5

502470 - Einführung in Sicherheit und Privatheit

Übung: Kryptographie

— Diskussion der Lösung während der Übung: 20./21. Juni 2024 —

1 Kryptographie

Aufgabe 1. Im Dateiverzeichnis zur Übung finden Sie zwei Java-Dateien: **Encrypt.java** und **Decrypt.java**. Vergleichen Sie den SHA-256 Hash nach dem Herunterladen der Java-Datei **Encrypt.java** mit diesem:
4C6FDB4E07CC783531F4524D12C0C00049433A346FC72A4107440A2FB5201F3B
Was wird dadurch sichergestellt?

Aufgabe 2. In der Datei **Encrypt.java** sind zwei Funkionen zu implementieren.

1. Die Funktion `makeSalt()` soll einen Salt-Value für die Hashfunktion generieren.
2. Die Funktion `makeHash()` soll aus dem Passwort und dem Salt einen Hash berechnen.

Aufgabe 3. In der Datei **Decrypt.java** sind eine Funkion und der Passwortcheck zu implementieren.

1. `makeHash()` kann von **Encrypt.java** übernommen werden
2. Wenn das eingegebene Passwort korrekt ist, soll CORRECT ausgegeben werden, sonst WRONG

Hinweise:

- Das Programm **Encrypt.java** stürzt ab, wenn die Funktionen noch nicht implementiert sind (Zeile 36)!
- Username, Passwort und Salt werden in eine generierte Datei `shadow.txt` geschrieben bzw. angehängt, wenn die Datei bereits existiert.
- Die Datei `shadow.txt` wird erstellt, wenn sie noch nicht existiert.
- **Decrypt.java** wirft einen Fehler, wenn die Datei `shadow.txt` nicht im selben Verzeichnis ist.

Aufgabe 4. Im Dateiverzeichnis zur Übung finden Sie eine Textdatei `reallybadpasswords.txt` in welcher die MD5 Hashes von 4 Passwörtern gespeichert sind, die jeweils aus nur einem Zeichen bestehen. Es wurde kein Salt angewendet. Versuchen Sie, sie zu entschlüsseln. Das Alphabet (mögliche Zeichen) ist $\{a, b, c, d, e, f\}$.

Aufgabe 5. Im Dateiverzeichnis zur Übung finden Sie eine Textdatei `badpasswords.txt` . In dieser sind die MD5 Hashes von 6 sehr kurzen und einfachen Passwörtern enthalten. Es wurde kein Salt angewendet. Versuchen Sie, sie zu entschlüsseln.

Hinweise

- Die Passwörter sind höchstens 5 Zeichen lang.
- In den Passwörtern kommen nur Kleinbuchstaben und Zahlen vor.

Aufgabe 6. Verschlüsseln Sie den Text `Computersicherheit` als Stromchiffre mit dem folgenden Schlüsselstrom $s_{i+1} = s_i + 1 \mod 2, s_0 = 0$. Machen Sie auch die Probe für die Entschlüsselung.