Rotorchiffer

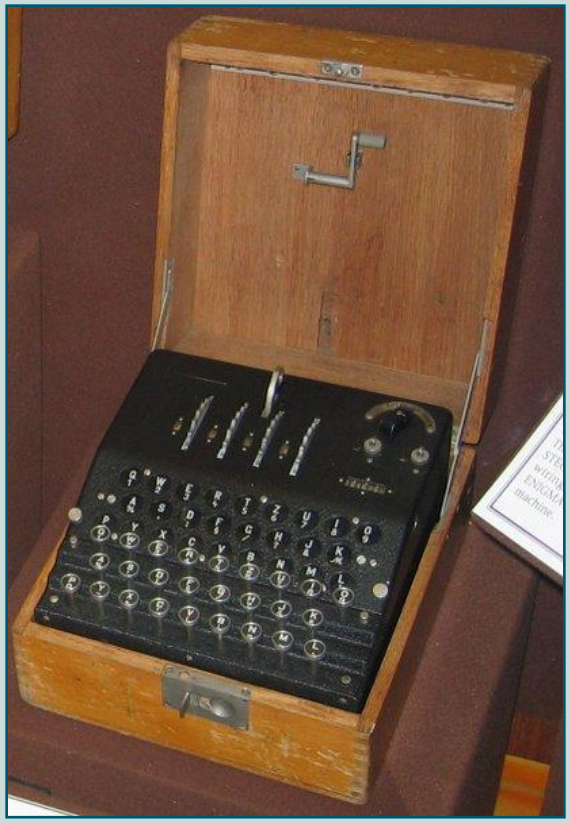
Enigma og Fialka

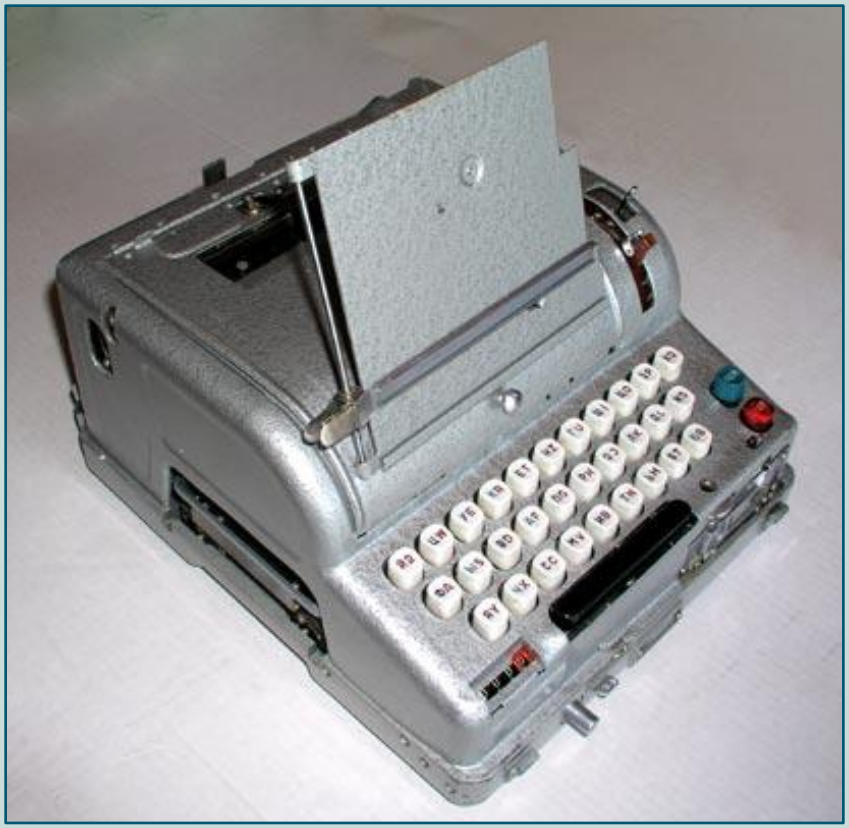
Turid Herland
Seksjon for kryptoteknologi
turid.herland@nsm.stat.no
www.nsm.stat.no

