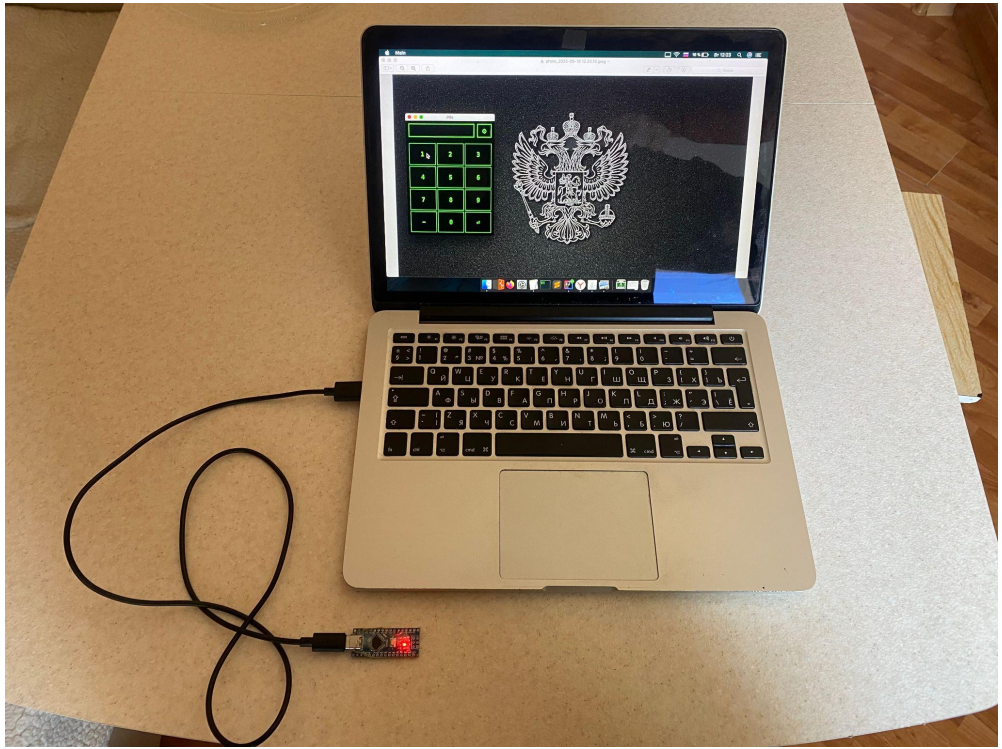
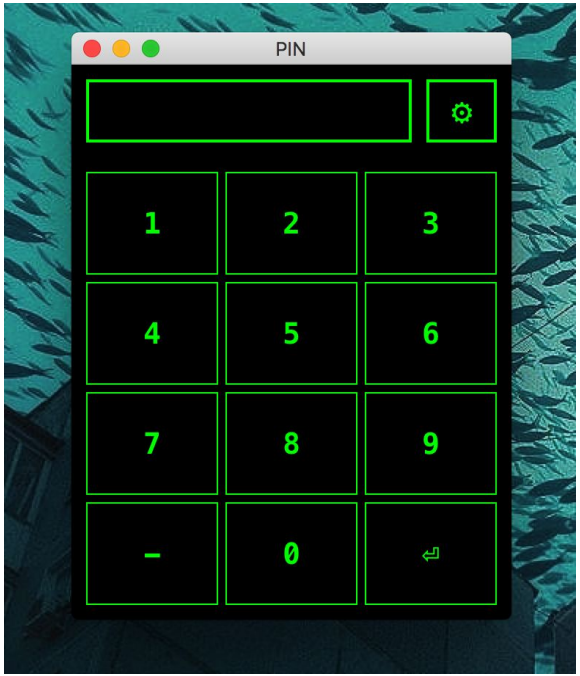
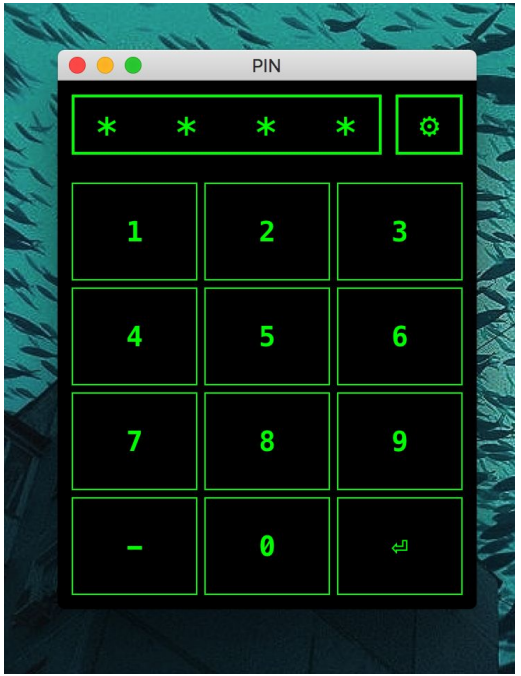
# МУЛЬТИ КРИПТО КЛЮЧ НА ARDUINO

