

Übungen zur Vorlesung
Systeme II / Netzwerke I
Sommer 2011
Blatt 3

AUFGABE 3:

Der Spielekonsolenhersteller Coney hat Ihnen mitgeteilt, dass durch einen Hackerangriff sämtliche Kundendaten inklusive Passwörter im Internet veröffentlicht wurden. Da die Passwörter aber nicht als Klartext, sondern als MD5 Hashcode verschlüsselt in der Datenbank gespeichert werden, bräuchten Sie sich keine Sorgen zu machen.

Über Google erfahren Sie, dass der Passwort-Hash des Users `SingStar`, einer Ihrer stärksten Rivalen, `bb5459bf19132d4dc1340654c17331df` lautet.

1. Beschreiben Sie MD5 und diskutieren die Sicherheit von MD5.
2. Beschreiben Sie mindestens zwei Möglichkeiten um an ein zu dem Hashwert passendes Passwort zu gelangen.
3. Schreiben Sie ein Programm das eine Brute-Force-Attacke durchführt unter der Annahme das Coney nur Kleinbuchstaben in Passwörtern erlaubt.