`ssh-keygen -t ed25519 -C [your_email@example.com](mailto:your_email@example.com)` — указываем вместо примера почту в настройках аккаунта на гит хаб`

`cat ~/.ssh/id_ed25519.pub` — копируем и вставляем в ключи в настройках аккаунта

`ssh -i ./key.pem [ubuntu@ip](mailto:ubuntu@ip)` - подключение к удаленному серверу по ssh

`ssh-keygen -y -f ~/.ssh/id_rsa` - узнать свой публичный ssh ключ

опирается на частный ключ (только у владельца ключа) и общий (у всех может быть)

можем *шифровать* данные и *проверять* подлинность.

подключение к другому серверу: ssh login@ip

`cat ~/.ssh/known_hosts` - показать доверенные хосты на компьютере

RSA - криптографический алгоритм с открытым ключом для подписи и шифрования

DSA - криптографический алгоритм с открытым ключом - только для подписи

`ssh-keygen -t rsa` - генерация ключа типа rsa (будет запрашивать парольную фразу (можно просто нажать enter и тогда пароля не будет))

`ssh-copy-id -i ~/.ssh/id_rsa.pub login@ip` - передача публичного ключа на другой компьютер (это необходимо, чтобы кто попало не закидывал свои ключи)

публичный ключ на удаленной машине лежит в папке **~/.ssh/authorized_keys**

`ssh-agent bash` - запустить ssh agent в bash -> ssh-add .ssh/id_rsa добавить закрытый ключ
(теперь текущая консоль хранит пароль-фразу в памяти компьютера в течение сеанса)

Если необходимо сгенерировать ssh-ключа не только для пользователя, но для всей машины в целом необходимо запустить команду под супер-пользователем `sudo ssh-keygen -t rsa -f etc/ssh/ssh_host_key`

Можно скидывать удаленный ключ на уровне хоста на сервер, чтобы сервер доверял целиком не только одному пользователю, но и всей машине в целом.

Обход блокировок портов

`ssh timofey@192.168.55.119 -N -L 12345:192.168.55.119:80`

(Еще можно использовать с ключом -R тогда будет работать все наоборот)

Что такое проброс X11?

Это метод, позволяющий пользователю запускать графические приложения, установленные на удаленной системе Linux, и пересылать эти окна приложений (экран) в локальную систему.

Удаленная система не должна иметь X-сервер или графическое окружение рабочего стола.

Следовательно, настройка пересылки X11 с использованием SSH позволяет пользователям безопасно запускать графические приложения через сеанс SSH.

- [ ] Узнать как работает тунелирование

Проброс файла на удаленный компьютер по ssh

`scp file.file timofey@192.168.55.119:/home/timofey`

Проброс публичного ключа на удаленный компьютер

`ssh-copy-id timofey@192.168.55.119`

`ssh-copy-id -i /path/to/public_key_file user@remote_host` - проброс кастомного ключа

> **Tip**
>
> у ssh файла должны стоять права 600

Симметричная криптография - текст зашифровывается и расшифровывается с помощью одного ключа.
Асимметричная криптография использует для зашифровки один ключ, а для расшифровки другой. (в таком случае можно передавать ключ для зашифровки по открытой сети)
`ssh-keygen -l -f ssh_host_rsa_key.pub` - узнать фингер принт ключа

Передача файлов по защищенному каталогу

`rsync -av /usr/share/doc student@192.168.16.108:/tmp`

> **Описание процессов подключения к серверу**

ssh -v timofey@192.168.55.119

`ssh-keyscan 192.168.55.119 >> ~/.ssh/known_hosts` - добавление хоста в известные

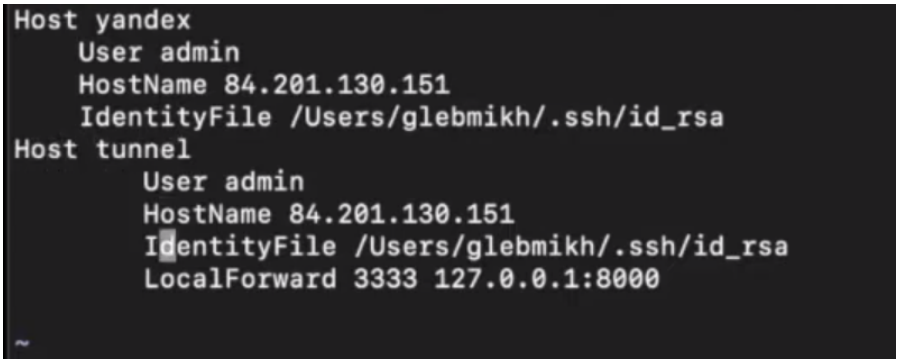
nohup ssh timofey@192.168.55.119 -N -L 12345:192.168.55.119:80 & *(Еще можно использовать с ключом -R тогда будет работать все наоборот)*
затем в консоль будет выведен PID процесса, чтобы выключить туннель `kill PID`

sshfs

sshfs скачать и настроить
sshfs timofey@192.168.55.119:/home/timofey/Desktop /home/timofej/testing_sshfs

Прикольная фишка

Можно сделать ssh config файл в папке ~/.ssh и будет проще подключаться к необходимым серверам, пример файла, указан ниже



linux
Linux (в частности Fedora)
IT