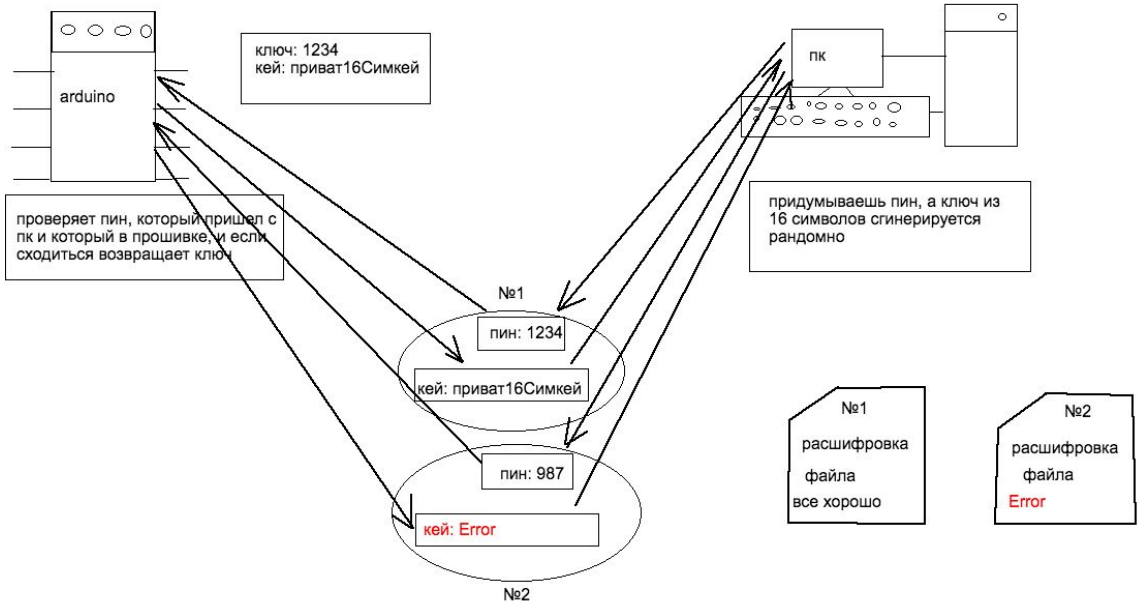


Данной статьей хочу поделиться опытом и идеей создания универсального ключа на arduino, который позволит по заранее заданному пин коду получать ключ, шифровать и расшифровывать свои данные.



