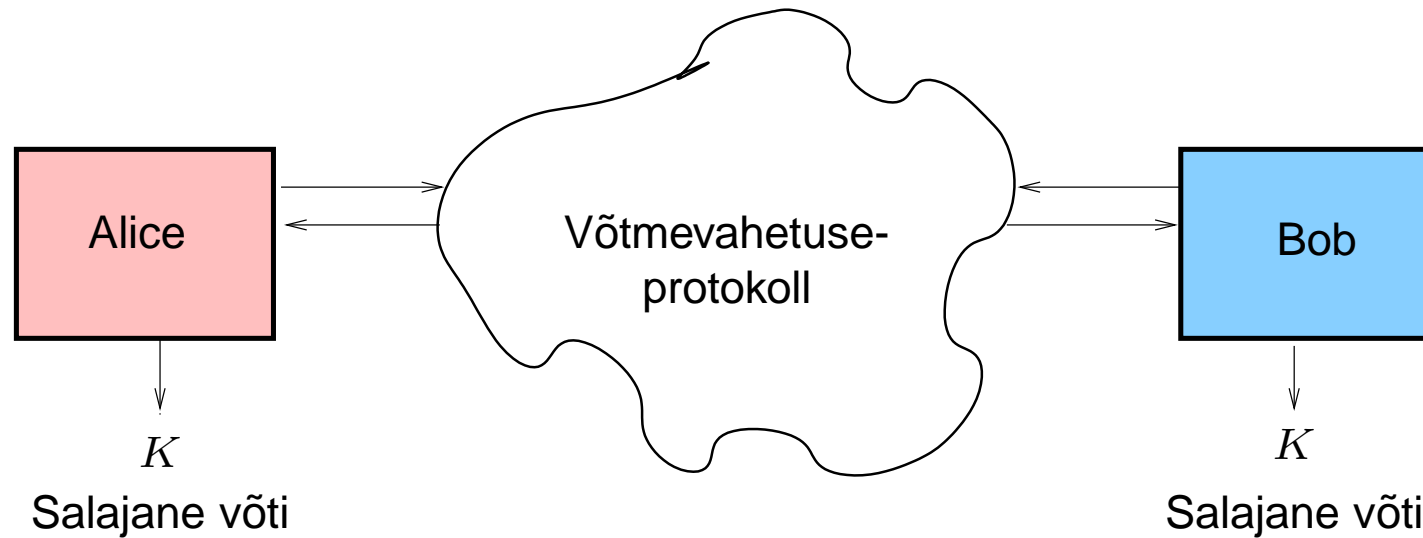


# Avaliku võtmega krüptograafia

Ahto Buldas

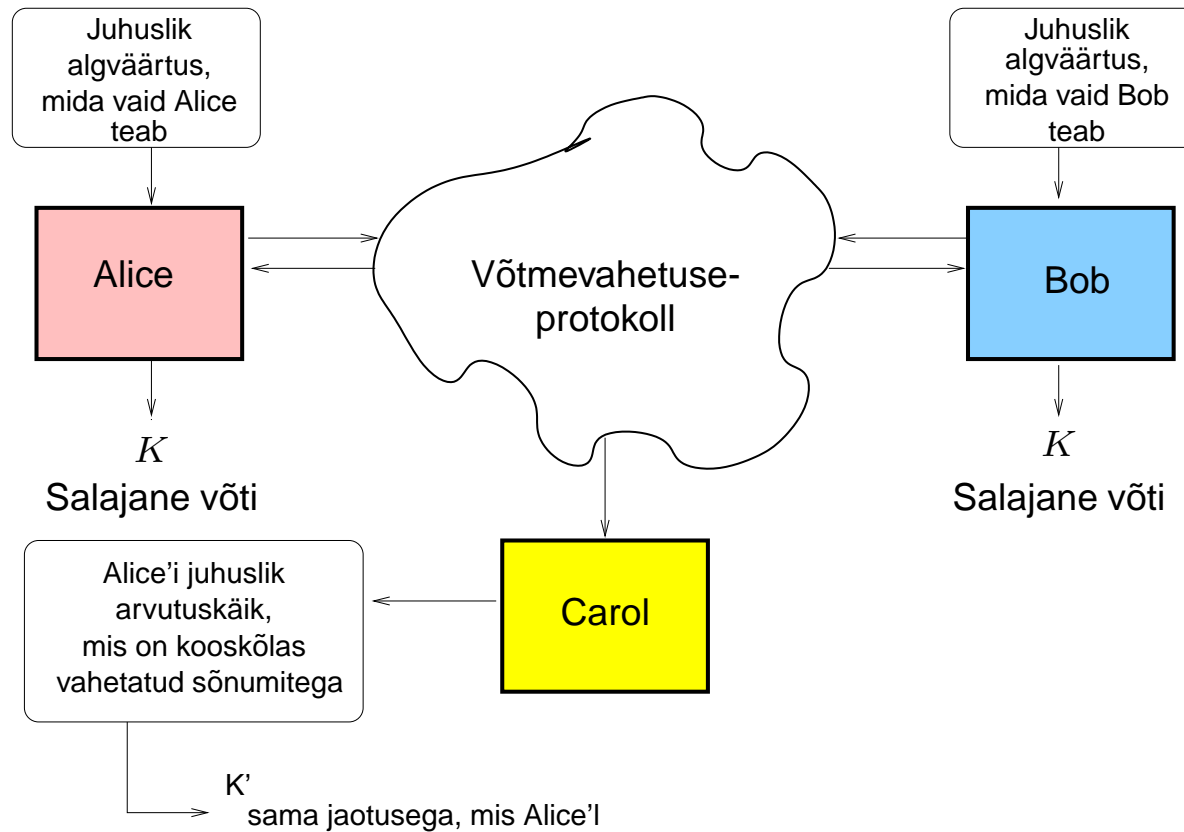
## Motiivid

- Salajase võtme vahetus on tülikas!
- Kas ei oleks võimalik salajases võtmes kokku leppida üle avaliku kanali?



## Probleem piiramatu vastasega!

- Kui vastane on piiramatu võimsusega, siis sellist protokollit ei leidu!



## Probleem piiramatu vastasega!

- Carol suudab leida kõik Alice'i salajase algväärtuse kandidaadid, mis on kooskõlas protokolliga käiguga!
- Seejärel valib Carol neist juhuslikult ühe välja ja arvutab oma võtme  $K'$
- Caroli väljundjaotus on täpselt samasugune, mis Alice'i väljundjaotus!
- Et protokoll on eeldatavasti korrektne, siis suure tõenäosusega on Alice'i ja Bob'i väljund sama.
- Kuid siis on ju umbes sama tõenäosusega Caroli väljund võrdne Bobi väljundiga!
- Järelikult on protokoll piiramatu jõuga Caroli vastu ebaturvaline.

## Võtmekehtestusprotokoll: definitsioon

*Võtmekehtestusprotokolliks* nimetatakse nelikut  $(A, K_A; B, K_B)$ , kus:

- $K_A$  ja  $K_B$  on funktsioonid tüüpi  $\Omega \times \{0, 1\}^* \rightarrow \{0, 1\}^m$  ja
- $A$  ja  $B$  on funktsioonid tüüpi  $\Omega \times \{0, 1\}^* \rightarrow \{0, 1\}^*$  ja  $\Omega = \{0, 1\}^k$ .

Eeldatakse, et üks kindel bitistring on defineeritud kui STOP sümbol, mis (juhul kui ta esineb funktsioonide  $A$  ja  $B$  väljundis) indikeerib protokollil lõppu.

## Protokoll transkript

Protokoll *transkriptiks* nimetatakse funktsiooni  $\Omega^2 \xrightarrow{\mathcal{T}} \{0, 1\}^*$ , mis arvutatakse iteratiivselt järgmise skeemi kohaselt:

$$\mathcal{T}_0(\omega_A, \omega_B) = A(\omega_A, \sqcup) \| B(\omega_B, \sqcup)$$

$$\mathcal{T}_1(\omega_A, \omega_B) = A(\omega_A, \mathcal{T}_0(\omega_A, \omega_B)) \| B(\omega_B, \mathcal{T}_0(\omega_A, \omega_B)) \| \mathcal{T}_0(\omega_A, \omega_B)$$

...

$$\mathcal{T}_n(\omega_A, \omega_B) = A(\omega_A, \mathcal{T}_{n-1}(\omega_A, \omega_B)) \| B(\omega_B, \mathcal{T}_{n-1}(\omega_A, \omega_B)) \| \mathcal{T}_{n-1}(\omega_A, \omega_B) .$$

Siin tähendab  $\|$  nn. "eraldajatega konkatenatsiooni", st  $w_1 \| w_2 = w'_1 \| w'_2$  parajasti siis kui  $w_1 = w'_1$  ja  $w_2 = w'_2$ .

$\mathcal{T}(\omega_A, \omega_B) := \mathcal{T}_n(\omega_A, \omega_B)$ , kus  $n$  on vähim indeks, mille korral  $\mathcal{T}_n$  sisaldab STOP sümbolit, või kui  $n$  oli eelnevalt kokku lepitud maksimaalne võimalik raundide arv.

