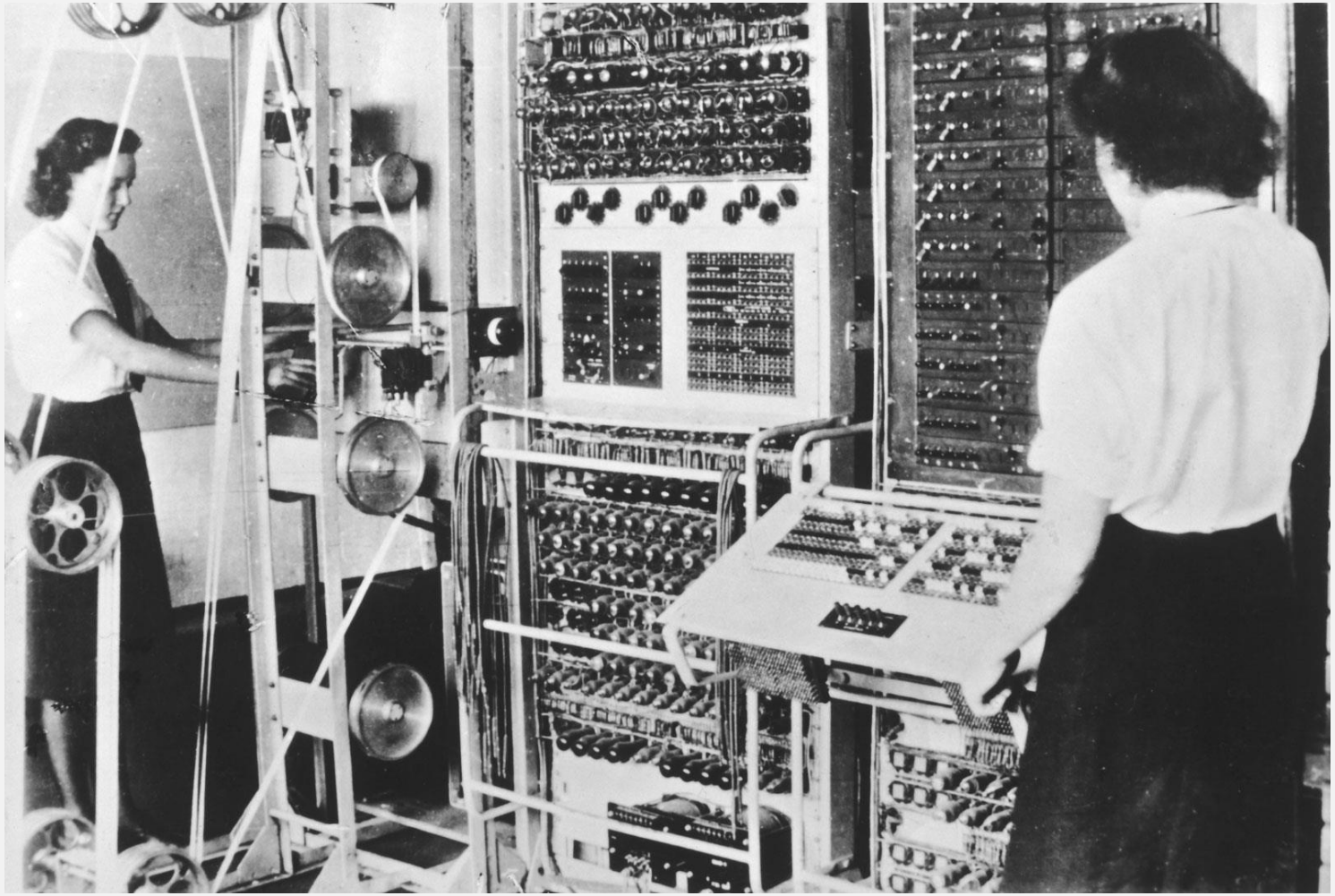
Vastutustundlikud informatsiooni töötlemise süsteemid