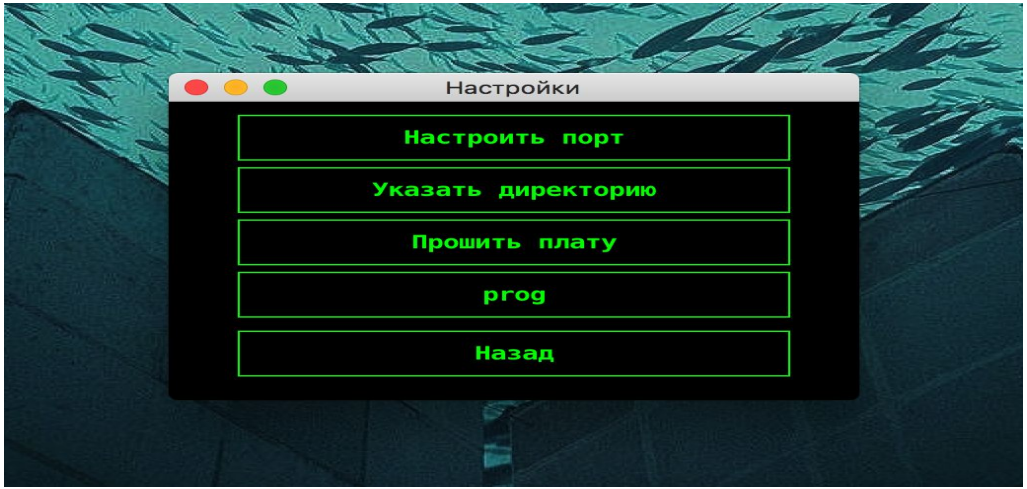



Главной задачей проекта стояла - создание такого ПО, которое бы защищало данные крипто стойким алгоритмом, с хранением ключа только в памяти, без записи на жесткий диск, и без ввода шестнадцатиричного пароля через клавиатуру(с защитой от кейлогера). И тогда и зародилась идея связать по на компьютере с внешним устройством, которое бы хранило ключ для шифрования и дешифрования, и выдавала бы его только по правильному введеному пин коду.



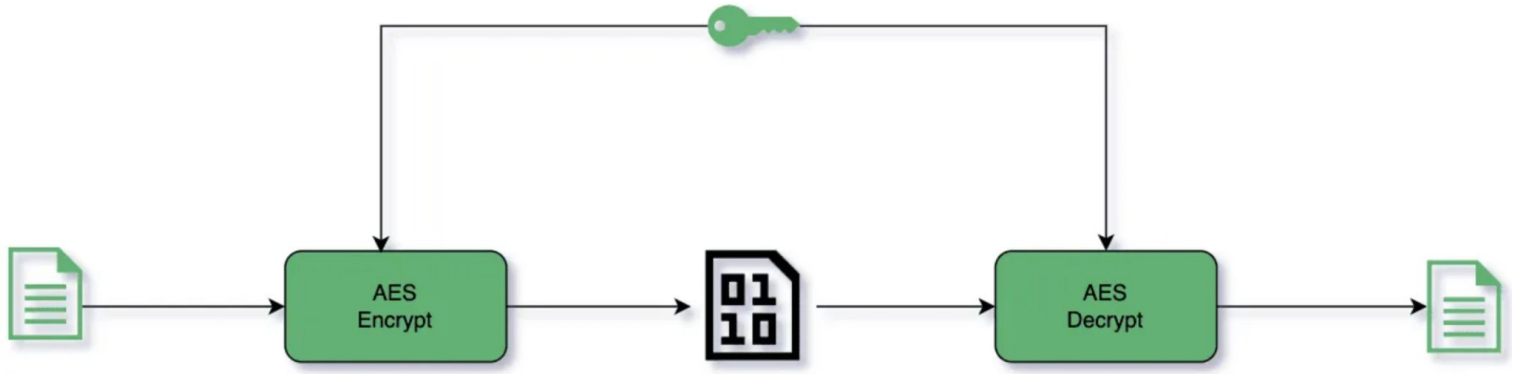
Важно отметить то, что ключ генерируется рандомно, и напрямую пользователь с ним не работает. Это особенно полезно в случае если ключ будут пытаться узнать у владельца, который предварительно уничтожил arduino, тк ключ сгенерировался рандомно, и был записан только на плату, востанавить его с поврежденной платы будет практически невозможно.

Основной язык программирования для программы которая настраивает порт подключения, шифруемую директорию и прошивает плату с пинкодом и рандомно сгенерированным шестнадцатиричным ключем, стала Java. Такое решение дает кроссплатформенность продукту - можно запускать на windows, linux, macos. Быстроту обработки данных, как для arduino с пользовательским интерфейсом, так и для работы с криптографией.



Говоря о криптографии, выбор пал на алгоритм AES-256, который позволяет в момент рекурсивного обхода директории, шифровать и дешифровывать файлы с огромной скоростью буквально за секунды. Но у данного подхода есть минус, AES-256 является синхронным алгоритмом, что говорит о том, что для шифрования и дешифрования используется один и тот же ключ, в отличии от асинхронных алгоритмов, таких как RSA-1024. Но RSA-1024 очень медленно работает с большими данными, что в нашем случае не подходит, так что остановим свой выбор на AES-256.

При запуске программы, нас встречает окно настроек, где нас просят ввести порт подключенной платы, шифруемую директорию и придумать пин код, для работы с платой.

