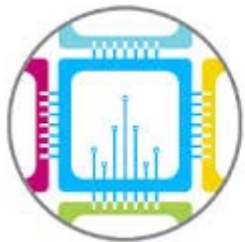


# Генерация SSH ключей



Суперкомпьютерная  
Академия

# SSH

- SSH-ключ используется программой ssh (или другим ssh-клиентом) для авторизации на удаленном сервере
- Ключ состоит из двух частей: публичная часть и закрытая часть
- Не компрометируйте свою закрытую часть ключа!

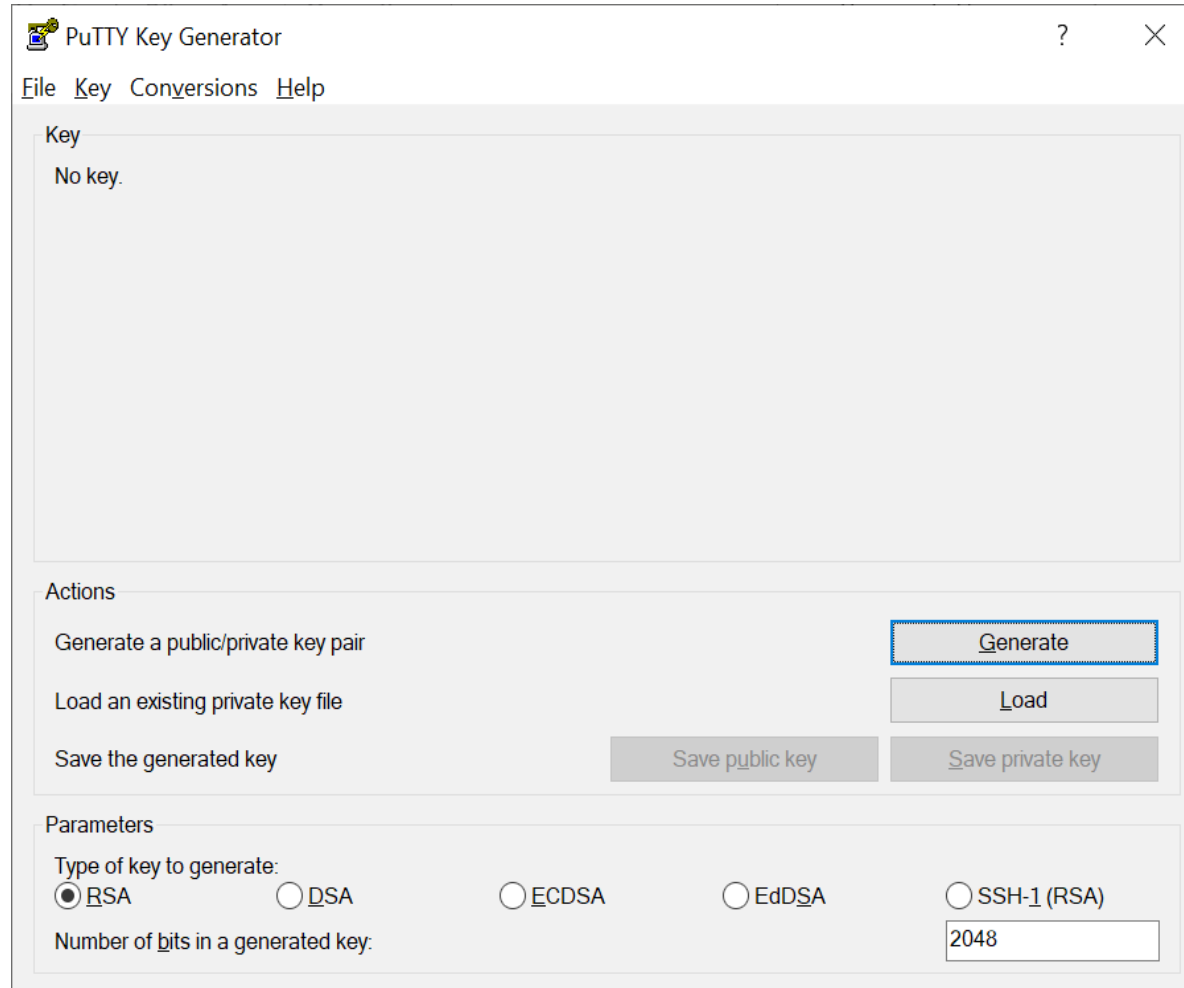


# SSH. Windows

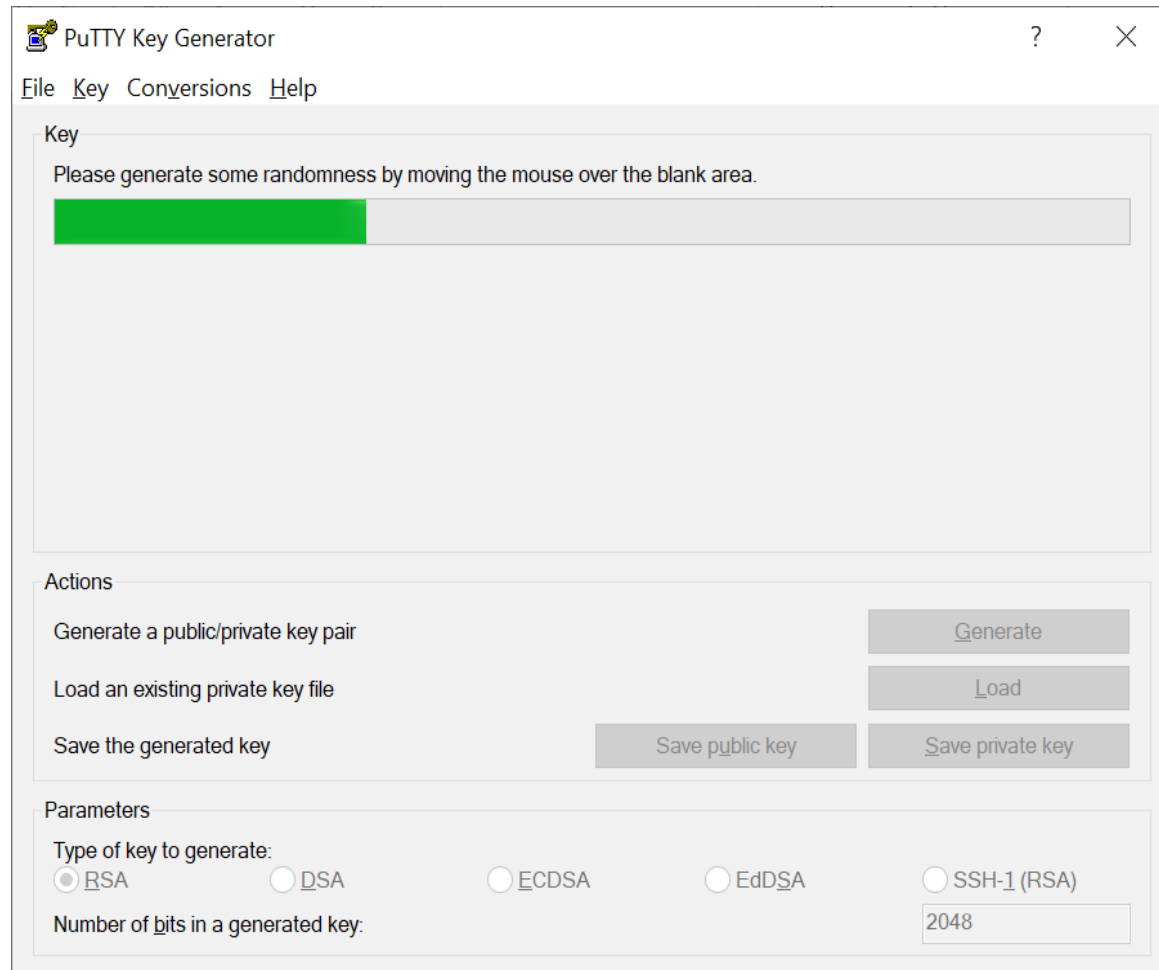
- ssh-клиент PuTTY
- PuTTYgen для создания ключа
- WinSCP для копирования файлов



# SSH. Windows



# SSH. Windows



# SSH. Windows

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized\_keys file:

```
ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQCFaTe5IRSpUSwbbUH2RK90CHcl9FRqQwIWDHQnf3bGqm3osY4  
709yiZ7pTgQ5dirGPMFaVforTuzYNMO0wyXn0uHWI7fluvB3JL6XFIJzLT3XJwjeg1K2AzOf3SEV9p  
+C/ZY6zccj5DyY6CrQErO7PFIBSGUY/hiYojXPUS/1/hErRBbc1nC4bmZ/h3A87VOaHZB9BH5DBj4nfxu  
+w8A7pN1OCULhreMRTIOqV4SMwZqMTg8DmTE9vTIniCLU+dg8GBgMgmNKm3h4b
```

Key fingerprint: ssh-rsa 2048 SHA256:D5DfAYy7jxGVuk+FD+ieOOemSzFEmMv3g59n66SDBJs

Key comment: rsa-key-20211011

Key passphrase:

Confirm:

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate:

RSA  DSA  ECDSA  EdDSA  SSH-1 (RSA)

Number of bits in a generated key: 2048



# SSH. Windows

PuTTY Configuration

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - SSH
  - Serial
  - Telnet
  - Rlogin
  - SUPDUP

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)  Port

Connection type:

SSH  Serial  Other:

Load, save or delete a stored session

Saved Sessions

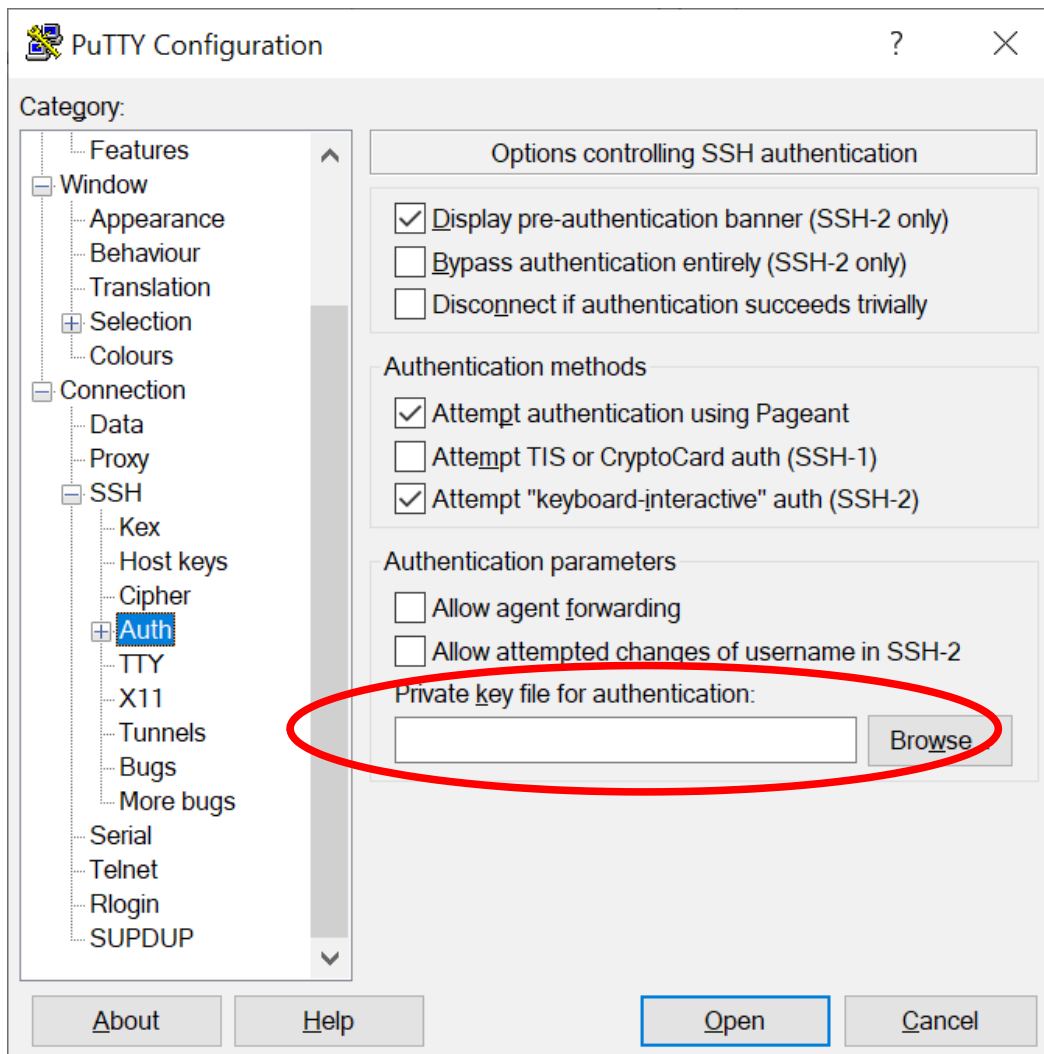
Default Settings

Close window on exit:

Always  Never  Only on clean exit



# SSH. Windows





# SSH. Linux

- ssh-клиент уже есть в системе
- Если нет, то: `sudo apt-get install openssh-client`



# SSH. Linux

- Перед созданием ключа убедитесь, что он еще не создан: `ls -l ~/.ssh`
- Если в выводе файлы `id_rsa/id_dsa`, то нужный ключ уже есть, создавать не требуется



# SSH. Linux

- `ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa_hpc`
- закрытый ssh-ключ (identification) будет сохранен в `~/.ssh/id_rsa_hpc`
- открытый ssh-ключ (public key) будет сохранен в `~/.ssh/id_rsa_hpc.pub`



# SSH. Linux

- Получение fingerprint:  
`ssh-keygen -l -f ~/.ssh/id_rsa_hpc.pub`
- Переименовать ключ `edu-acad2022-Nxx.pub`
- Адрес для ключей: `academy-hpc@yandex.ru`
- Еще более подробно  
<https://wiki.cs.msu.ru/Main/SSHKeysManual>

