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

Übungsblatt 5 **Entwicklung sicherer Software – SS 2021** Datum: 12.05.2021

Aufgabe 5.1 Unterstütztes Selbstlernen

Bereiten Sie die nächste Vorlesung basierend auf [Hook and Eaves, 2020, Seiten 35 – 42] vor, indem Sie

- die Texte lesen und verstehen,
- sich Fragen und Notizen aufschreiben sowie
- den dargestellten Quellcode selbst praktisch ausprobieren.

Anmerkungen:

Um das Textverständnis zu verbessern, müssen Sie typischerweise weitere Quellen zu Rate ziehen. Halten Sie Ihre aktuellen Implementierungsergebnisse bereit, sodass wir Ihren Quellcode besprechen können.

Der Quellcode aus Hook and Eaves [2020] ist unter folgender URL bereitgestellt:
`https://leanpub.com/s/XCxd95GsH0-8tLTunJ6rhA.zip`

Aufgabe 5.2

Erweitern Sie die Kryptographie-Komponente Ihrer Software basierend auf [Hook and Eaves, 2020, Seiten 35 – 42] um die dort vorgestellten Block Cipher Modi, d. h. CTR, CFB und OFB. Dokumentieren Sie Ihren Quellcode weiterhin mit Javadoc und Doxygen.

Welche Vor- und Nachteile haben die Verfahren jeweils? Ergänzen Sie die im Rahmen einer vorherigen Aufgabe erstellte Vergleichstabelle entsprechend.

Aufgabe 5.3

Erweitern Sie die Kryptographie-Komponente Ihrer Software um das Stream Cipher Verfahren ARC4.
Testen Sie Ihre Erweiterung mit neuen JUnit-Tests und analysieren Sie die Testabdeckung mithilfe von JaCoCo. Dokumentieren Sie Ihren Quellcode und Test-Quellcode weiterhin mit Javadoc und Doxygen.

Aufgabe 5.4

Erstellen Sie Unit Tests mithilfe von JUnit[1] für Ihre Implementierung. Analysieren Sie die Testabdeckung hinsichtlich Anweisungs-, Zweig- und Bedingungsabdeckung mithilfe eines Werkzeugs wie z. B. `JaCoCo`[2]. Dokumentieren Sie auch Ihren Test-Quellcode mit Javadoc und Doxygen.

Anmerkungen:

[1] `http://junit.org`, aufgerufen am 18. März 2021
[2] `http://www.eclemma.org/jacoco/`, aufgerufen am 18. März 2021

JUnit kann in Ubuntu über die offiziellen Paketquellen installiert werden (Paketname *junit5*). Zur Installation von JaCoCo folgen Sie bitte den Hinweisen auf der Webseite von JaCoCo.

Aufgabe 5.5

Beantworten Sie folgende Frage:

a) Was ist wahrscheinlich das Problem, wenn via `CipherOutputStream` geschriebene Daten abgeschnitten sind?

Diese Aufgabe basiert auf Fragen (Exercises) aus [Hook, 2005, Seite 55f.].

Literatur

David Hook. *Beginning Cryptography with Java*. John Wiley & Sons, 2005.

David Hook and Jon Eaves. *Java Cryptography: Tools and Techniques*. Leanpub, 2020. Version from 2020-10-10.