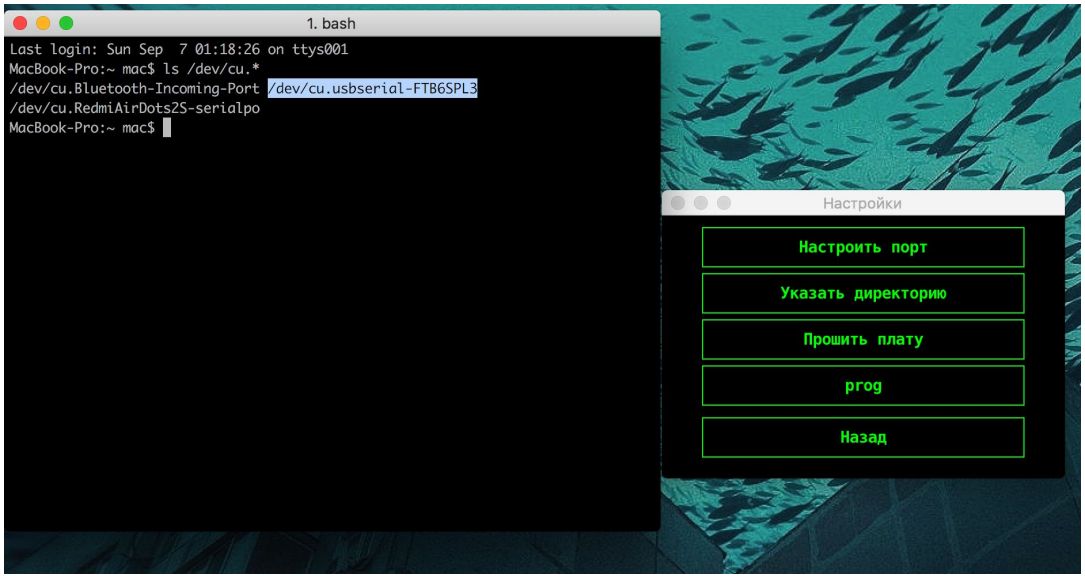


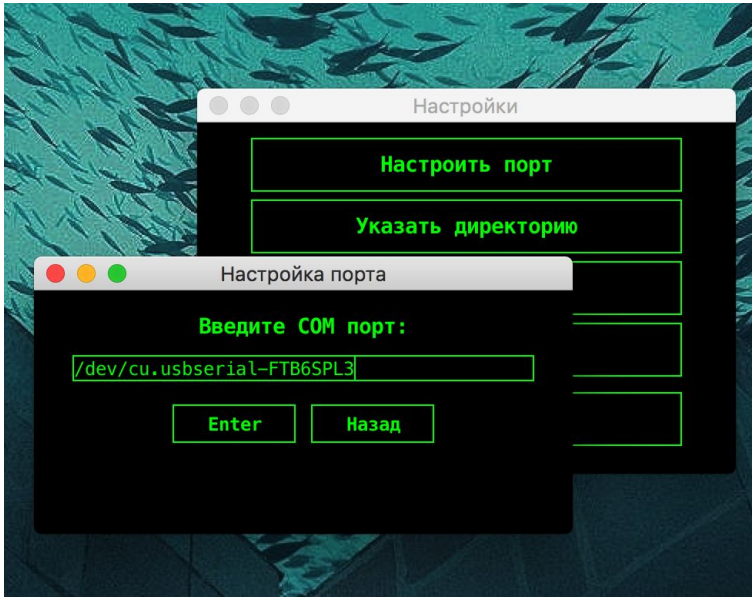
Важно, что вы можете использовать любую плату, будь то arduino uno/nano/pro/micro, esp8266, esp32 и тд. Самое главное скачайте и поставьте драйвер для чипа, который расположен на вашей плате, для моей платы arduino nano, с чипом ch340, понадобилось поставить драйвер именно под мой чип, что бы она отображалась в подключенных usb устройствах на пк.

Так же вам понадобиться jdk 11+ версии. Но можете поставить самую последнюю, на данный момент это jdk 23. Jdk нужна для работы java программы на вашем компьютере.

