Hochschule Düsseldorf
University of Applied Sciences

Prof. Dr. Holger Schmidt
Professur für Informatik, insb. IT-Sicherheit
Fachbereich Medien – Hochschule Düsseldorf

Fachbereich Medien
Faculty of Media

Lastenheft „File Crypt“

Ziel ist die Implementierung von *File Crypt* (FC), einer Software welche beliebige Dateien unter Verwendung verschiedener kryptografischer Verfahren schützen kann.

Funktionale Anforderungen

FC MUSS Dateien auslesen und abspeichern können. Folgende kryptografische Verfahren MÜSSEN zur Auswahl stehen:

- Symmetrische Verschlüsselung:
  - `AES` mit Schlüssellängen 128, 192, 256 Bit
- Passwort-basierte Verschlüsselung:
  - AES 256 Bit, GCM, SCRYPT
  - `PBEWithSHA256And128BitAES-CBC-BC`
  - `PBEWithSHAAnd40BitRC4`
- Digitale Signatur (Erzeugung und Verifikation):
  - `SHA256withDSA`

In Abhängigkeit des gewählten Verfahrens, MÜSSEN die Padding Mechanismen `NoPadding`, `PKCS7Padding` und `ZeroBytePadding`, sowie als Blockmodi `ECB`, `CBC`, `OFB`, `CTS`[1] und `GCM` zur Verfügung stehen. FC MUSS die benötigten Schlüssel generieren können.
FC MUSS Manipulationen an abgespeicherten Texten erkennen können, indem ein Hashwert mit abgespeichert und beim Laden des Textes verifiziert wird. Dazu MUSS der Nutzer auf folgende Hashfunktion und MACs zurückgreifen können:

- `SHA-256`
- `AESCMAC`
- `HMACSHA256`

Das Speichern der Schlüssel, Texte, Hashwerte und MACs mit entsprechenden Metadaten MUSS (ggf. jeweils separat) in einem strukturierten Dateiformat (z. B. basierend auf XML oder JSON) erfolgen.

[1] CTS wird manchmal auch als Padding bezeichnet.

Nicht-funktionale Anforderungen

FC SOLL in Java und MUSS mithilfe der aktuellsten Version von `The Legion of the Bouncy Castle`[2] implementiert werden. Die Nutzerinteraktion kann über ein command-line-interface (z. B. basierend auf `Picocli`[3]) oder über eine graphische Benutzeroberfläche (z. B. als Web Frontend oder basierend auf `Java FX`[4]) erfolgen. Die Softwarearchitektur MUSS eine einfache Erweiterbarkeit erlauben, sodass zusätzliche Kryptografiekomponenten leicht ergänzt werden können.
FC MUSS inline dokumentiert werden. Dazu MUSS für Java `Javadoc` und `Doxygen`[5] verwendet werden. Weiterhin MUSS eine Validierung basierend auf dem Unit-Test-Framework implementiert werden Dazu MUSS für Java `JUnit`[6] verwendet werden. Weiterhin MUSS eine Analyse der Testabdeckung hinsichtlich Anweisungs-, Zweig- und Bedingungsabdeckung mithilfe eines Werkzeugs wie z. B. `JaCoCo`[7] durchgeführt werden.
Idealerweise arbeiten Sie mit `IntelliJ IDEA`[8] oder `Eclipse`[9], `Git`[10] und `Maven`[11].
`IntelliJ IDEA Ultimate` ist als Teil des `JetBrains Product Pack for Students` kostenlos `for educational use only` durch Registrierung auf https://account.jetbrains.com/login erhältlich.

[2] https://www.bouncycastle.org, aufgerufen am 8. März 2021
[3] https://picocli.info/, aufgerufen am 8. März 2021
[4] https://openjfx.io/, aufgerufen am 8. März 2021
[5] https://www.doxygen.nl/, aufgerufen am 8. März 2021
[6] http://junit.org/, aufgerufen am 8. März 2021
[7] http://www.eclemma.org/jacoco/, aufgerufen am 8. März 2021
[8] https://www.jetbrains.com/idea/, aufgerufen am 8. März 2021
[9] https://eclipse.org/, aufgerufen am 8. März 2021
[10] https://git-scm.com/, aufgerufen am 8. März 2021
[11] https://maven.apache.org/, aufgerufen am 8. März 2021