Tik-79.159 Tiedon salaus ja suojaus	kevät 98
Laskuharjoitus 6, viikko 11	Tuomas Aura, Antti Huima

1. Julkinen RSA-avaimesi on $(3, 4897)$ ja salainen $(3171, 4897)$. Avaa julkisella avaimellasi salattu sanoma 4109.

2. Julkinen RSA-allekirjoitusavaimesi on $(17, 1189)$.

   (a) Modulin 1189 salaiset tekijät ovat $29 \cdot 41$. Mikä on salainen allekirjoitusavaimesi?

   (b) Sanoman "Moi, mitä kuuluu?" sormenjälki sovitulla yksisuuntaisella hajautusfunktiolla laskettuna on 321. Esitä allekirjoitettu sanoma kokonaisuudessaan.

3. Miksei RSA:ssa pidä käyttää samaa modulia n useammassa avainparissa, vaikka yksityiset avaimet olisivat saman henkilön hallussa?

4. Toimiiko RSA-algoritmi, kun $p|m$ tai $q|m$?

5. Julkinen RSA-avaimesi on $(3, 4897)$ ja salainen $(3171, 4897)$. Luet luultavasti itse allekirjoittamasi sanoman $2345, 689$, missä 2345 on sanoma ja 689 allekirjoitus. Tarkista julkisen avaimen avulla, onko allekirjoitus aito.

6. Generoi (pseudo)satunnainen alkuluku p: valitse (pseudo)satunnainen kokonaisluku ja etsi propabilistisella Miller–Rabin-testillä (Schneier s.259) seuraava sitä suurempi alkuluku. Vakuutu luvun jaottomuudesta vähintään todennäköisyydellä 99 %. (Havainnollisuuden vuoksi laske sopivan pienillä luvuilla.)