Akadeemikukandidaatide konverents
25. oktoobril 2022, Tallinnas

Dan Bogdanov, PhD Cybernetica Infoturbeinstituudi direktor

CYBERNETICA

Esimesed arvutid ehitati turvalisuse murdmiseks

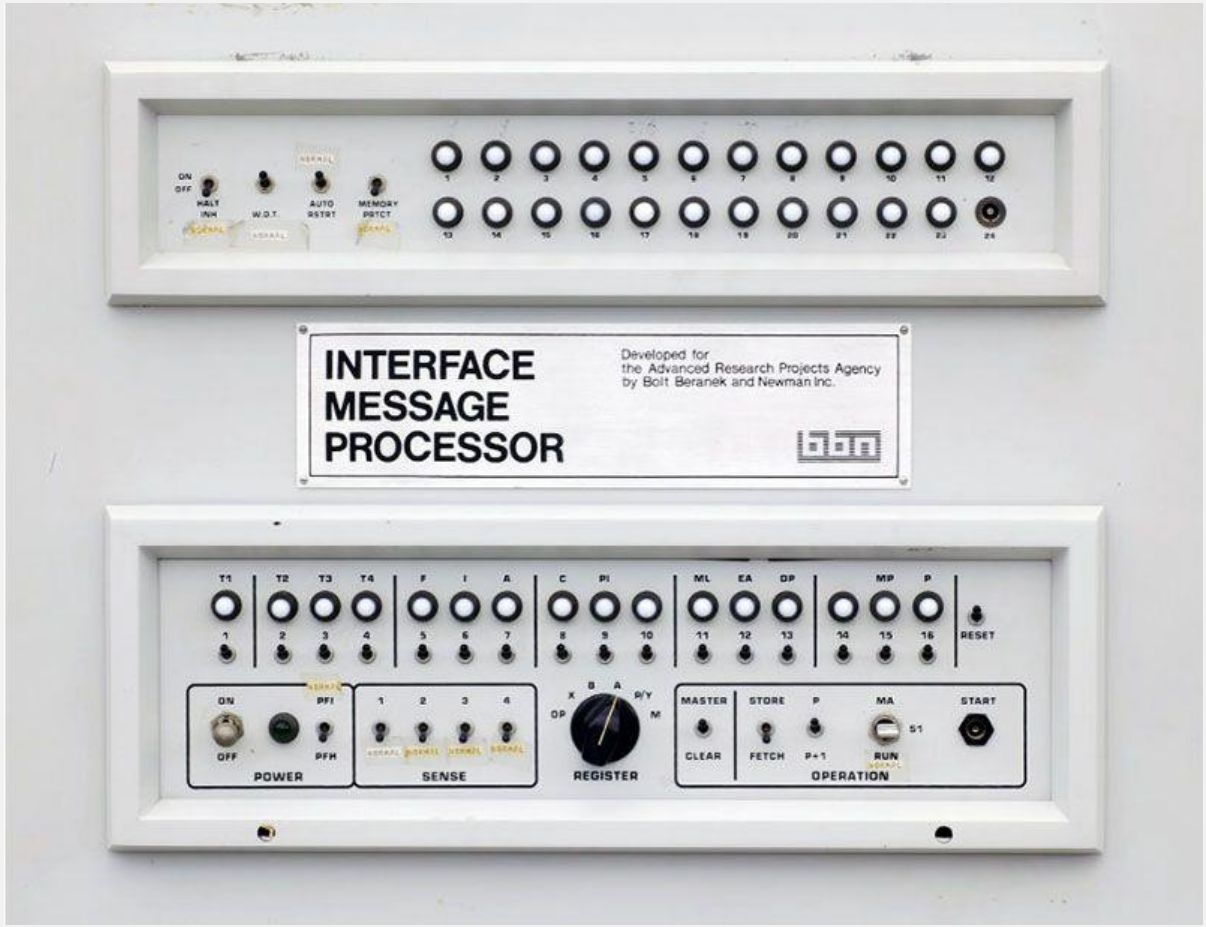


Colossust loetakse esimeseks digitaalseks programmeeritavaks arvutiks.

Colossuse ehitas 1943. aastal Inglismaa, et murda sakslaste Lorenz SZ šifreerimissüsteemi.

Foto allikas:
The History Blog

Esimene arvutivõrk ehitati andmete kopeerimiseks



Interface Message Processor oli esimene pakette vahetav ruuter, mille ehitasid 1969. aastal Ameerika firma BBN insenerid.

Eesmärk oli lihtsustada andmete levitamist.

