Secure Shell Cheatsheet

Task	Command
Logging in	
Connect to remote host	ssh 192.168.1.100
Connect as another user	ssh -l bob 192.168.1.100
Connect on alternate port number	ssh -p 1022 192.168.1.100
Combine all of the above	ssh bob@192.168.1.100:1022
SSH Options	
Connect with alternate cipher	ssh -c blowfish 192.168.1.100
Connect and Forward X traffic	ssh -X 192.168.1.100
Execute command remotely	ssh 192.168.1.100 “tail /var/log/messages”
Secure Copy	
Copy files securely	scp file.tar.gz 192.168.1.100:/home/
Copy files as another user	scp file.tar.gz bob@192.168.1.100:/home/
Copy files with alternate cipher	scp -c blowfish file.tar.gz 192.168.1.100:/home/
Copy files on alternate port number	scp -P 1022 file.tar.gz 192.168.1.100:/home/
Copy files and preserve permissions	scp -p file.tar.gz 192.168.1.100:/home/
Copy recursively	scp -r /home/user 192.168.1.100:/home/
Key Based Authentication	
Create new ssh keys	ssh-keygen -t dsa
Cache ssh keys	ssh-agent
Add identity to ssh-agent	ssh-add
SSH files	
SSH server configuration	/etc/ssh/sshd_config
SSH client configuration	/etc/ssh/ssh_config
User Private/Public keys	~/.ssh/id_dsa, ~/.ssh/id_dsa.pub
Public Keyring	~/.ssh/authorized_keys
Known Hosts	~/.ssh/known_hosts
Port Forwarding	
Forward local 8080 to remote host 80	ssh -L 8080:remote.server.com:80 bob@remote.server.com
Forward remote 1022 to local 22	ssh -R 1022:remote.server.com:22 bob@remote.server.com