Rotorchiffer

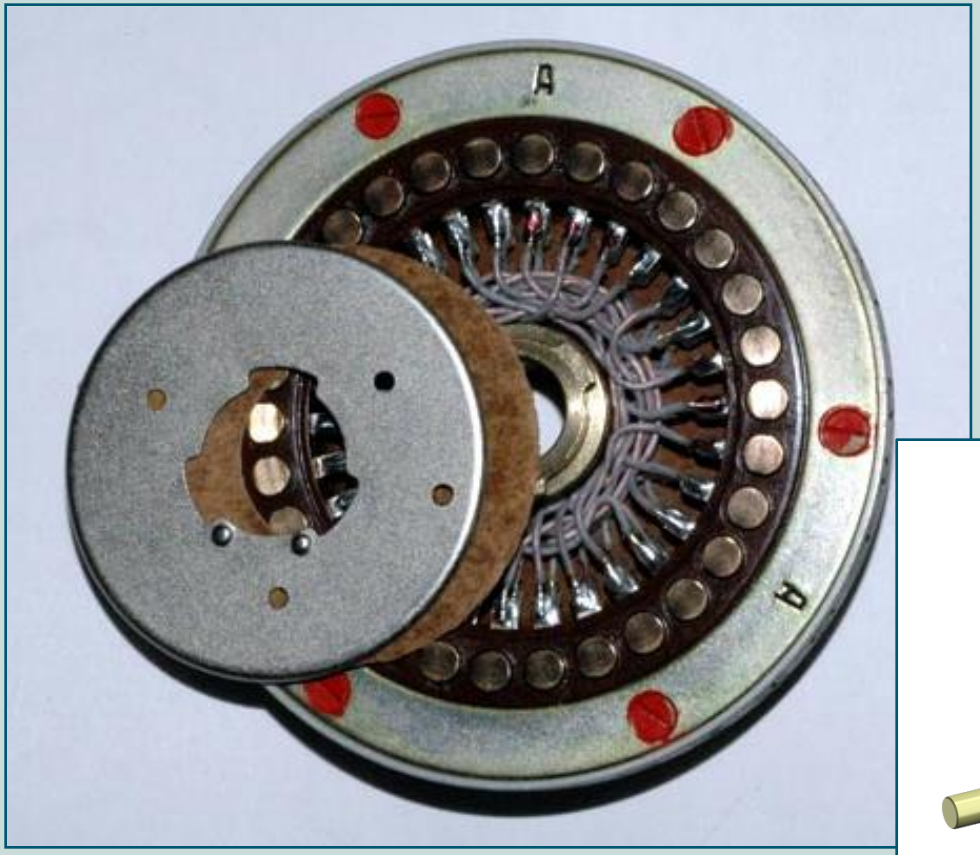
- Krypterer eit teikn om gongen.
- Polyalfabetisk substitusjonschiffer.
- Implementert i elektromekaniske maskinar.
- I bruk frå ca. 1920 til 1980-talet.

