

## Praktikum 5

### zur Vorlesung Kryptologie

1. Installieren Sie sich eine Version von PGP, OpenPGP oder GnuPG.
2. a) Erzeugen Sie sich ein Schlüsselpaar und legen Sie Ihren Schlüssel auf PGP-Keyservern ab oder senden Sie ihn mir.  
Achten Sie dabei darauf, ob/wann/wie „Zufall“ zur Generierung des Schlüssels einfließt.
- b) Besorgen Sie sich meinen PGP-Schlüssel von einem Schlüsselservers.  
Der Fingerprint meines Schlüssels ist  
  
72A8 45B1 1A79 F4AD 73B7 324C 8A62 2D46 5A3C DE1E.  
  
Achten Sie darauf, was Sie bei dem Schlüssel einrichten können/müssen.
3. Achten Sie bei den folgenden Aufgaben darauf, welcher Schlüssel zum Einsatz kommt bzw. ob Sie das Passwort für Ihren privaten Schlüssel brauchen.
  - a) Senden Sie mir eine verschlüsselte (nicht signierte) Nachricht.
  - b) Senden Sie mir eine signierte (nicht verschlüsselte) Nachricht.
  - c) Sie erhalten von mir eine verschlüsselte Nachricht. Bestätigen Sie die erfolgreiche Entschlüsselung durch Rücksendung des Klartextes.
  - d) Sie erhalten von mir eine signierte Nachricht. Können Sie meine Signatur verifizieren?