Universität Klagenfurt
Informatik – Systemsicherheit
P. Schartner · R. Wigoutschnigg

UE Systemsicherheit
SS 2015
Übungstermine:
`http://www.syssec.at/ss15`

Abgabe 1

Abgabe: 14.04.2015 12 Uhr

Implementieren Sie das Interface `RSA` des bereitgestellten Java-Projekts in dem dafür vorgesehenen Paket (bitte nennen Sie das Paket `Nachnamen` entsprechend der Nachnamen der Gruppenmitglieder um). Die Verwendung von zusätzlichen Bibliotheken ist nicht erlaubt. Sie können Gruppen von bis zu 3 Personen bilden. Bei Unklarheiten ist es in Ihrer Verantwortung Ihren LV-Leiter zu kontaktieren.

Zu implementierende Teilaufgaben

a) Primzahl der Länge n Bit erzeugen
b) Schlüsselparameter e geeignet erzeugen
c) Schlüsselparameter d berechnen
d) Verschlüsselung eines Byte-Arrays
e) Entschlüsselung eines Byte-Arrays

Abzugeben ist der gesamte, lauffähige Quellcode.

Hinweise

a) Recherchieren Sie geeignete öffentliche Exponenten.
b) Die Klasse `BigInteger` bietet alle nötigen mathematischen Operationen und Algorithmen an.
c) Verwenden Sie den beiliegenden (einfachen) JUnit-Test, um Ihren Code zu testen. Weitere Tests können natürlich selbstständig erzeugt werden.
d) Testen Sie ihren Algorithmus auch mit aktuell gängigen Schlüssellängen.
e) Ihr Algorithmus darf zumindest bei dem bereitgestellten JUnit-Test keine Exceptions produzieren (sonst massiver Punkteabzug) und muss die JUnit-Tests positiv abschließen (sonst ebenfalls Punkteabzug).
f) Pro Gruppe ist nur eine Abgabe nötig. Die Abgabe muss klar die Namen der Gruppenmitglieder enthalten.