Anonyymi elektroninen raha

- Alice on maksaja, Bob maksun saaja.
  Pankin julkinen RSA-avain on $(3, n)$ ja salainen (d, n).

1. Alice arpoo sarjanumeron ja satunnaisluvun R. SN = setelin sarjanumero yhdistettynä allekirjoituksen vaatimaan redundanttiin dataan. Alice lähettää pankille
$$SN \cdot R^3 \bmod n.$$
2. Pankki allekirjoittaa sanoman salaisella avaimellaan ja lähettää Alicelle
$$(SN \cdot R^3)^d \bmod n \ = \ SN^d \cdot R \bmod n.$$
3. Alice jakaa R:n pois ja muodostaa setelin
$$(SN,\ SN^d \bmod n).$$

- Markkamäärä ei lue setelissä, vaan erikokoiset rahat allekirjoitetaan eri avaimella ($e = 3, 5, 7, \dots$).
- Pankki ei pysty yhdistämään seteliä Aliceen. Entä Bob?
- Setelin kaksinkertainen käyttö huomataan sarjanumerosta.
  Ongelma: Kuinka Alice saadaan kiinni?

Ecash

- David Chaum 1988
- Anonyymi raha, jossa kaksinkertainen käyttäjä paljastuu.
- Idea: jaetaan nimi "Alice" kahteen osaan, jotka yhdessä paljastavat nimen.
$$a, \quad a \oplus \text{"Alice"}.$$
  Bob valitsee satunnaisesti, kumman osan Alice kertoo.
- Pankki allekirjoittaa setelin sokeasti, mutta haluaa varmistua, että setelissä olevat osat yhdessä todella tuottavat nimen "Alice". Käytetään *cut and choose*-menetelmää.

- Setelin luonti

1. Alice generoi 200 satunnaislukua a_i ja laskee sormenjäljet

$$x_i = h(a_i), \quad y_i = h(a_i \oplus \text{"Alice"}).$$

2. Alice generoi 200 satunnaislukua R_i ja lähettää Trentille sanomat

$$h(x_i, y_i) \cdot R_i^3 \bmod n.$$

3. Trent pyytää Alicelta 100 paria satunnaislukuja R_i ja a_i ja tarkistaa, ettei Alice yritä huijata. (*cut and choose*)

4. Trent allekirjoittaa loput 100 sormenjälkeä ja lähettää Alicelle

$$\left(h(x_i, y_i) \cdot R_i^3\right)^d \bmod n \;=\; h(x_i, y_i)^d \cdot R_i \bmod n.$$

5. Alice jakaa pois R_i:t,

$$h(x_i, y_i)^d \bmod n.$$

- Seteli on muotoa

$$S = \prod_{j=1}^{100} h(x_j, y_j)^d.$$

- Huijauksen onnistumistodennäköisyys on $\frac{(50!)^2}{100!} \approx 2^{-96}$.

Tuomas Aura TKK / Digitaalitekniikka

- Maksaminen

1. Alice lähettää Bobille setelin S.

2. Bob generoi 64 satunnaista bittiä, liittää ne 36-bittiseen myyjätunnukseensa ja lähettää Alicelle.

3. Jos js bitti on 0, Alice lähettää Bobille

$$x_j,\ a_j \oplus \text{"Alice"}.$$

Jos bitti on 1, Alice lähettää Bobille

$$y_j,\ a_j.$$

4. Bob tarkistaa, että

$$S^3 = \prod_{j=1}^{100} h(x_j, y_j).$$

- Bob ei saa selville Alicen nimeä, sillä hän tietää parista $(a_j,\ a_j \oplus \text{"Alice"})$ vain toisen osan.

- Myöhemmin Bob lähettää pankkiin setelin S ja Alicelta saamansa luvut.

  Jos Alice käyttää setelin kahteen kertaan ja Bob valitsee eri 64 satunnaista bittiä, paljastuu Alice. Huijauksen onnistumistodennäköisyys on 2^{-64}.