

- 15.) HÜ9 auf S. 85 der VO-Slides.
- 16.) HÜ10 auf S. 86 der VO-Slides.
- 17.) HÜ2 auf S. 93 der VO-Slides.
- 18.) Führen sie eine Geburtstagsattacke (beschrieben auf S. 87 der VO-Slides) durch:
Erstellen sie zwei semantisch unterschiedliche Dokumente (wie im besprochenen Beispiel die beiden unterschiedlichen Mietverträge) im Format ihrer Wahl (Word, Postscript, etc.), und modifizieren sie beide Varianten Semantik-erhaltend automatisiert (beschreiben sie das detailliert, wie sie dabei vorgehen), bis sie auf zwei Varianten mit dem gleichen hash-Wert treffen (verwenden sie dafür die eigentlich obsoletere Hashfunktion MD-5).

VIEL ERFOLG !!