FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
06.12.2023

9. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Sei n_h das Produkt zweier großer unbekannter Primzahlen und e_h fest gewählt.

Ist dann

$$h : \mathbb{N} \to \mathbb{Z}_n,\ h(m) \ = \ m^{e_h} \bmod n_h$$

eine Einwegfunktion bzw. schwach und/oder stark kollisionsresistent?

Übung 2

Die folgenden Vorschläge erzeugen aus einer symmetrischen Verschlüsselungsfunktion E_k mit Schlüssel k, z.B. AES, eine Hashfunktion. Warum sind dies keine kryptografischen Hashfunktionen?

a) Ein Schlüssel k_0 wird von einer Behörde festgelegt und veröffentlicht.

   Der Hashwert $h(m)$ einer Nachricht m errechnet sich dann, indem m per CBC-Mode mit dem Schlüssel k_0 verschlüsselt wird, und nur der letzte Block als Hashwert genommen wird.

b) Eine Nachricht M wird von einer Behörde festgelegt und veröffentlicht.

   Der Hashwert $h(m)$ einer Nachricht m errechnet sich dann, indem die Nachricht m entsprechend der Schlüssellänge in Blöcke m_i zerlegt wird, und dann $E_{m_i}(M)$ berechnet und die Ergebnisse XOR-verknüpft werden.

(Um eine entsprechende Blockzerlegung sinnvoll durchführen zu können, wird jeweils ein geeignetes Padding durchgeführt.)

Übung 3

Eine Passwort-Datei enthalte die Hashwerte vieler Passwörter. Ein *Wörterbuchangriff* berechnet zu Wörtern eines Wörterbuchs oder Abwandlungen davon die entsprechenden Hashwerte und vergleicht sie mit den Werten in der Datei. Hat ein unvorsichtiger Nutzer ein solches Wort als Passwort gewählt, wird der entsprechende Wert gefunden, und der Angreifer kann in das System eindringen.

Eine Verbesserung besteht darin, dass in der Datei zu jedem Nutzer eine Zufallszahl (auch *Salt* genannt) unverschlüsselt gespeichert wird, und dass der gespeicherte Hashwert aus dem Passwort und dieser Zufallszahl gebildet wird.

Warum ist dies eine Verbesserung?