PS Einführung Kryptographie und IT-Sicherheit

Salzburg, T01, 14:45 *05.05.2025*
***Abgabe**: bis DO 01.05. 15:00 an uhl@cs.sbg.ac.at*

21.) Fortsetzung Aufgabe 20.): Erklären sie, warum die Verwendung von Hashfunktionen im Kontext mit digitalen Signaturen die Protokollattacke gegen digitale Empfangsbestätigungen verunmöglicht. Bedenken sie dabei insbesondere, dass in diesem Fall NachrichtenHash und Nachricht übermittelt werden (die Fragen in Item 2 auf Skriptum S. 93 müssen bearbeitet werden).

22.) HÜ10 auf S. 86 der VO-Slides.

23.) 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 obsolete Hashfuntion MD-5).

VIEL ERFOLG !!