Krüptograafia

Margus Niitsoo

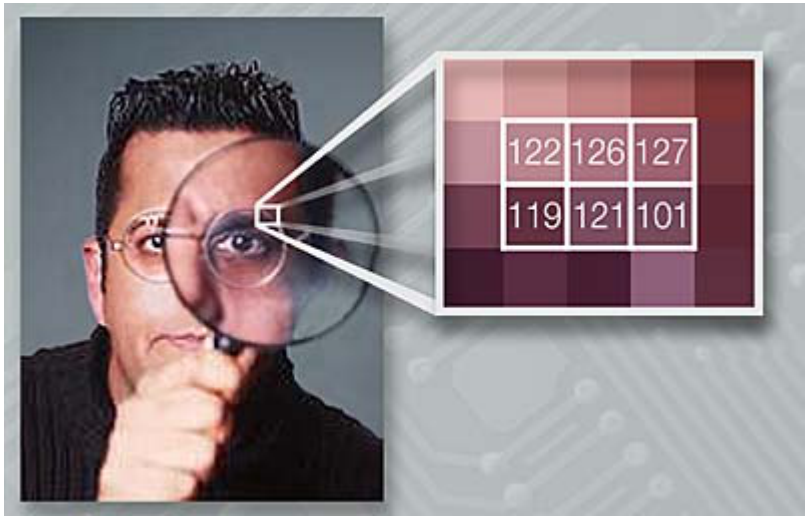
Tänane loeng

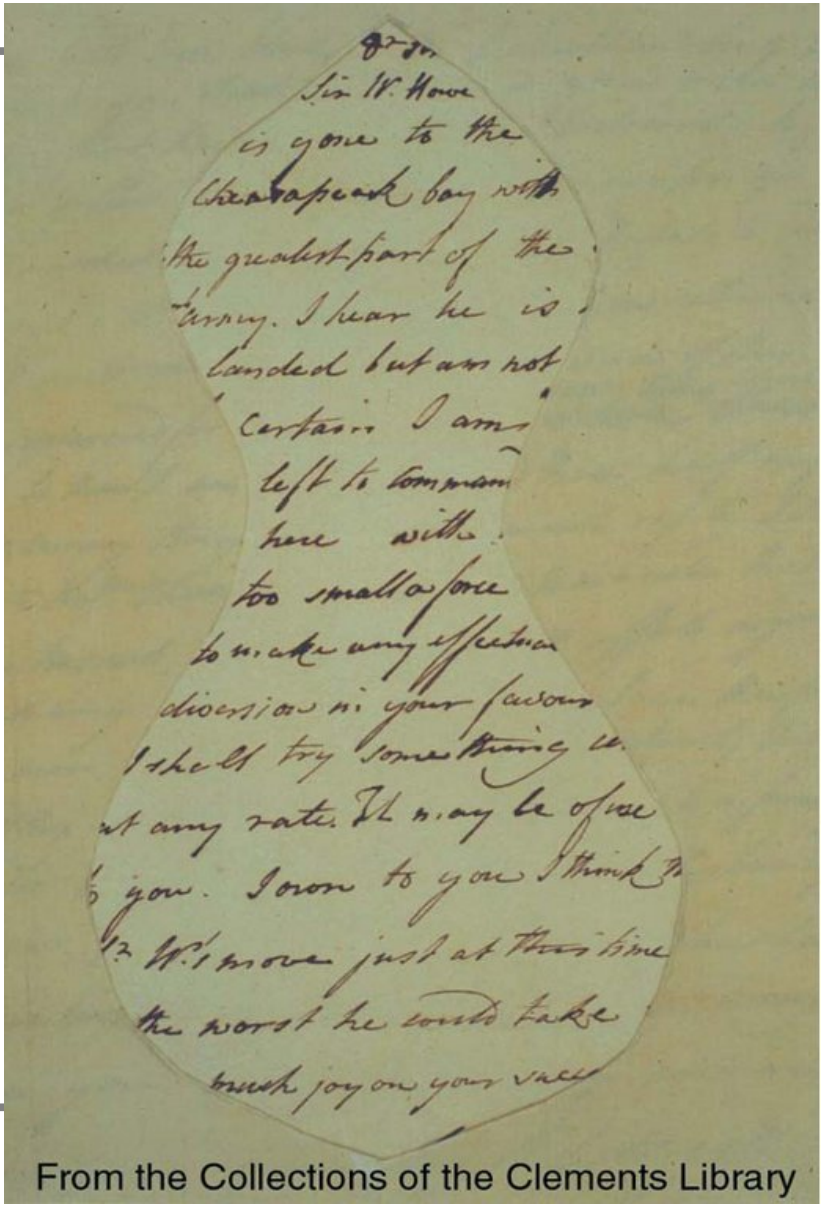
- Krüptoloogia
  - Olemus
  - Ajalugu
  - Tänapäev
  - Võimalused
  - Olukord Eestis
- Kokkuvõte

Krüptoloogia

- Teadus informatsiooni varjamisest
- Erineb:
  - Steganograafiast
  - Andmeturvest

