# Практические занятия 3,4

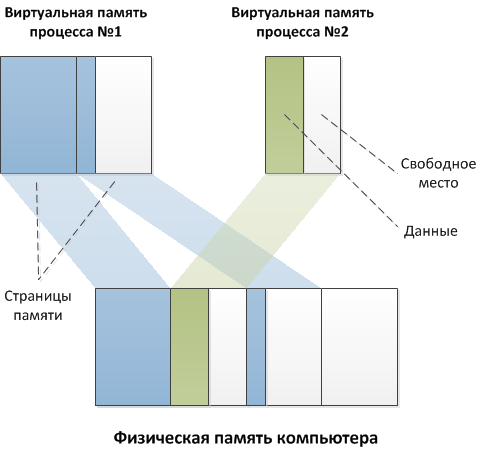
## Теоретическая часть

### Многопоточность

Наиболее очевидная область применения многопоточности – это программирование интерфейсов. Многопоточность незаменима тогда, когда необходимо, чтобы графический интерфейс продолжал отзываться на действия пользователя во время выполнения некоторой обработки информации. Например, поток, отвечающий за интерфейс, может ждать завершения другого потока, загружающего файл из интернета, и в это время выводить некоторую анимацию или обновлять прогресс-бар. Кроме того он может остановить поток загружающий файл, если была нажата кнопка «отмена».  
  
Еще одна популярная и, пожалуй, одна из самых хардкорных областей применения многопоточности – игры. В играх различные потоки могут отвечать за работу с сетью, анимацию, расчет физики и т.п.  
  
Давайте начнем. Сначала о процессах.

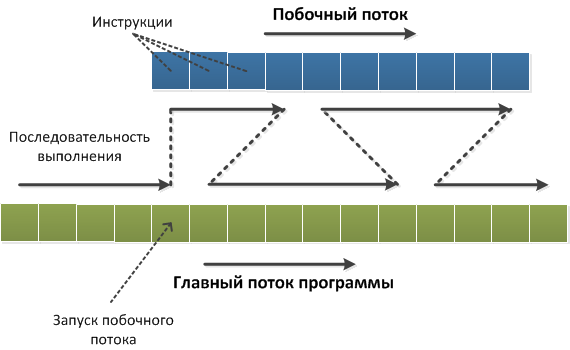
### Процессы

Процесс — это совокупность кода и данных, разделяющих общее виртуальное адресное пространство. Чаще всего одна программа состоит из одного процесса, но бывают и исключения (например, браузер Chrome создает отдельный процесс для каждой вкладки, что дает ему некоторые преимущества, вроде независимости вкладок друг от друга). Процессы изолированы друг от друга, поэтому прямой доступ к памяти чужого процесса невозможен (взаимодействие между процессами осуществляется с помощью специальных средств).  
  
Для каждого процесса ОС создает так называемое «виртуальное адресное пространство», к которому процесс имеет прямой доступ. Это пространство принадлежит процессу, содержит только его данные и находится в полном его распоряжении. Операционная система же отвечает за то, как виртуальное пространство процесса проецируется на физическую память.  
  
Схема этого взаимодействия представлена на картинке. Операционная система оперирует так называемыми страницами памяти, которые представляют собой просто область определенного фиксированного размера. Если процессу становится недостаточно памяти, система выделяет ему дополнительные страницы из физической памяти. Страницы виртуальной памяти могут проецироваться на физическую память в произвольном порядке.



При запуске программы операционная система создает процесс, загружая в его адресное пространство код и данные программы, а затем запускает главный поток созданного процесса.

### Потоки

Один поток – это одна единица исполнения кода. Каждый поток последовательно выполняет инструкции процесса, которому он принадлежит, параллельно с другими потоками этого процесса.  
  