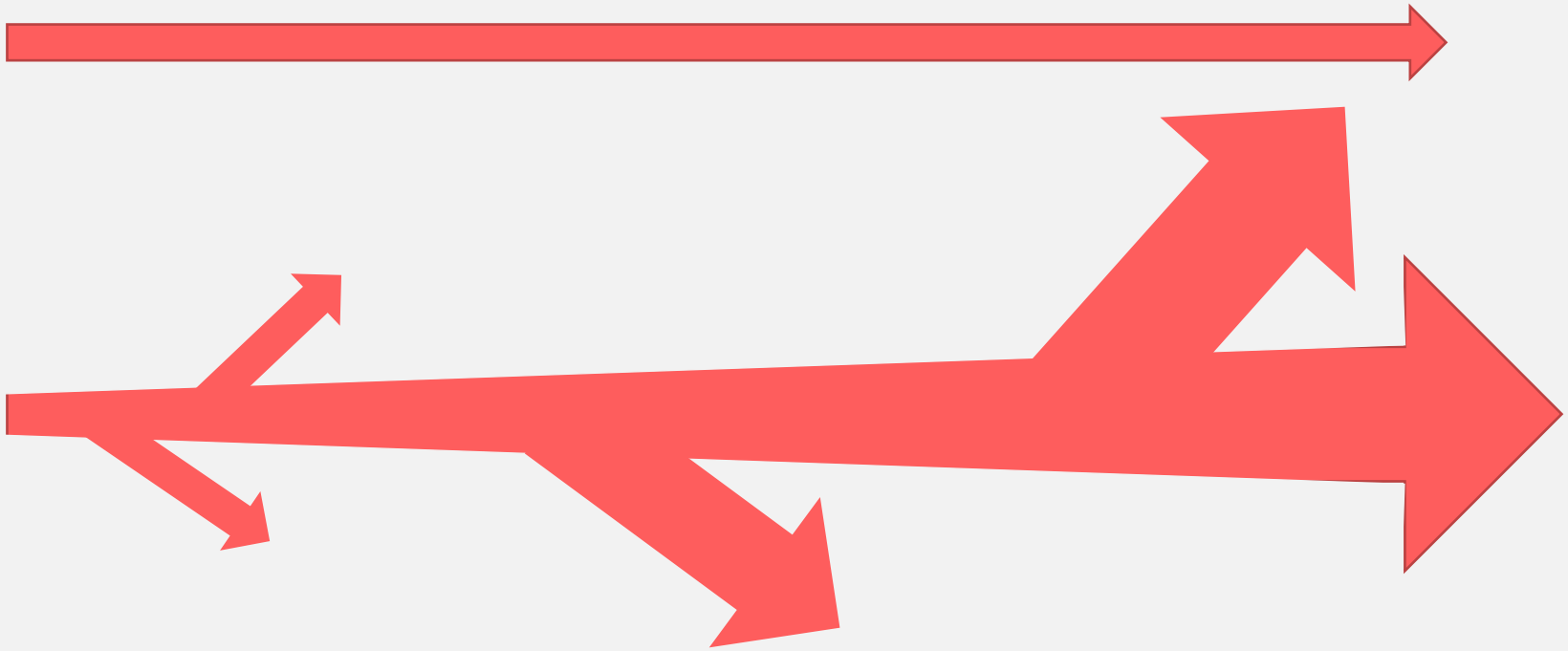
Foto allikas:
Computer History Museum

Kopeerimise lihtsus raskendab andmete kaitset

Aja möödudes

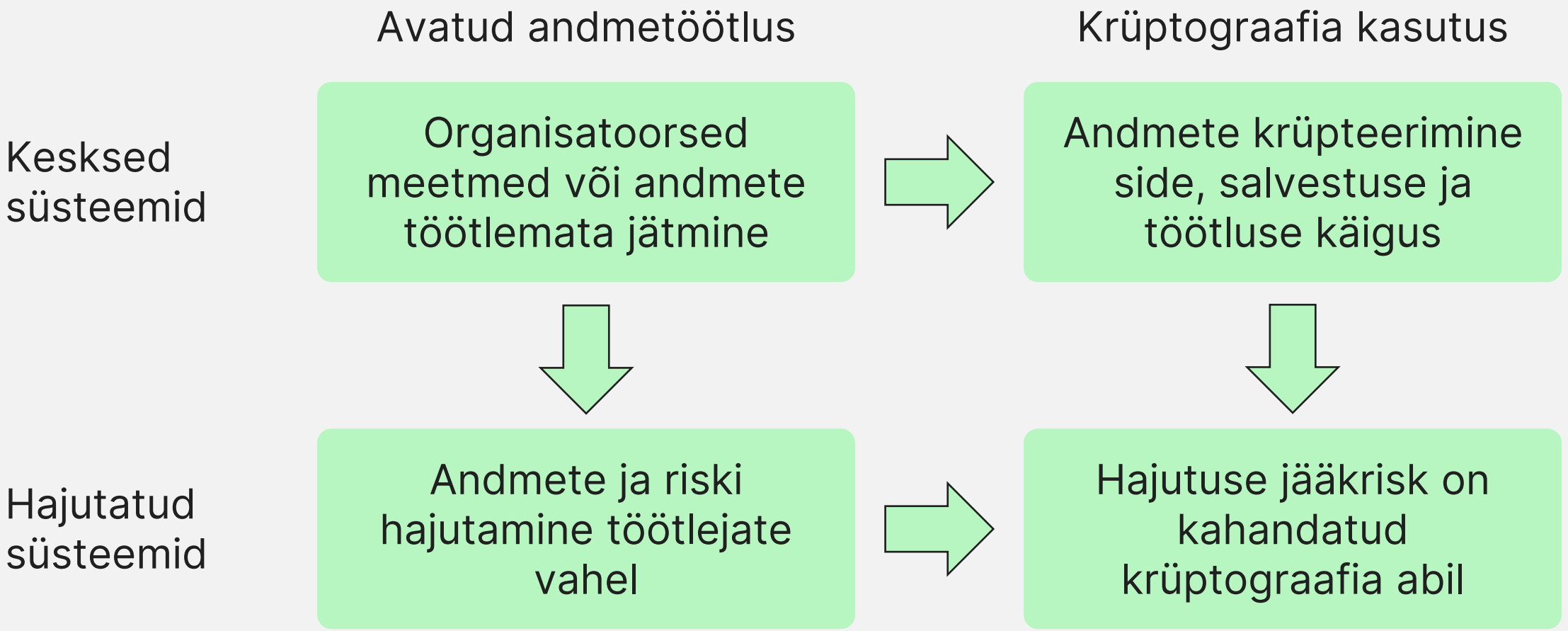
andmete hulk süsteemides kasvab

ning kontroll andmete üle on üha keerukam.



Väline või sisemine ründaja lekitab või kahjustab andmeid.	Andmete haldaja kasutab andmeid lubamatul moel.	Taristu või teenusepakkuja lekitab või kahjustab andmeid suures ulatuses.

Lahendused leiame krüptograafiast ja hajutusest



Sharemind-süsteemi lihtsustatud tööpõhimõte

Isik A

Saladus: 25

1. Vali juhuslik arv $a_1 = 57$
2. Vali juhuslik arv $a_2 = 13$
3. $a_3 = 25 - 57 - 13 \equiv 55 \bmod 100$
4. Saada iga a_k eraldi serverile

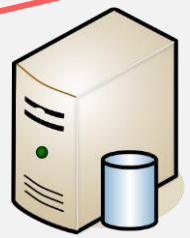
1. Vali juhuslik arv $b_1 = 44$
2. Vali juhuslik arv $b_2 = 57$
3. $b_3 = 33 - 44 - 57 \equiv 32 \bmod 100$
4. Saada iga b_k eraldi serverile