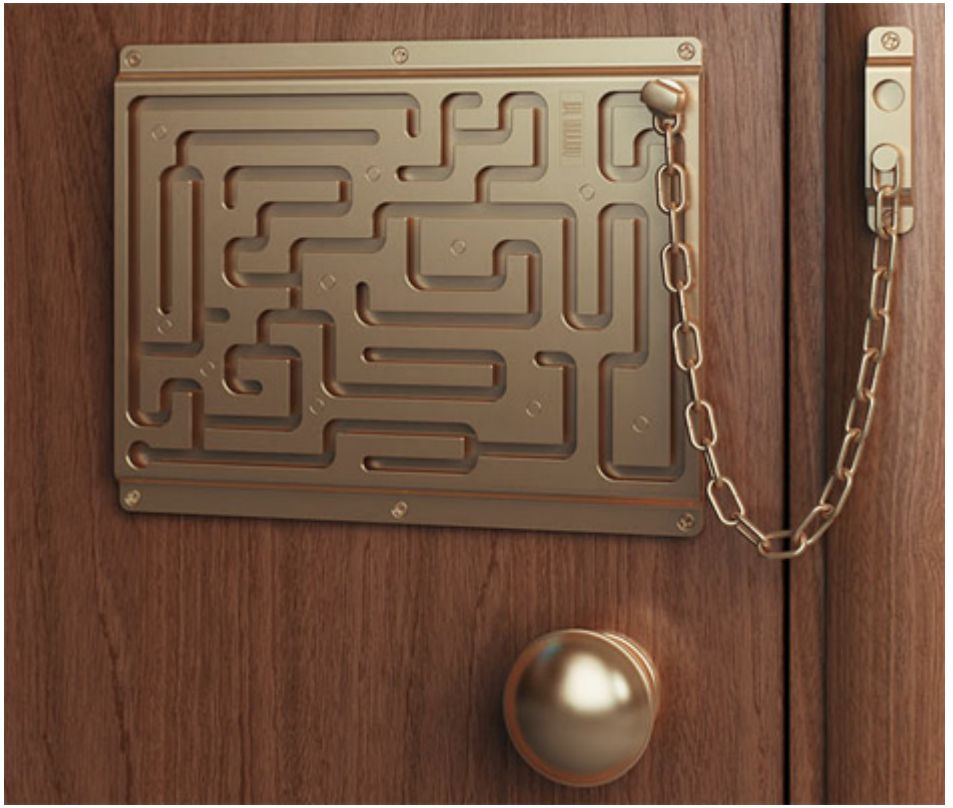
Steganograafia




From the Collections of the Clements Library

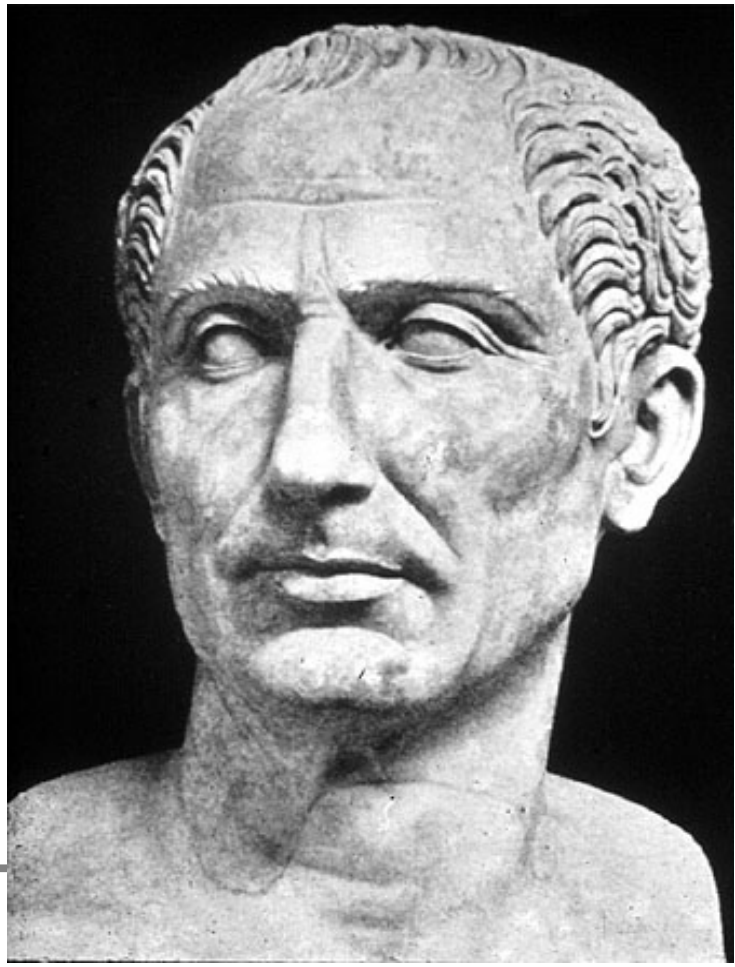
Andmeturve

Krüptoloogia



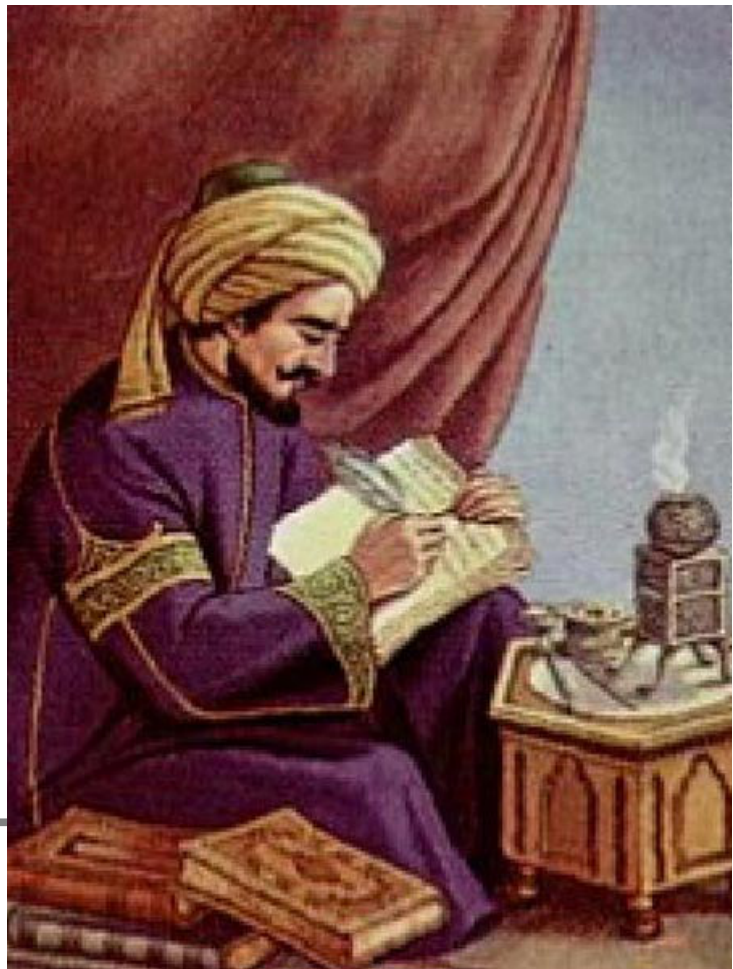
Ajalugu

- Caesari šiffer
  - Iga täht 3 kohta edasi
- Üldine asendušiffer
  - A → k, B → x, C → a, ...



