

# Anleitung zur Nutzung von SSH - Unix-Crashkurs 2024

## Inhalt

|                                                                                                            |          |
|------------------------------------------------------------------------------------------------------------|----------|
| <b>Einleitung</b>                                                                                          | <b>1</b> |
| <b>Vorbereitung</b>                                                                                        | <b>1</b> |
| <b>Anleitung für Windows 10/11</b>                                                                         | <b>2</b> |
| <b>Anleitung für macOS</b>                                                                                 | <b>2</b> |
| <b>Anleitung für Linux, insbesondere Ubuntu und Debian</b>                                                 | <b>3</b> |
| <b>ssh von der Kommandozeile</b>                                                                           | <b>3</b> |
| Muss ich diesen langen Befehl jetzt jedes mal von vorne eintippen, wenn ich mich verbinden will? . . . . . | 4        |
| <b>Anleitung für Windows 7, XP, Vista, 8, 8.1, etc.</b>                                                    | <b>4</b> |
| <b>Das hat nicht funktioniert!</b>                                                                         | <b>6</b> |
| <b>Ich brauche eine schnelle Lösung</b>                                                                    | <b>6</b> |
| <b>Ich studiere nicht Informatik</b>                                                                       | <b>6</b> |
| <b>Was ist SSH eigentlich? Wie funktioniert das? Ich will mehr wissen!</b>                                 | <b>7</b> |
| <b>Anhang: Fingerprints der gruenau-Server (Stand Oktober 2024)</b>                                        | <b>7</b> |

## Einleitung

Diese Anleitung erklärt, wie man sich von verschiedenen Systemen auf die Server der Uni einloggt. Warum man das braucht und ähnliche Details besprechen wir im Verlauf des Kurses.

Normalerweise ist es eine sehr schlechte Idee, unreflektiert Code aus dem Internet in sein System zu kopieren. Trotzdem bitten wir dich, uns zu vertrauen und das hier ausnahmsweise mal zu tun.

Diese Anleitung versucht die gängigsten Betriebssysteme abzudecken. Sollte dein System fehlen, bist du sicherlich in der Lage, die Lücken zu füllen. Falls du trotzdem Hilfe brauchst, folge den Schritten unter "Das hat nicht funktioniert".

Die Anleitung zu Beginn ganz zu lesen kann helfen, Überraschungen zu vermeiden.

## Vorbereitung

### Login-Daten raussuchen

Deine Accounts bei der Uni laufen über ein Kürzel, dies benötigst du. Im Normalfall hat das Kürzel 8 Buchstaben und fängt mit deinem Nachnamen an, z.B. `mustemax`. Außerdem benötigst du natürlich noch dein Passwort, mit dem du dich beispielsweise in dein Uni-E-Mail-Konto einloggst.

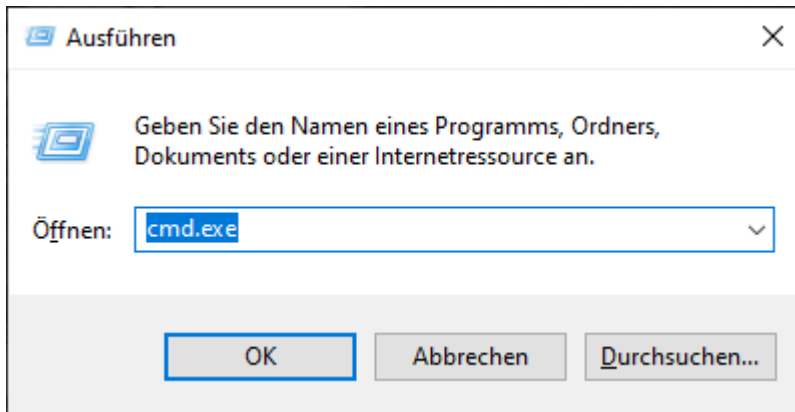
Wenn du einen Informatik-Account hast, kannst du `mustemax` so benutzen wie er ist.

Wenn nicht, musst du noch ein `@hu-berlin.de` dranhängen, also überall wo du deinen Benutzernamen einsetzen musst, `mustemax@hu-berlin.de` einsetzen. Das ist nötig, damit dein CMS-Account benutzt werden kann. CMS-Accounts sind seit September 2024 nicht mehr benutzbar. Es ist also zwingend notwendig, einen [Informatik-Account zu beantragen](#), falls nicht schon geschehen.

