Universität Klagenfurt
Informatik – Systemsicherheit
R. Wigoutschnigg

UE Systemsicherheit
SS 2018
Übungstermine: siehe ZEUS

Abgabe 3

Abgabe: 08.07.2018

Implementieren Sie folgenden Code, welches die Möglichkeit zur Erzeugung von Salted-Hashes, zur Authentifikation (dh. prüfen, ob das Passwort korrekt ist) von Benutzern sowie zur Erzeugung von Zufallszahlen bietet. Bei der Erzeugung von Saltes-Hashes wenden Sie die Hashfunktion mehrfach an, um es Angreifern noch schwerer zu machen, das dazugehörige Passwort zu bestimmen. Wählen Sie die Anzahl der Iterationen nur so hoch, dass dieser Zusatzaufwand die Verwendbarkeit im Rahmen eines Zutrittssystems nicht nennenswert reduziert. Implementieren Sie zudem das PBKDF2 nach PKCS #5 V2. Nehmen Sie hierfür das RFC2898 zur Hand. Zum *selbständigen* Test ihrer Implementierung verwenden Sie bitte das RFC6070. Implementieren Sie die Methoden zur Analyse von Zertifikaten (verwenden Sie geeignete Funktionalitäten des JDK, um diese Aufgaben zu lösen).

Zu implementierende Teilaufgaben

a) Implementieren Sie die Schnittstelle `PasswordTools`.
b) Implementieren Sie die Schnittstelle `CertTools`.

Sie können Gruppen von bis zu 3 Personen bilden. Bei Unklarheiten ist es in Ihrer Verantwortung Ihren LV-Leiter zu kontaktieren.