FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
06.12.2023

Musterlösung zum 9. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Nach heutigem Stand ist h eine Einwegfunktion. Denn wäre sie es nicht, so könnte man zu gegebenem h_0 ein m mit

$$h_0 \;=\; h(m) \;=\; m^{e_h} \bmod n_h$$

berechnen, d.h., man könnte modulare e_h-te Wurzeln ziehen und damit das RSA-Verfahren brechen; nach heutigem Stand des Wissens ist das nicht möglich.

h ist allerdings nicht schwach (und damit auch nicht stark) kollisionsresistent, denn gibt man ein m vor, so hat $m' = m + n_h$ den gleichen Hashwert:

$$h(m') \;=\; h(m + n_h) \;=\; (m + n_h)^{e_h} \bmod n_h \;=\; m^{e_h} \bmod n_h \;=\; h(m).$$

Übung 2

Sie D_k die Entschlüsselungsfunktion zu E_k.

a) Keine kryptografische Hashfunktion, da keine Einwegfunktion: Zu beliebig vorgegebenem h ist $m = D_{k_0}(h)$ eine Nachricht (ein Block lang) mit Hashwert h.

b) Keine kryptografische Hashfunktion, da nicht kollisionsresistent: Fügt man an eine Nachricht zwei gleiche Blöcke $\hat{m}$ an, so ergeben diese zwei mal $E_{\hat{m}}(M)$, die sich bei der XOR-Verknüpfung genau wieder wegheben.

   Bei einer CBC-ähnlichen Verschachtelung erhält man aber tatsächlich eine kryptografische Hashfunktion: $h_0 = M$ und $h_i = E_{m_i}(h_{i-1}) \oplus h_{i-1}$.

Übung 3

Bei einer Passwortdatei in der einfachen Form reicht es, dass einer der Nutzer ein Wort des Wörterbuchs als Passwort hat. Der Angreifer muss nicht wissen, wer das ist, sondern entdeckt das durch die Gleichheit der Hashwerte.

Benutzt man Salt, muss der Angreifer genau den Salt des unvorsichtigen Nutzers benutzen, um zu entdecken, dass genau dieser Nutzer ein einfaches Passwort hat. Für einen Angriff muss er also sämtliche Worte mit sämtlichen Salt-Werten verknüpfen. Besitzt die Datei n Einträge bedeutet das einen n-fachen Aufwand gegenüber der einfachen Variante.