Следует отдельно обговорить фразу «параллельно с другими потоками». Известно, что на одно ядро процессора, в каждый момент времени, приходится одна единица исполнения. То есть одноядерный процессор может обрабатывать команды только последовательно, по одной за раз (в упрощенном случае). Однако запуск нескольких параллельных потоков возможен и в системах с одноядерными процессорами. В этом случае система будет периодически переключаться между потоками, поочередно давая выполняться то одному, то другому потоку. Такая схема называется псевдо-параллелизмом. Система запоминает состояние (контекст) каждого потока, перед тем как переключиться на другой поток, и восстанавливает его по возвращению к выполнению потока. В контекст потока входят такие параметры, как стек, набор значений регистров процессора, адрес исполняемой команды и прочее…  
  
Проще говоря, при псевдопараллельном выполнении потоков процессор мечется между выполнением нескольких потоков, выполняя по очереди часть каждого из них.  
  
Вот как это выглядит:  
  
  
  
Цветные квадраты на рисунке – это инструкции процессора (зеленые – инструкции главного потока, синие – побочного). Выполнение идет слева направо. После запуска побочного потока его инструкции начинают выполняться вперемешку с инструкциями главного потока. Кол-во выполняемых инструкций за каждый подход не определено.   
  
То, что инструкции параллельных потоков выполняются вперемешку, в некоторых случаях может привести к конфликтам доступа к данным. Проблемам взаимодействия потоков будет посвящена следующая статья, а пока о том, как запускаются потоки в Java…

### Запуск потоков

Каждый процесс имеет хотя бы один выполняющийся поток. Тот поток, с которого начинается выполнение программы, называется главным. В языке Java, после создания процесса, выполнение главного потока начинается с метода main(). Затем, по мере необходимости, в заданных программистом местах, и при выполнении заданных им же условий, запускаются другие, побочные потоки.  
  
В языке Java поток представляется в виде объекта-потомка класса Thread. Этот класс инкапсулирует стандартные механизмы работы с потоком.  
  
Запустить новый поток можно двумя способами:

#### Способ 1

Создать объект класса Thread, передав ему в конструкторе нечто, реализующее интерфейс Runnable. Этот интерфейс содержит метод run(), который будет выполняться в новом потоке. Поток закончит выполнение, когда завершится его метод run().  
  
Выглядит это так:

classSomeThing //Нечто, реализующееинтерфейсRunnable

implementsRunnable //(содержащееметодrun())

{

publicvoidrun()*//Этот метод будет выполняться в побочном потоке*

{

System.out.println("Привет из побочного потока!");

}

}

publicclassProgram //Класссметодомmain()

{

staticSomeThingmThing;*//mThing - объекткласса, реализующегоинтерфейс Runnable*

publicstaticvoidmain(String[] args)

{

mThing = newSomeThing();

Thread myThready = new Thread(mThing); *//Созданиепотока "myThready"*

myThready.start(); *//Запускпотока*

System.out.println("Главныйпотокзавершён...");

}

}

Для пущего укорочения кода можно передать в конструктор класса Thread объект безымянного внутреннего класса, реализующего интерфейс Runnable:

publicclassProgram //Класссметодомmain().

{

publicstaticvoidmain(String[] args)

{

*//Созданиепотока*

Thread myThready = newThread(new Runnable()

{

publicvoidrun() *//Этот метод будет выполняться в побочном потоке*

{

System.out.println("Привет из побочного потока!");

}

});

myThready.start(); *//Запуск потока*

System.out.println("Главный поток завершён...");

}

}

#### Способ 2

Создать потомка класса Thread и переопределить его метод run():

classAffableThreadextendsThread

{

@Override

publicvoidrun() *//Этот метод будет выполнен в побочном потоке*

{

System.out.println("Привет из побочного потока!");

}

}

publicclassProgram

{

staticAffableThreadmSecondThread;

publicstaticvoidmain(String[] args)

{

mSecondThread = newAffableThread(); *//Созданиепотока*

mSecondThread.start(); *//Запускпотока*

System.out.println("Главный поток завершён...");

}

}

В приведённом выше примере в методе main() создается и запускается еще один поток. Важно отметить, что после вызова метода mSecondThread.start() главный поток продолжает своё выполнение, не дожидаясь пока порожденный им поток завершится. И те инструкции, которые идут после вызова метода start(), будут выполнены параллельно с инструкциями потока mSecondThread.  
  