## Võtmekehtestusprotokolli modelleerimine

- $A$  ja  $B$  genereerivad võtmed  $\omega_A \leftarrow \mathcal{U}_k$  ja  $\omega_B \leftarrow \mathcal{U}_k$ .
- $A$  ja  $B$  vahetavad sõnumeid (loovad transkripti)  $T = \mathcal{T}(\omega_A, \omega_B)$ .
- $A$  ja  $B$  leiavad võtmed  $k_A = K_A(\omega_A, T)$  ja  $k_B = K_B(\omega_B, T)$ .

Protokoll on *edukas* kui  $k_A = k_B$ .

Protokolli *korreksuseks* nim. tõenäosust

$$\gamma(k) = \Pr[\omega_A, \omega_B \leftarrow \mathcal{U}_k, T \leftarrow \mathcal{T}(\omega_A, \omega_B) : K_A(\omega_A, T) = K_B(\omega_B, T)] .$$

Vastase  $C$  *edukuseks* nimetatakse tõenäosust:

$$\delta(k) = \Pr[\omega_A, \omega_B \leftarrow \mathcal{U}_k, T \leftarrow \mathcal{T}(\omega_A, \omega_B), k \leftarrow C(T) : k = K_B(\omega_B, T)] .$$

## Transkripti omadus: Juhuarvude vahetatavus

**Lemma 1**  $\mathcal{T}(\omega_A, \omega_B) = \mathcal{T}(\omega'_A, \omega'_B)$  siis ja ainult siis kui  $\mathcal{T}_n(\omega_A, \omega_B) = \mathcal{T}_n(\omega'_A, \omega'_B)$  iga  $n$  korral, mis ei ületa raundide arvu.

Tõestus. Lemma väide tuleneb otseselt transkripti definitsioonist.  $\square$

## Juhuarvude vahetatavus II

**Lemma 2** Kui  $\mathcal{T}(\omega_A, \omega_B) = T = \mathcal{T}(\omega'_A, \omega'_B)$ , siis  $\mathcal{T}(\omega'_A, \omega_B) = T = \mathcal{T}(\omega_A, \omega'_B)$ .

Tõestus. Vastavalt Lemmale 1 ja esimesele eeldusele, saame  $A(\omega_A, \square) = A(\omega'_A, \square)$  ja  $B(\omega_B, \square) = B(\omega'_B, \square)$ , mistõttu

$$\begin{aligned} \mathcal{T}_0(\omega'_A, \omega_B) &= A(\omega'_A, \square) \parallel B(\omega_B, \square) = A(\omega_A, \square) \parallel B(\omega_B, \square) \\ &= T_0 = A(\omega_A, \square) \parallel B(\omega'_B, \square) \\ &= \mathcal{T}_0(\omega_A, \omega'_B) . \end{aligned} \tag{1}$$

Lemma eeldusest tulenevalt  $\mathcal{T}_n(\omega_A, \omega_B) = T_n = \mathcal{T}_n(\omega'_A, \omega'_B)$ , ja seega

$$\begin{aligned} A(\omega_A, \mathcal{T}_{n-1}(\omega_A, \omega_B)) &= A(\omega'_A, \mathcal{T}_{n-1}(\omega'_A, \omega'_B)) \\ B(\omega_B, \mathcal{T}_{n-1}(\omega_A, \omega_B)) &= B(\omega'_B, \mathcal{T}_{n-1}(\omega'_A, \omega'_B)) \\ \mathcal{T}_{n-1}(\omega_A, \omega_B) &= \mathcal{T}_{n-1}(\omega'_A, \omega'_B) . \end{aligned}$$

Olgu  $T_{n-1} = \mathcal{T}_{n-1}(\omega_A, \omega_B)$ .

Induktsiooni eeldusest  $\mathcal{T}_{n-1}(\omega'_A, \omega_B) = \mathcal{T}_{n-1}(\omega_A, \omega'_B) = T_{n-1}$ , saame

$$\begin{aligned}\mathcal{T}_n(\omega'_A, \omega_B) &= A(\omega'_A, \mathcal{T}_{n-1}(\omega'_A, \omega_B)) \parallel B(\omega_B, \mathcal{T}_{n-1}(\omega'_A, \omega_B)) \parallel \mathcal{T}_{n-1}(\omega'_A, \omega_B) \\ &= A(\omega'_A, \mathcal{T}_{n-1}(\omega'_A, \omega'_B)) \parallel B(\omega_B, \mathcal{T}_{n-1}(\omega_A, \omega_B)) \parallel T_{n-1} \\ &= A(\omega_A, \mathcal{T}_{n-1}(\omega_A, \omega_B)) \parallel B(\omega'_B, \mathcal{T}_{n-1}(\omega'_A, \omega'_B)) \parallel T_{n-1} \\ &= A(\omega_A, \mathcal{T}_{n-1}(\omega_A, \omega'_B)) \parallel B(\omega'_B, \mathcal{T}_{n-1}(\omega_A, \omega'_B)) \parallel T_{n-1} \\ &= \mathcal{T}_n(\omega_A, \omega'_B) .\end{aligned}$$

Võrdus  $\mathcal{T}_n(\omega'_A, \omega_B) = \mathcal{T}_n(\omega_A, \omega_B) = T_n$  tõestatakse analoogilisel viisil.

□

## Juhuarvude sõltumatuse säilivus

Võtmevahetusprotokollis (nagu eelnevalt kirjeldatud) genereeritakse kaks sõltumatut juhuarvu  $\omega_A$  ja  $\omega_B$ , ning seejärel transkript  $T$ , mis samuti on juhuslik suurus mingi tõenäosusjaotusega hulgal  $\{0, 1\}^*$ .

**Lemma 3** *Olgu  $T$  mingi fikseeritud transkript. Olgu  $W_T = \mathcal{T}^{-1}(T) = \{(\omega_a, \omega_b) : \mathcal{T}(\omega_a, \omega_b) = T\}$ ,  $W_{T,A} = \{\omega_a : \exists \omega_b \mathcal{T}(\omega_a, \omega_b) = T\}$ , ja  $W_{T,B} = \{\omega_b : \exists \omega_a \mathcal{T}(\omega_a, \omega_b) = T\}$ . Siis*

$$W_T = W_{T,A} \times W_{T,B} .$$

Tõestus. Sisalduvus  $W_T \subseteq W_{T,A} \times W_{T,B}$  on ilmne, mistõttu piisab du-aalse sisalduvuse näitamisest. Olgu  $(\omega_A, \omega_B) \in W_{T,A} \times W_{T,B}$ . Vastavalt definitsioonidele, leiduvad  $\omega'_A$  ja  $\omega'_B$  nii et  $\mathcal{T}(\omega'_A, \omega_B) = \mathcal{T}(\omega_A, \omega'_B) = T$ . Vastavalt Lemmale 2,  $\mathcal{T}(\omega_A, \omega_B) = T$  ja seega  $(\omega_A, \omega_B) \in W_T$ .  $\square$

## Juhuarvude sõltumatuse säilivus II

**Lemma 4** *Olgu  $\omega_A, \omega_B \leftarrow \mathcal{U}_k$ ,  $T \leftarrow \mathcal{T}(\omega_A, \omega_B)$  ja  $(\omega'_A, \omega'_B) \leftarrow \mathcal{T}^{-1}(T)$ , st paar  $(\omega'_A, \omega'_B)$  on ühtlaselt valitud kõigi arvupaaride hulgast, mis on kooskõlas transkriptiga  $T$  (mis ise on genereeritud tavalisel viisil). Olgu  $\omega''_A \leftarrow W_{T,A}$  ja  $\omega''_B \leftarrow W_{T,B}$  (ühtlase jaotusega). Siis  $\langle \omega_A, \omega_B, T \rangle$ ,  $\langle \omega'_A, \omega'_B, T \rangle$  ja  $\langle \omega''_A, \omega''_B, T \rangle$  on identsed jaotused.*

Tõestus. Vastavalt Lemmale 3 on  $\mathcal{T}(\omega''_A, \omega''_B) = T$  ja  $(\omega''_A, \omega''_B)$  ühtlaselt valitud hulgast  $\mathcal{T}^{-1}(T)$ . Kuna valik toimus sõltumatult  $(\omega'_A, \omega'_B)$  valikust, siis on jaotused  $\langle \omega''_A, \omega''_B \rangle$  ja  $\langle \omega'_A, \omega'_B \rangle$  identsed.

Kõigis kolmes jaotuses on  $T$ -komponent üheselt määratud kahe esimese komponendiga, siis piisab kui tõestame  $\langle \omega_A, \omega_B \rangle$  ja  $\langle \omega'_A, \omega'_B \rangle$  identsuse.

