ALLU-salauskiekon käyttöohje ver 1.1

1 Yleistä

ALLU on salauskiekko, jolla kaukopartioradisti salasi nopeasti viestin. Kiekko on albertinkiekon sovellus. (Jos haluat tietää lisää albertinkiekosta, katso seuraava linkki:
https://www.cs.helsinki.fi/u/kerola/tkhist/k2000/alustukset/salakirjoitus/crypto.html#sec3.1

Sodan aikana päämajan kaukopartioradistien kouluttaja Matti Wihuri, OH2OH; ja sotilasmestari Alvar Ahonen kehittivät ALLU-salauslevyn sekoitetusta tritheimin taulukosta eli ns matolaatikosta.
(Tritheimin taulukko: Aakkostaulukkoon perustuva menetelmä, jossa taulukon jokainen uusi rivi muodostetaan kiertämällä edellistä riviä askeleen vasemmalle. Matriisin sarakkeilla on selväkielikirjaimisto ja riveillä avainkirjaimisto. Ks.
https://www.secmeter.com/salakirjoitusmenetelmat.html)

2 Rakenne

Allu-levy koostuu kahdesta alumiinilevystä, joiden halkaisijat ovat 12 cm ja 9 cm. Ulompi kiekko on jaettu 26 sektoriin. Alumiinikiekkojen päälle asetetaan kaksi paperista kiekkoa. Kiekkojen päällä oli kuttaperka-muovi sääsuojana

Sisemmässä kiekossa sisäkehiä on viisi.
Sisimmäinen ja ulommainen paperikiekko voitiin lukita salpajousella toisiinsa.

Ulommassa kiekossa oli kaksi riviä:
- Ensimmäisessä rivissä oli sekä selväkielimerkintöjä esim ”LeKo”, ”H-auto”, ”juna”, ”silta” että numeroita
- Toisessa rivissä oli Suomen kielen aakkoset 24 merkkinä.

Lisäksi ulommassa kiekossa oli kaksi sektorimerkintää, jolla siirryttiin käyttämää jompaa kumpaa ulommaisen kiekon riviä Sisemmässä kiekossa on viidessä rivissä sekoitettuna englannin kieliset aakkoset. Ko. aakkoset arvottiin puukuulilla joita säilytettiin kangaspussissa.

Kiekkoja valmistettiin kaksi, toinen tukikohtaan toinen kaukopartiolle.
Lisäksi tehtiin varalle vielä yhdet kiekkoparit, jos vihollinen sieppaa shifferin tms.

3 ALLU levyllä koodaaminen ja dekoodaus

ALLU levyä käytettiin näin:

Selkokielien viesti voisi olla vaikka seuraava:
”SILTA TUHOTTU”

”SILTA” on oma selväkielimerkintä ulomman kiekon ensimmäisellä rivillä sektorissa 24 (kts näköisliite)
”TUHOTTU” on normaalia salattavaa tekstiä.

Käytetään sovittua lähtötilan salpa-asetusta (joka olisi tilanne vaikka ALLU-liitteessä)

Viesti siis kuuluu **”SILTA TUHOTTU”**

Luetaan ulommankiekon ensimmäisen rivin siirtokäsky seuraavasti:
Mene sektorille 25 ja lue sisemmän kiekon **ensimmäisestä rivistä** salattu kirjain joka on **Q** (eli se tarkoittaa että mene seuraavaksi ulommankiekon ulkoriville)

Kohta ”SILTA” salataan menemällä sektorin 24 kohdalle (jossa lukee SILTA)

Salattava koodi luetaan sisemmän kiekon **toisesta rivistä.**
Salattava viesti kuuluu nyt **U**

”TUHOTTU” on normaalia salattavaa tekstiä ja siksi pitää ensin siirtyä ulommankiekon toiselle riville. Se tehdään näin:

Mene sektorille 26 ja lue siirtokäsky sisimmän kiekon **kolmannen rivin** kohdalta, joka on **Y**

Eli viesti on nyt **QUY**

Selkokielinen teksti oli **T**UHOTTU. Otetaan T kirjainta vastaava merkki **sisemmän kiekon 4 riviltä** joka on **Z**
Eli nyt salattu viesti on **QUYZ**