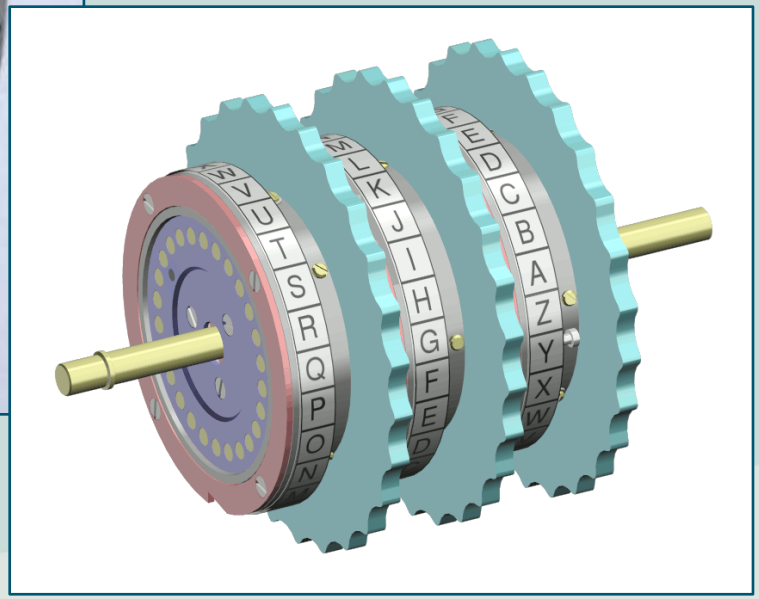
Rotormaskinar





Rotorhjul



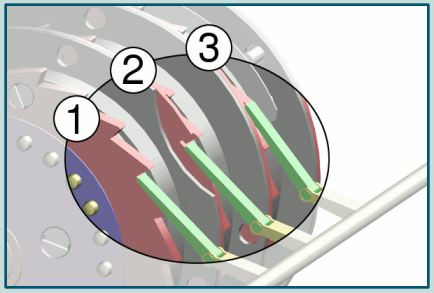


Enigma

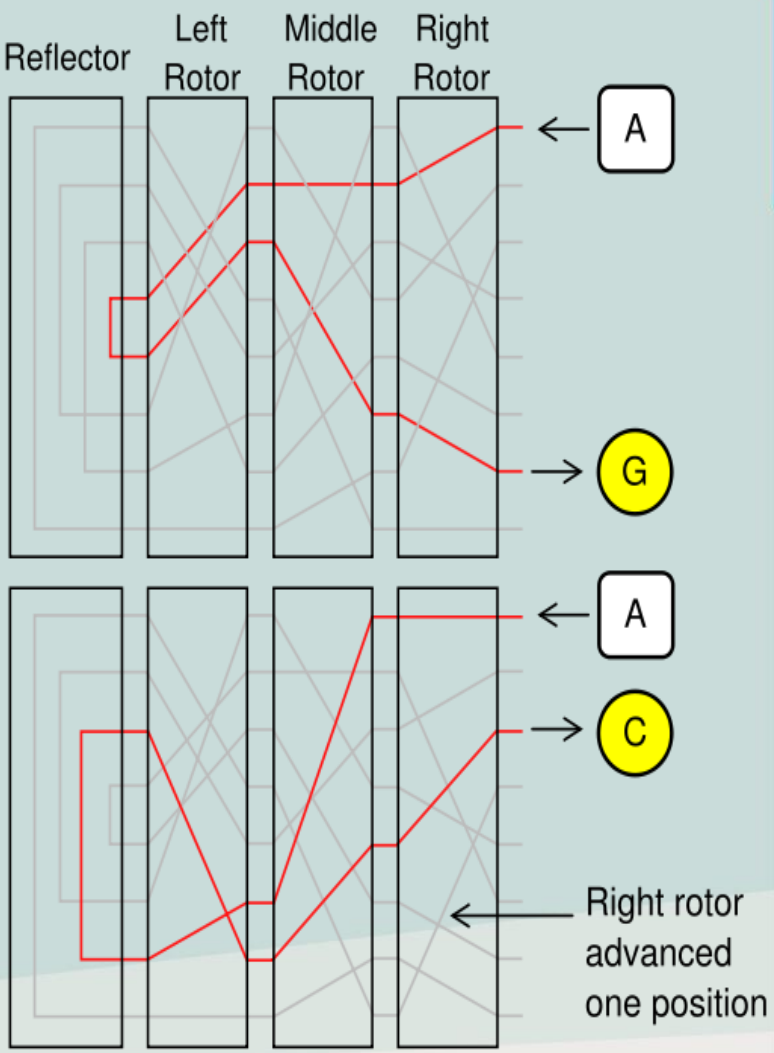
- I bruk av tyskarane før og under 2. verdskrigen.
- Trykk inn klatrekst-bokstav på tastaturet.
- Kryptert bokstav lyser opp på lampebrettet.

Enigma rotor

- 3-4 hjul.
- Første hjul roterer ein heil runde før neste hjul roterer eit steg.