## Anleitung für Windows 10/11

### Cmd öffnen

Mit **Windows** + **R** öffnet sich ein "Ausführen" Fenster. Durch Eintippen von `cmd.exe` und Bestätigung mit Enter öffnet sich das Windows-Terminal. Alternativ kannst du auch das Programm "Windows Terminal" aus dem Startmenü öffnen.



### Test auf Installation

Mittels Tippen von `ssh` (und danach Enter) kannst du testen, ob ssh installiert ist und es sollte dir angezeigt werden, wie du ssh benutzen kannst:

```
Microsoft Windows [Version 10.0.12345.678]
(c) 2020 Microsoft Corporation. Alle Rechte Vorbehalten.

C:\Users\MaxMustermann>ssh
usage: ssh [-46AaCfGgKkMMNnqsTtVvXxYy] [-B bind_interface]
          [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
          [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
          [-i identity_file] [-J [user@]host[:port]] [-L address]
          [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
          [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
          [-w local_tun[:remote_tun]] destination [command]
```

Fahre jetzt bitte mit der Anleitung "ssh von der Kommandozeile" unten fort.

## Anleitung für macOS

### Terminal öffnen

Finde und starte Terminal.app, z.B. über Spotlight oder das Launchpad.

### Test auf Installation

Mittels Tippen von `ssh` (und danach Enter) kannst du testen, ob ssh installiert ist und es sollte dir angezeigt werden, wie du ssh benutzen kannst:

```
username@macName ~ % ssh
usage: ssh [-46AaCfGgKkMMNnqsTtVvXxYy] [-B bind_interface]
          [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
          [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
          [-i identity_file] [-J [user@]host[:port]] [-L address]
```

```
[-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
[-Q query_option] [-R address] [-S ctl_path] [-W host:port]
[-w local_tun[:remote_tun]] destination [command]
```

Fahre jetzt bitte mit der Anleitung "ssh von der Kommandozeile" unten fort.

## Anleitung für Linux, insbesondere Ubuntu und Debian

Da Linux-Distributionen viele verschiedene Unterschiede haben können, kann es sein, dass die Anleitung hier und da nicht bis ins letzte Detail stimmt. Wir gehen davon aus, dass das Paket `openssh` installiert ist (ist es fast immer) und du in Linux ein Terminal öffnen kannst. Das geht meistens mit `Strg + Alt + T`.

### Test auf Installation

Wenn das Terminal offen ist, kannst du mittels Tippen von `ssh` (und danach Enter) testen, ob ssh installiert ist und es sollte dir angezeigt werden, wie du ssh benutzen kannst:

```
$ ssh
usage: ssh [-46AaCfGgKkMMNnqsTtVvXxYy] [-B bind_interface]
          [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
          [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
          [-i identity_file] [-J [user@]host[:port]] [-L address]
          [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
          [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
          [-w local_tun[:remote_tun]] destination [command]
```

Fahre jetzt bitte mit der Anleitung "ssh von der Kommandozeile" unten fort.

## ssh von der Kommandozeile

### Verbinden

Jetzt stellst du eine Verbindung mit einem der Uni-Server her. Dazu musst du dir einen Server von [der Liste](#) aussuchen (z.B. `gruenau5`). Wenn du merkst, dass ein Server ganz schön langsam ist, such dir einfach einen anderen. Im Internet kann man sich auch die [Server-Auslastung](#) vorher anschauen. Abgesehen von der Hardware gibt es auf den Servern keine signifikanten Unterschiede für den täglichen Gebrauch.

Um dich mit dem Server `gruenauX` zu verbinden, musst du

`ssh mustemax@gruenauX.informatik.hu-berlin.de` (natürlich `mustemax` mit deinem Kürzel ersetzen) eingeben und Enter drücken.

Wenn du dich das erste Mal mit einem Server verbindest, wird zur Sicherheit der "Fingerabdruck" des Servers angezeigt, damit du verifizieren kannst, dass sich nicht ein anderer Server als `gruenauX` ausgibt. [Diesen Fingerprint musst du online abgleichen](#), und falls der Fingerprint stimmt, `yes` eingeben und mit Enter bestätigen (der Fingerabdruck wird gespeichert und in Zukunft automatisch mit dem verglichen, mit dem sich der Server meldet). z.B.

```
C:\Users\MaxMustermann> ssh mustemax@gruenau6.informatik.hu-berlin.de
The authenticity of host 'gruenau6.informatik.hu-berlin.de (141.20.21.169)'
  can't be established.
ECDSA key fingerprint is SHA256:84DYxhsp6nrZpBhG2pnP/GbZVuq9INxt6DDoXVX9afs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'gruenau6.informatik.hu-berlin.de,141.20.21.169'
  (ECDSA) to the list of known hosts.
mustemax@gruenau6.informatik.hu-berlin.de's password:
```

Jetzt musst du dein Passwort eingeben. Falls du noch nie im Terminal dein Passwort eingegeben hast, kommt jetzt der Hinweis, dass hier kein \*\*\* für die schon eingegebenen Zeichen deines Passworts angezeigt wird sondern einfach gar nix. Wenn du fertig bist, bestätige mit Enter.

