Universität Klagenfurt
Informatik – Systemsicherheit
R. Wigoutschnigg

UE Systemsicherheit
SS 2018
Übungstermine: siehe ZEUS

Abgabe 2

Abgabe: 03.06.2018

Implementieren Sie das Interface `ElGamal` des bereitgestellten Java-Projekts in dem dafür vorgesehenen Paket (bitte nennen Sie das Paket Nachnamen entsprechend der Nachnamen der Gruppenmitglieder um). Für die Implementierung ist eine Standard-JDK ausreichend. Die Verwendung von zusätzlichen Bibliotheken, welche wesentliche Teile der Aufgabe lösen, ist nicht erlaubt. Sie können Gruppen von bis zu 3 Personen bilden. Bei Unklarheiten ist es in Ihrer Verantwortung Ihren LV-Leiter zu kontaktieren.

Erzeugen Sie die Schlüsselkomponenten geeignet und dokumentieren Sie dies im Quellcode. Recherchieren Sie, wie bei der Erzeugung vorzugehen ist, um sichere Komponenten zu erhalten (Hinweis: rein zufällige Daten können Sicherheitsrisiken bergen). Achten Sie auf eine möglichst performante Implementierung (verwenden Sie passende Funktionalitäten des JDK wie Zb die `BigInteger`-Klasse).

Für die Funktionalität der Implementierung selbst (siehe JUnit-Test) sind bis zu 10 Punkte erreichbar. Für die Art der Implementierung (zB Erzeugung der Zufallskomponenten), die Lesbarkeit des Quellcodes sowie die Kommentierung wesentlicher Teile des Quellcodes sind weitere 5 Punkte erreichbar.

Abzugeben ist der gesamte, lauffähige Quellcode.