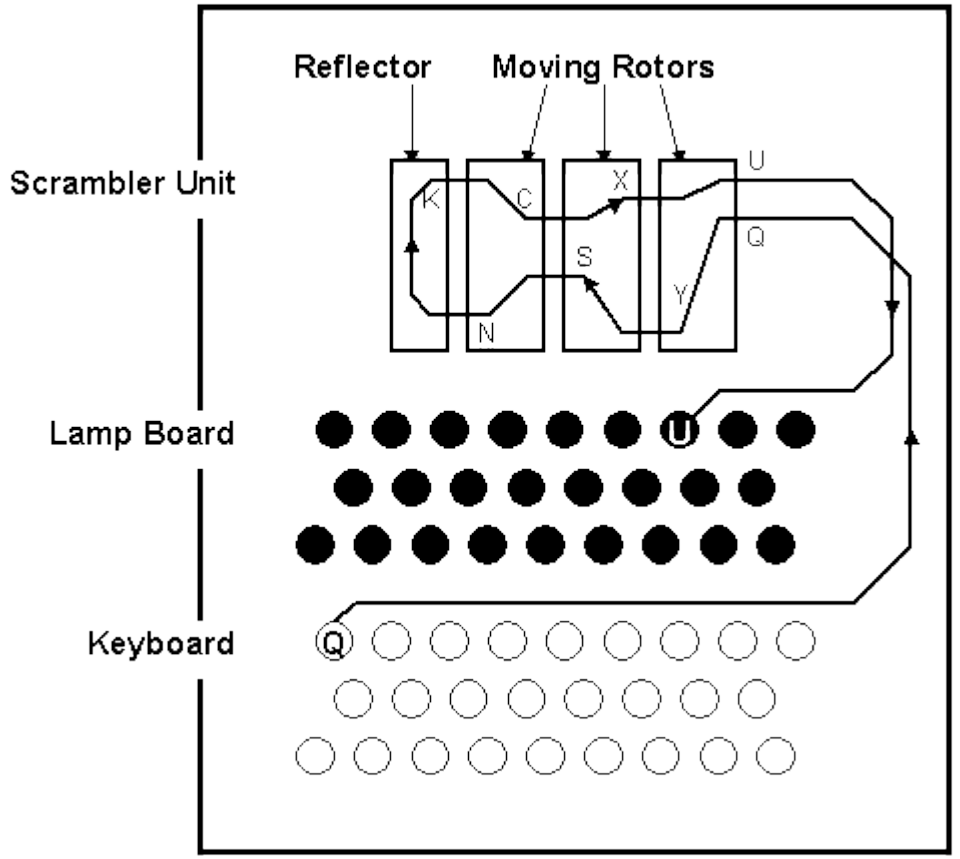
Turvaline tuhat aastat..

- Kuni Al Kindi Statistika leiutas
  - 750 AD Süüria
  - Tähtede sagedustabel
- Edasisised kavalused
  - Ühtlusta jaotust
  - Polüalfabeetiline



Tänapäeva krüptograafia

Enigma



26*26*26 = 17576 rootorite võimalust

Plugboard lisas ~200000000000000 võimalust

Enigma peamine probleem?