Wenn dein Passwort richtig war, öffnet sich die "Shell", die Kommandozeile für den Server.

```
mustemax@gruenau6.informatik.hu-berlin.de's password:
Last login: Sun Oct 4 13:12:45 2024 from 10.20.30.40
Have a lot of fun...
gruenau6 mustemax 1 ( ~ ) $
```

Herzlichen Glückwunsch, du hast dich mit den Servern der Informatik verbunden!

### Verbindung beenden

Um da wieder rauszukommen und die Verbindung zu beenden, tippe `exit` und bestätige mit Enter.

```
gruenau6 mustemax 1 ( ~ ) $ exit
Abgemeldet
Connection to gruenau6.informatik.hu-berlin.de closed.
C:\Users\MaxMustermann>
```

Jetzt kannst du das Terminalfenster in deinem Betriebssystem schließen. Das sollte in den meisten Betriebssystemen auch mit einem zweiten `exit`, Enter funktionieren, natürlich geht auch das X oben am Fenster, Alt+F4, Cmd+Q, usw.

### Muss ich diesen langen Befehl jetzt jedes mal von vorne eintippen, wenn ich mich verbinden will?

Nein. Du kannst dir auch einen Shortcut einrichten, indem du eine SSH-Config anlegst.

Nachdem du dich mit der Anleitung oben das erste mal angemeldet hast, wurde in deinem Benutzerverzeichnis auf deinem Rechner ein `.ssh` -Ordner angelegt. In diesem musst du jetzt eine neue Datei erstellen, die `config` heißt (ohne Datei-Endung!). Eine genaue Erklärung dieser Datei gibts im Kurs selbst und ausführlich nachzulesen in zB. [https://manpages.debian.org/testing/manpages-de/ssh\\_config.5.de.html](https://manpages.debian.org/testing/manpages-de/ssh_config.5.de.html).

Kurzgesagt legt ihr in `Host` fest, wie das Kürzel heißt und alles nach `Host` beschreibt die Konfiguration für das Kürzel.

Hier ein Beispiel für `.ssh/config` :

```
Host g5
  User mustemax
  Hostname gruenau5.informatik.hu-berlin.de
```

Nach dem Speichern könnt ihr dann mit einem einfachen `ssh g5` (eurem Kürzelnamen) auf dem Server kommen.

Noch besser ist allerdings, wenn ihr euch nicht per Passwort, sondern mit einem Schlüsselpaar anmeldet. Das erklären wir euch dann im Kurs, aber falls ihr neugierig seid, findet ihr auch in der Windows-Shortcut-Anleitung oder zB. auf <https://wiki.ubuntuusers.de/SSH/#Public-Key-Authentifizierung> eine Hilfestellung.