Для демонстрации параллельной работы потоков давайте рассмотрим программу, в которой два потока спорят на предмет философского вопроса «что было раньше, яйцо или курица?». Главный поток уверен, что первой была курица, о чем он и будет сообщать каждую секунду. Второй же поток раз в секунду будет опровергать своего оппонента. Всего спор продлится 5 секунд. Победит тот поток, который последним изречет свой ответ на этот, без сомнения, животрепещущий философский вопрос. В примере используются средства, о которых пока не было сказано (isAlive() sleep() и join()). К ним даны комментарии, а более подробно они будут разобраны дальше.

classEggVoiceextendsThread

{

@Override

publicvoidrun()

{

for(inti = 0; i<5; i++)

{

try{

sleep(1000); *//Приостанавливаетпотокна 1 секунду*

}catch(InterruptedException e){}

System.out.println("яйцо!");

}

*//Слово «яйцо» сказано 5 раз*

}

}

publicclassChickenVoice //Класссметодомmain()

{

staticEggVoicemAnotherOpinion; *//Побочныйпоток*

publicstaticvoidmain(String[] args)

{

mAnotherOpinion = newEggVoice(); *//Созданиепотока*

System.out.println("Спорначат...");

mAnotherOpinion.start(); *//Запускпотока*

for(inti = 0; i<5; i++)

{

try{

Thread.sleep(1000); *//Приостанавливает поток на 1 секунду*

}catch(InterruptedException e){}

System.out.println("курица!");

}

*//Слово «курица» сказано 5 раз*

if(mAnotherOpinion.isAlive()) *//Если оппонент еще не сказал последнее слово*

{

try{

mAnotherOpinion.join(); *//Подождать пока оппонент закончит высказываться.*

}catch(InterruptedException e){}

System.out.println("Первым появилось яйцо!");

}

else *//если оппонент уже закончил высказываться*

{

System.out.println("Первой появилась курица!");

}

System.out.println("Спор закончен!");

}

}

Консоль:

Спор начат...

курица!

яйцо!

яйцо!

курица!

яйцо!

курица!

яйцо!

курица!

яйцо!

курица!

Первой появилась курица!

Спор закончен!

В приведенном примере два потока параллельно в течении 5 секунд выводят информацию на консоль. Точно предсказать, какой поток закончит высказываться последним, невозможно. Можно попытаться, и можно даже угадать, но есть большая вероятность того, что та же программа при следующем запуске будет иметь другого «победителя». Это происходит из-за так называемого «асинхронного выполнения кода». Асинхронность означает то, что нельзя утверждать, что какая-либо инструкция одного потока, выполнится раньше или позже инструкции другого. Или, другими словами, параллельные потоки независимы друг от друга, за исключением тех случаев, когда программист сам описывает зависимости между потоками с помощью предусмотренных для этого средств языка.  
  
Теперь немного о завершении процессов…

### Завершение процесса и демоны

В Java процесс завершается тогда, когда завершается последний его поток. Даже если метод main() уже завершился, но еще выполняются порожденные им потоки, система будет ждать их завершения.  
  
Однако это правило не относится к особому виду потоков – демонам. Если завершился последний обычный поток процесса, и остались только потоки-демоны, то они будут принудительно завершены и выполнение процесса закончится. Чаще всего потоки-демоны используются для выполнения фоновых задач, обслуживающих процесс в течение его жизни.  
  
Объявить поток демоном достаточно просто — нужно перед запуском потока вызвать его метод setDaemon(true);  
Проверить, является ли поток демоном, можно вызвав его метод boolean isDaemon();

### Завершение потоков

В Java существуют (существовали) средства для принудительного завершения потока. В частности метод Thread.stop() завершает поток незамедлительно после своего выполнения. Однако этот метод, а также Thread.suspend(), приостанавливающий поток, и Thread.resume(), продолжающий выполнение потока, были объявлены устаревшими и их использование отныне крайне нежелательно. Дело в том что поток может быть «убит» во время выполнения операции, обрыв которой на полуслове оставит некоторый объект в неправильном состоянии, что приведет к появлению трудноотлавливаемой и случайным образом возникающей ошибке.  
  