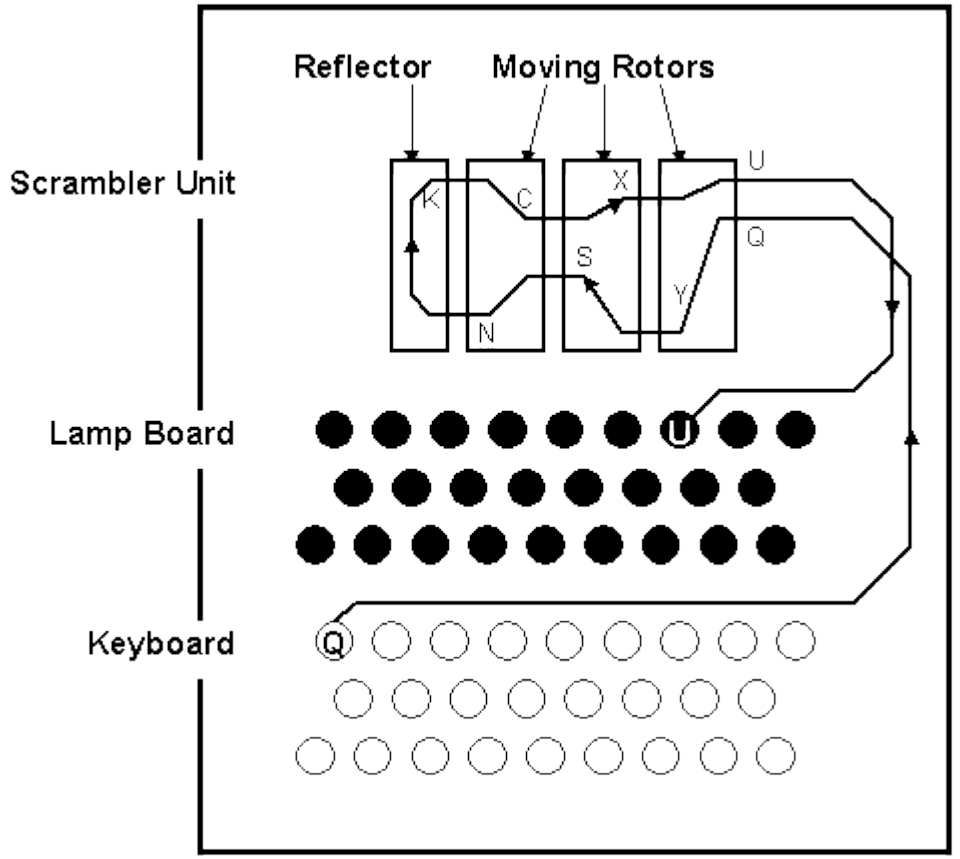
<Sõjasaladused>

“Das Passwort wird E-D-E-L-Weiss”

“Passwort?” “E-D-E-L-Weiss”

Objektiivne probleem

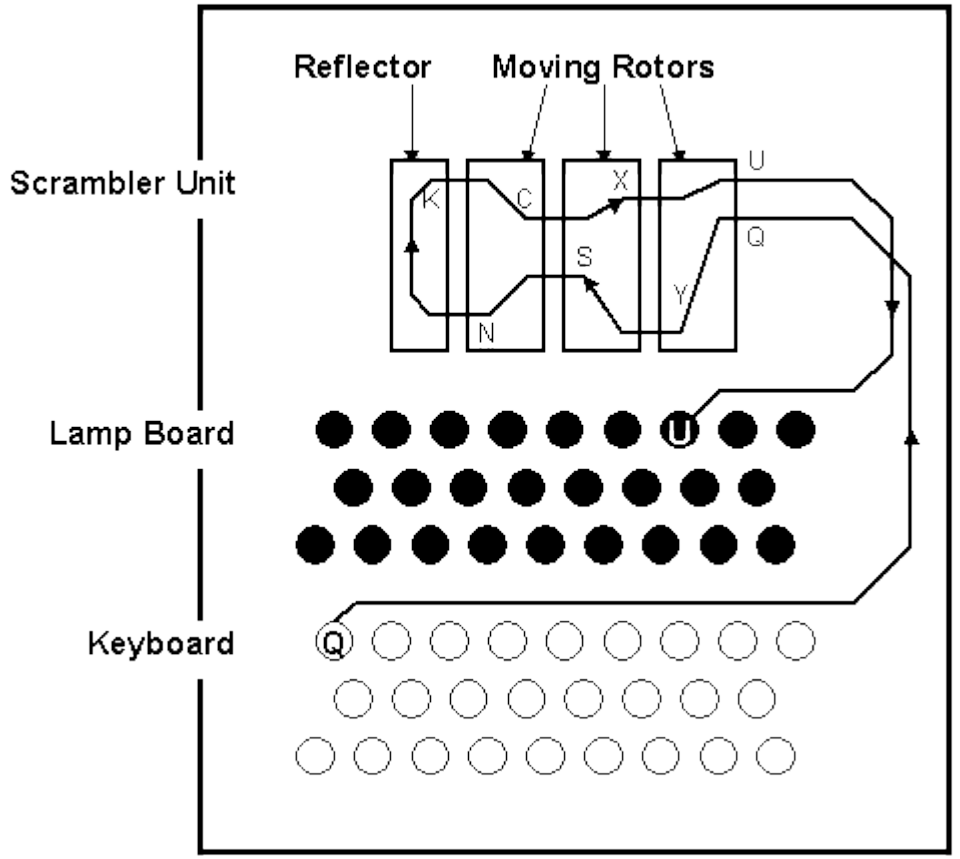
Enigma



26*26*26 = 17576 rootorite võimalust

Plugboard lisas ~200000000000000 võimalust

Enigma



26*26*26 = 17576 rootorite võimalust

Plugboard lisas ~200000000000000 võimalust

Enigma peamine probleem?

<Sõjasaladused>

“Das Passwort wird
E-D-E-L-Weiss”

“Passwort?”
“E-D-E-L-Weiss”