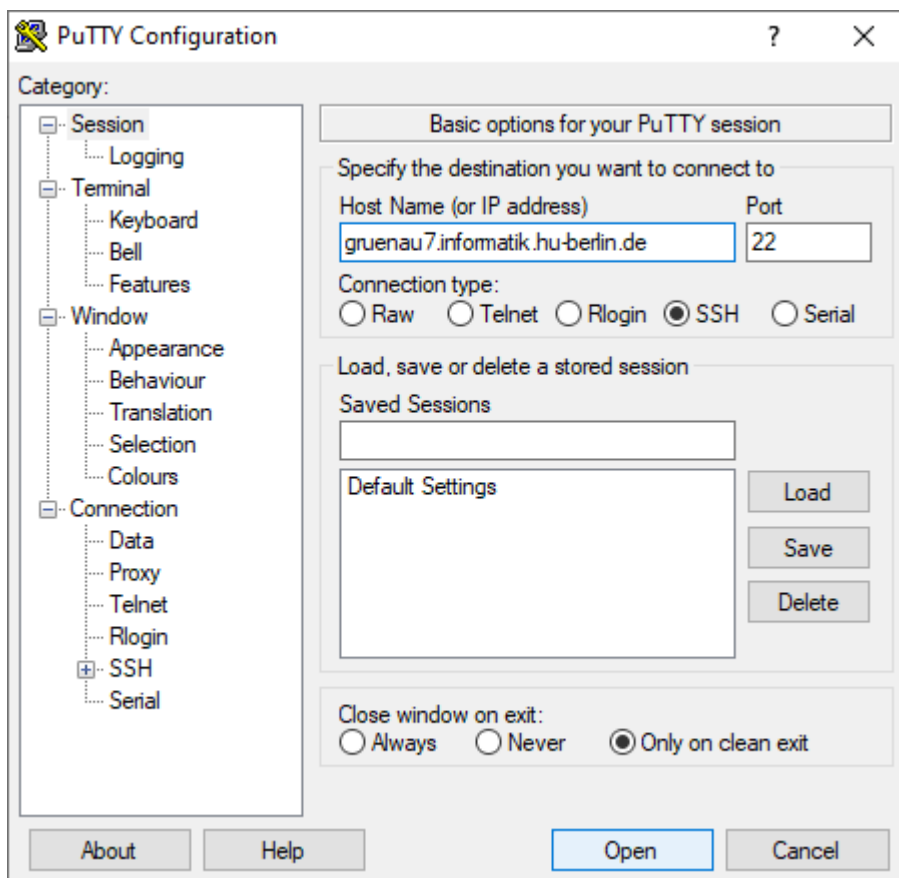
## Anleitung für Windows 7, XP, Vista, 8, 8.1, etc.

Bitte lade PuTTY herunter und installiere es.

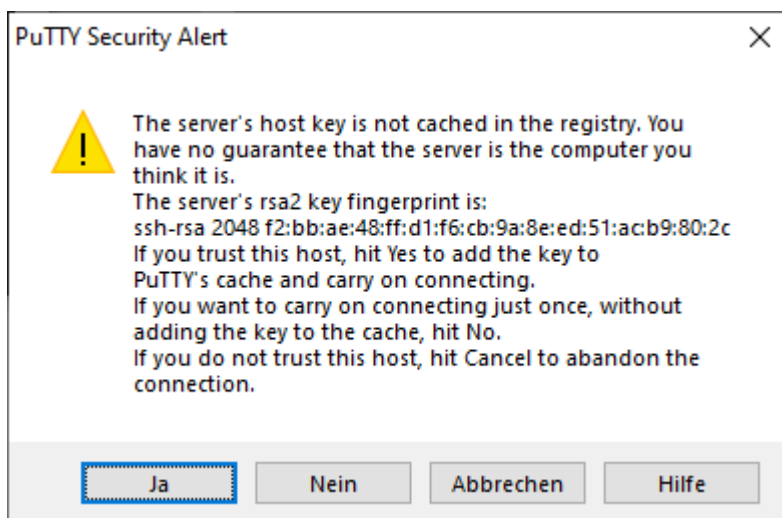
Nach dem Öffnen von PuTTY kannst du bei `Host Name` einen Server eintragen, den du dir von [der Liste](#) aussuchen (z.B. `gruenau5` ) musst. Wenn du merkst, dass ein Server ganz schön langsam ist, such dir einfach einen anderen aus. Im Internet kann man sich auch die [Server-Auslastung](#) vorher anschauen. Abgesehen von der Hardware gibt es auf den Servern keine signifikanten

Unterschiede für den täglichen Gebrauch. In unserem Beispiel haben wir `gruenau7` ausgesucht, das heißt unser Server ist `gruenau7.informatik.hu-berlin.de`

Stelle sicher, dass der Port `22` ist und der Connection type `SSH` ist. Dann klicke unten auf `Open`.



Wenn du dich das erste Mal mit einem Server verbindest, wird zur Sicherheit der "Fingerabdruck" des Servers angezeigt, damit du verifizieren kannst, dass sich nicht ein anderer Server als `gruenauX` ausgibt. [Diesen Fingerprint musst du online abgleichen](#), und falls der Fingerprint stimmt, `Ja` anklicken (der Fingerabdruck wird gespeichert und in Zukunft automatisch mit dem verglichen, mit dem sich der Server meldet).



Jetzt musst du dein Benutzer-Kürzel und Passwort eingeben. Falls du noch nie im Terminal dein Passwort eingegeben hast, kommt jetzt der Hinweis, dass hier kein `***` für die schon eingegebenen Zeichen deines Passworts angezeigt wird sondern einfach gar nix. Wenn du fertig bist, bestätige

jeweils mit Enter.

