****

**Московский авиационный институт**

**(Национальный исследовательский университет)**

**Институт № 3**

**Кафедра 311**

**Информационная безопасность**

**Лабораторная работа № 2**

**«Шифр Подстановки»**

**Выполнил студент  
Максимов Евгений Викторович**

**Группа М3З-302-БК**

**Дата 11.05.2022 г.**

**Принял преподаватель  
Кос Оксана Игоревна**

Оглавление

[Цель лабораторной работы 3](#_Toc103685176)

[Глава 1. Принцип Шифра Подстановки. 4](#_Toc103685177)

[Глава 2. Шифрование с помощью Шифра Подстановки. 5](#_Toc103685178)

[Глава 3. Расшифровка текста 7](#_Toc103685179)

[Итоги лабораторной работы 9](#_Toc103685180)

[Список литературы 10](#_Toc103685181)

# Цель лабораторной работы

Изучить:

* 1. Принцип Шифра Подстановки;
  2. Зашифровать текст с помощью Шифра Подстановик;
  3. Расшифровать зашифрованный текст.

# Глава 1. Принцип Шифра Подстановки.

Шифр Подстановки — это метод шифрования, в котором элементы исходного открытого текста заменяются зашифрованным текстом в соответствии с некоторым правилом. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. В классической криптографии различают четыре типа шифра подстановки:

* Одноалфавитный шифр подстановки (шифр простой замены) — шифр, при котором каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.
* Однозвучный шифр подстановки похож на одноалфавитный за исключением того, что символ открытого текста может быть заменен одним из нескольких возможных символов.
* Полиграммный шифр подстановки заменяет не один символ, а целую группу. Пример: шифр Плейфера.
* Полиалфавитный шифр подстановки состоит из нескольких шифров простой замены. Примеры: шифр Виженера, шифр Бофора, одноразовый блокнот.

# Глава 2. Шифрование с помощью Шифра Подстановки.

**Задача**: зашифровать исходный текст Шифром Подстановки.

**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 свое тело, взяв силу из земли мертвых. Затем он собрался и пошел по тропе к озеру с лотосами, воин победил великана и отсек 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 заселен 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.»

**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%цзук$чкру%$змEз%цнрш%нм%мксрн@скхчзAъ$%Мечкс#ут#цужхерцE#н#фуэкр%фу@чхуфк%п@умкхш#ц%ручуцесн@#зунт%фужкйнр@зкрнпете@н%учцкп#ксш!иурузш$цзунс$пнтлерус@$пучухеE$шфере@те#мксрD!н@цчере%уцчхузус$$Фучуспн#зунте!цчерн!темAзечBцE!хепBEч%н#мецкрнрн$уцчхуз!%Фумйткк%уцчхуз%жAр$учпхAч$н%ьецчньту@мецкркт%фкхкцкрктыесн$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$yt#jfy@ny$Бfx$f@mtggny#mtqj!!fsi!ymfy#rjfsx$htrktwy%»

**Листинг программы**:

*Метод формирования алфавита шифрования*

private static void fillCypherMap() {  
 List<Character> copyAlphabet = new ArrayList<>(ALPHABET);  
 ALPHABET.forEach(alphabetChar -> {  
 char randomChar = getRandomChar(copyAlphabet);  
 System.out.println("\"" + alphabetChar + "\"" + " = \"" + randomChar + "\"");  
 CYPHER\_MAP.put(alphabetChar, randomChar);  
 DECYPHER\_MAP.put(randomChar, alphabetChar);  
 });  
}

*Метод нахождения случайного символа*

private static Character getRandomChar(List<Character> copyAlphabet) {  
 Random random = new Random();  
 Character character = copyAlphabet.get(random.nextInt(copyAlphabet.size()));  
 copyAlphabet.remove(character);  
 return character;  
}

*Метод шифрования*

private static String encrypt(String inputText) {

StringBuilder sb = new StringBuilder();

for (Character ch : inputText.toCharArray()) {

Character character = CYPHER\_MAP.get(ch);

if (character == null) {

throw new RuntimeException("Can't find char " + character + " by " + ch);

}

sb.append(CYPHER\_MAP.get(ch));

}

return result = sb.toString();

}

# 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%цзук$чкру%$змEз%цнрш%нм%мксрн@скхчзAъ$%Мечкс#ут#цужхерцE#н#фуэкр%фу@чхуфк%п@умкхш#ц%ручуцесн@#зунт%фужкйнр@зкрнпете@н%учцкп#ксш!иурузш$цзунс$пнтлерус@$пучухеE$шфере@те#мксрD!н@цчере%уцчхузус$$Фучуспн#зунте!цчерн!темAзечBцE!хепBEч%н#мецкрнрн$уцчхуз!%Фумйткк%уцчхуз%жAр$учпхAч$н%ьецчньту@мецкркт%фкхкцкрктыесн$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$yt#jfy@ny$Бfx$f@mtggny#mtqj!!fsi!ymfy#rjfsx$htrktwy%»

**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 свое тело, взяв силу из земли мертвых. Затем он собрался и пошел по тропе к озеру с лотосами, воин победил великана и отсек 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 заселен 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.»

**Листинг программы:**

*Метод обработки входящей строки:*

private static String decrypt(String encryptedString) {

StringBuilder sb = new StringBuilder();

for (Character ch : encryptedString.toCharArray()) {

sb.append(DECYPHER\_MAP.get(ch));

}

return sb.toString();

}

# Итоги лабораторной работы

Мы научились шифровать и расшифровывать текст с помощью метода Подстановки.

# 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 Подстановки;
2. [[lingua.com](https://lingua.com/english/reading/wonderful-family/)] – Исходный английский текст;
3. «Война и Мир», Л.Н. Толстой, 1873 г. – Исходный русский текст.