Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Fachhochschule Dortmund
University of Applied Sciences and Arts

Aufgabe 6.1 K2+2

a) Wie definiert man im Allgemeinen kryptographische Hashfunktionen?

b) Geben Sie mindestens zwei mögliche Einsatzszenarien für Hashfunktionen an.

Aufgabe 6.2 K10+6

Folgender Umstand ist als Geburtstagsparadoxon bekannt: Es müssen mindestens 23 Personen in einem Raum anwesend sein, so dass mit einer Wahrscheinlichkeit von 50% wenigstens zwei von ihnen am selben Tag Geburtstag haben.

a) Formulieren Sie eine Beweisskizze.

b) Wie viele Hashwerte mit 96 Bits Länge aus nicht identischen Urbildern muss man demnach durchschnittlich berechnen, bevor es zu einer Kollision kommt?

Aufgabe 6.3

a) Wie funktioniert das Padding der SHA-2 Familie[1]? Recherchieren Sie und erklären Sie das Verfahren mit eigenen Worten und/oder einer Abbildung.

b) Führen Sie das SHA-256 Padding für das Urbild „hello, world“ (ohne Anführungsstriche, als 8 Bit ASCII) aus und notieren Sie das Ergebnis.

[1] https://www.rfc-editor.org/rfc/rfc6234, aufgerufen am 17. Mai 2023