Labor Kryptologie, Blatt 2

Johannes Bauer & Reinhold Hübl & Miriam Weigel *

Sommersemester 2025

Allgemeiner Hinweis: Wenn nicht explizit anders spezifiziert hat Ihre Abgabe als PDF zu erfolgen, das grundsätzlich handschriftlich ausgeführt ist. Die Ausnahme stellt Programmcode dar, den Sie in Ihr PDF *maschinenlesbar* einbetten dürfen (also *nicht* als Screenshot). Zulässige Programmiersprachen sind C, C++, Python, Java, Rust, Go, x86-64 Assembly

1 Hashfunktionen

Gegeben sei eine 40-Bit Hashfunktion H, die auf MD5 basiert. Statt des 128-Bit Outputs von MD5 werden nur die ersten 40 Bit als Ausgabe verwendet. Folgende Testvektoren sind Ihnen für H gegeben:

```
H("") = d41d8cd98f
H("Leeroy Jenkins") = eddda4a630
```

1. (1 Punkt) Schreiben Sie Programmcode, der H implementiert und die Testvektoren validiert.
2. (3 Punkte) Schreiben Sie Programmcode, der einen Kollisionsangriff auf H ausführt. Hierbei sollen Kollisionen von Nachrichten gefunden werden, die jeweils mit Ihrem vollständigen Namen anfangen. Beinhalten Sie in der Ausgabe Ihres Programms unbedingt die gefundene Kollision. Nach wie vielen Versuchen haben Sie diese gefunden?

2 Schlüsselräume

1. (1 Punkt) Ein Passwort wird randomisiert erstellt und besteht aus Kleinbuchstaben, Großbuchstaben, den Ziffern 0 bis 9 sowie acht weiteren Sonderzeichen. Es beinhaltet zwölf Zeichen. Schätzen Sie das Sicherheitsniveau des Passworts ab. Handelt es sich um ein qualitativ gutes Passwort?
2. (1 Punkt) Das Alphabet des in der vorigen Aufgabe randomisiert generierten Passworts wird auf lediglich Kleinbuchstaben reduziert. Wie viele Zeichen werden mindestens benötigt um das Sicherheitsniveau der vorigen Aufgabe mindestens zu halten?
3. (1 Punkt) Untersuchen Sie die Mindestlänge, die ein Passwort haben muss um ein Sicherheitsniveau von 128 Bit zu erreichen mit Alphabeten das
   - Nur aus den Buchstaben X und Y besteht
   - Nur aus Ziffern besteht
   - Nur aus Kleinbuchstaben besteht
   - Nur aus Kleinbuchstaben und Großbuchstaben besteht
   - Nur aus Kleinbuchstaben, Großbuchstaben und Ziffern besteht

*johannes.bauer@dhbw.de reinhold.huebl@dhbw.de; miriam.weigel@dhbw.de; DHBW Mannheim

- Nur aus Kleinbuchstaben, Großbuchstaben, Ziffern und zehn Sonderzeichen besteht

4. (1 Punkt) Eine ideale Hashfunktion habe eine Hashlänge von 200 Bit. Schätzen Sie die Komplexität der drei in der Vorlesung gezeigten Angriffe ab.