Генерация SSH ключей



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-клиент PuTTY

• PuTTYgen для создания ключа



PuTTY Key Generator	? X
<u>File K</u> ey Con <u>v</u> ersions <u>H</u> elp	
_ Key	
No key.	
Actions	
Generate a public/private key pair	<u>G</u> enerate
Load an existing private key file	<u>L</u> oad
Save the generated key	Save public key <u>S</u> ave private key
Parameters	
Type of key to generate: ○ SSH- <u>1</u> (RSA)	◯ SSH-2 <u>D</u> SA
Number of <u>b</u> its in a generated key:	2048
	,

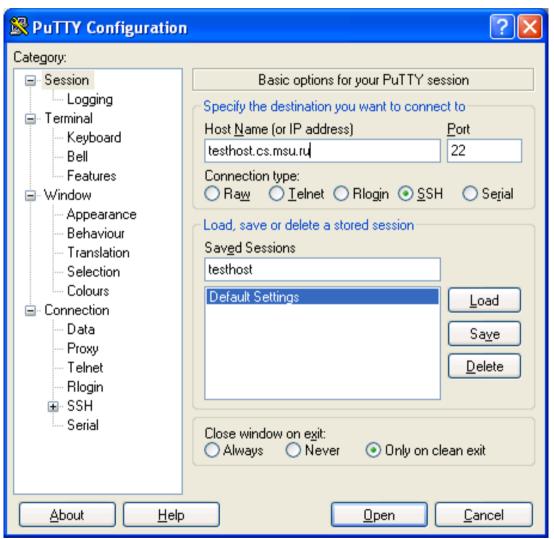


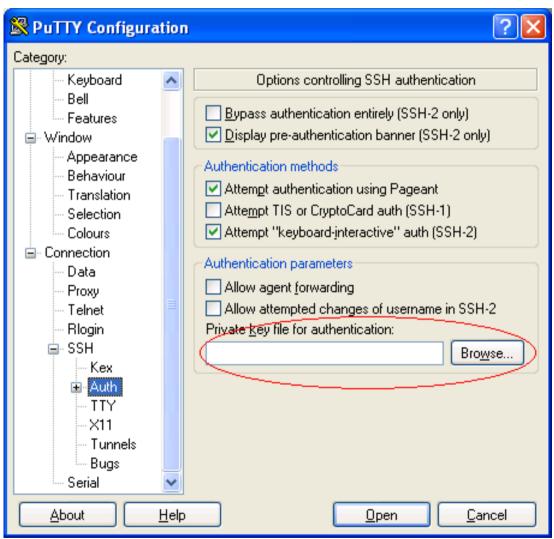
PuTTY Key Generator	?X
File Key Conversions Help	
Key	
Please generate some randomness by moving the mouse over the blan	k area.
Actions	
Generate a public/private key pair	<u>G</u> enerate
Load an existing private key file	<u>L</u> oad
Save the generated key Save public key	Save private key
Parameters	
Type of key to generate:	3.004
SSH-1 (RSA) SSH-2 RSA SSH- Number of bits in a generated key:	2 <u>U</u> SA 2048
Number of bits in a generated key.	2040

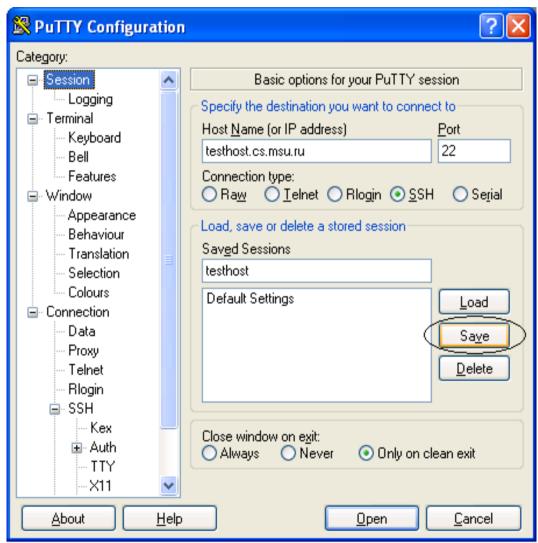


PuTTY Key Gene	rator	?Х	
<u>Fi</u> le <u>K</u> ey Con <u>v</u> ersions	<u>H</u> elp		
Key Public key for pasting	into OpenSSH authorized_keys file:		
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAnSMUixHdKkoFv8q07ZCRvkN6WLuo/+UqeR 223VIKXTuXmexq0tTZ5F4f5oQ+Gdjl0tqwgdj5tcYHoYQET6alT1i6Wst1qJykkpTYFD EL3hkfYgH1DIv3d6hezV0myypwN0ihr/dF0JfCfH3CDQgqd0Z48heP+BBSmI0A0Beh +pKRBHykzz0aNnly8NxsEb34nRm04qq70RTgUJPGRX4LQzfS4I4UyudDSk30FPmFi			
Key fingerprint:	ssh-rsa 2048 d4:ff:37:d9:2d:0f:35:3	9:bb:36:27:53:96:3e:3a:f1	
Key <u>c</u> omment:	rsa-key-20140227		
Key p <u>a</u> ssphrase:			
Confirm passphrase:			
Actions			
Generate a public/priv	ate key pair	<u>G</u> enerate	
Load an existing prival	e key file	<u>L</u> oad	
Save the generated k	ey Save p <u>u</u> b	olic key <u>S</u> ave private key	
Parameters			
Type of key to genera SSH-1 (RSA)	te:	◯ SSH-2 <u>D</u> SA	
Number of <u>b</u> its in a ge	nerated key:	2048	





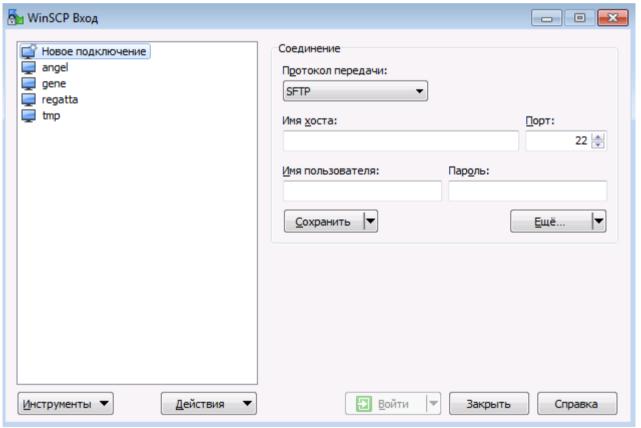




RuTTY Configuration		
Category:		
Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin Serial	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Connection type: Raw Ielnet Rlogin SSH Serial Load, save or delete a stored session Saved Sessions Default Settings Load Saye Delete Close window on exit: Always Never Only on clean exit	
<u>A</u> bout <u>H</u> elp	<u>O</u> pen <u>C</u> ancel	

Копирование файлов. Windows

WinSCP





SSH. Linux

• ssh-клиент уже есть в системе

• Если нет, то: sudo apt-get install opensshclient

Получение fingerprint:
 ssh-keygen -l -f ~/.ssh/id_rsa_hpc.pub



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 coxpaнeн в ~/.ssh/id_rsa_hpc.pub