Wenn dein Passwort richtig war, öffnet sich die "Shell", die Kommandozeile für den Server.

```
login as: mustemax
mustemax@gruenau7.informatik.hu-berlin.de's password:
Last login: Sun Oct 4 13:12:45 2024 from 10.20.30.40
Have a lot of fun...
gruenau7 mustemax 1 ( ~ ) $
```

Herzlichen Glückwunsch, du hast dich mit den Servern der Informatik verbunden!

Um die Verbindung zu beenden, geh zum Abschnitt **Verbindung beenden** oben.

## Das hat nicht funktioniert!

**Q:** Die Verbindung wird geschlossen bevor ich mich anmelden kann!

**Q:** Der Verbindungsaufbau dauert ewig/wird nicht fertig!

**A:** Das kann passieren, wenn du (zu oft) dein Passwort/ deinen Benutzernamen falsch eingegeben hast. In dem Fall werden alle Verbindungen von deiner IP auf diesen Server für eine Weile gesperrt. Du kannst einfach einen anderen Server versuchen.

---

**Q:** Der Fingerprint stimmt nicht überein!

**A:** Wenn bei dir zB.

```
ECDSA key fingerprint is SHA256:4IwYoiBhbz31XhqQ81ibtcZ6YU+XXe89Nhk1b/FDZUI.
```

steht und das nicht im Format f0:0b:aa:... dann schau gerne in der Liste am Ende der Anleitung nach. Die Keys haben auf den Seiten der RBG ein anderes Format.

---

**Q:** Das Verbinden braucht sehr lange

**A:** Falls du dir als Server gruenau9 oder 10 ausgesucht hast, versuche es nochmal mit einem anderen, da diese Server nur aus dem Uni-Netz erreichbar sind, aber nicht aus dem Internet. Um ins Uni-Netz zu kommen, kannst du zB. eine VPN-Verbindung aufbauen (<https://hu.berlin/vpn>) oder dich zuerst mit einem anderen Server verbinden, und dann eine SSH-Verbindung von diesem aus aufzubauen.

Bitte wende dich bei anderen Problemen an andere Student:innen oder die RBG mit einer genauen Beschreibung deines Systems, was du getan hast, was du erwartet hast und was nicht funktioniert hat, zusammen mit dem Output von den Befehlen die du versucht hast.

## Ich brauche eine schnelle Lösung

Wir empfehlen das nicht, weil es einigen Nachteile wie fehlendes Copy&Paste oder Input-Lag mit sich bringt, aber du kannst dich auch mit den Informatik-Servern verbinden, in dem mit deinem Browser (Firefox/Safari/Chrome) auf <https://webconnect.informatik.hu-berlin.de/guacamole/#/> gehst und dich anmeldest.

Unter der Kategorie SSH-gruenaus kannst du auf einen Server doppelklicken, dich ein weiteres Mal am Server einloggen und schon ist eine SSH-Sitzung offen.

## Ich studiere nicht Informatik

Alle, die nicht Informatik studieren, wie z.B. Mathematiker:innen, Physiker:innen, usw. können zwar die Server der Informatik nutzen, sollten aber besser auf die Ressourcen ihrer eigenen

Fakultäten zurückgreifen. Dafür reicht es, den Server beim tippen des `ssh` -Befehls durch einen anderen zu ersetzen.

Wenn du z.B. Mathematik studierst, findest du [die Mathe-Server hier](#).

Wenn du IMP studierst, bist du wahrscheinlich während des Studiums auf allen genannten Servern unterwegs und bist für die Zwecke dieser Anleitung ein(e) Informatiker:in.

## Was ist SSH eigentlich? Wie funktioniert das? Ich will mehr wissen!

Wir werden SSH noch etwas mehr im Unix-Crashkurs beleuchten. Ansonsten gibts hier ein paar Links wo man mehr lesen kann:

- [Was ist eigentlich SSH? Die Secure Shell einfach erklärt](#)
- [Secure Shell \(deutsche Wikipedia\)](#)
- [SSH \(im deutschen Ubuntu-Wiki\)](#)
- [Englische Referenzseite zu ssh](#)

