Christian Schindelhauer

Freiburg, den 23.Mai.2012
Besprechung 23.Mai.2012

Übungen zur Vorlesung

Systeme II / Netzwerke I

Sommer 2012

Blatt 4

AUFGABE 1:

- Verschlüsseln Sie mit dem RSA-Algorithmus die Nachricht M.

  p = 541
  q = 409
  e = 65537
  M = 2

- Geben Sie den öffentlichen und den geheimen Schlüssel an.
- Entschlüsseln Sie zur Kontrolle die Nachricht von Hand, d.h. ohne Zuhilfenahme eines Computeralgebrasystems.

AUFGABE 2:
Sie möchten das Admin-Passwort eines Online-Forums rekonstruieren und besitzen nur noch den MD5-Hash-Code des Passworts: `e770dac72193f75f8d5a7858bd6a1393`

- Beschreiben Sie MD5 und diskutieren die Sicherheit von MD5.
- Wie kann man die Sicherheit der mit MD5 verschleierten Passwörter erhöhen ?
- Finden Sie das verschlüsselte Passwort, indem Sie ein Programm schreiben, das eine Brute-Force-Attacke durchführt. Sie können hierbei annehmen, dass das Passwort aus 6 Buchstaben besteht und nur die Buchstaben aus $\{a, b, c, d, e, f, g, h, i, j, 1, 2, 3, 4, 5, 6, 7, 8, 9, \#, \$\}$ verwendet.