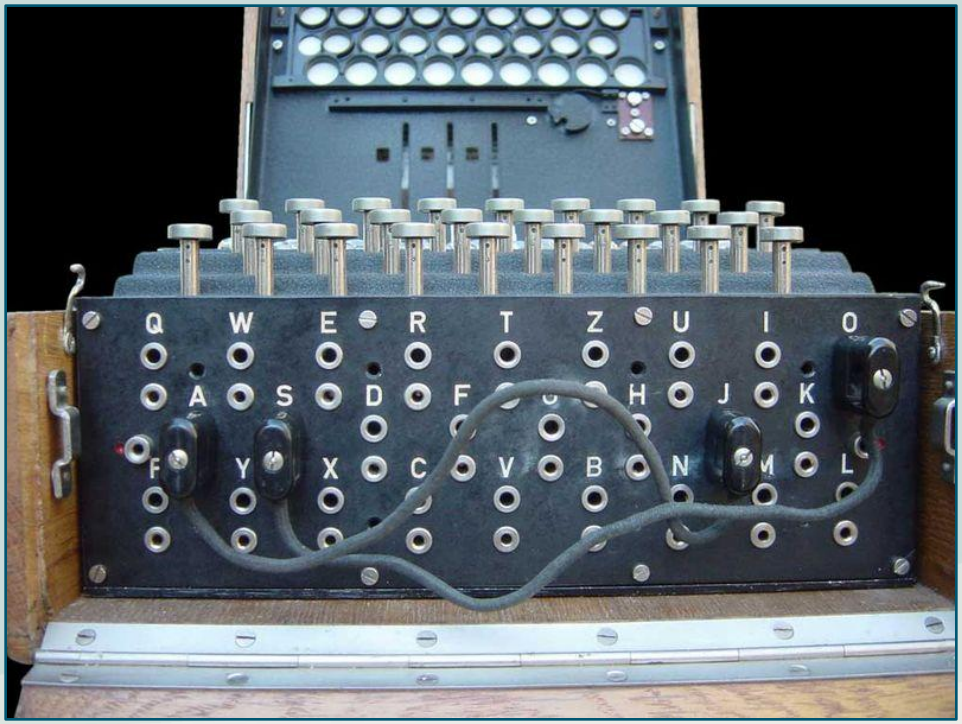


- Reflektor gjer kryptering og dekryptering til same operajson.

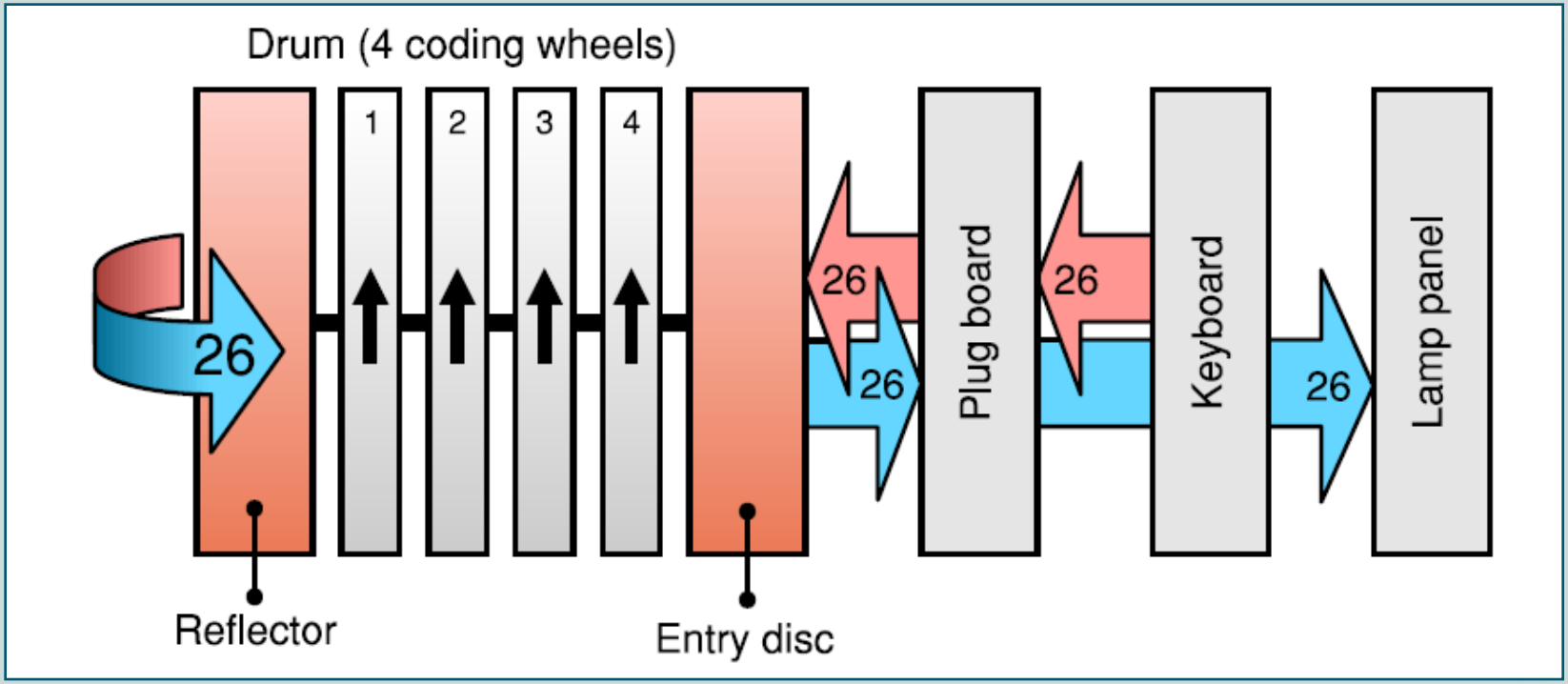


Enigma plugboard

- Enkel substitusjon mellom tastatur og rotorhjul.
- X → Y <=> Y → X.