## Anhang: Fingerprints der gruenau-Server (Stand Oktober 2024)

```
gruenau(RSA): SHA256:iB/5YFX3ZPdUqspGeZPNPgXPquufnNFcS2JbYvKYK2w
gruenau(ECDSA): SHA256:eI/KoXyIGBWeYoML+aSRtLvy5ILMmulgpmGdHcF1334
gruenau(ED25519): SHA256:e30H7wzxKqRjxAQFH57pKCVK7uC01+Y3yH8qpq/pt/s
gruenau1(RSA): SHA256:KDlQQV0dTzz0/o/0WuUdjuHEpx2KWjbLa0mbjvtwwTo
gruenau1(ECDSA): SHA256:Yj03bbbWf0RbTzz5lv2/u5kb8iZkbbpoVw8CmZdbkvM
gruenau1(ED25519): SHA256:G8YgSoBJe0NbdqQgaN/QB2UnvyT7UC1zah496bCPeRg
gruenau2(RSA): SHA256:2Kk7cKoQIbp/c3ZwysrSVfH1636WBi3ZnmXnJXbdiE
gruenau2(ECDSA): SHA256:6C4WwR+Mf6qGxk//aUs+0ZlW2QZpQdeJzjCd+6dU818
gruenau2(ED25519): SHA256:xwfVR6yJAnQKb5+QC3vTEMvIq0QubdAAIypb82ycpbC
gruenau3(RSA): SHA256:YCFf3eLqM0G29ycpl59IUmfFbFy0QcFvKi83L918MEg
gruenau3(ECDSA): SHA256:0CL5NtAKnyrWG/bbUqVHvDtwS2VGbUWHaTt8bDBcYac
gruenau3(ED25519): SHA256:8D47BZGj00T1t7j8YSToTXPxa+xkJdzE8tIukMvqQ8A
gruenau4(RSA): SHA256:OMx+5PxrCjYYPch/8z/2sw10HYc+2fXyUyC5FjcytqM
gruenau4(ECDSA): SHA256:I0scGaX0opwdoA0f3nLVabvKbKVU6Ic1QEBsAht+0b0
gruenau4(ED25519): SHA256:uA0pB8Vm1LGzH6f/h9/bQNUP7S3aUnubzuosvty/thE
gruenau5(RSA): SHA256:GYZSjqgSLWq8NCiSkQNM80ygcvkJ9GB6KpaM09mtyHk
gruenau5(ECDSA): SHA256:a2QrTYIyZULb0yzanqoluYR8ibq0bztlf2Ww1co7h0
gruenau5(ED25519): SHA256:+I5pzI6g/lwAP5Rlc24tmrJ31pfcvpI2qTtqzasEcLE
gruenau6(RSA): SHA256:TMH383ydzDjqAJX60krKHnI0YuGAQ6F75yen2dDzsyw
gruenau6(ECDSA): SHA256:84DYxhsp6nrZpBhG2pnP/GbZVuq9INxt6DDoXVX9afs
gruenau6(ED25519): SHA256:V7i5oA6tpl7eTNvUWfpe/qLXqXpZUV2wpLNC4qJa6hU
gruenau7(RSA): SHA256:Rx9f7EM9Dt8eRDzXbox4+w+HFH42E63lllGJU4tT4mA
gruenau7(ECDSA): SHA256:wZgPCc5TeXak1rfCnXnq2rWg/JD73qRatfpSIna221A
gruenau7(ED25519): SHA256:vMu86ZfcQw8dsvIVTr7AQIXJjaRjqu8R1hWHpoyLijY
gruenau8(RSA): SHA256:3+f8W2vwaEC8tbsIUIacswBJF3UIxA20DqV17ppaCbs
gruenau8(ECDSA): SHA256:nGhFQ9vMynGAYd1iF0CWcm7uq6+0TQYp001AWlcK9lM
gruenau8(ED25519): SHA256:bcvCrMch+gI1z1ofPXRkKGr6QAPXHXrtByKBYFay4rg
gruenau9(RSA): SHA256:cLRYcujbYXBrjTn618ElDJFcLAJLMx4UQ6dh8BLQmrc
gruenau9(ECDSA): SHA256:T8BorEXop9btn/wqFP8Fnygj8q/SUfJHPem+I0uprqA
gruenau9(ED25519): SHA256:LxjHNFmvpItZvSuSNKHilMrT3R7ZfaIXEKS1NAjoBQM
gruenau10(RSA): SHA256:v+vyhDnUBeX9f64xeYY25IsVkJ3yL6nlWTSqJ+kE
gruenau10(ECDSA): SHA256:ba8G4qIQVUfCylJ8bGFR9bvgTwcMW/dz+d+MRLIy2eQ
gruenau10(ED25519): SHA256:lzc9iixn6kQsXIoflGaStAEL6S6QAaIUurzyp/RgQBM
```