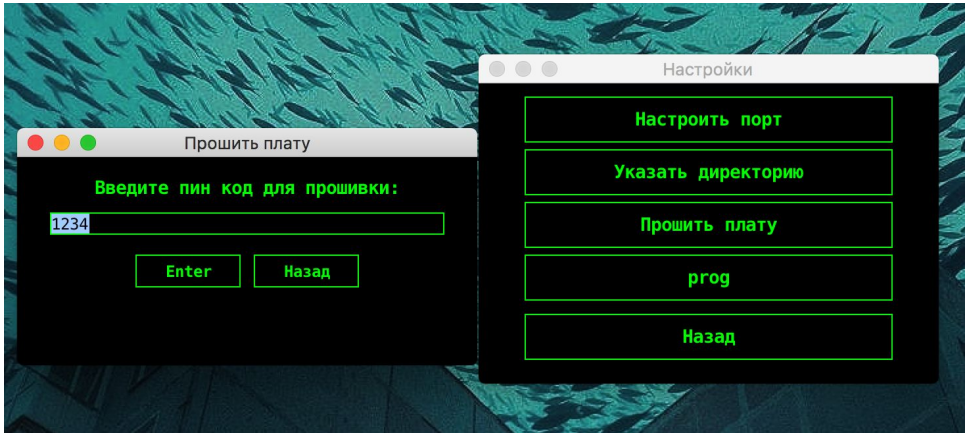
И последнее что вам нужно установить, это библиотека для работы java с последовательным портом, для общения и обмена данными с arduino. это библиотека RXTX.