Selleks valime mingid  $\omega_A^0, \omega_B^0 \in \{0, 1\}^k$  ja kasutame valemit:

$$\Pr[\omega'_A = \omega_A^0, \omega'_B = \omega_B^0] = \sum_T \Pr[\mathcal{T}(\omega_A, \omega_B) = T] \Pr[\omega'_A = \omega_A^0, \omega'_B = \omega_B^0 | T], \quad (2)$$

kus viimane tinglik tõenäosus avaldub järgmiselt:

$$\Pr[\omega'_A = \omega_A^0, \omega'_B = \omega_B^0 | T] = \begin{cases} \frac{1}{|\mathcal{T}^{-1}(T)|}, & \text{kui } \mathcal{T}(\omega_A^0, \omega_B^0) = T; \\ 0, & \text{kui } \mathcal{T}(\omega_A^0, \omega_B^0) \neq T \end{cases}. \quad (3)$$

Arvestades, et  $(\omega_A, \omega_B)$  jaotus hulgal  $\{0, 1\}^{2k}$  on ühtlane, saame valemis (2) esimese tõenäosuse väärtuseks  $\Pr[\mathcal{T}(\omega_A, \omega_B) = T] = |\mathcal{T}^{-1}(T)| \cdot 2^{-2k}$ . Arvutades summa, saame  $\Pr[\omega'_A = \omega_A^0, \omega'_B = \omega_B^0] = 2^{-2k}$ , mis langeb kokku tõenäosuse  $\Pr[\omega_A = \omega_A^0, \omega_B = \omega_B^0]$  väärtusega. Seega on jaotused  $\langle \omega_A, \omega_B \rangle$  ja  $\langle \omega'_A, \omega'_B \rangle$  tõepoolest identsed.  $\square$

## Alice'i ja Caroli jaotuste identsus

**Lemma 5** Olgu  $\omega_A, \omega_B \leftarrow \mathcal{U}_k$ ,  $T \leftarrow \mathcal{T}(\omega_A, \omega_B)$  ja  $(\omega'_A, \omega'_B) \leftarrow \mathcal{T}^{-1}(T)$ . Siis jaotused  $\langle \omega_A, \omega_B, T \rangle$  ja  $\langle \omega'_A, \omega_B, T \rangle$  on identsed.

Tõestus. Asendame esimese jaotuse vastavalt Lemmale 4 jaotusega, kus  $\omega_A \leftarrow W_{T,A}$  ja  $\omega_B \leftarrow W_{T,B}$  on ühtlaselt (ja sõltumatult) valitud). Vastavalt Lemmale 4 võib ka teise jaotuse asendada kahe sõltumatu (ja ühtlase) valikuga  $\omega'_A \leftarrow W_{T,A}$  ja  $\omega'_B \leftarrow W_{T,B}$ , kus  $T$  on sama, mis esimese jaotuse juures, st  $T \leftarrow \mathcal{T}(\mathcal{U}_k, \mathcal{U}_k)$ .

Eeldusel, et  $T$  on fikseeritud, on ka suurused  $\omega'_A$  ja  $\omega_B$  sõltumatud ja

seega (kasutades tähistust  $p(T) = \Pr[\mathcal{T}(\mathcal{U}_k, \mathcal{U}_k) = T]$ ):

$$\begin{aligned}\Pr[\omega'_A = \omega_A^0, \omega_B = \omega_B^0] &= \sum_T p(T) \cdot \Pr[\omega'_A = \omega_A^0 \mid T] \cdot \Pr[\omega_B = \omega_B^0 \mid T] \\ &= \sum_T p(T) \cdot \Pr[\omega_A = \omega_A^0 \mid T] \cdot \Pr[\omega_B = \omega_B^0 \mid T] \\ &= \Pr[\omega_A = \omega_A^0, \omega_B = \omega_B^0] .\end{aligned}$$

□

## Ebaturvalisus piiramatu vastase vastu

**Teoreem 1** *Igale võtmekehtestusprotokollile  $(A, K_A; B, K_B)$  korrektsusega  $\gamma(k)$  leidub (piiramatu) vastane  $C$  edukusega  $\delta(k) \geq \gamma(k)$ .*

Tõestus. Võtmevahetusprotokolli tavalises mudelis genereeritakse esmalt juhuarvud  $(\omega_A, \omega_B)$ , misjärel genereeritakse transkript  $T = \mathcal{T}(\omega_A, \omega_B)$  ja osapooled  $A$  ja  $B$  arvutavad  $k_A$  ja  $k_B$ . Vastavalt Lemmale 4 saab aga sama jaotuse kui esmalt genereerida transkript  $T = \mathcal{T}(\mathcal{U}_k, \mathcal{U}_k)$  ja seejärel sõltumatult juhuarvud  $\omega_A \leftarrow W_{T,A}$  ja  $\omega_B \leftarrow W_{T,B}$ .

Vastane  $C$  töötab sisendi  $T$  korral järgmiselt: (1) genereerib  $\omega'_A \leftarrow W_{T,A}$  (piiramatule vastasele igati jõukohane!) ja (2) arvutab  $k'_A = K_A(\omega'_A, T)$ .

Vastavalt Lemmale 5 on  $\langle \omega_A, \omega_B, T \rangle$  sama jaotusega, mis  $\langle \omega'_A, \omega_B, T \rangle$ . Seega on sündmused  $k_A = k_B$  ja  $k'_A = k_B$  võrdtõenäosed ( $\gamma(k)$ ). Järelikult arvab  $C$  võtme  $k_B$  tõenäosusega vähemalt  $\gamma(k)$ .  $\square$

## Lisamärkus protokoli käsitluse kohta

Vaadates tagasi Teoreemi 1 tõestusele, märkame et selle suhteliselt intuitiivse väite tõestus osutus võrdlemisi keeruliseks – oli vaja tõestada koguni viis tehnilist lemmat. Paratamatult tekib siin küsimus: kas kuidagi lihtsamalt ei saa? Üks keerukuse põhjusi on kahtlemata transkripti  $\mathcal{T}$  iteratiivne definitsioon. Esimene mõte lihtsustusest võikski seostuda küsimusega, kas toodud aruteludes on tingimata vaja tunda funktsiooni  $\mathcal{T}$  "siseehitust", või ehk kehtib toodud arutelu ka siis kui  $\mathcal{T}$  on suvaline funktsioon?

Näitamaks et see nii ei ole, piisab kui defineerida  $\mathcal{T}(\omega_A, \omega_B) = \omega_A \oplus \omega_B$ , st transkript saadakse juhuarvude bitikaupa liitmise teel mooduliga kaks, ja võtmete arvutamise funktsioonid defineerida järgmiselt:

$$k_A = K_A(\omega_A, T) = \omega_A \parallel \omega_A \oplus T, \text{ ja } k_B = K_B(\omega_B, T) = \omega_B \oplus T \parallel \omega_B .$$

Ühelt poolt,  $k_A = k_B$  tõenäosusega 1. Teiselt poolt aga on vastasele teada ainult summa  $\omega_A \oplus \omega_B$ , milles ei sisaldu infot  $\omega_B$  kohta. Seega ei saa vastase edukus olla suurem kui  $2^{-k}$ , mis tuleneb tähelepanekust, et võimalikke  $\omega_B$  väärtusi on  $2^k$ .

Toodud näitest järeldub (lisaks sellele, et transkripti "siseehitus" on oluline), et ei leidu protokoll, mille transkript sisaldaks täieliku informatsiooni  $\omega_A \oplus \omega_B$  kohta, kuid mitte mingit informatsiooni juhuarvude  $\omega_A$  ja  $\omega_B$  kohta. Sellise protokoll olemasolust järelduks ka piiramatult vastase suhtes turvalise \* võtmekehtestusprotokoll olemasolu, mille me aga ülaltoodud aruteluga välistasime.

\*Käesoleva kirjutise kontekstis.

## Loogilise konjunktsiooni arvutamine

Oletame, et  $A$  valib ühe biti  $a \in \{0, 1\}$  ja  $B$  ühe biti  $b \in \{0, 1\}$ . Valikud toimugu mingite sõltumatute tõenäosusjaotuste  $\mathcal{D}_A$  ja  $\mathcal{D}_B$  järgi. Nad soovivad arvutada loogilist konjunktsiooni (korrutist)  $a \cdot b$ , kusjuures sellisel viisil, et partner ei saaks teada muud informatsiooni kui see, mis järeldub korrutisest  $a \cdot b$  ja omaenda bitist. Näiteks kui  $a = 1$ , siis  $a \cdot b$  järgi saab  $A$  muidugi tuletada partneri biti  $b$ , kuid kui  $a = 0$ , siis  $a \cdot b$  ei anna  $A$ -le mingit teavet  $b$  kohta. Oluline on koostada protokoll nii, et kui  $a = 0$  siis ka transkripti  $T$  teadmine ei anna midagi  $b$  tuletamiseks.

Arvutustes võib kumbki pool kasutada juhuarve, mis ei ole partnerile teada. Eeldame, et  $\omega'_A \leftarrow \{0, 1\}^{k-1}$  on  $A$  juhuarv ja  $\omega'_B \leftarrow \{0, 1\}^{k-1}$  on  $B$  juhuarv. Kooskõla saavutamiseks eelnevalt kasutatud tähistustega olgu

$\omega_A = a \parallel \omega'_A$  ja  $\omega_B = b \parallel \omega'_B$ . Märgime, et  $\omega_A$  ja  $\omega_B$  ei tarvitse olla ühtlase jaotusega.

