

HUMBOLDT-UNIVERSITÄT ZU BERLIN



Humboldt-Universität zu Berlin

UNIX-Crashkurs

SSH

Eure FSInI · Tag 1 - II

SSH-Secure Shell

- ▶ Ermöglicht verschlüsselten Zugriff auf die Shell eines anderen Systems
- ▶ `$ ssh Benutzer@Server`
 - ▶ `$ ssh mustermm@gruenau6.informatik.hu-berlin.de`
 - ▶ `$ ssh mustermm@hu-berlin.de@gruenau6.informatik.hu-berlin.de`
- ▶ Verlassen der entfernten Shell: `$ exit`
 - ▶ Notfalls nacheinander: `Enter`, `~`, `.`

Dateien übertragen

- ▶ `$ scp Datei Benutzer@Server:ZielPfad`
 - ▶ `$ scp file.java mustermm@gruenau6.informatik.hu-berlin.de:GdP/`
 - ▶ Kopiert die lokale Datei `file.java` in das Verzeichnis `GdP` des Benutzers `mustermm` auf dem Server `gruenau6`
- ▶ Alternativ (und besser): `rsync`
- ▶ Oder grafisch: SFTP (z. B. WinSCP, FileZilla)

`~/.ssh/config`

- ▶ **Anlegung von Kürzeln**
 - ▶ Kürzel → Benutzer@Adresse:Port
 - ▶ gruenau6 → mustermm@gruenau6.informatik.hu-berlin.de
- ▶ **Realisiert als Einträge in der Datei `~/.ssh/config`**

Login mit öffentlichem Schlüssel

- ▶ Alternative zum Passwort: Öffentlicher Schlüssel
- ▶ `$ ssh-keygen` – Generiert ein Schlüsselpaar
 - ▶ `.ssh/id_rsa` - Privater Schlüssel (geheim halten!)
 - ▶ `.ssh/id_rsa.pub` - Öffentlicher Schlüssel (für den Server)
- ▶ `$ ssh-copy-id -i ~/.ssh/id_rsa.pub Benutzer@Server`