Enigma blokkdiagram

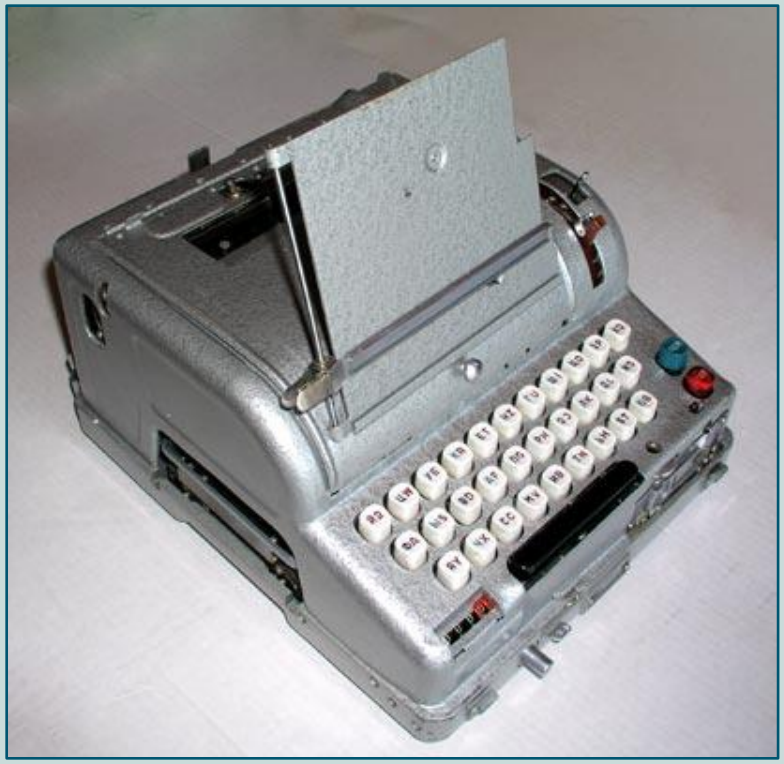


Kryptanalyse av Enigma

- Polen 1930-talet.
  - Utnytta at meldingsnøkkel blei kryptert to gonger.
  - Bygde maskinar (bomber) for å simulera Enigma.
- UK under 2. verdskrigen.
  - Reflektor gjer at ingen bokstavar kan krypterast som seg sjølv.
  - Utnytta kjente klartekstar.
  - Bygde større bomber enn Polen hadde.