Eeldame, et protokoll on korrektne, st

$$K_A(a \parallel \omega'_A; \mathcal{T}(a \parallel \omega'_A; b \parallel \omega'_B)) = a \cdot b = K_B(b \parallel \omega'_B; \mathcal{T}(a \parallel \omega'_A; b \parallel \omega'_B)) . \quad (4)$$

Ütleme, et juhuarvupaar  $(\omega'_A, \omega'_B)$  on *hea B* suhtes, kui ta ei võimalda *A*-l (tingimusel  $a = 0$ ) välja arvutada *B* bitti  $b$ , st leiduvad  $\omega'_{0,B}$  ja  $\omega'_{1,B}$ , nii et

$$\begin{aligned} \mathcal{T}(0 \parallel \omega'_A; 1 \parallel \omega'_{1,B}) &= \mathcal{T}(0 \parallel \omega'_A; 0 \parallel \omega'_B) \\ \mathcal{T}(0 \parallel \omega'_A; 0 \parallel \omega'_{0,B}) &= \mathcal{T}(0 \parallel \omega'_A; 1 \parallel \omega'_B) . \end{aligned}$$

Analoogiliselt, paari  $(\omega'_A, \omega'_B)$  nimetatakse *heaks A* suhtes, kui leiduvad  $\omega'_{0,A}$  ja  $\omega'_{1,A}$ , nii et:

$$\begin{aligned} \mathcal{T}(1 \parallel \omega'_{1,A}; 0 \parallel \omega'_B) &= \mathcal{T}(0 \parallel \omega'_A; 0 \parallel \omega'_B) \\ \mathcal{T}(0 \parallel \omega'_{0,A}; 0 \parallel \omega'_B) &= \mathcal{T}(1 \parallel \omega'_A; 0 \parallel \omega'_B) . \end{aligned}$$

Vahetatavuse omadusest saame, et  $\mathcal{T}(0\|\omega'_A; 1\|\omega'_{1,B}) = \mathcal{T}(1\|\omega'_{1,A}; 1\|\omega'_{1,B})$ , millest korrektsuse tingimuse tõttu:

$$1 \cdot 1 = K_B(\mathcal{T}(1\|\omega'_{1,A}; 1\|\omega'_{1,B}); 1\|\omega'_{1,B}) = K_B(\mathcal{T}(0\|\omega'_A; 1\|\omega'_{1,B}); 1\|\omega'_{1,B}) = 0 \cdot 1 .$$

Saime vastuolu, mistõttu võime järeldada, et ükski juhuarvude paar ei saa olla korraga hea mõlema osapoole suhtes. Seega oleme tõestanud järgmise teoreemi:

**Teoreem 2** *Ei leidu loogilist konjunktsiooni arvutavat protokollit, mis oleks turvaline piiramatu (passiivse) vastase suhtes.*

## Piiratud arvutusjõuga vastased.

- *Turingi masin* – arvuti matemaatiline mudel, millel on sisendolek (lint), programm (käskude jada), ja väljundolek (lint)
- *Turingi masina peatumine* – arvutuskäik defineeritakse kui teatud olekute jada, milles naaberolekud on omavahel kindlal viisil seotud ja mis lõpeb teatud liiki olekuga (stop!)
- *Arvutusaeg* – peatumisele eelnenud olekute arv. Arvutusaega (kindla programmi korral) esitatakse kui funktsiooni  $T(n)$  sisendoleku mahust  $n$  (bitti)

## O-tähistused

**Def.** Kirjutame  $f(n) = O(g(n))$ , kui leiduvad  $c \in \mathbb{R}$  ja  $n_0 \in \mathbb{N}$ , nii et iga  $n \leq n_0$  korral:

$$f(n) \leq c \cdot g(n) .$$

**Def.** Kirjutame  $f(n) = \Omega(g(n))$ , kui  $g(n) = O(f(n))$ .

**Def.** Kirjutame  $f(n) = \Theta(g(n))$ , kui  $f(n) = O(g(n))$  ja  $f(n) = \Omega(g(n))$ .

**Def.** Kirjutame  $f(n) = o(g(n))$ , kui  $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$ .

**Def.** Kirjutame  $f(n) = \omega(g(n))$ , kui  $g(n) = o(f(n))$ .

## Polünomiaalne aeg ja efektiivsed arvutused

Kui Turingi masina  $M$  arvutusaeg on  $T(n) = n^{O(1)}$ , siis ütleme, et  $M$  töötab *polünomiaalses ajas*.

- NB!  $T(n)$  on *maksimaalne* arvutusaeg antud sisendi pikkuse  $n$  korral!
- Arvutus on *efektiivne* (kokkuleppeliselt), kui ta toimub polünomiaalses ajas.

## Ühesuunalised funktsioonid

Funktsiooni  $f: \{0, 1\}^* \rightarrow \{0, 1\}^*$  nimetatakse *ühesuunaliseks*, kui:

- leidub polünoomiaalses ajas töötav Turingi masin  $M$ , nii et  $f(x) \leftarrow M(x)$  iga  $x \in \{0, 1\}^*$  korral.

- iga efektiivse vastase (Turingi masina)  $A$  korral on:

$$\Pr[x \leftarrow \{0, 1\}^k, x' \leftarrow A(f(x)): f(x') = f(x)] = k^{-\omega(1)},$$

st pööramine õnnestub kaduvväikese tõenäosusega.

*Näide:* Kas nullfunktsioon  $f(x) \equiv 0$  on ühesuunaline?

## Diskreetne eksponentfunktsioon

Kui  $p$  on suur algarv ja  $\alpha$  on primitiivne element korpuses  $\mathbb{Z}_p$ , siis funktsioon

$$f_{\alpha,p}(x) = \alpha^x \pmod{p}$$

usutakse olevat ühesuunaline.

## Diffie-Hellmani võtmevahetus

1976 – Diffie ja Hellman pakkusid välja järgmise ühesuunalisel funktsioonil põhineva võtmekehtestusprotokolli:

- Valitakse suur algarv  $p$  ja primitiivne element  $\alpha$ .
- Kasutajad  $A$  ja  $B$  genereerivad salajased võtmed  $\omega_A \leftarrow \{1, \dots, p - 1\}$  ja  $\omega_B \leftarrow \{1, \dots, p - 1\}$ .
- Kasutaja  $A$  arvutab  $y_A = \alpha^{\omega_A} \pmod p$  ja saadab  $y_A$  kasutajale  $B$ .
- Kasutaja  $B$  arvutab  $y_B = \alpha^{\omega_B} \pmod p$  ja saadab  $y_B$  kasutajale  $A$ .
- Kasutaja  $A$  arvutab  $k_A = y_B^{\omega_A} \pmod p = \alpha^{\omega_A \omega_B} \pmod p$ .
- Kasutaja  $B$  arvutab  $k_B = y_A^{\omega_B} \pmod p = \alpha^{\omega_B \omega_A} \pmod p = k_A$ .

## RSA krüptosüsteem

- **Võtme genereerimine.** Leitakse kaks suurt algarvu  $p$  ja  $q$  ja leitakse  $n = p \cdot q$ . Leitakse  $e$  ja  $d$ , nii et  $e \cdot d \equiv 1 \pmod{\varphi(n)}$ . Siis  $(n, e)$  on avalik võti ja  $(n, d)$  salajane võti. NB!  $\varphi(n) = (p - 1)(q - 1)$ .
- **Krüpteerimine.**  $y = E_{n,e}(x) = x^e \pmod{n}$
- **Dekrüpteerimine.**  $D_{n,d}(y) = y^d \pmod{n} = x$

*Küsimused:*

- Kas  $E$  ja  $D$  on efektiivselt arvutatavad?
- Miks  $D_{n,d}(E_{n,e}(x)) = x$ ?
- Kuidas saada suuri algarve?

## Astendamisalgoritm

Selleks, et arvutada  $x^e \pmod n$ , esitame astendaja kahendsüsteemis:

$$e = e_m \cdot 2^m + e_{m-1} \cdot 2^{m-1} + \dots + e_1 \cdot 2^1 + e_0 \cdot 2^0 ,$$

kus  $e_m, \dots, e_0 \in \{0, 1\}$ . Seejärel kasutame valemit:

$$\begin{aligned} x^{e_m \cdot 2^m + \dots + e_0 \cdot 2^0} &= x^{e_m \cdot 2^m} \cdot x^{e_{m-1} \cdot 2^{m-1}} \cdot \dots \cdot x^{e_0 \cdot 2^0} \\ &= \left(x^{2^m}\right)^{e_m} \cdot \left(x^{2^{m-1}}\right)^{e_{m-1}} \cdot \dots \cdot \left(x^{2^0}\right)^{e_0} . \end{aligned}$$

Hüperastmed  $x^{2^0}, \dots, x^{2^m}$  arvutame skeemi  $x^{2^k} = \left(x^{2^{k-1}}\right)^2$  järgi.

