# Creating and Using SSH Keys from a Computer Running Microsoft Windows

SSH keys are what you will use to establish an encrypted connection over the network, e.g. the internet, between your system and a remote machine. The default type of key to generate is RSA which is good for most purposes. RSA is universally supported among SSH clients. Note that EdDSA performs much faster and provides the same level of security with significantly smaller keys. In general, though, for what you need to do, RSA encryption should just work.

#### Section I. Install PuTTY

To create and use SSH keys on a device running Microsoft Windows, you need to first download and install both PuTTY and PuTTYgen on that device. PuTTY is the utility used to connect your to a remote desktop or server through SSH, and PuTTYgen is the utility used to create SSH keys. On <u>the PuTTY website</u>, download the .msi file in the **Package files** section at the top of the page, under **MSI ('Windows Installer')**. Next, install it on your local computer by double clicking it and using the installation wizard.

After the programs are installed, start the PuTTYgen program through your Start Menu or by tapping the Windows key and typing puttygen. The PuTTY key generation program will launch and open in a window.

🚰 PuTTY Key Generator			? ×
ile Key Conversions Help			
Key No key.			
Actions Generate a public/private key pair			Generate
Load an existing private key file			Load
Save the generated key		Save public key	Save private key
Parameters Type of key to generate:			
●RSA ○DSA	OECDSA	OEdDSA	OSSH-1 (RSA)

## Section II. Create a Set of SSH Keys

Click the button [Generate] to begin the process of generating an RSA set of keys. By "set" this means you will generate two keys, a private key and a public key. The public key is a key that gets installed on the remote host that you want access to. The private key is saved on the device that you are using and is not to be moved, shared or given to anyone, whence its name "private".

After you click [Generate] you will be prompted to move the mouse around in order to generate some randomness that will be used in the creation of your keys.

, Full in Key Ochelator		? >
e Key Conversions Help		
Key Please generate some randomness by moving the mouse ov	rer the blank area.	
\ctions Generate a public/private key pair		Generate
Actions Generate a public/private key pair Load an existing private key file		Generate
Actions Generate a public/private key pair Load an existing private key file Save the generated key	Save public key	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters	Save public key	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Parameters Type of key to generate: © RSA OECDSA	Save public key	Generate Load Save private key O SSH-1 (RSA)

After moving the mouse around for a short while, the program will create your keys and display something as follows.

PuTTY Key Genera	tor			?	
e Key Conversion	s Help				
Key					
Public key for pasting	into OpenSSH authoriz	ed_keys file:			
ssh-rsa AAAAB3NzaC1yc2E/ JcLAC5JxH1bwh4Hi5 +2ig5NzeY1Lm31Ha +hW6sZnl/jr0Z7PqZw	AAAADAQABAAABAQ LxwK2akT/ZXsB2qiQC petiU52/6J7ARN491RS rioj3CLCGdvGJFVepAł	CEQsQXNZAqO4t7G( zHckT4cx+e6WiaBPt y4DdQG9oLQl6s8yvu HteyOWAFiB92njotdg	0Z7B7DcS6m2XXXZb6kdW ivxmf36Y9Pqu iyd VqWFfH+0NlfVSu3r0dYuTb	asXFMT9wZF/36y54yjFk2T )WTjgP	-
Key fingerprint	ssh-rsa 2048 SHA256	WLN43ZNg2pSdSR4	4/Qs6B6shQgEX0/xvuseu3/0	QYNsiw	
Key comment	rsa-key-20220829				_
Key passphrase:					
Confirm passphrase:					
Actions					
Conorato a public/pris	vate key pair			Generate	
Generate a public/pin					
Load an existing priva	te key file			Load	
Load an existing priva Save the generated k	ite key file		Save public key	Load Save private key	
Load an existing priva Save the generated k Parameters	ite key file ey		Save public key	Load Save private key	
Load an existing priva Save the generated k Parameters Type of key to genera RSA	tte key file ey tte: ODSA	OECDSA	Save public key	Load Save private key O SSH-1 (RSA)	

Notice that the public key is displayed at the top and that several other fields have been added. One notable field is the "Key Passphrase". Some facilities require its users to set a passphrase whereas others leave it to you to decide. A passphrase is like a password that you must enter

each time you use these keys. For now, we will choose to skip using a pass phrase and proceed to save our keys into files on our local system.