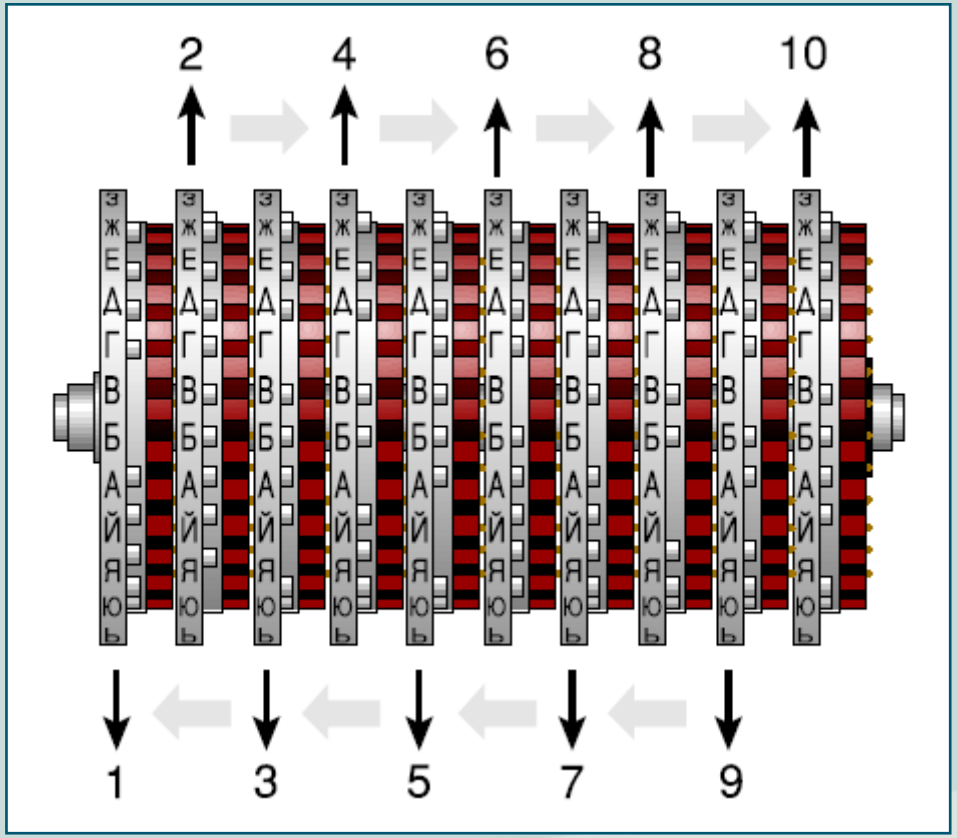
Fialka

- Russisk maskin brukt under den kalde krigen.
- Printer/puncher ut chifferteksten på papirtape.
- Kan lesa inn tekst frå tape og kryptera/ dekryptera denne.