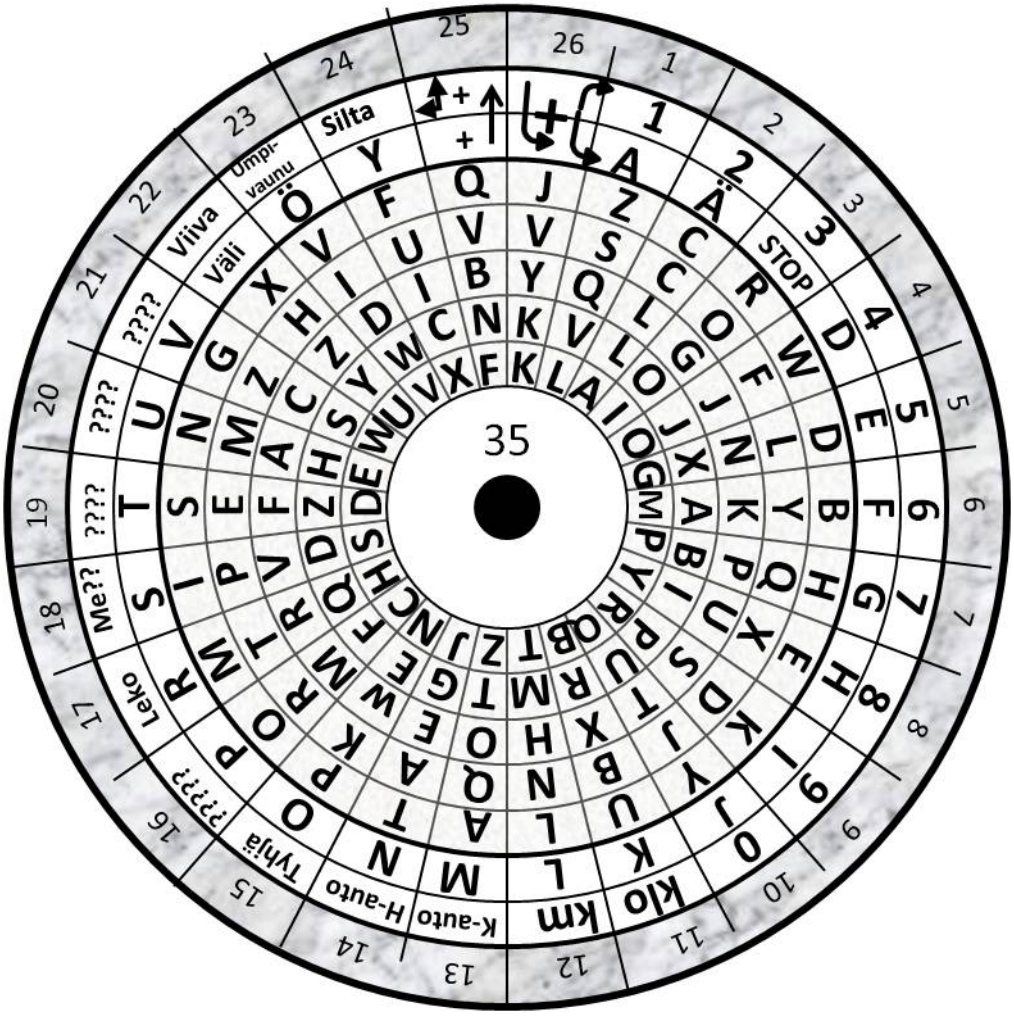
sitten tulee T**U**HOTTU joka katsottaa **sisemmänkiekon 5 riviltä** joka on E
QUYZE

Tämän jälkeen irrotetaan salpa ja siirretään sisintä kiekkoa yhden sektorin verran myötäpäivään.

Jatketaan koodausta samalla tavalla.

Vastaavasti dekoodaus tehdään lukemalla sisäkehän ensimmäiseltä sektorilta Q kirjain ja katsotaan mitä se vastaa ulokiekolla jne

Jaakko, OH8FCK


35
26
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
STOP
Silta
Umpi-vaunu
Viiva
Väli
????
????
????
Me??
Leko
¿¿¿¿
Tyhjä
H-auto
K-auto
km
klo