## Euleri teoreem

**Teoreem (Euler).** Kui  $(x, n) = 1$ , siis  $x^{\varphi(n)} \equiv 1 \pmod{n}$ , iga  $n$  ja iga  $x$  korral.

- Euleri teoreemi tõestuseks teeme kõrvalepõike üldisesse rühmateooriasse.
- Euleri teoreemi kasutades näitame, et kui avatekst  $x$  on pööratav mooduli  $n$  järgi, st  $(x, n) = 1$ , siis

$$(x^e)^d = x^{e \cdot d} = x^{1+k \cdot \varphi(n)} = x \cdot (x^{\varphi(n)})^k \equiv x \cdot 1^k \equiv x \pmod{n} .$$

- Näitamaks, et RSA krüptosüsteem on korrektne ka mittepööratavate  $x$ -de korral on samuti vaja üldisi algebratulemusi – nn. Hiina jäägiteoreemi (tõestame hiljem)

## Rühma mõiste

**Rühm**  $G$  on hulk, millel on defineeritud üks binaarne operatsioon  $\cdot$ , mis on:

- **Assotsiatiivne**:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- **Ühikelemendiga**: Leidub  $e \in G$ , nii et  $x \cdot e = e \cdot x = x$  iga  $x \in G$  korral
- **Pööratav**: Igal elemendil  $a \in G$  on pöördelement  $b \in G$ , nii et  $a \cdot b = e$ . Tähistame  $b = a^{-1}$ .

**Näited**:

- $(\mathbb{Z}, +)$
- $(\mathbb{Z}_n, +)$ , st mooduliga liitmine
- $(\mathbb{Z}_n^*, \cdot)$ , st mooduliga korrutamine

## Alamrühmad

Rühma  $(G, \cdot)$  *alamrühmaks* nimetatakse alamhulka  $H \subseteq G$ , mis ise on rühm korrutustehte  $\cdot$  suhtes.

Näiteks täisarvude aditiivses rühmas  $(\mathbb{Z}, +)$  on kõigi paarisarvude hulk  $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$  alamrühm.

Selleks, et mingi alamhulk  $H$  oleks alamrühm, on tarvilik ja piisav, et  $H$  oleks kinnine korrutamise ja pöördelemendi võtmise suhtes.

Pöördelemendi nõue on oluline, sest näiteks rühmas  $(\mathbb{Z}, +)$  on hulk  $\mathbb{N} = \{0, 1, 2, \dots\}$  küll kinnine tehte  $+$  suhtes, kuid ise ta rühma ei moodusta. Selgub, et lõplike rühmade korral ei ole sellised kontranäited võimalikud:

*Ülesanne.* Tõesta, et lõpliku rühma  $(G, \cdot)$  alamhulk  $H$  on alamrühm parajasti siis kui  $H$  on kinnine tehte  $\cdot$  suhtes.

## Elemendi järk rühmas

Eelnevast on selge, et kui  $G$  on lõplik rühm ja  $g \in G$ , siis astmete hulk  $H = \{g, g^2, g^3, \dots\}$  on alamrühm. See tuleneb otseselt hulga  $H$  kinnisusest korrutamise suhtes.

Et iga alamrühm sisaldab ühikelementi, siis järelikult ka  $1 \in H$ . Olgu  $k$  minimaalne selline astendaja, mille korral  $g^k = 1$ . Siit järeldub, et  $|H| = k$ , sest astmed  $g, g^2, \dots, g^k$  on erinevad ja kui  $\ell > k$ , siis  $g^\ell = g^{\ell \bmod k}$ .

Rühma  $H$  tähistatakse  $\langle g \rangle$  ja tema elementide arvu  $|\langle g \rangle|$  nimetatakse elemendi  $g$  *järguks*.

*Järeldus.* Kui  $G$  on lõplik rühm ja  $g \in G$ , siis  $g^{|\langle g \rangle|} = 1$ .

## Lagrange'i teoreem

**Teoreem (Lagrange).** Lõpliku rühma  $G$  elementide arv jagub iga alamrühma  $H \subseteq G$  elementide arvuga.

*Tõestus.* Olgu  $H = \{h_1, \dots, h_m\}$  ja  $g \notin H$  mingi hulka  $H$  mittekuuluv rühma  $G$  element. Moodustame hulga  $gH = \{gh_1, \dots, gh_m\}$ , mille kõik elemendid on erinevad, sest eeldusest  $gh_i = gh_j$  järelduks  $h_i = g^{-1}gh_i = g^{-1}gh_j = h_j$ . Seega  $|H| = |gH|$ .

Hulgad  $H$  ja  $gH$  on ühisosata ( $H \cap gH = \emptyset$ ), sest muidu  $gh_i = h_j$  mingi  $i, j \in \{1, \dots, m\}$  korral ja seega  $g = gh_i h_i^{-1} = h_j h_i^{-1} \in H$ , mis on eeldusega  $g \notin H$  vastuolus.

Kui  $G = H \cup gH$ , siis on rühmas  $G$  järelikult  $2 | H |$  elementi ja väide kehtiks.

Olgu  $g_2$  element, mis ei kuulu hulka  $H \cup gH$ . Moodustame hulga  $g_2H = \{g_2h_1, \dots, g_2h_m\}$ . Selge, et  $|H| = |g_2H|$  ja  $g_2H \cap H = \emptyset$ .

Näitame, et ka  $gH \cap g_2H = \emptyset$ . Kui viimane hulk ei oleks tühi, siis  $gh_i = g_2h_j$  mingite  $i, j \in \{1, \dots, m\}$  korral. Siis aga oleks  $g_2 = g(h_i h_j^{-1}) \in gH$ , mis on eeldusega  $g_2 \notin H \cup gH$  vastuolus. Seega on hulgad  $H$ ,  $gH$  ja  $g_2H$  ühisosata ja võrdse võimsusega.

Kui nüüd  $G = H \cup gH \cup g_2H$ , siis oleks  $|G| = 3 |H|$  ja väide kehtiks.

Nii edasi arutledes jõuamegi järeldusele, et  $G$  on tükeldatav võrdse suurusega  $|H|$  tükkeks, mistõttu teoreemi väide kehtib.  $\square$

## Euleri teoreemi tõestus

Euleri teoreemi tõestuseks piisab, kui panna tähele, et hulk

$$\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} : (a, n) = 1\}$$

on rühm, milles on  $\phi(n)$  elementi. Seega leidub  $k$ , nii et  $\phi(n) = |\langle a \rangle| \cdot k$ .  
Seega,

$$a^{\phi(n)} = a^{|\langle a \rangle| \cdot k} = \left(a^{|\langle a \rangle|}\right)^k \equiv 1^k \equiv 1 \pmod{n}.$$

## Algarvude leidmine: Fermat' teoreem

*Teoreem (Fermat')*. Kui  $p$  on algarv, siis  $b^{p-1} \equiv 1 \pmod{p}$  iga  $0 < b < p$  korral. (Otsene järeldus Euleri teoreemist!)

*Fermat' test (Kas  $n$  on algarv?)*: Genereerime  $b \leftarrow \{1, \dots, n-1\}$  ja arvutame  $c = b^{n-1} \pmod{n}$ .

- Kui  $c \neq 1$ , siis Fermat' teoreemi tõttu  $n$  *ei ole algarv!*
- Kui  $c = 1$ , siis kordame testi.
- Kui testi on korratud  $k$  korda, siis lõpetame ja kuulutame  $n$ -i algarvuks!

*Küsimus*: Kui usaldatav on Fermat' test?

## Pseudoalgarvud baasil $b$

Olgu  $0 < b < n$  ja  $b^{n-1} \equiv 1 \pmod{n}$ . Siis öeldakse, et  $n$  on *pseudoalgarv baasil  $b$* .

Olgu  $H_n = \{b : b \in \mathbb{Z}_n^*, b^{n-1} \equiv 1 \pmod{n}\}$ , st  $H_n$  on kõigi pööratavate baaside hulk  $\mathbb{Z}_n$ -s, mille suhtes  $n$  on pseudoalgarv.

**Teoreem.** Hulk  $H_n$  on alamrühm multiplikatiivses rühmas  $G = \mathbb{Z}_n^*$ .

**Tõestus.** Kui  $b_1, b_2 \in H_n$ , siis  $(b_1 \cdot b_2)^{n-1} \equiv b_1^{n-1} \cdot b_2^{n-1} \equiv 1 \pmod{n}$ , millest järeljub  $b_1 \cdot b_2 \in H_n$ .  $\square$

**Def.** Kui  $n$  on kordarv ja  $H_n = \mathbb{Z}_n^*$ , siis  $n$  on *Carmichaeli arv*. (Vähim Carmichaeli arv on 561).

## Fermat' testi usaldatavus (I)

**Teoreem.** Kui  $n$  on kordarv ja ei ole Carmichaeli arv, siis

$$|H_n| \leq \frac{1}{2} |\mathbb{Z}_n^*| = \frac{\varphi(n)}{2} .$$

**Tõestus.** Carmichaeli arvude definitsiooni järgi  $H_n \neq \mathbb{Z}_n^*$ , millest järeldub  $\frac{|\mathbb{Z}_n^*|}{|H_n|} > 1$ . Et aga Lagrange'i teoreemi järgi on vaadeldud suhe täisarvuline, siis järelikult

$$\frac{|\mathbb{Z}_n^*|}{|H_n|} \geq 2 ,$$

mis tõestabki teoreemi väite.  $\square$

**Järeldus.** Kui kordarv  $n$  ei ole Carmichaeli arv, siis (ühekordne) Fermat' test eksib tõenäosusega  $\leq \frac{1}{2}$  ja  $k$ -kordne tõenäosusega  $\leq \frac{1}{2^k}$ .

