**Подключение к удалённым машинам по закрытому ключу**

Начнём с генерации RSA-ключа.

Rivest-Shamir-Adleman — это асимметричный алгоритм шифрования, который шифрует и расшифровывает данные с использованием двух разных ключей: открытого и закрытого.

$ ssh-keygen -t rsa -b 4096

В результате мы получим публичный (открытый) и приватный (закрытый) ключи. Они будут по умолчанию в домашнем каталоге в скрытой папке .ssh - файлы id\_rsa и id\_rsa.pub.

Для доступа к удалённой машине необходимо разместить публичный ключ в очередной строчке файла .ssh/authorized\_keys.

Часто используемые атрибуты при генерации:

-t — тип ключа

-b — длина ключа в битах (по умолчанию 3072 для RSA)

-f — путь к файлу ключа (по умолчанию ~/.ssh/id\_rsa)

-C — комментарий к ключу (по умолчанию username@hostname)

-P — пароль для доступа к ключу

После того как сгенерировали, публичный ключ можно закинуть на нужную машину.   
Это удобнее всего делать через ssh-copy-id :

$ ssh-copy-id -i $HOME/.ssh/id\_rsa.pub <имя пользователя>@<ip сервера куда хотим получить доступ>

SSH — важный инструмент для работы удалённых серверов и обеспечения безопасного доступа к ним.