Click [Save public key] to save the public key to a file. This is the file that you will install on a remote host that you want to connect with using SSH keys rather than typing a password. A Windows save file box opens. You can create a folder called "PuttyKeys" or whatever you want to name it or simply save it to a location you will not forget and will not delete.

						2
$ ightarrow$ $ ightarrow$ $\uparrow$ $ ightarrow$ This PC $ ightarrow$ Documents $ ightarrow$ Put	tyKeys	~	Ö	,₽ Searc	h PuttyKeys	
rganize • New folder						8
<ul> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Windows 10 (C)</li> <li>Google Drive (G.</li> </ul>	Date modified No items match	Type	Size			
File name: public-key-20220829						

Once you save your public key, you need to save your private key. Click on [Save private key].

PuTTY Key Gener	ator			?	×
e Key Conversio	ns Help				
Key					
Public key for pastin	g into OpenSSH authori	zed_keys file:			
ssh-rsa AAAAB3NzaC1yc28 JcLAC5JxH1bwh4H +2ig5NzeY1Lm31H +hW6sZnl/jr0Z7PqZ	EAAAADAQABAAABA i5LxwK2akT/ZXsB2qiQi aoetiU52/6J7ARN491R wioj3CLCGdvGJFVepA	2CEQsQXNZAqO4t7 CzHckT4cx+e6WiaB Sy4DdQG9oLQl6s8y HteyOWAFiB92njot	GOZ7B7DcS6m2XXXZb6kdW Phvxmf36Y9Pqu vuyd dgVqWFfH+ONlfVSu3r0dYuTb	asXFMT9wZF/36y54yjFk2T WTjgP	*
Key fingerprint	ssh-rsa 2048 SHA25	6:WLN43ZNg2pSdS	R4/Qs6B6shQgEX0/xvuseu3/	QYNsiw	
Key comment	rsa-key-20220829				
Key passphrase:					_
Confirm passphrase					
Actions					
Generate a public/p	ivate key pair			Generate	
Load an existing priv	ate key file			Load	
Save the generated	key		Save public key	Save private key	
Parameters					
Type of key to gene	DSA	OECDSA	OEdDSA	OSSH-1 (RSA)	
<b>O</b> RSA					

After you click [Save private key], if you did not set a passphrase, then you will be asked "Are you sure you want to save this key without a passphrase to protect it?

(ev			
Public key for pasting	into OpenSSH	authorized keys file:	
ssh-rsa AAAAB3NzaC1yc2E JcLAC5JxH1bwh4Hit +2ig5NzeY1Lm31Ha +hW6sZnl/jr0Z7PqZw	AAAADAQABA 5LxwK2akT/ZXs oetiU52/6J7AR vioj3CLCGdvGJ	AABAQCEQsQXNZAqO4t7GQZ7B7DcS6m2XXXZb6kdWasXF B2qiQc2HckT4cx+e6WiaBPhxxm36fY9Pqu N491RSy4DdG9b2Ql68yvuyd FVepAHtey0WAFiB92njotdgVqWFfH+ONIfVSu3r0dYuTbWTj	MT9wZF/36y54yjFk2T
Key fingerprint	ssh-rsa 2048	SHA256:WLN43ZNg2pSdSR4/Qs6B6shQgEX0/xvuseu3/QYN	siw
Key comment	rsa-key-2022	0829	
Key passphrase:			
Confirm passphrase:			
Actions		PuTTYgen Warning 🛛 🕹	
	vate key pair		Generate
Generate a public/pri	vale key pan		
Generate a public/pri Load an existing priva	ate key file	Are you sure you want to save this key without a passphrase to protect it?	Load
Generate a public/pri Load an existing prive Save the generated k	ate key file key	Are you sure you want to save this key without a passphrase to protect it?	Load Save private key
Generate a public/pri Load an existing priva Save the generated k Parameters	ate key file key	Are you sure you want to save this key without a passphrase to protect it?	Load Save private key
Generate a public/pri Load an existing priva Save the generated k 'arameters Type of key to genera © RSA	ate key file key ate: ODSA	Are you sure you want to save this key without a passphrase to protect it?	Load Save private key

If you don't want to use a passphrase, then click [Yes] to close out the message box and proceed to save the file. Note that the file is save with a PuTTY Private Key (\*.ppk) extension.