## Fermat' testi usaldatavus (II)

*Teoreem (Alford, Granville, Pomerance; 1994)* Olgu  $C(n)$  Carmichaeli arvude arv vahemikus  $[0...n]$ , siis  $C(n) > n^{2/7}$ . Järelikult on olemas lõpmatu arv Carmichaeli arve.

*Järeldus:* Fermat' test ei ole täiesti usaldatav ka väga suurte arvude korral.

Õnneks on olemas algarvutestid, mis töötavad ka Carmichaeli arvude korral.

## Miller-Rabini test (Kas $n$ on algarv?)

- Vali juhuslikult  $a \leftarrow \{1, \dots, n - 1\}$ .
- Kui  $(a, n) \neq 1$ , siis  $n$  on *kordarv*.
- Olgu  $n - 1 = 2^k \cdot m$ , kus  $m$  on paaritu.
- Kui  $a^m \pmod n = 1$  siis väljasta *algarv*.
- Kui  $a^{m \cdot 2^i} \equiv -1 \pmod n$  mingi  $i = 0 \dots k - 1$  korral, siis *algarv*.
- Muidu väljasta *kordarv*.

**Teoreem.** Kui  $n$  on algarv, siis Miller-Rabini test väljastab *algarv*.  
Kui  $n$  on kordarv, siis test väljastab *kordarv* tõenäosusega  $\geq \frac{1}{2}$ .

## Hiina jäägiteoreem

**Teoreem.** Kui  $n_1, n_2 \in \mathbb{N}$  ja  $(n_1, n_2) = 1$ , siis  $\mathbb{Z}_{n_1 n_2} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ , st leidub bijektiivne  $f: \mathbb{Z}_{n_1 n_2} \rightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ , nii et  $f(x + y) = f(x) + f(y)$  ja  $f(x \cdot y) = f(x) \cdot f(y)$  iga  $x, y \in \mathbb{Z}_{n_1 n_2}$  korral.

*Tõestus.* Defineerime  $f(x) = (x \bmod n_1, x \bmod n_2)$ . On selge, et  $f$  säilitab tehted ja  $|\mathbb{Z}_{n_1 n_2}| = |\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}|$ , mistõttu piisab kui näitame, et  $f$  on injektiivne. Tingimusest  $(n_1, n_2) = 1$  saame, et leiduvad  $\alpha, \beta \in \mathbb{Z}$ , nii et  $\alpha n_1 + \beta n_2 = 1$ . Defineerime  $g: \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \rightarrow \mathbb{Z}_{n_1 n_2}$  järgmiselt:

$$g(x_1, x_2) = \beta n_2 x_1 + \alpha n_1 x_2 \pmod{n_1 n_2} .$$

Olgu  $x \in \mathbb{Z}_{n_1 n_2}$ ,  $x \bmod n_1 = x + c_1 n_1$ , ja  $x \bmod n_2 = x + c_2 n_2$ . Siis:

$$\begin{aligned} g(f(x)) &= \beta n_2 (x + c_1 n_1) + \alpha n_1 (x + c_2 n_2) \pmod{n_1 n_2} \\ &= (\alpha n_1 + \beta n_2)x + n_1 n_2 \cdot (\dots) \pmod{n_1 n_2} = x . \quad \square \end{aligned}$$

## Järeldus1: RSA korrektsus

**Teoreem (RSA korrektsus).** Olgu  $e \cdot d \equiv 1 \pmod{\varphi(n)}$  ja  $n = p \cdot q$ , kus  $p$  ja  $q$  on erinevad algarvud. Siis iga  $x \in \mathbb{Z}_n$  korral:

$$x^{ed} \equiv x \pmod{n} .$$

*Tõestus.* Vastavalt Hiina jäägiteoreemile piisab, kui näidata, et  $x^{ed} \equiv x$  kehtib ringis  $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ . Olgu  $(x_1, x_2)$  selle ringi suvaline element. Siis

$$\begin{aligned} (x_1, x_2)^{ed} &= (x_1^{ed} \pmod{p}, x_2^{ed} \pmod{q}) \\ &= (x_1^{1+c\varphi(n)} \pmod{p}, x_2^{1+c\varphi(n)} \pmod{q}) \\ &= (x_1 \cdot x_1^{(p-1)c(q-1)} \pmod{p}, x_2 \cdot x_2^{(q-1)c(p-1)} \pmod{q}) \\ &= (x_1, x_2) , \end{aligned}$$

sest Fermat' teoreemi tõttu  $x_1^{(p-1)} \pmod{p} = 1$  kui  $x_1 \neq 0$  (ja 0 kui  $x_1 = 0$ ) ning  $x_2^{(q-1)} \pmod{q} = 1$  kui  $x_2 \neq 0$  (ja 0 kui  $x_2 = 0$ ).  $\square$

## Järeldus 2: Võrrandite lahendamine

Kui  $(n_1, n_2) = 1$ , siis iga  $a \in \mathbb{Z}_{n_1}$  ja  $b \in \mathbb{Z}_{n_2}$  korral on võrrandisüsteemil

$$\begin{cases} x \pmod{n_1} = a \\ x \pmod{n_2} = b \end{cases}$$

parajasti üks lahend  $x$  vahemikus  $\{0, \dots, n_1 n_2 - 1\}$ .

*Näiteülesanne.* Leia võrrandisüsteemi kõik lahendid vahemikus  $[0 \dots 21]$ :

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 6 \pmod{7}. \end{cases}$$

*Lahendus.* Et  $(-2) \cdot 3 + 1 \cdot 7 = 1$ , siis saame Hiina jäägiteoreemist, et  $x \equiv 7 \cdot 2 + (-2) \cdot 3 \cdot 6 \equiv 20 \pmod{21}$ , millest järeldub, et  $x = 20$  on ainus lahend vahemikus  $[0 \dots 21]$ .

## Järeldus3: Ruutjuured

**Teoreem.** Ringis  $\mathbb{Z}_{pq}$  (kus  $p$  ja  $q$  on paaritud algarvud) on elemendil  $a \in \mathbb{Z}_{pq}^*$  parajasti neli ruutjuurt.

**Tõestus.** Piisab kui näidata, et nii on ringis  $\mathbb{Z}_p \times \mathbb{Z}_q$ . Lihtne on näha, et

$$(\mathbb{Z}_p \times \mathbb{Z}_q)^* = \mathbb{Z}_p^* \times \mathbb{Z}_q^* .$$

Olgu  $(x_1, x_2) \in \mathbb{Z}_p \times \mathbb{Z}_q$  ja  $(x_1, x_2)^2 = (x_1^2, x_2^2) = (a \bmod p, a \bmod q)$ . Piisab kui näitame, et võrrandil  $x^2 = a$  on ringides  $\mathbb{Z}_p$  ja  $\mathbb{Z}_q$  parajasti kaks lahendit. Oletame, et ringis  $\mathbb{Z}_p$  nimetatud võrrandil kaks lahendit  $x$  ja  $y$ , st  $x^2 - y^2 = (x - y)(x + y) \equiv 0 \pmod{p}$ . Et  $p$  on algarv, siis nullitegurid puuduvad ja üks teguritest peab olema null. Seega  $x = \pm y$ , millest järeldub, et võrrandil  $x^2 = a$  on *ülimalt kaks* lahendit.

Teiselt poolt, kui  $x^2 = a$ , siis alati ka  $(-x)^2 = a$ . Kui  $p > 2$ , siis  $x \not\equiv -x$ , mistõttu lahendeid on *vähemalt kaks*.  $\square$

## Miller-Rabini testi korrektsus I

**Teoreem 3** *Kui  $p$  on paaritu algarv ja  $\alpha \geq 2$ , siis multiplikatiivne rühm  $\mathbb{Z}_{p^\alpha}^*$  (milles on  $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$  elementi) on tsükliline.*

