1. Dokumenttien ja tapahtumien sitominen nykyhetkeen tai tiettyyn ajanhetkeen menneisyydessä tai tulevaisuudessa on ongelmallista. Miten voidaan varmistua seuraavista seikoista?

   (a) Allekirjoitus on tuore eli laadittu äskettäin.

   (b) Myöhemmin voidaan todeta, että dokumentti oli olemassa jo hetkellä T.

   (c) Myöhemmin voidaan todeta, että dokumenttia ei ollut olemassa vielä hetkellä T.

   (d) Allekirjoittaja ei voi itse päivätä allekirjoitusta menneisyyteen eikä tulevaisuuteen.

   (e) Salaisuus paljastuu vasta tulevaisuudessa hetkellä T, vaikka alkuperäistä kirjoittajaa ei enää olisi järjestelmässä.

   Kaikkiin kysymyksiin ei ole hyvää yleistä ratkaisua. Pohdi ratkaisuvaihtoehtojen luotettavuutta ja kustannuksia, esim. sanomien määrää eri osapuolten välillä ja luotetun osapuolen tai laitteen tarvetta.

2. 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?

3. 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.?

4. RSA-allekirjoitus (potenssiinkorotus suurella eksponentilla) maksaa noin 10000 kertaa ja allekirjoituksen tarkistus (potenssiinkorotus pienellä eksponentilla) noin 100 kertaan niin paljon kuin yksisuuntaisen hajautufunktion laskeminen lyhyestä sanomasta. Vertaa 10 perättäisen saman myyjän samalta asiakkaalta perimän PayWord-mikromaksun ja Ecash-maksun vaatimaa laskenta-aikaa.

5. Kuinka kaksi henkeä voi heittää noppaa sähköisten sanomien välityksellä niin, että toisen huomaamatta ei pysty huijaamaan? (Ulkopuolisia uhkia ei tarvitse huomioida.) Entä n henkeä?

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?