Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Blatt 1

Es geht etwas oberflächlich um klassische Kryptographie.
Sie sollen aber jedenfalls ein wenig Übung im Umgang mit dem Programmpaket openssl erlangen.

Aufgabe 1

a) Beschaffen Sie sich im Internet eine Beschreibung des AES-Algorithmus und googeln Sie auch nach „AES demo“. Versuchen Sie zumindest oberflächlich zu verstehen, wie der Algorithmus funktioniert.

b) Laden Sie das Programmpaket openssl auf Ihren Rechner.
Googeln Sie nach „test vectors aes cbc“. Überprüfen Sie den Output der AES-Ver- und Entschlüsselungsbefehle, z.B. des Befehls `openssl enc -aes-256-ecb` anhand dieser Testvektoren. Die Syntax von `openssl enc` können Sie z.B. unter https://www.openssl.org/docs/apps/enc.html nachlesen.

c) Überprüfen Sie in analoger Weise, ob in Ihrer Version von openssl die kryptographische Hashfunktion sha512 vorschriftsmäßig funktioniert.

Dokumentieren Sie Ihre Recherche und Ihr Vorgehen.

Binärdateien unter Linux analysieren Sie am einfachsten mit dem Befehl xxd, unter Windows installieren Sie einen geeigneten Hex-Editor, z.B. Neo.