Tõestus. Olgu  $g_0$  tsüklilise rühma  $\mathbb{Z}_p^*$  moodustaja. Kui  $g_0^{p-1} \not\equiv 1 \pmod{p^2}$ , siis võtame  $g = g_0$ , vastasel juhul olgu  $g = g_0(p+1)$ . Näitame, et  $g$  on rühma  $\mathbb{Z}_{p^\alpha}^*$  moodustaja. Kõigepealt paneme tähele, et mõlemal juhul kehtivad seosed:

$$(I) \ g \equiv g_0 \pmod{p}, \quad \text{ja} \quad (II) \ g^{p-1} = 1 + g_1 p,$$

kus  $(g_1, p) = 1$ . Tõepoolest, kui  $g_0^{p-1} \not\equiv 1 \pmod{p^2}$ , siis  $g^{p-1} \not\equiv 1 \pmod{p^2}$ , sest siis peaks olema ka  $(p+1)^{p-1} \equiv 1 \pmod{p^2}$ , mis viiks vastuolule. Oletame nüüd, et mingi  $j$  korral:

$$g^j \equiv 1 \pmod{p^\alpha}. \tag{5}$$

Kõigepealt näitame, et  $(p - 1) \mid j$ . Tõepoolest, olgu  $j = j_1 \cdot (p - 1) + r$ , kus  $r < p - 1$ . Siis seostest (I), (5), ja Fermat' teoreemist tulenevalt:

$$g^j \bmod p = g_0^j \bmod p = g_0^r \bmod p = 1 ,$$

millest  $g_0$  primitiivsuse tõttu  $r = 0$ . Seega  $j = (p - 1) \cdot j_1$  mingi  $j_1$  korral ja seega eesldusest (5) tulenevalt:

$$g^j = (1 + g_1 p)^{j_1} \equiv 1 \pmod{p^\alpha} . \quad (6)$$

Samas  $(1 + g_1 p)^{j_1} = 1 + g_1 j_1 p + c p^2$ . Seosest (6) järeldeb, et  $g^j \bmod p^\beta = 1$  iga  $\beta \leq \alpha$  korral. Olgu  $m$  suurim astendaja, mille korral  $p^m \mid j_1$ , st  $j_1 = j_2 \cdot p^m$  ja  $(j_2, p) = 1$ . Kui oleks  $m < \alpha - 1$ , siis järelikult  $m + 2 \leq \alpha$  ja seega (võttes  $\beta = m + 2$ ), saame

$$\begin{aligned} (1 + g_1 p)^{j_1} \bmod p^{m+2} &= [1 + g_1 j_2 p^{m+1} + c' \cdot p^{m+1}] \bmod m + 2 \\ &= 1 + g_1 j_2 p^{m+1} = 1 , \end{aligned}$$

millest järeldub, et  $g_1 j_2 p^{m+1} \equiv 0 \pmod{p^{m+2}}$ . See on aga vastuolus seostega  $(g_1, p) = (j_2, p) = 1$  ja seetõttu viib oletus  $m < \alpha - 1$  vastuolule. Järelikult  $m \geq \alpha - 1$  ja seega

$$\phi(p^\alpha) = p^{\alpha-1}(p-1) \mid j .$$

Seega on  $g$  tõepoolest primitiivne ja  $\mathbb{Z}_{p^\alpha}^* = \langle g \rangle$ .  $\square$

## Miller-Rabini testi korrektsus II

**Teoreem 4** *Ükski Carmichaeli arv ei ole algarvu aste.*

Tõestus. Olgu  $n = p^k$  (kus  $p$  on algarv ja  $k \geq 2$ ) Carmichaeli arv. Olgu  $g$  multiplikatiivse rühma  $\mathbb{Z}_n^*$  moodustaja. Et  $g^{n-1} \bmod n = 1$ , siis järelikult peaks  $n - 1$  jaguma  $g$  järguga  $\phi(n) = p^{k-1}(p - 1)$ . Kuid siis jaguvad nii  $n$  kui  $n - 1$  arvuga  $p$ , mis ei ole võimalik.  $\square$

## Miller-Rabini testi korrektsus III

**Teoreem 5** Kui  $n$  on algarv,  $n - 1 = 2^k \cdot m$  ja  $m$  on paaritu, siis iga  $a \in \{1, \dots, n - 1\}$  korral kas  $a^m \equiv 1 \pmod{n}$  või leidub  $0 < i < k$ , nii et  $a^{2^i m} \equiv -1 \pmod{n}$ .

Tõestus. Kui  $a^m \not\equiv 1 \pmod{n}$ , siis  $a^{n-1} \equiv 1 \pmod{n}$  tõttu (Fermat' teoreem!) saame, et leidub  $0 < i < k$ , nii et  $a^{2^i m} \pmod{n} \neq 1$  ja  $a^{2^{i+1} m} \pmod{n} = 1$ . Kui teine eeldus ei kehtiks, siis võttes  $b = a^{2^i m} \pmod{n}$  saame, et ka  $b \not\equiv \pm 1 \pmod{n}$ , kuid  $b^2 \equiv 1 \pmod{n}$ . Seega oleks  $b$  mittetrivialne ühejuur, mis aga ei saa eksisteerida kui  $n$  on algarv.  $\square$

## Miller-Rabini testi korrektsus III

**Teoreem 6** Olgu  $n$  kordarv, kuid mitte Carmichaeli arv,  $n - 1 = 2^k \cdot m$  ja  $m$  on paaritu. Kui mingi  $1 < a < n$  korral kas  $a^m \equiv 1 \pmod{n}$  või leidub  $0 < i < k$ , nii et  $a^{2^i m} \equiv -1 \pmod{n}$ ; siis  $a^{n-1} \equiv 1 \pmod{n}$ .  
(Tõestus triviaalne)

## Miller-Rabini testi korrektsus IV

**Teoreem 7** Olgu  $n$  Carmichaeli arv,  $n - 1 = 2^k \cdot m$  ja  $m$  on paaritu. Siis Miller-Rabini test on korrektne tõenäosusega vähemalt  $\frac{1}{2}$ .

Tõestus. Olgu  $t = \max\{0 \leq i < k \mid \exists a \in \mathbb{Z}_n^* : a^{2^i m} \equiv -1 \pmod{n}\}$  (võtame  $t = 0$  kui sellist  $i$ -d ei leidu!) ja

$$B_t = \{a \in \mathbb{Z}_n^* : a^{2^t m} \equiv \pm 1 \pmod{n}\} .$$

Kui  $a \notin B_t$ , siis selle  $a$  korral Miller-Rabini test väljastab "kordarv". Definitsiooni tõttu kas  $t = 0$  või eksisteerib  $a \in \mathbb{Z}_n^*$  nii et  $a^{2^t m} \equiv -1 \pmod{n}$ .

Et  $n$  ei saa olla algarvu aste, siis on võimalik leida tegurid  $n = cd$ , kus  $3 \leq c, d < n$  ja  $(c, d) = 1$  ja seega:

- Juhul  $t = 0$  saame Hiina jäägiteoreemist, et leidub  $b \in \mathbb{Z}_n^*$ , nii et

$$\begin{aligned} b &\equiv 1 \pmod{c} \\ b &\equiv -1 \pmod{d} . \end{aligned}$$

Et nii 1 kui  $-1$  on pööratavad elemendid, siis ka  $b \in \mathbb{Z}_n^*$ . Samal ajal aga

$$\begin{aligned} b^{2^t m} &\equiv 1^m \equiv +1 \pmod{c} \\ b^{2^t m} &\equiv (-1)^m \equiv -1 \pmod{d} . \end{aligned}$$

Siit tuleneb, et  $b^{2^t m} \not\equiv \pm 1 \pmod{n}$  ja seega  $b \notin B_t$ .

- Juhul  $a^{2^t m} \equiv -1 \pmod{n}$  järeldeb Hiina jäägiteoreemist, et leidub  $b \in \mathbb{Z}_n$  nii et

$$\begin{aligned} b &\equiv a \pmod{c} \\ b &\equiv 1 \pmod{d} . \end{aligned}$$

Et nii  $a$  kui  $1$  on pööratavad elemendid, siis ka  $b \in \mathbb{Z}_n^*$ . Samal ajal aga

$$\begin{aligned} b^{2^t m} &\equiv a^{2^t m} \equiv -1 \pmod{c} \\ b^{2^t m} &\equiv 1^{2^t m} \equiv +1 \pmod{d} . \end{aligned}$$

Siit tuleneb, et  $b^{2^t m} \not\equiv \pm 1 \pmod{n}$  ja seega  $b \notin B_t$ .

Lihtne on veenduda, et  $B_t$  on rühma  $\mathbb{Z}_n^*$  alamrühm ja seega  $\frac{|B_t|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$ .  $\square$

## RSA praktiline kasutamine: nõrgad protokollid

Parim teadaolev tegurdamisalgoritm töötab ajas  $e^{(c+o(1)) \cdot \sqrt[3]{|n|} \cdot \log^{2/3}|n|}$   
(nn. *General Number Field Sieve*)

Järgnevalt näitame, et RSA kasutamisel tuleb olla väga ettevaatlik.

Meie ülesanne on koostada salastatud sõnumivahetuse süsteem, kus kasutajatel on võimalik üksteisele saata salajasi sõnumeid.

Näitame, et:

- Igal kasutajal peab olema eraldi moodul  $n$ . Ühise mooduli kasutamine on ebaturvaline.
- Kui avalik astendaja  $e$  on väike, siis  $E_{n,e}(x) = x^e \pmod n$  on krüpteerimisfunktsioonina ebaturvaline.

## Ühise mooduliga protokoll

Kasutajal  $A$  on avalik  $e_A$  ja salajane  $d_A$ , nii et  $e_A d_A \equiv 1 \pmod{\varphi(n)}$ .

Kasutajal  $B$  on avalik  $e_B$  ja salajane  $d_B$ , nii et  $e_B d_B \equiv 1 \pmod{\varphi(n)}$ .

**Simmons'i rünne:** Kui  $(e_A, e_B) = 1$  (täiesti võimalik juhtum!) kui üks ja sama sõnum  $m$  saadetakse kasutajatele  $A$  ja  $B$ , siis ründajal on olemas  $y_A = m^{e_A} \pmod{n}$  ja  $y_B = m^{e_B} \pmod{n}$ .