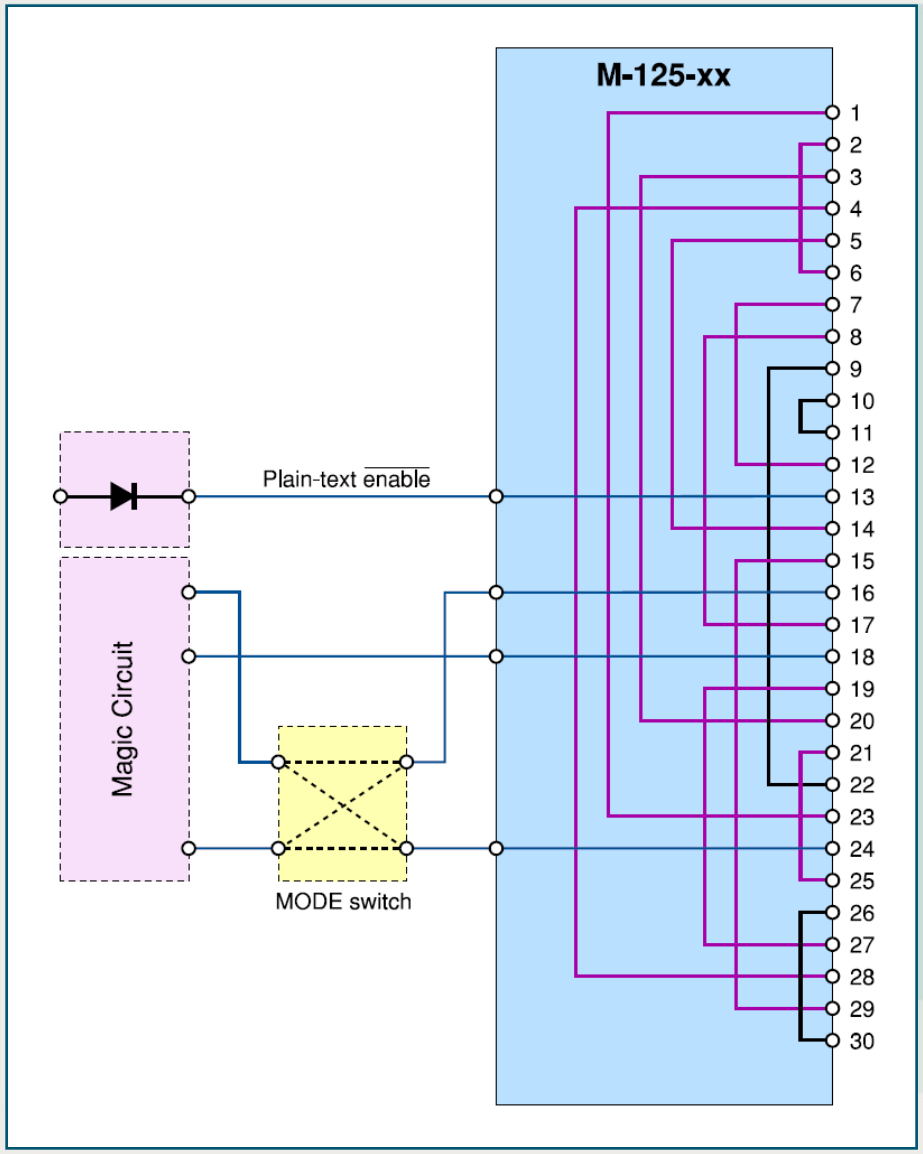


Fialka rotor

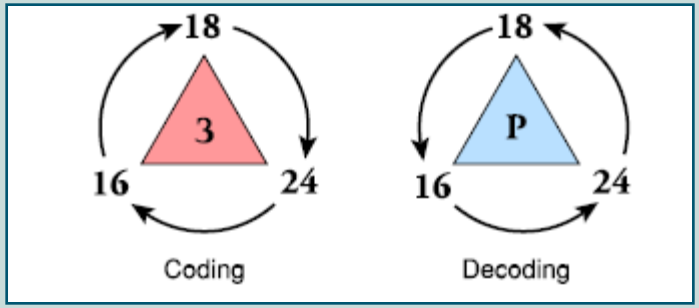
- 10 hjul, avansert rotor-system.



