***Passphrases***

What's this passphrase thing I just mentioned? A passphrase is like a password, but longer. It includes spaces, words, special characters, numbers, and anything else you can type. The passphrase is used to encrypt and decrypt the private key. A key with a passphrase cannot be used until someone enters the correct passphrase.

Passphrases are most often used with user authentication keys. A user with a key pair can access a system without providing a password for that system. Desktop and laptop systems are usually less secure than servers, and get infected, hijacked, or outright stolen depressingly often. If a user's authentication key pair is stolen, the intruder can use that key pair to access servers just as if he was the legitimate user! Encrypting the private key with a passphrase means that even if the users' private key file is stolen, the intruder cannot use the key without the passphrase. If an intruder gets either your private key file or your passphrase, but not the other, the damage is contained. Make the passphrase too long to guess by brute force and complex enough to discourage attempts to steal it.

Could a passphrase be a single word, like a password? Yes, but it's a *really* bad idea. Computers are now so fast that they can quickly discover short passwords rapidly by trying all possible passwords in succession. Using a short password for a passphrase considerably reduces your private key's security.

A passphrase should be at least several words long, something you can easily remember, and shouldn't be obvious to others – even to people who know you. Include special characters such as #, !, ~, and so on. Peculiar words from specialized non-computing vocabularies are useful. Substitute numbers for letters. Never use anything

from pop culture, and never use any of your own personal catch phrases. Anything you've said to friends or co-workers that was catchy enough to repeat is a poor choice. If your imagination completely fails, Diceware (http://www.diceware.com) is a tool for randomly generating mostly-memorable passphrases from real words using ordinary dice. While intruders can ruin your week, a co-worker with your private key and a sense of humor can be even more aggravating.

Host keys do not use passphrases, because the SSH service must start when the system boots. You could use a passphrase with a server key, but SSH would not start until someone entered the passphrase at the server console. This is unacceptable in most environments.