Introduction to Secure Remote Computing Access

To ensure the integrity of your account on our computer systems, all of The Department of Computer Science remote access severs require the use of SSH.

The Secure Shell (SSH) provides encrypted access to our computing environments through private key-based access, which takes the places of a password. Using keys for access helps defend your account against common threats, and lowers your risk. Of course, private key file grants access to systems in the same way as the password, and so it must be protected.

Your private key file should be stored somewhere that no one else will have access to it. If you must store it on Departmental computer systems, use the ssh-keygen command to encrypt it with a passphrase. As an alternative to copying your private key, we highly recommend that you read our articles on ssh-agent forwarding, and other security topics in this wiki.

Additional protection of your SSH session is supported with MFA tokens and secure-store systems.