Isik B

Saladus: 33

$a_1 = 57$
$b_1 = 44$
$c_1 = a_1 + b_1 = 101$
$\equiv 1 \bmod 100$

Arvuti 1



$a_2 = 13$
$b_2 = 57$
$c_2 = a_2 + b_2 = 70$
$\equiv 70 \bmod 100$

Arvuti 2

$a_3 = 55$
$b_2 = 32$
$c_3 = a_3 + b_3 = 87$
$\equiv 87 \bmod 100$

Arvuti 3

Isik C

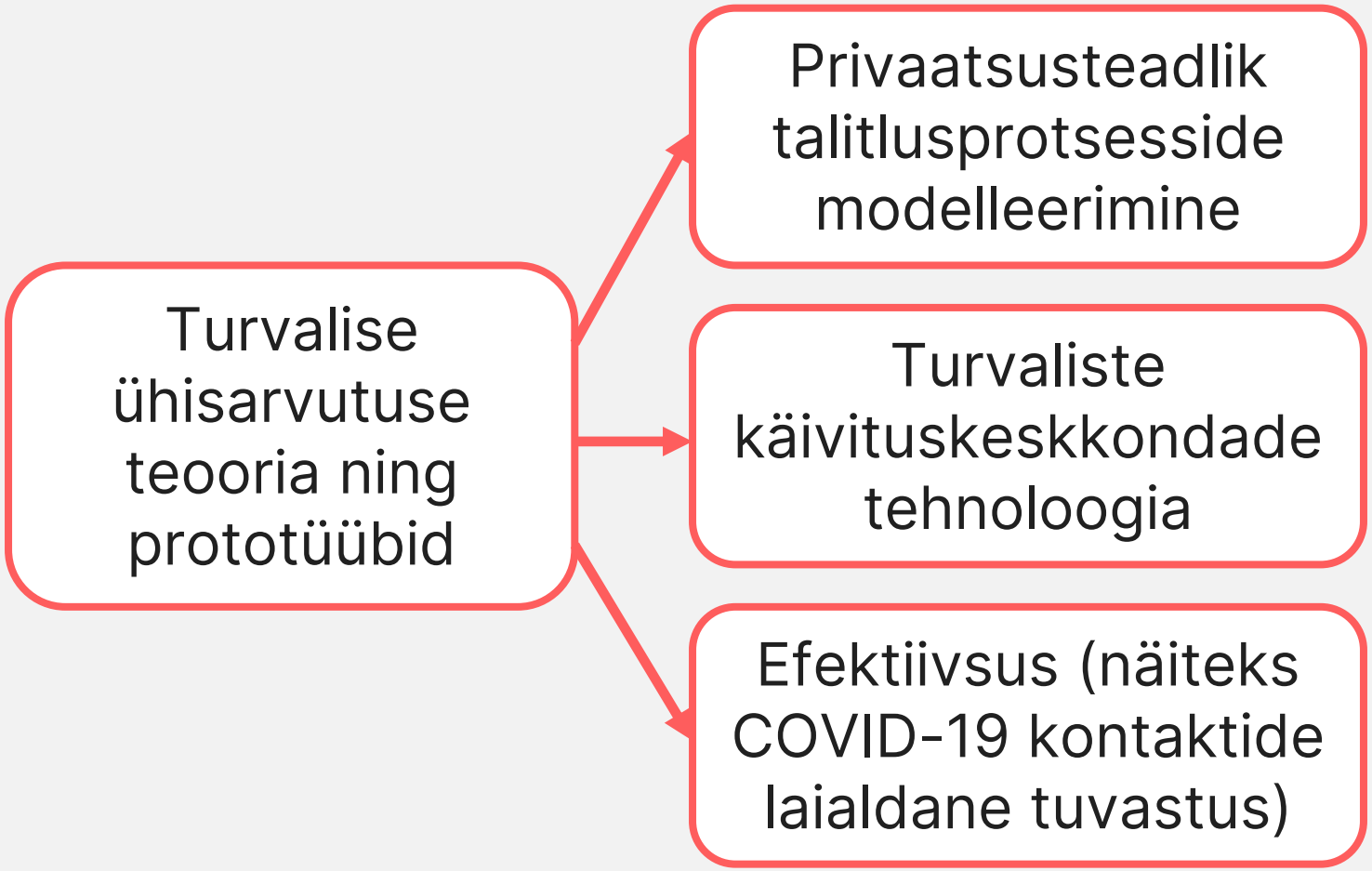
Isik C arvutab $c = 1 + 70 + 87 = 158 \equiv 58 \bmod 100$

C sai teada, et A ja B vanuste summa on 58
Ei C ega arvutid ei näinud A ja B saladusi

Sharemindi teadussuuna tähtsamad tulemused

- 2006 – protokollide ja protüüpide arendus algab
- 2008 – valmivad alusuuringud, esmane aritmeetikasüsteem
- 2012 – reaalse maailma rakendus: ettevõtete majandusstatistika (ITL)
- 2013 – genoomi hõlmavate assotsiatsiooniuuringute prototüüp
- 2014 – käibemaksupettuste tuvastamise süsteemi prototüüp
- 2015 – satelliitide kokkupõrgete ennustamise prototüüp *(Kamm et al)*
- 2016 – reaalne rakendus: Eesti IT-erialade tudengite õpikäitumise statistiline uuring maksu- ja haridusandmete põhjal
- 2016 – Inglismaa valitsuskabinet katsetab Sharemindi tehnoloogiat sotsiaaltoetuste pettuste tuvastamise süsteemi jaoks

Vastutustundlikud süsteemid - uued uurimissuunad



- Millal on otstarbekas millist tehnoloogiat rakendada?
- Kuidas lihtsustada turvalise arvutamise juurutamist?
- Kuidas ehitada privaatseid lahendusi miljonitele kasutajatele?

Koostöö Teaduste Akadeemiaga

- Uudsed teadusuuringud, mis saavad kasutada rohkem andmeid tänu paremale andmekaitsele (nt terviseuuringud).
- Eesti riigi ja ettevõtete uute andmepõhiste teenuste jaoks vastutustundlike tehniliste lahenduste loomine.
- Järgmise põlvkonna andmeteadlastele ja infosüsteemide arendajatele vastutustundlike tehnoloogiate õpetamine.
- Eesti rahvusvaheliste teaduskoostöö kontaktide kasvatamine ja uute koostöövõimaluste loomine
- Kui mul tekib võimalus, siis ma kindlasti osalen Akadeemia töös sobivate ekspertkomisjonide kaudu.

Tänan kuulamast!

25. oktoobril 2022
Tallinnas

cybernetica
CyberneticaAS
cybernetica_ee
Cybernetica

CYBERNETICA