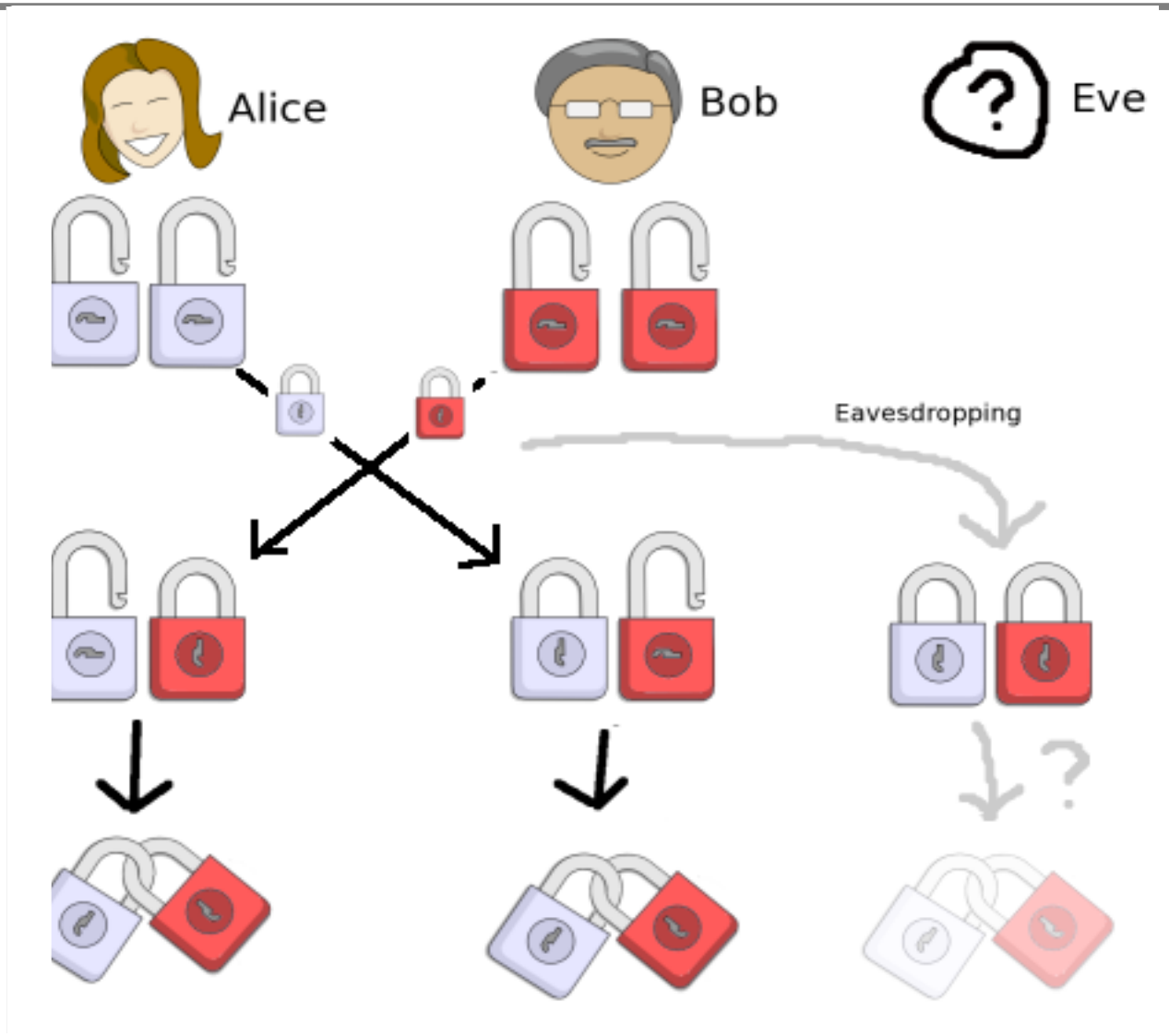
“Ah - Edelweiss!!”

Subjektiivne probleem:

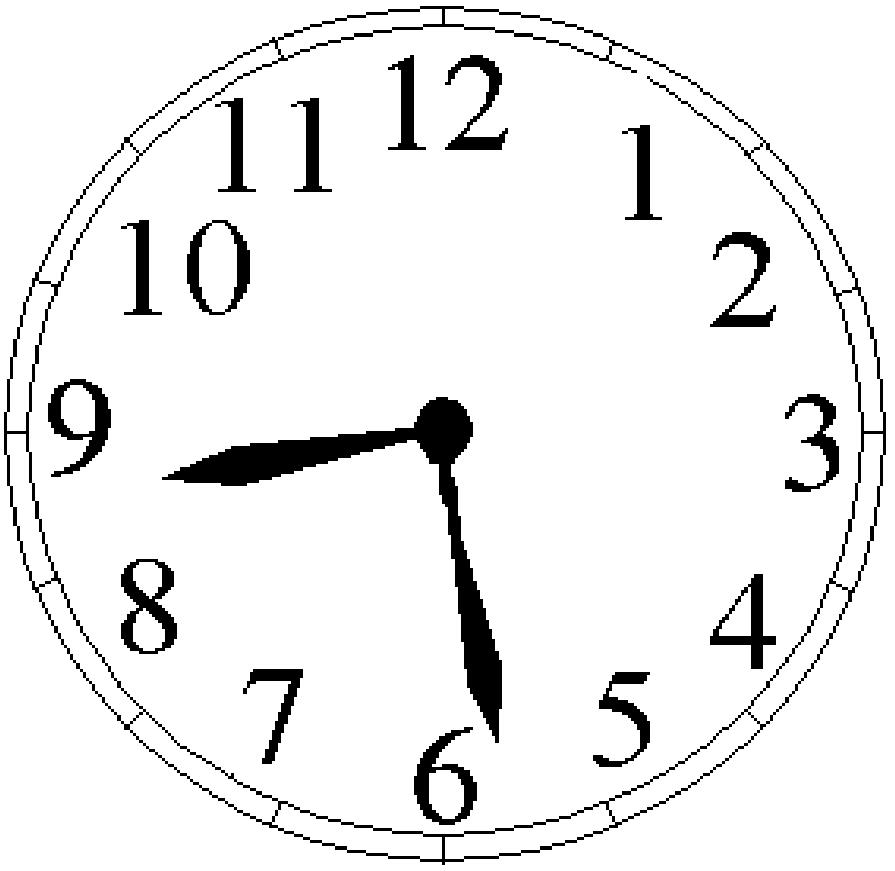
1976 leiti lahendus

1976 leiti lahendus

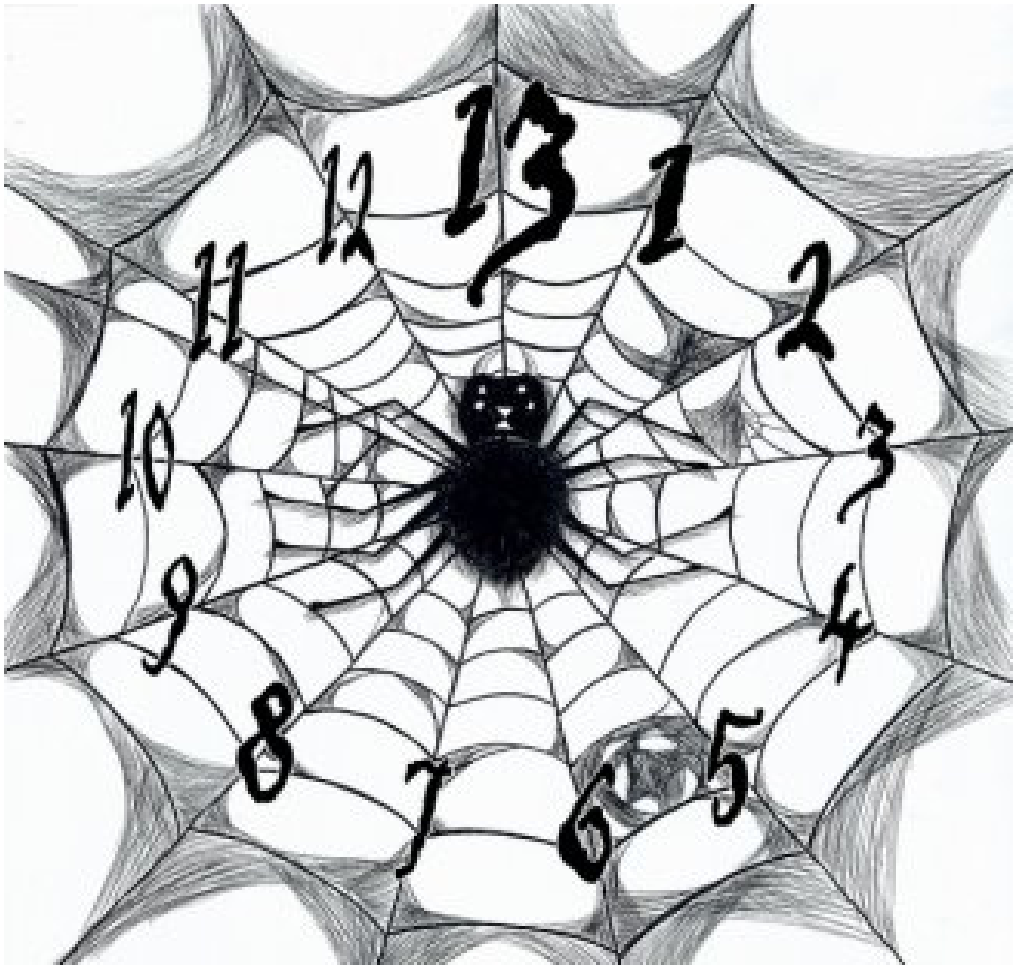
Diffie ja Helmanni lahendus



Kõrvalpõige matemaatikasse



Kõrvalpõige matemaatikasse



Kõrvalpõige matemaatikasse

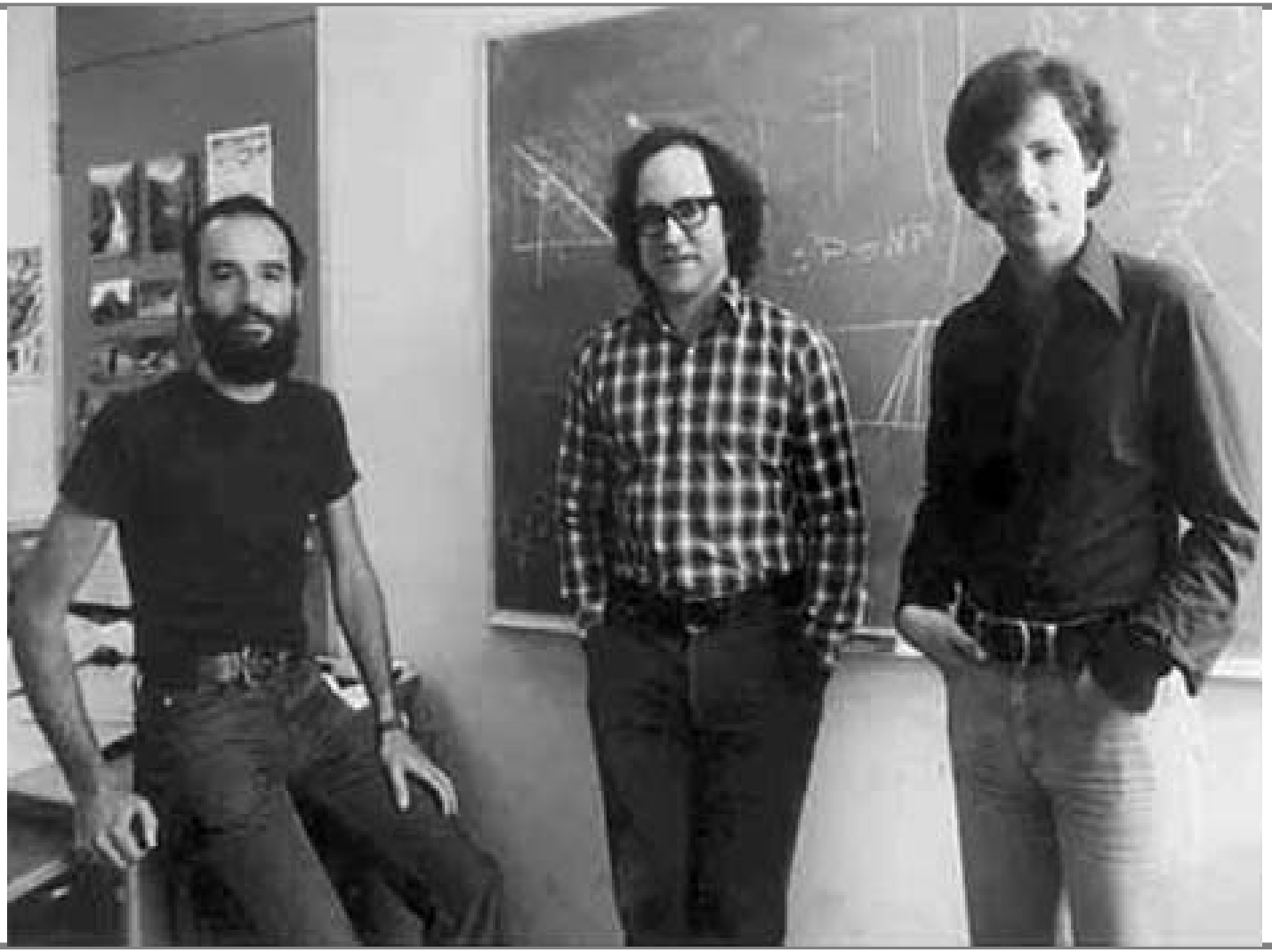
- Astendamine on lihtne
  - Lihtne leida et $2^4=3 \pmod{13}$
- Logaritmi võtmine on raske
  - Raske leida et $3=2^x \pmod{13}$ korral $x=4$

