How to SSH from APPLE / OSX to Cisco Routers / Switches by enabling dhg-sha1

https://pbxbook.com/other/mac-ssh.html

Issues:

Sierra (macOS 10.12) uses OpenSSH v7.2 (El Capitan used OpenSSH v6.9) which no longer supports some of the older, less secure algorithms by default. If an SSH connection is refused with one of the following errors, the fix is to re-enable them in `ssh_config`.

Unable to negotiate with x.x.x.x port 22: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1Unable to negotiate with x.x.x.x port 22: no matching host key type found. Their offer: ssh-dss

Enter the command: `sudo nano /etc/ssh/ssh_config` and add the following two lines to the end of the file:

```
HostkeyAlgorithms +ssh-dss ( for MacOS Ventura use HostkeyAlgorithms +ssh-rsa )
KexAlgorithms +diffie-hellman-group1-sha1
```

A 'better' solution is to create `~/.ssh/config` with those two lines, or better yet, applied more specifically:

```
# settings for all hosts
HostkeyAlgorithms +ssh-dss ( for MacOS Ventura use HostkeyAlgorithms +ssh-rsa )
KexAlgorithms +diffie-hellman-group1-sha1
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc


# host specific settings
Host cs1k
HostName 10.10.10.5
KexAlgorithms +diffie-hellman-group1-sha1
User admin2
```

This example only allows 'diffie-hellman-group1-sha1' for a specific host, and sets a default username - connect with `ssh cs1k`
The 'diffie-hellman-group1-sha1' algorithm is used on most Cisco routers, firewalls and switches, so *may* be added to 'all hosts'.

If an SSH connection is refused with the following error, the fix is to update the offending fingerprint.@@@ @ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @ @@@

Enter the command: `ssh-keygen -R <host>` to clear the old fingerprint, and then try connecting again.
Alternatively, remove the specific host entry fingerprint in `~/.ssh/known_hosts` (or remove the file).

Note: on Unix-based systems like OS X, the tilde character (~) references the user's home directory.