Вместо принудительного завершения потока применяется схема, в которой каждый поток сам ответственен за своё завершение. Поток может остановиться либо тогда, когда он закончит выполнение метода run(), (main() — для главного потока) либо по сигналу из другого потока. Причем как реагировать на такой сигнал — дело, опять же, самого потока. Получив его, поток может выполнить некоторые операции и завершить выполнение, а может и вовсе его проигнорировать и продолжить выполняться. Описание реакции на сигнал завершения потока лежит на плечах программиста.  
  
Java имеет встроенный механизм оповещения потока, который называется Interruption (прерывание, вмешательство), и скоро мы его рассмотрим, но сначала посмотрите на следующую программку:  
  
Incremenator — поток, который каждую секунду прибавляет или вычитает единицу из значения статической переменной Program.mValue. Incremenator содержит два закрытых поля – mIsIncrement и mFinish. То, какое действие выполняется, определяется булевой переменной mIsIncrement — если оно равно true, то выполняется прибавление единицы, иначе — вычитание. А завершение потока происходит, когда значение mFinish становится равно true.

classIncremenatorextendsThread

{

*//Оключевомслове volatile - чутьниже*

privatevolatilebooleanmIsIncrement = true;

privatevolatilebooleanmFinish = false;

publicvoidchangeAction() *//Меняет действие на противоположное*

{

mIsIncrement= !mIsIncrement;

}

publicvoidfinish() *//Инициируетзавершениепотока*

{

mFinish = true;

}

@Override

publicvoidrun()

{

do

{

if(!mFinish) *//Проверка на необходимость завершения*

{

if(mIsIncrement)

Program.mValue++; *//Инкремент*

else

Program.mValue--; *//Декремент*

*//Вывод текущего значения переменной*

System.out.print(Program.mValue + " ");

}

else

return; *//Завершение потока*

try{

Thread.sleep(1000); *//Приостановка потока на 1 сек.*

}catch(InterruptedException e){}

}

while(true);

}

}

publicclassProgram

{

*//Переменая, которой оперирует инкременатор*

publicstaticintmValue = 0;

staticIncremenatormInc; *//Объектпобочногопотока*

publicstaticvoidmain(String[] args)

{

mInc = newIncremenator(); *//Созданиепотока*

System.out.print("Значение = ");

mInc.start(); *//Запуск потока*

*//Троекратное изменение действия инкременатора*

*//синтерваломвi\*2 секунд*

for(inti = 1; i<= 3; i++)

{

try{

Thread.sleep(i\*2\*1000); *//Ожидание в течении i\*2 сек.*

}catch(InterruptedException e){}

mInc.changeAction(); *//Переключениедействия*

}

mInc.finish(); *//Инициация завершения побочного потока*

}

}

Консоль:

Значение = 1210 -1 -2 -101234

Взаимодействовать с потоком можно с помощью метода changeAction() (для смены вычитания на сложение и наоборот) и метода finish() (для завершения потока).  
  
В объявлении переменных mIsIncrement и mFinish было использовано ключевое слово volatile (изменчивый, не постоянный). Его необходимо использовать для переменных, которые используются разными потоками. Это связано с тем, что значение переменной, объявленной без volatile, может кэшироваться отдельно для каждого потока, и значение из этого кэша может различаться для каждого из них. Объявление переменной с ключевым словом volatile отключает для неё такое кэширование и все запросы к переменной будут направляться непосредственно в память.  
  
В этом примере показано, каким образом можно организовать взаимодействие между потоками. Однако есть одна проблема при таком подходе к завершению потока — Incremenator проверяет значение поля mFinish раз в секунду, поэтому может пройти до секунды времени между тем, когда будет выполнен метод finish(), и фактическим завершения потока. Было бы замечательно, если бы при получении сигнала извне, метод sleep() возвращал выполнение и поток незамедлительно начинал своё завершение. Для выполнения такого сценария существует встроенное средство оповещения потока, которое называется Interruption (прерывание, вмешательство).