Diffie-Hellman

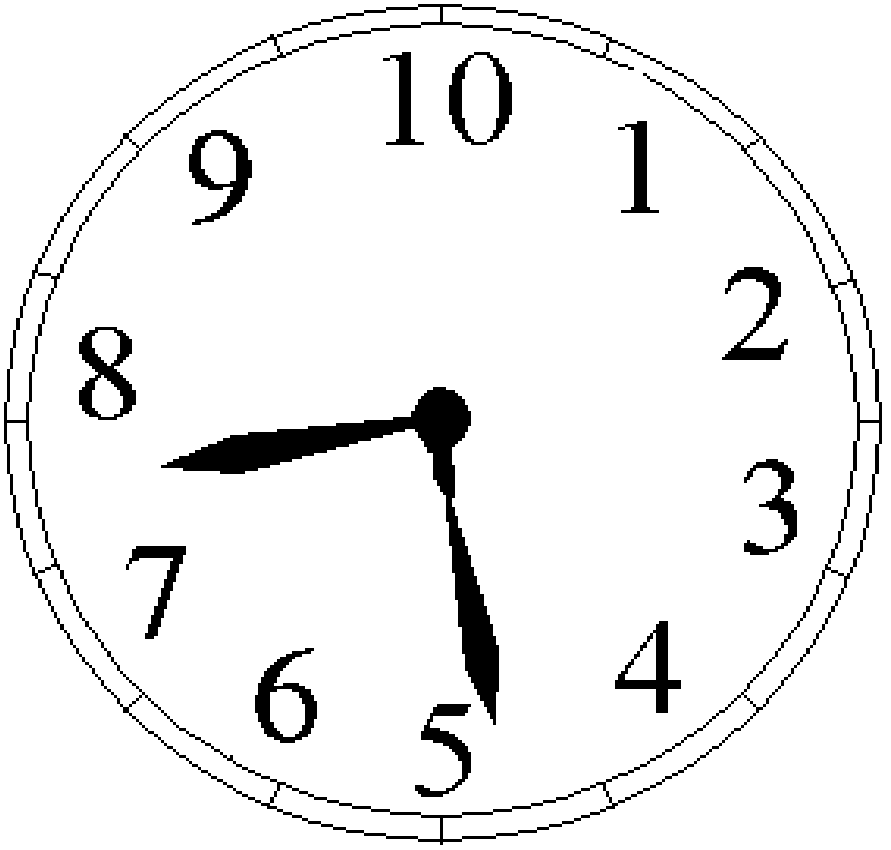
-  Alice
  - Valib a
  - Saadab $A=g^a$
  - Arvutab $K=B^a$
-  Bob
  - Valib b
  - Saadab $B=g^b$
  - Arvutab $K=A^a$

- Mõlemal pool $K=g^{ab}$

RSA (1977)



Kõrvalpõige matemaatikasse



Kõrvalpõige matemaatikasse

- n=pq, p ja q algarvud
- Astendamine on endiselt lihtne
  - Lihtne leida et $2^4=6 \pmod{10}$
- Juurimine on raske, kui ei tea 10=2*5
  - Raske leida et $x^4=6 \pmod{10}$ korral x=2

1997 selgus

- Briti salaluureagentuur (GCHQ)
  - James Ellis 1969
  - Clifford Cocks 1973
  - Malcolm Williamson 1974

Rakendused

- Digiallkiri
- Isikutuvastus

Aga see pole veel kõik

- 1982 Andrew Yao
  - Kaks miljonäri tahavad teada kumb neist on rikkam
  - Kumbki ei taha oma kontojääki avalikustada
  - Vahekohtunik pole ka variant