Teame, et leiduvad täisarvud  $\alpha$  ja  $\beta$ , nii et  $\alpha e_A + \beta e_B = 1$ . Üks arvudest  $\alpha, \beta$  peab olema negatiivne. Eeldame, et  $\alpha = -|\alpha|$ .

Ründaja arvutab esmalt  $y_A^{-1} \pmod{n}$  ja seejärel:

$$\left[ y_A^{-1} \right]^{|\alpha|} \cdot [y_B]^\beta = m^{\alpha e_A} \cdot m^{\beta e_B} = m^{\alpha e_A + \beta e_B} = m .$$

## Tegurdamine ühejuurte abil

Näitame, et kui on teada  $b \neq \pm 1$ , nii et  $b^2 \equiv 1 \pmod{n}$  (kus  $n = pq$ ), siis saab arvu  $n$  tegurdada.

Seosest  $b^2 = 1$  järeldeb, et  $(b + 1)(b - 1) = 0 \pmod{n}$ . Kuna  $b \neq \pm 1$ , siis ei ole kumbki sulg kongruentne nulliga ja seega on mõlemad sulud nullitegurid.

Et sulgude korrutis jagub  $n = pq$ -ga, kuid kumbki sulg ei jagu  $n$ -ga, siis üks sulg jagub  $p$ -ga ja teine  $q$ -ga.

Seega,  $(b + 1, n) \in \{p, q\}$  ja ühekordsest suurima ühisteguri leidmisest piisab  $n$  tegurdamiseks.

## Ühejuurte leidmine korrektse võtmepaari $(e, d)$ abil

Näitame, et kui kasutajal on võtmepaar  $e, d$ , nii et  $ed \equiv 1 \pmod{\varphi(n)}$ , siis saab kasutaja kui tahes suure tõenäosusega leida mittetriviaalse ühejuure ja seega tegurdada avalikku moodulit  $n$ .

**Juure leidmine (DeLaurentis):** Olgu  $ed - 1 = c \cdot \varphi(n) = 2^k \cdot \ell$ , kus  $\ell$  on paaritu arv.

- Vali juhuslikult  $a \in \{2, \dots, n - 2\}$ , nii et  $(a, n) = 1$ .
- Leia vähim  $j > 0$ , nii et  $a^{2^j \ell} = 1$ . (Leidub, sest  $2^k \ell$  jagub  $\varphi(n)$ -ga).
- Võtame  $b = a^{2^{j-1} \ell}$ . Kui  $b \neq -1$ , siis väljasta  $b$ , muidu korda protseduuri.

Saaab näidata, et igas tsüklis leitakse mittetriviaalne juur tõenäosusega  $\frac{1}{2}$ .

2004 – Alexander May näitas efektiivse deterministliku protseduuri!

## Teise kasutaja salajase astendaja leidmine

Näitame efektiivse deterministliku protseduuri, kuidas kasutaja  $B$  võtme-paariga  $(e_2, d_2)$  saab leida teise kasutaja  $A$  salajase astendaja  $d_1$  avaliku astendaja  $e_1$  abil.

Piisab, kui leida  $t$ , nii et  $(e_1, t) = 1$  ja  $t = c \cdot \varphi(n)$ . Tõepoolest, kuna  $\alpha e_1 + \beta t = 1$  mingite  $\alpha, \beta \in \mathbb{Z}$  korral, siis järelikult  $\alpha e_1 = 1 - \beta c \varphi(n) \equiv 1 \pmod{\varphi(n)}$ . Ründaja toimib järgmiselt:

- Leiab  $f = (e_1, e_2 d_2 - 1)$  kasutades Eukleidese algoritmi.
- Võtab  $t = \frac{e_2 d_2 - 1}{f}$ .

On tõenäoline (vt järgmine slaid), et  $(e_1, t) = 1$ . Definitsiooni järgi  $(e_1, \varphi(n)) = 1$ . Kuna  $f \mid e_1$ , siis ka  $(f, \varphi(n)) = 1$ . Kuid  $ft = e_2 d_2 - 1 = j \cdot \varphi(n)$ , millest järeldub, et  $\varphi(n) \mid t$ . Seega on vajalike omadustega  $t$  leitud.

## Teise kasutaja salajase astendaja leidmine: II

Tegelikult ei ole alati  $(e_1, t) = 1$  ja seetõttu ei tööta murdmisalgoritm alati.

Näiteks kui  $n = 41 \cdot 5 = 205$ , siis  $\varphi(n) = 160$ .

Võttes  $e_1 = 3$ , saame et  $d_1 = 107$ ; ja  $e_2 = 11$ , saame et  $d_2 = 131$ .

Nüüd  $e_2 d_2 - 1 = 1440 = 9 \cdot 160$ . Seega  $f = (e_1, e_2 d_2 - 1) = (3, 9 \cdot 160) = 3$  ja  $t = \frac{e_2 d_2 - 1}{f} = 9 \cdot 160 / 3 = 3 \cdot 160$ .

Seega,  $(e_1, t) = 3 \neq 1$ .

## Väike astendaja $e$

Kasutajatel  $A$ ,  $B$  ja  $C$  olgu vastavalt RSA moodulid  $n_1$ ,  $n_2$  ja  $n_3$ . Avalik astendaja on kõigil  $e = 3$ . Oletame, et üks ja sama sõnum  $m$  saadetakse korraga kõigile kolmele kasutajale ja ründaja saab kätte kõik krüptogrammid:

$$y_A = m^3 \pmod{n_1}, \quad y_B = m^3 \pmod{n_2}, \quad y_C = m^3 \pmod{n_3} .$$

Ründaja toimib järgmiselt: Kui  $(n_i, n_j) \neq 1$ , siis ründaja tegurdab  $n_i$ , leiab salajase võtme  $d_i$  ja dekrüpteerib sõnumi  $m$ . Kui kolm moodulit  $n_1, n_2, n_3$  on paarikaupa ühistegurita, siis vastane leiab  $x \in \mathbb{Z}_{n_1 n_2 n_3}$ , nii et

$$\begin{cases} x \equiv y_A & (\text{mod } n_1) \\ x \equiv y_B & (\text{mod } n_2) \\ x \equiv y_C & (\text{mod } n_3) \end{cases}$$

Kuna  $m < \min\{n_1, n_2, n_3\}$ , siis  $m^3 < n_1 n_2 n_3$ , mistõttu  $m^3$  on samuti kongruenside süsteemi lahend hulgas  $\mathbb{Z}_{n_1 n_2 n_3}$ . Hiina jäägiteoreemi tõttu  $x = m^3$ . Seega piisab  $m$  leidmiseks, kui leida  $\sqrt[3]{x}$ , mis on lihtne!

## Väike astendaja $d$

RSA algoritmi praktilistes rakendustes võib tekkida kiusatus valida  $d$  väike.

Selgub, et liiga väike  $d$  on ebaturvaline:

***d leidmine (M.Wiener):*** Kui  $q < p < 2q$  ja  $d < \frac{1}{3}n^{1/4}$ , siis paarist  $(n, e)$  (kus  $ed \equiv 1 \pmod{\varphi(n)}$ ) saab efektiivselt arvutada  $d$ .

Kui  $n$  on 1024-bitine, siis  $d$  peaks olema vähemalt 256-bitine.

***Lahtine probleem:*** Kui  $d < n^{0.5}$ , kas siis alati saab efektiivselt leida  $d$ ?

## Homomorfsus

RSA krüpteerimisalgoritmil on järgmine omadus:

$$\begin{aligned} E(m_1 m_2) &= (m_1 m_2)^e \pmod n = m_1^e \cdot m_2^e \pmod n \\ &= E(m_1) \cdot E(m_2) \pmod n . \end{aligned}$$

Näiteks:

$$E(2m) = E(2) \cdot E(m) \pmod n ,$$

mistõttu saab krüptogrammist  $E(m)$  ilma privaativõtmeta efektiivselt koostada krüptogrammi  $E(2m)$ .

## Homomorfisuse kuritarvitamine: näide

Olgu meil server, kellel on avalik võti  $(e, n)$ .

Kasutajad saadavad serverile krüpteeritud sõnumeid  $E(m)$ , kusjuures  $m$  esimene bitt peab olema 1.

Vastasel korral saadab server kasutajale veateate.

**Nõrkus:** Serveriga suheldes, saab dekrüpteerida suvalise krüptogrammi  $E(m)$ .

## Homomorfisuse kuritarvitamine: näide

Saadame serverile  $E(m)$  ja saame teada, kas  $m$  on paaris või paaritu.

Arvutame ja saadame serverile  $E(2m) = E(2) \cdot E(m)$ .

Kui  $m < \frac{n}{2}$ , siis  $2m < n$  ja  $2m \bmod n$  on paaris ja saame veateate.

Kui  $\frac{n}{2} \leq m < n$ , siis  $n \leq 2m < 2n$  ja  $2m \bmod n = 2m - n$  on paaritu, sest  $n$  on paaritu ja  $2m$  paaris. Seega, me ei saa veateadet!

Seega, me saame teada, kummas vahemiku  $[0 \dots n - 1]$  pooles asub  $m$ .