### Interruption

Класс Thread содержит в себе скрытое булево поле, подобное полю mFinish в программе Incremenator, которое называется флагом прерывания. Установить этот флаг можно вызвав метод interrupt() потока. Проверить же, установлен ли этот флаг, можно двумя способами. Первый способ — вызвать метод bool isInterrupted() объекта потока, второй — вызвать статический метод bool Thread.interrupted(). Первый метод возвращает состояние флага прерывания и оставляет этот флаг нетронутым. Второй метод возвращает состояние флага и сбрасывает его. Заметьте что Thread.interrupted() — статический метод класса Thread, и его вызов возвращает значение флага прерывания того потока, из которого он был вызван. Поэтому этот метод вызывается только изнутри потока и позволяет потоку проверить своё состояние прерывания.  
  
Итак, вернемся к нашей программе. Механизм прерывания позволит нам решить проблему с засыпанием потока. У методов, приостанавливающих выполнение потока, таких как sleep(), wait() и join() есть одна особенность — если во время их выполнения будет вызван метод interrupt() этого потока, они, не дожидаясь конца времени ожидания, сгенерируют исключение InterruptedException.  
  
Переделаем программу Incremenator – теперь вместо завершения потока с помощью метода finish() будем использовать стандартный метод interrupt(). А вместо проверки флага mFinish будем вызывать метод bool Thread.interrupted();  
Так будет выглядеть класс Incremenator после добавления поддержки прерываний:

classIncremenatorextendsThread

{

privatevolatilebooleanmIsIncrement = true;

publicvoidchangeAction() *//Меняет действие на противоположное*

{

mIsIncrement= !mIsIncrement;

}

@Override

publicvoidrun()

{

do

{

if(!Thread.interrupted()) *//Проверкапрерывания*

{

if(mIsIncrement) Program.mValue++; *//Инкремент*

elseProgram.mValue--; *//Декремент*

*//Вывод текущего значения переменной*

System.out.print(Program.mValue + " ");

}

else

return; *//Завершение потока*

try{

Thread.sleep(1000); *//Приостановка потока на 1 сек.*

}catch(InterruptedException e){

return; *//Завершение потока после прерывания*

}

}

while(true);

}

}

classProgram

{

*//Переменая, которой оперирует инкременатор*

publicstaticintmValue = 0;

staticIncremenatormInc; *//Объектпобочногопотока*

publicstaticvoidmain(String[] args)

{

mInc = newIncremenator(); *//Созданиепотока*

System.out.print("Значение = ");

mInc.start(); *//Запуск потока*

*//Троекратное изменение действия инкременатора*

*//синтерваломвi\*2 секунд*

for(inti = 1; i<= 3; i++)

{

try{

Thread.sleep(i\*2\*1000); *//Ожидание в течении i\*2 сек.*

}catch(InterruptedException e){}

mInc.changeAction(); *//Переключениедействия*

}

mInc.interrupt(); *//Прерывание побочного потока*

}

}

Консоль:

Значение = 1210 -1 -2 -101234

Как видите, мы избавились от метода finish() и реализовали тот же механизм завершения потока с помощью встроенной системы прерываний. В этой реализации мы получили одно преимущество — метод sleep() вернет управление (сгенерирует исключение) незамедлительно после прерывания потока. Заметьте что методы sleep() и join() обёрнуты в конструкции try-catch. Это необходимое условие работы этих методов. Вызывающий их код должен перехватывать исключение InterruptedException, которое они бросают при прерывании во время ожидания.С запуском и завершением потоков разобрались, дальше я расскажу о методах, использующихся при работе с потоками.

#### Метод Thread.sleep()

Thread.sleep() — статический метод класса Thread, который приостанавливает выполнение потока, в котором он был вызван. Во время выполнения метода sleep() система перестает выделять потоку процессорное время, распределяя его между другими потоками. Метод sleep() может выполняться либо заданное кол-во времени (миллисекунды или наносекунды) либо до тех пор пока он не будет остановлен прерыванием (в этом случае он сгенерирует исключение InterruptedException).

Thread.sleep(1500); *//Ждет полторы секунды*

Thread.sleep(2000, 100); *//Ждет 2 секунды и 100 наносекунд*

Несмотря на то, что метод sleep() может принимать в качестве времени ожидания наносекунды, не стоит принимать это всерьез. Во многих системах время ожидания все равно округляется до миллисекунд а то и до их десятков. 

