Kryptografische Protololle
Übung

El Gamal Signatur, Grundlage für DSS Digital signature standard

1. Die Teilnehmer haben gemeinsam p prim und g kleiner als p-2.
2. Anton wählt ein privates ta kleiner als p-2 und teilt allen Teilnehmern $t_{anton} :\underset{p}{\equiv} g^{ta}$ mit.
3. Anton will einen Klartext *klar* signieren. m sei die zugehörige Zahl.
   Zum Üben brauchen klar und m nicht zusammenzupassen. Wähen Sie m irgendwie beliebig lang..
4. Erzeugung der Signatur: Anton wählt ra aus $\mathbb{Z}^*_{p-1}$ und bestimmt dazu das Inverse ri in dieser Gruppe.
5. Er berechnet $kra :\underset{p}{\equiv} g^{ra}$
6. Er berechnet $sa :\underset{p-1}{\equiv} (m - ta \cdot kra) \cdot ri$
7. Anton versendet {klar, m, sa, kra}
8. Jeder Teilnehmer, z.B. Tobi, kann nun verifizieren.
   Tobi berechnet $test1 :\underset{p}{\equiv} g^{m}$
9. Tobi berechnet $test2 :\underset{p}{\equiv} t_{anton}{}^{kra} \cdot kra^{sa}$
10. Wenn beide Zahlen übereinstimmen, traut Tobi dem Klartext

---

a) Führen Sie mit eigenen Zahlen das Protokoll nachvollziehbar durch.
b) Beweisen Sie die Durchführbarkeit.
c) Es gibt ungeeignete Zahlen m. Nennen Sie solche.
d) Kann Mister X ta oder ra bestimmen?
e) Kann MisterX ri bestimmen, wenn er ra hat?
f) Kann MisterX m verändern, ohne dass Tobi es merkt