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

UE Systemsicherheit
SS 2016
Übungstermine:
`http://www.syssec.at/ss16`

Abgabe 2

Abgabe: 17.04.2016

Recherchieren Sie die Funktionsweise des ElGamal-Signaturverfahrens. Implementieren Sie das Interface `ElGamalSig` des bereitgestellten Java-Projekts.

Zu implementierende Teilaufgaben

a) Geeignete Primzahl der Länge n Bit erzeugen
b) Generator bestimmen
c) geheimen Schlüsselparameter erzeugen
d) öffentlichen Schlüsselparameter erzeugen
e) Erzeugung eines Hashwertes
f) Signieren eines Byte-Arrays
g) Verifizieren einer Signatur

Abzugeben ist der gesamte, lauffähige Quellcode.

Hinweise

a) Recherchieren Sie, welche Eigenschaften Primzahlen für das ElGamal-System haben sollen und erzeugen Sie geeignete Primzahlen.
b) Recherchieren Sie, welche Eigenschaften der Generator besitzen soll und erzeugen Sie geeignete Generatoren. Recherchieren Sie auch, wie man die gesuchten Generatoren effizient bestimmen kann.
c) Die Klasse `BigInteger` bietet alle nötigen mathematischen Operationen und Algorithmen an.
d) Testen Sie ihren Algorithmus auch mit aktuell gängigen Schlüssellängen.