#### Метод yield()

Статический метод Thread.yield() заставляет процессор переключиться на обработку других потоков системы. Метод может быть полезным, например, когда поток ожидает наступления какого-либо события и необходимо чтобы проверка его наступления происходила как можно чаще. В этом случае можно поместить проверку события и метод Thread.yield() в цикл:

*//Ожидание поступления сообщения*

while(!msgQueue.hasMessages()) *//Пока в очереди нет сообщений*

{

Thread.yield(); *//Передать управление другим потокам*

}

#### Метод join()

В Java предусмотрен механизм, позволяющий одному потоку ждать завершения выполнения другого. Для этого используется метод join(). Например, чтобы главный поток подождал завершения побочного потока myThready, необходимо выполнить инструкцию myThready.join() в главном потоке. Как только поток myThready завершится, метод join() вернет управление, и главный поток сможет продолжить выполнение.

Метод join() имеет перегруженную версию, которая получает в качестве параметра время ожидания. В этом случае join() возвращает управление либо когда завершится ожидаемый поток, либо когда закончится время ожидания. Подобно методу Thread.sleep() метод join может ждать в течение миллисекунд и наносекунд – аргументы те же.

С помощью задания времени ожидания потока можно, например, выполнять обновление анимированной картинки пока главный (или любой другой) поток ждёт завершения побочного потока, выполняющего ресурсоёмкие операции:

Thinker brain = newThinker(); *//Thinker - потомоккласса Thread.*

brain.start(); *//Начать "обдумывание".*

do

{

mThinkIndicator.refresh(); *//mThinkIndicator - анимированнаякартинка.*

try{

brain.join(250); *//Подождать окончания мысли четверть секунды.*

}catch(InterruptedException e){}

}

while(brain.isAlive()); *//Пока brain думает...*

*//brain закончил думать (звучат овации).*

В этом примере поток brain (мозг) думает над чем-то, и предполагается, что это занимает у него длительное время. Главный поток ждет его четверть секунды и, в случае, если этого времени на раздумье не хватило, обновляет «индикатор раздумий» (некоторая анимированная картинка). В итоге, во время раздумий, пользователь наблюдает на экране индикатор мыслительного процесса, что дает ему знать, что электронные мозги чем то заняты.

### Приоритеты потоков

Каждый поток в системе имеет свой приоритет. Приоритет – это некоторое число в объекте потока, более высокое значение которого означает больший приоритет. Система в первую очередь выполняет потоки с большим приоритетом, а потоки с меньшим приоритетом получают процессорное время только тогда, когда их более привилегированные собратья простаивают.  
  
Работать с приоритетами потока можно с помощью двух функций:  
  
void **setPriority**(int priority) – устанавливает приоритет потока.  
Возможныезначения priority — MIN\_PRIORITY, NORM\_PRIORITY и MAX\_PRIORITY.

int **getPriority**() – получает приоритет потока.

### Некоторые полезные методы класса Thread

Это практически всё. Напоследок приведу несколько полезных методов работы с потоками.  
  
boolean **isAlive**() — возвращает true если myThready() выполняется и false если поток еще не был запущен или был завершен.  
  
**setName**(String threadName) – Задает имя потока.  
String getName() – Получает имя потока.  
Имя потока – ассоциированная с ним строка, которая в некоторых случаях помогает понять, какой поток выполняет некоторое действие. Иногда это бывает полезным.  
  
**static Thread Thread.currentThread**() — статический метод, возвращающий объект потока, в котором он был вызван.  
  
long **getId**()– возвращает идентификатор потока. Идентификатор – уникальное число, присвоенное потоку.

## Функции хэширования

В Java вы можете использовать класс MessageDigest для хеширования [SHA](https://en.wikipedia.org/wiki/SHA-2). В этой статье мы покажем вам, как использовать алгоритм SHA-256 для хеширования строки и создания контрольной суммы для файла.