😴 Save private key as:				×
$\leftarrow \rightarrow \checkmark \uparrow$ 🖡 > This PC > Documents > PuttyKeys			・ じ	arch PuttyKeys
Organize • New folder				⊫ • 👔
<ul> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Documents</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Windows 10 (C:)</li> <li>Google Drive (G:</li> </ul>	Date modified No items mat	Type	Size	
File name: private-key-20220829 Save as type: PUTTY Private Key Files (*.ppk) A Hide Folders			Save	e Cancel

To alleviate some frustration and pain on your part, we note that the format of the public key file is not very user friendly to the Linux world. So for now we are going to save the public key (not the private key!) again but in a text file. From the PuTTYgen utility you will notice the public key is displayed in a box at the top of that utility.

🥐 PuTTY Key Genera	ator				?	×
le Key Conversion	ns Help					
Key						
Public key for pasting	g into OpenSSH author	rized_keys file:				
ssh-rsa			077870686m2¥¥¥7b	6kdWaeXEMT9w7E/	36v54viEk2	^
JcLAC5JxH1bwh4Hi	5LxwK2akT/ZXsB2qiC	CzHckT4cx+e6WiaBPI	hvxmf36Y9Pqu	okurraski witsw21j	30 <b>9</b> 349]i kz	
+2ig5NzeY1Lm31Ha +hW6sZnl/jr0Z7PqZi	ioet/U52/6J/ARN491F wioj3CLCGdvGJFVep/	ISy4DdQG9oLQl6s8yvi AHteyOWAFiB92njotdg	uyd  VgWFfH+ONlfVSu3r0o	dYuTbWTjgP		~
Key fingerprint	ssh-rsa 2048 SHA2	56:WLN43ZNg2pSdSR	4/Qs6B6shQqEX0/xvu	seu3/QYNsiw		_
Key comment	rsa-key-20220829					_
Key comment						_
Key passphrase:						_
Confirm passphrase:						
Actions						
Generate a public/pr	ivate key pair			Ge	nerate	
Load an existing priv	ate key file			L	oad	
Save the generated	key		Save public key	Save p	rivate key	
Parameters						
Type of key to gener	ate:	ECDSA		Ossi	I-1 (RSA)	
		0	0	0	1 1 1	

Click on that window to highlight or select everything in that box. Copy and paste that information to Notepad. It is important to note that everything that is being copied is just one very long line. It is not two or three lines, but a single line. Make certain you paste it into Notepad and save it as such.

/ *Un	titled - Note	pad						_		×
File Ed	lit Format	View	Help							
File Ec ssh-rs AAAAB xT/ZXs +hW6sZ +ITpFh	iit_Format ia WIZaClyc2 MI/jr0Z7 MI/jr0Z7 GJ7mVYLu	View REAAAA IckT4c YPqZwi iyyNx0f	Help DAQABAAABAQCEQsQXHZ x+e6WiaBPhvxmf3GY9P oj3CLCGdvGJFVepAHte utT9PU3CKAAxSBsNNEV	ZAqO4t7GOZ7B7DcS qu+21g5NzeY1Lm3 syONAF1B92njotdg /uPALrRQ5vBXpA2/i	Sm2XXXZb6kdWasXFMT9w HHaoetiU52/6J7ARN491 /qWFfH+ONIfVSu3r0dYu MaRcejXFFRsr0g/yki4	ZF/36y54y RSy4DdQG9 TbWTjgP u9JcQEchB	jFk2TJcLAC5JxH1 oLQI6s8yvuyd Gc0lql rsa-key-	20220	H15Lxw	K2a

Now save this file to the same location where you previously saved your public and private keys.

