;  
 if (key > CYPHER\_ALPHABET.size() / 2) {  
 key = mostOccuredLetterIdx - mostOccuredRuLetterIdx;  
 }  
  
 return key;  
}

*Метод поиска наиболее часто встречающейся буквы:*

private static Character getMostOccuredCharacter(Map<Character, Integer> letter2count) {  
 int count = 0;  
 Character result = null;  
 for (Entry<Character, Integer> entry : letter2count.entrySet()) {  
 if (entry.getValue() > count) {  
 count = entry.getValue();  
 result = entry.getKey();  
 }  
 }  
  
 return result;  
}

*Метод пересчёта букв в зашифрованном тексте:*

private static Map<Character, Integer> countLetters(String encryptedString) {  
 Map<Character, Integer> char2count = new HashMap<>();  
 for (Character character : encryptedString.toCharArray()) {  
 if (CYPHER\_ALPHABET\_FOR\_SPEC\_SYMBOLS.contains(character)) {  
 continue;  
 }  
 if (char2count.containsKey(character)) {  
 char2count.put(character, char2count.get(character) + 1);  
 } else {  
 char2count.put(character, 1);  
 }  
 }  
  
 return char2count;  
}

# Итоги лабораторной работы

Мы научились шифровать, расшифровывать текст с помощью Шифра Цезаря, а также взламывать этот Шифр.

# 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)] – Шифр Цезаря;
2. [[eng4school.ru](https://eng4school.ru/the_alphabet/687-chastota-vstrechaemosti-bukv.html)] – Частота втречаемости букв английского алфавита;
3. [[dpva.ru](https://dpva.ru/Guide/GuideUnitsAlphabets/Alphabets/FrequencyRuLetters/)] – Частот встречаемости букв русского алфавита;
4. [[lingua.com](https://lingua.com/english/reading/wonderful-family/)] – Исходный английский текст;
5. «Война и Мир», Л.Н. Толстой, 1873 г. – Исходный русский текст.