### 1. MessageDigest

1.1 Хеш-строка

PasswordSha256.java

package com.mkyong.hashing;

import java.nio.charset.StandardCharsets;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

public class PasswordSha256 {

public static void main(String[]args) throws NoSuchAlgorithmException {

String password = "123456";

MessageDigest md = MessageDigest.getInstance("SHA-256");

byte[]hashInBytes = md.digest(password.getBytes(StandardCharsets.UTF\_\_8));

//bytes to hex

StringBuilder sb = new StringBuilder();

for (byte b : hashInBytes) {

sb.append(String.format("%02x", b));

}

System.out.println(sb.toString());

}

}

Выход

8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92

1.2 Файловая контрольная сумма.

d: \ server.log

123456

FileCheckSum.java

package com.mkyong.hashing;

import java.io.FileInputStream;

import java.io.IOException;

import java.security.DigestInputStream;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

public class FileCheckSum {

public static void main(String[]args) throws NoSuchAlgorithmException, IOException {

MessageDigest md = MessageDigest.getInstance("SHA-256");

byte[]hashInBytes = checksum("d:\\server.log", md);

System.out.println(bytesToHex(hashInBytes));

}

private static byte[]checksum(String filepath, MessageDigest md) throws IOException {

try (DigestInputStream dis = new DigestInputStream(new FileInputStream(filepath), md)) {

while (dis.read() != -1) ;//empty loop to clear the data

md = dis.getMessageDigest();

}

return md.digest();

}

private static String bytesToHex(byte[]hashInBytes) {

StringBuilder sb = new StringBuilder();

for (byte b : hashInBytes) {

sb.append(String.format("%02x", b));

}

return sb.toString();

}

}

Выход

8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92

### 2. Кодек Apache Commons

Или попробуйте эту библиотеку [Apache Commons Codecs](https://commons.apache.org/proper/commons-codec/)для хеширования.

pom.xml

<dependency>

<groupId>commons-codec</groupId>

<artifactId>commons-codec</artifactId>

<version>1.11</version>

</dependency>

2.1 Хеш-строка

PasswordSha256.java

package com.mkyong.hashing;

import org.apache.commons.codec.digest.DigestUtils;

public class PasswordSha256 {

public static void main(String[]args) {

String password = "123456";

String result = DigestUtils.sha256Hex(password);

System.out.println(result);

}

}

Выход

8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92

2.2 Контрольная сумма файла.

FileCheckSum.java

package com.mkyong.hashing;

import org.apache.commons.codec.digest.DigestUtils;

import java.io.FileInputStream;

import java.io.IOException;

public class FileCheckSum {

public static void main(String[]args) throws IOException {

String result = DigestUtils.sha256Hex(new FileInputStream("d:\\server.log"));

System.out.println(result);

}

}

Выход

8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92

## Задание (неделя)

Переборщик паролей

Краткое описание  
Найдите с помощью алгоритма брут форс пятибуквенные пароли, соответствующие следующим хэшам SHA-256:

1. 1115dd800feaacefdf481f1f9070374a2a81e27880f187396db67958b207cbad

2. 3a7bd3e2360a3d29eea436fcfb7e44c735d117c42d1c1835420b6b9942dd4f1b

3. 74e1bb62f8dabb8125a58852b63bdf6eaef667cb56ac7f7cdba6d7305c50a22f

Ваша программа должна перебрать все возможные пароли, состоящие только из пяти строчных букв английского алфавита ASCII. Необходимо использовать параллельную обработку. Вы можете вычислить хэши SHA-256, вызвав библиотеку ( java.security.MessageDigest) или используя пользовательскую реализацию. Напечатайте каждый соответствующий пароль вместе с его хешем SHA-256.

Количество потоком от 2 до 7.

Необходимо вывести время, затраченное на перебор каждого хеша.

Задание расчитано на 1 практическое занятия.

Литература:

1. [Архитектура компьютера, Э.Танненбаум](https://nsu.ru/xmlui/bitstream/handle/nsu/9054/tanenbaum_AC.pdf?sequence=1&isAllowed=y)
2. [Хеш-Функция](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F#:~:text=%D0%A1%D0%BB%D1%83%D1%87%D0%B0%D0%B9%2C%20%D0%BF%D1%80%D0%B8%20%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D0%BE%D0%BC%20%D1%85%D0%B5%D1%88%2D%D1%84%D1%83%D0%BD%D0%BA%D1) (Википедия)
3. <https://www.codeflow.site/ru/article/java__java-sha-hashing-example>