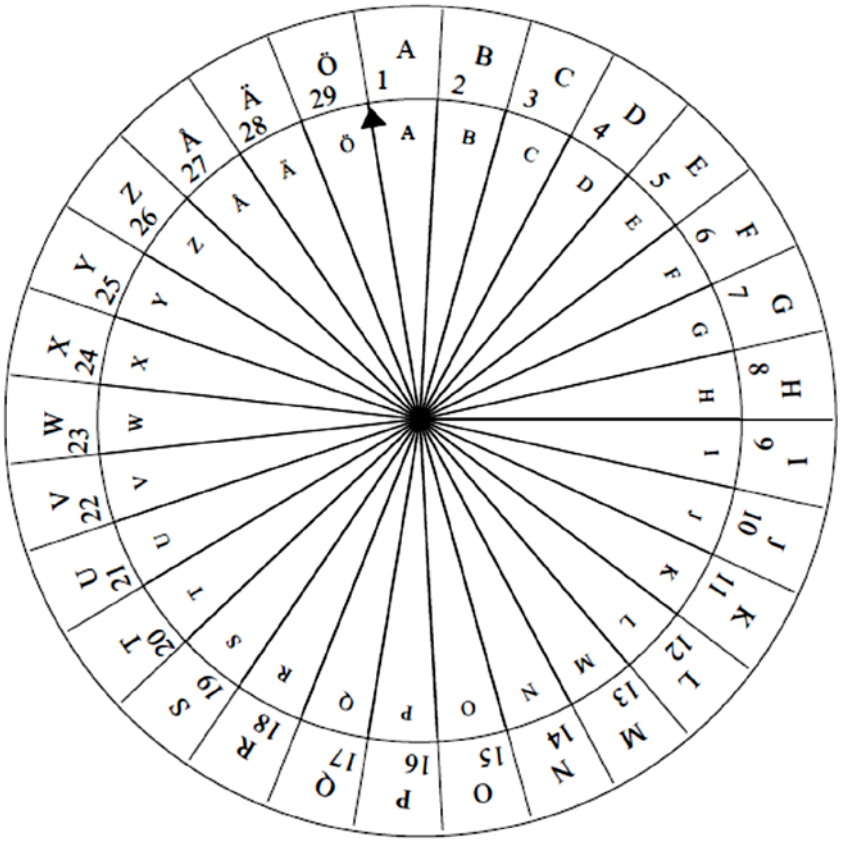
CAESARIN SALAKIRJOITUS

Caesarin salakirjoitus kantaa Julius Caesarin nimeä, koska tiedetään, että Caesar salasi armeijalleen lähettämänsä viestit, etteivät viholliset saisi niitä selville. Caesar-salakirjoitus ei ole kuitenkaan Julius Caesarin itsensä keksimä.

Salakirjoitukseen liittyy aina avain. Caesarin salauksessa suomenkielisellä aakkostolla avain on luku väliltä 1–29. Luku 1 on tosin huono avain, koska se ei muuta aakkostoa mitenkään.

Salauskiekko

Salauskiekossa ympyrä on jaettu 29:ään yhtä suureen sektoriin.
Lisää pienempään kiekkoon A-kirjaimen vasemmalla puolella olevan säteen päähän nuolenkärki.
Lisäksi kirjoita isompaan kiekkoon kunkin kirjaimen vasemmalle puolelle, säteen viereen luvut 1–29. Kirjoita luvut niin, että A:n vieressä on 1, B:n vieressä 2 ja lopulta Ö:n viereen tulee 29. Perusasennossa olevan salauskiekon kuva selventää asiaa.
Tämän jälkeen leikkaa kiekot mahdollisimman tarkkaan.
Kiinnitä lopuksi kiekot toisiinsa keskipisteestä haaraniitillä.



Salauskiekon käyttö

Salauskiekkoa käytetään seuraavasti. Salattaessa viestiä kiekkoa luetaan **kehältä keskipisteeseen päin** ja purettaessa salausta **keskipisteestä kehälle päin**.

Salaaminen

1. Käännä kiekossa oleva nuoli osoittamaan avainluvun vasemmalla puolella olevaa sädettä.
2. Muunna salattava sana vaihtamalla kirjain kerrallaan siten, että alkuperäisessä sanassa oleva kirjain katsotaan ulommalta kehältä ja sitä vastaava salattu kirjain sisemmältä.

Salauksen avaaminen

1. Käännä kiekossa oleva nuoli osoittamaan avainluvun vasemmalla puolella olevaa sädettä.
2. Muunna salattu sana vaihtamalla kirjain kerrallaan siten, että salatussa sanassa oleva kirjain katsotaan sisemmältä kehältä ja sitä vastaava salaamaton kirjain ulommalta.

Valitaan esimerkiksi avaimeksi luku 7 ja salataan sana keisari. Sana muunnetaan siis kirjain kerrallaan kehältä keskipisteeseen päin, kuten alla olevassa kuvassa on tehty. Avataan samalla avaimella salattu sana liigx. Avaaminen tapahtuu muuntamalla kirjain kerrallaan keskipisteestä kehälle päin, kuten alla olevassa kuvassa on tehty.

K	E	I	S	A	R	I	L	I	I	G	X
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
E	Ä	C	M	X	L	C	R	O	O	M	A

Tehtäviä

1. Salaa oma nimesi.
2. Salatkaa toisillenne yksittäisiä sanoja ja avatkaa parin salaamat sanat.
3. Salatkaa toisillenne jokin pidempi viesti ja avatkaa parin salaama viesti.
4. Avaa salatut viestit. Jokainen alla olevista viesteistä on salattu käyttäen eri avainlukua.
   Vinkki: jokainen viesti on salattu edellistä suuremmalla avaimella.

RÖKÖJHQINHSTRJÖMSÖÖ
ALCÖLJWUYJUIÖEEÖDYS
ÅBFÅQFUBAÅUÅFYGGL
PGVMVSGÅSDÅÄGGV

5. Miksi viestejä salataan?
6. Arvioi kuinka hyvä salausmenetelmä Caesarin salakirjoitus on?
7. Kerro kolme paikkaa, missä voit törmätä salakirjoituksiin?

Tehtävien ratkaisuja

4. Salakirjoitus kantaa (avain=2)
   Julius Caesarin nimeä (avain=9)
   koska se on keksitty (avain=13)
   hänen käskystään (avain=21)

5. Jotta ulkopuoliset eivät saisi niitä selville.

7. Esimerkiksi pankkien rahansiirtoviestit, verkkopankki, sähköpostiviestit, kännykkäpuhelut ja tekstiviestit salataan.