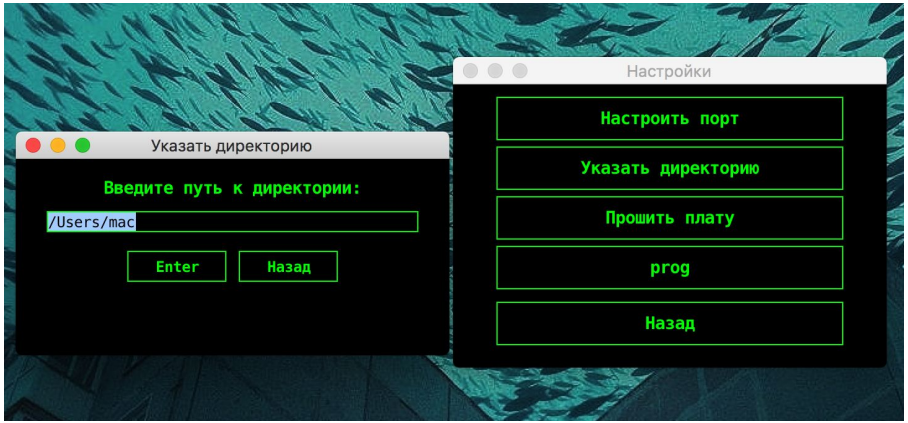
# настройка порта подключения платы



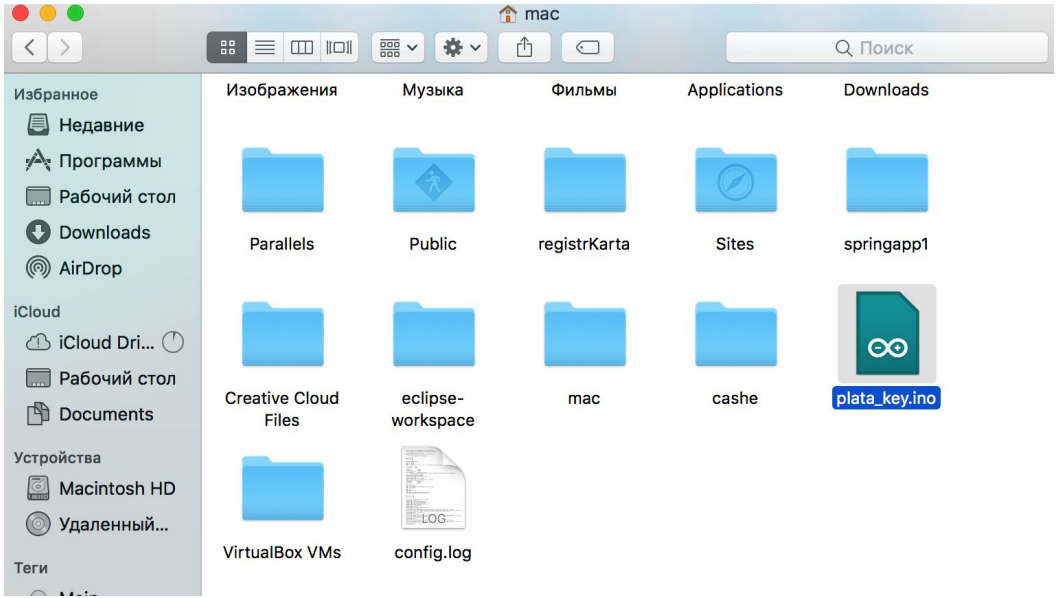
# настройка директории и пин кода

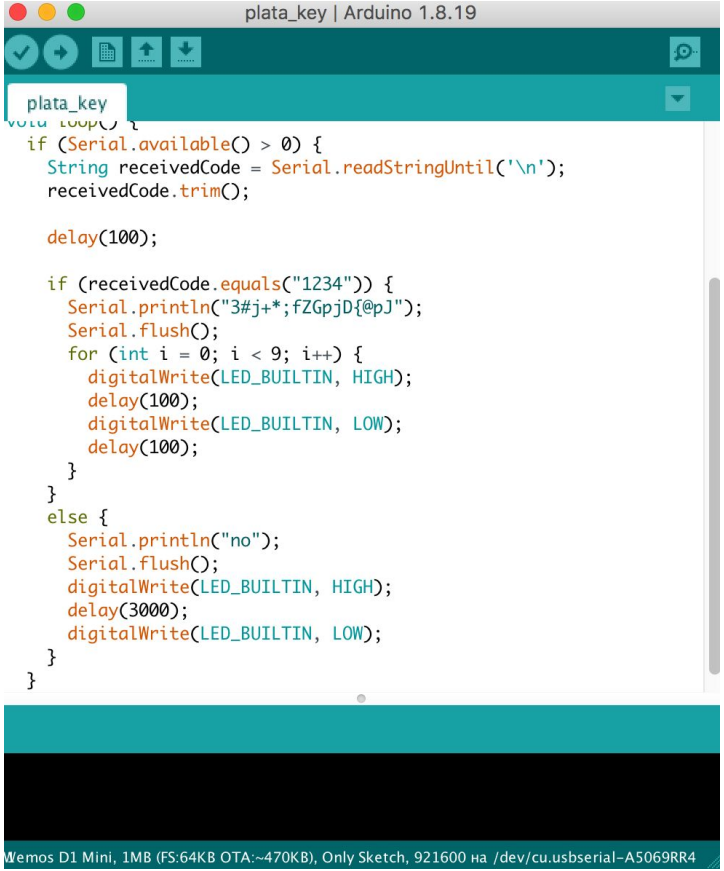


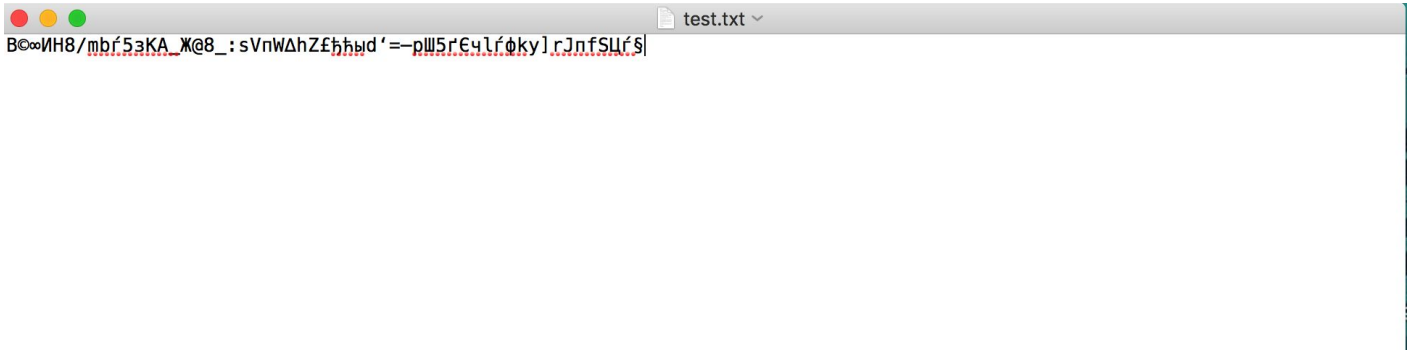
Программа для пк по мимо того что написана только на чистой Java, к тому же не имеет почти никаких зависимостей, кроме RXTX для взаимодействия с arduino. Весь GUI стоит на Swing библиотеке, который идет в коробке с JDK. Это позволяет без проблем добавлять и изменять уже имеющиеся функции проекта. Код написан по принципам ООП и использует такую архитектуру программирования, как Наблюдатель. Код разделен на модули, для удобной отладки и разработки.

# прошивка платы



# пример шифрования файла при разных режимах работы

интерактивное окно для ввода пин кода для разных режимов работы программы