FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2025/26
zu bearbeiten bis
14.01.26

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 Schlüsselserver.

   Der Fingerprint meines Schlüssels ist

   B936 98C6 AEF8 DC01 D08A 95AA 1108 352B C06E F63A.

   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?