Save As							×
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ ] $\blacktriangleright$ This PC $\Rightarrow$ Documents $\Rightarrow$ Putt	yKeys	~	Q	Q	Search Putt	yKeys	
Organize 👻 New folder							?
<ul> <li>This PC</li> <li>3D Objects</li> <li>Desktop</li> <li>Downloads</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> </ul>	٨	Date mod	ified		Туре		Size
5 _ Windows 10 (C:) 🗸 <							>
File name: public-key-20220829-for-Linux							~
Save as type: Text Documents (*.txt)							~
∧ Hide Folders	Encoding:	UTF-8	~		Save	Cano	cel

#### Section III. Install your Public Key on the Remote Host

If you can SSH to the host then you can copy and paste that PUBLIC key into a file under your home account as

~/.ssh/authorized keys

or

/home/your\_username/.ssh/authorized\_keys

where the symbol "~" represents a shortcut for "/home/your username".

If the hidden .ssh sub-directory does not exist, then you need to create it manually as

\$ cd
\$ mkdir .ssh
\$ chmod 700 .ssh
\$ cd .ssh
\$ touch authorized\_keys
\$ chmod 600 authorized\_keys

You will then copy/paste the public key into this "authorized\_keys" file.

### Section IV. Configure a PuTTY Session to Use the Key file

Launch the PuTTY utility program. Enter

Host Name or IP Address:remote-computer.cs.vassar.edu(or the IP address)Saved Sessions:computerPort:22

NOTE: Here the default port for SSH is 22, but it may be different at different sites.

	^	Basic options for your PuT	TY ses	sion
⊡ ·· Terminal Keyboard		Specify the destination you want to of Host Name (or IP address)		Port
Bell Features		Connection type:	T 1	
BehaviourTranslation		Load, save or delete a stored sessio Saved Sessions remote-computer	'n	
- Connection		Default Settings	^	Load
Proxy SSH		с. к	~	Save Delete
	~	Close window on exit: Always Never  Only	y on cle	Save Delete ean exit

Next, under "Connection" select "Data" and enter your "username" which is the name of the account you will use to login with to the remote computer.

RepuTTY Configuration ? Х Category: - Session Data to send to the server ^ Logging Login details - Terminal Auto-login usemame your-login-name Keyboard Bell When usemame is not specified: Features Prompt Ouse system usemame (dfrey) . Window Terminal details Appearance --- Behaviour Terminal-type string xterm - Translation Terminal speeds 38400,38400 . Selection --- Colours Environment variables - Connection Variable Add Data - Proxy Value Remove SSH Kex - Host keys - Cipher + Auth TTY X11 ¥ About Help Open Cancel

Auto-login username: your\_loginname

Now, under "Connection" click on "SSH" and then "Auth". Click the [Browse] button and navigate to where you saved your private key in a key file. Select the private key file.



Finally, go back to the "Sessions" category and click [Save] so that this configuration will be saved and you won't have to repeat these steps!

🕵 PuTTY Configurat	ion		? ×
Category:		Davia antiana (annum Du TTV a	!
⊡ · <u>Session</u> Logging ⊡ · Terminal Keyboard		Specify the destination you want to conn Host Name (or IP address)	ect to Port
Bell Features		Connection type:	
Appearance     Behaviour     Translation     Selection		Load, save or delete a stored session Saved Sessions	7
Colours Connection Data Proxy		Default Settings	Load Save
⊟- SSH Kex Host keys		~	Delete
⊕ Auth TTY X11	,	Close window on exit: Always Never Only on	clean exit
About	Help	Open	Cancel

Now when you launch PuTTY all you have to do is locate under your saved sessions the session you want to use, click on the name once to select it and then click [Load] and then click [Open]. A shorter way to do this is to just double-click on the session name from the list of sessions and that will start a remote SSH session.

#### References

SSH Keys

https://www.ssh.com/academy/ssh-keys

What are SSH Keys?

https://www.appviewx.com/education-center/what-are-ssh-keys/

How to Create SSH Keys with PuTTY

https://docs.digitalocean.com/products/droplets/how-to/add-ssh-keys/create-with-putty/