1. Millä todennäköisyydellä kaksi k alkion satunnaisesti valittua osajoukkoa n alkion joukosta ovat samoja? Millä k:n arvolla todennäköisyys on pienin, kun n on vakio? Kuinka suuri tällöin pitää n:n olla, jotta todennäköisyys on pienempi kuin 2^{-64}.

   Millä todennäköisyydellä kaksi satunnaisesti valittua n bitin jonoa ovat samoja?

2. Halutaan ecash-setelin väärinkäytön onnistumistodennäköisyyden olevan enintään 2^{-64}. Monestako lukuparista x_i, y_i setelin pitää muodostua? Montako paria pitää seteliä luotaessa lähettää pankille allekirjoitettavaksi ja montako niistä paljastetaan *cut-and-choose* -menettelyssä.?

3. LaGrange-kynnysrakenne:

   (a) Laadi $(3, 5)$-kynnysrakenne, jossa salaisuus on 4321.

   (b) $(3, 5)$-kynnysrakenteesta $(\mathrm{mod}\ 2^{16}+1)$ tunnetaan varjot (2,19535),(4,1583),(5,44146). Laske salainen sanoma.

4. Kiinalaiseen jäännöslauseeseen perustuva kynnysrakenne:

   (a) $p = 983$. Tunnetaan varjot $(1013, 64)$, $(1019, 421)$ ja $(1021, 840)$. Laske salainen sanoma.

   (b) Lisää kynnysrakenteeseen uusi varjo.

5. Kiinalaiseen jäännöslauseeseen perustuvassa (m, n)-kynnysrakenteessa valitaan alkuluku p ($p >$ suurin mahdollinen salainen sanoma) ja modulit $d_1 < d_2 < \ldots < d_n$, joilla ei ole yhteisiä alkutekijöitä. Moduleille on lisäksi vaatimus

$$d_1 \cdot d_2 \cdots d_m > p \cdot d_{n-m+2} \cdot d_{n-m+3} \cdots d_n.$$

   Alkuperäinen sanoma s sekoitetaan $s' = s + rp$, missä r on satunnaisluku. Varjot saadaan laskemalla $k_i = s' \bmod d_i$.

   (a) Mitä tapahtuu, jos modulit valitaan väärin ja

$$d_1 \cdot d_2 \cdots d_m < d_{n-m+2} \cdot d_{n-m+3} \cdots d_n?$$

   (b) Entä, jos

$$d_1 \cdot d_2 \cdots d_m < p \cdot d_{n-m+2} \cdot d_{n-m+3} \cdots d_n?$$

   (c) Miltä väliltä sekoituskerroin r pitää valita?

6. Mikä vika on seuraavassa lantinheittoprotokollassa:

   (1) Alice valitsee satunnaisluvun R ja bitin b ja lähettää Bobille (h on yksisuuntainen hajautus funktio)

$$h(R, b).$$

   (2) Bob valitsee satunnaisluvun R' ja bitin b' ja lähettää Alicelle

$$h(R', b').$$

   (3) Alice lähettää Bobille (R, b).

   (4) Bob lähettää Alicelle (R', b').

   (5) Tulos on $b \oplus b'$.

   Mitä keinoja on vian korjaamiseksi?