MPC

- MPC ehk turvaline ühisarvutus
  - Igal osapoolel on oma sisend x_i
  - Tulemusena saavad kõik teada $F(x_1,...,x_n)$ ja ei midagi muud
- Näide:

Krüptograafid restoranis

- 3 krüptograafi söövad lõunat
  - Avastavad, et arve on makstud
    - Kas üks nende hulgast või NSA?
    - Keegi ei taha välja öelda, kas ta maksis
  - Lahendus:
    - Viska salaja münti
    - Ütle paremale käele oma tulemus
    - Avalda XOR enda kolmest infobitist

Reaalse elu näited

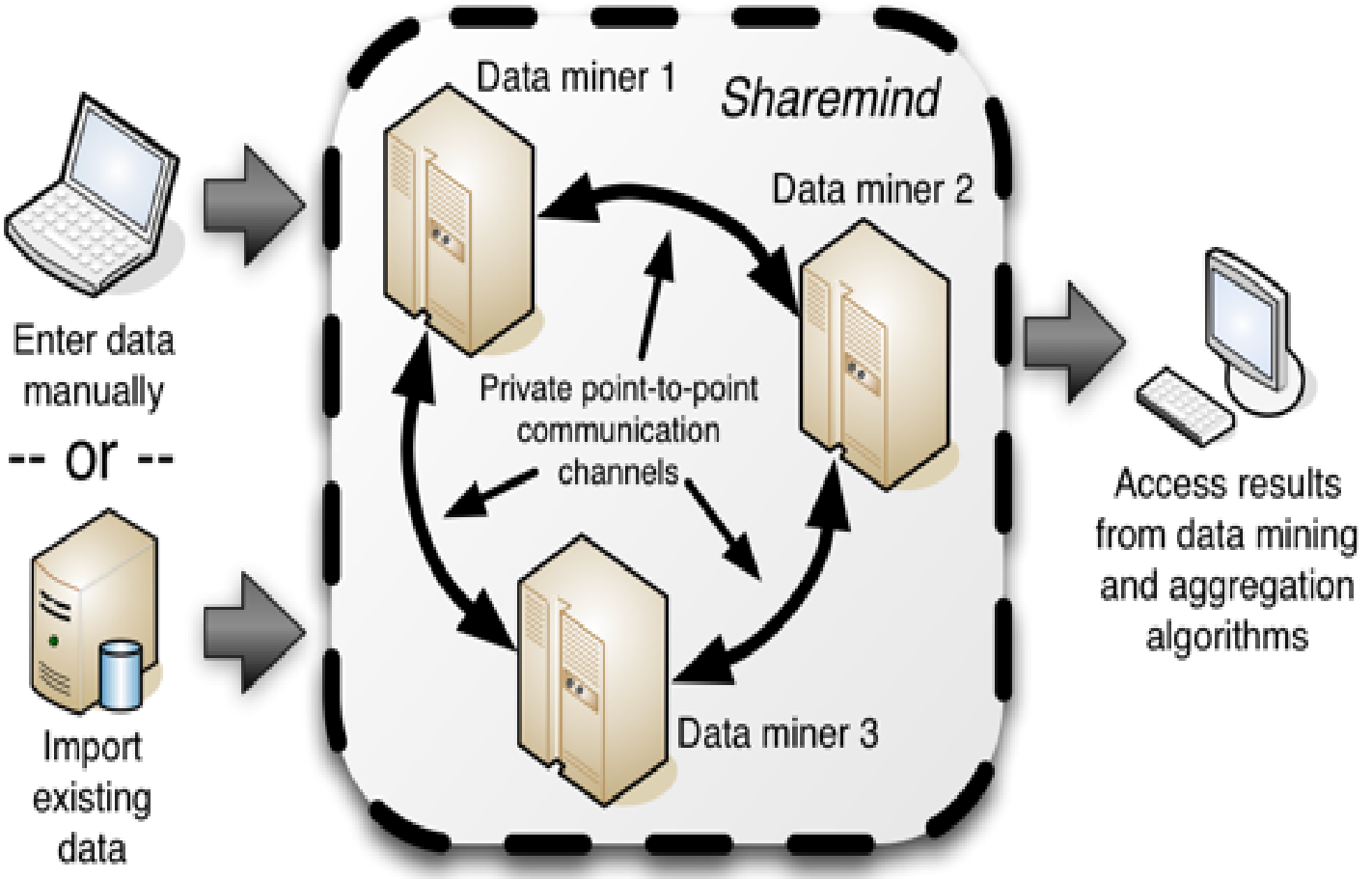
- Oksjon
  - Pakkujad ei taha, et teised nende pakutud summat teaks
  - Vaja tuvastada see, kes võidab

Reaalse elu näited

- Firmad tahavad ühist statistikat
- Andmeid otse jagada ei tohi
  - Andmekaitseseadus
  - Konkureerivad huvid
- Statistika tuleb arvutada MPC meetoditega

Lahendus

- ShareMind (Dan Bogdanov)



Krüpto Eestis

- http://Crypto.cs.ut.ee
- Teemad:
  - ShareMind (Dan, Jan, Sven)
  - 2 osapoole MPC (Helger Lippmaa)
  - Riskianalüüs ründepuudega (Jan, Mina)
  - Protokollide tõestamine (Peeter, Liina)
- Vajalik hea matemaatiline taust!

Kokkuvõtteks

- Krüpto pakub väga palju erinevaid võimalusi
  - Krüpteerimine
  - Digiallkiri
  - Isikutuvastus
  - Salajane ühisarvutus
- Samas:

Krüpto üksi pole lahendus!