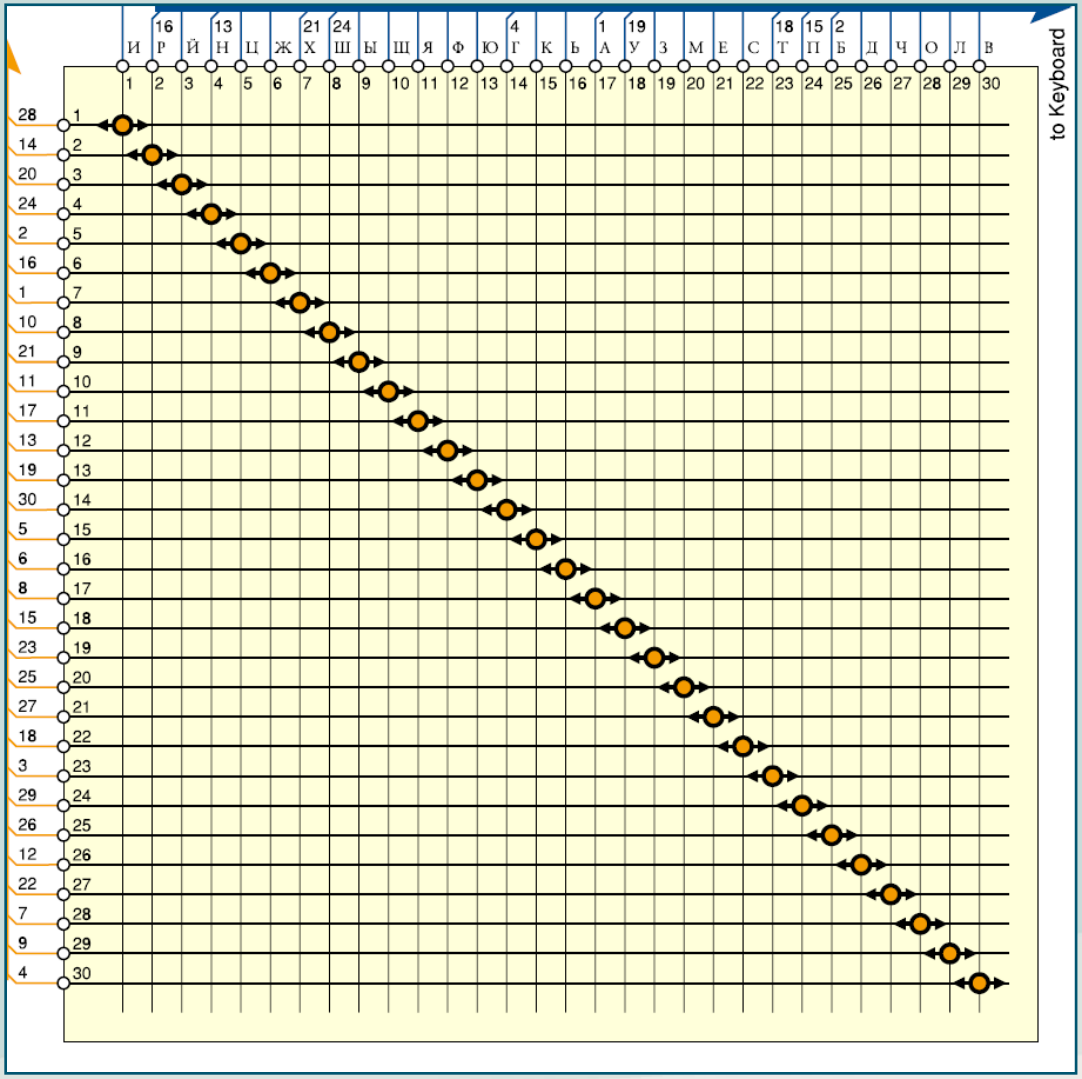
Fialka reflektor



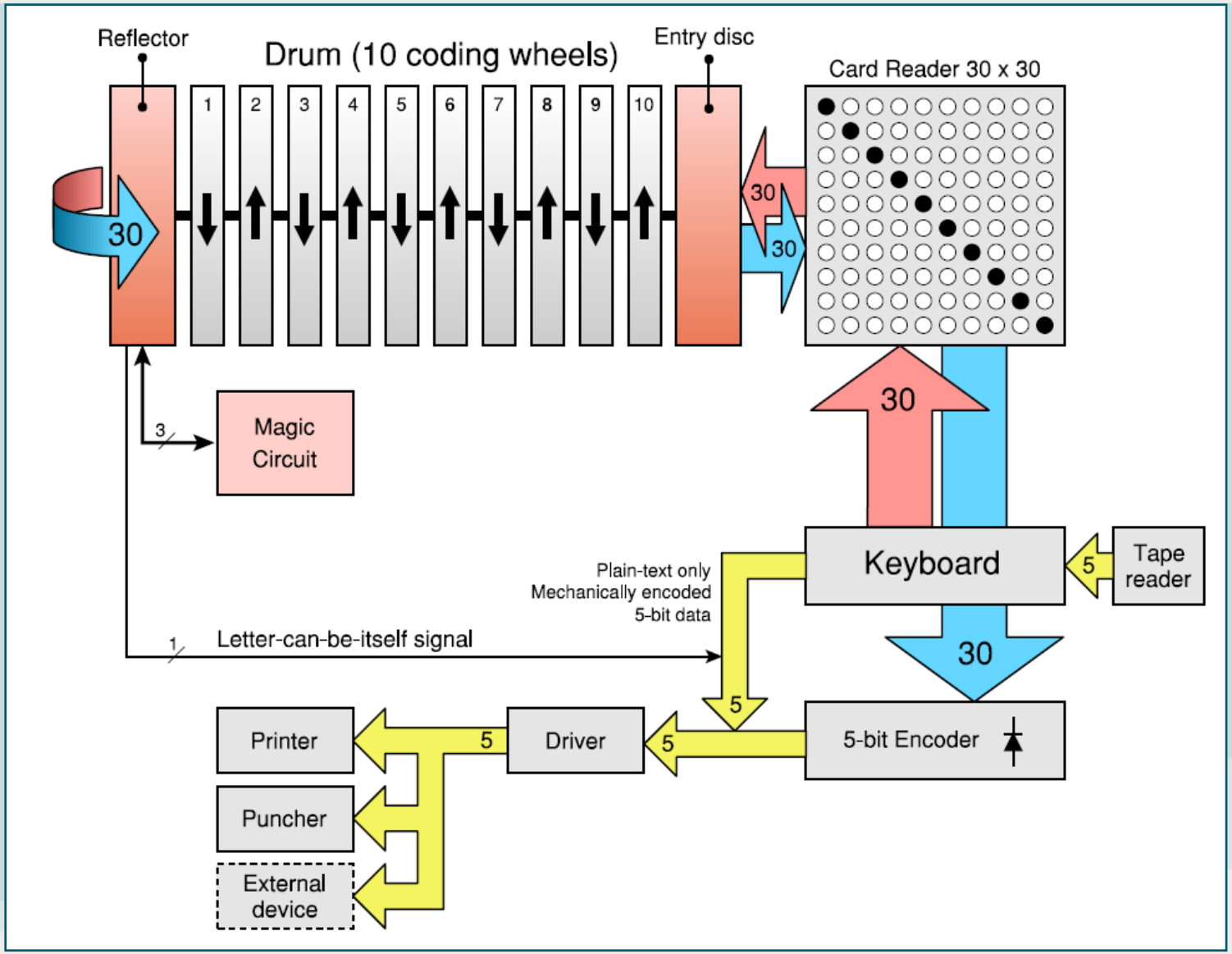
Magic Circuit



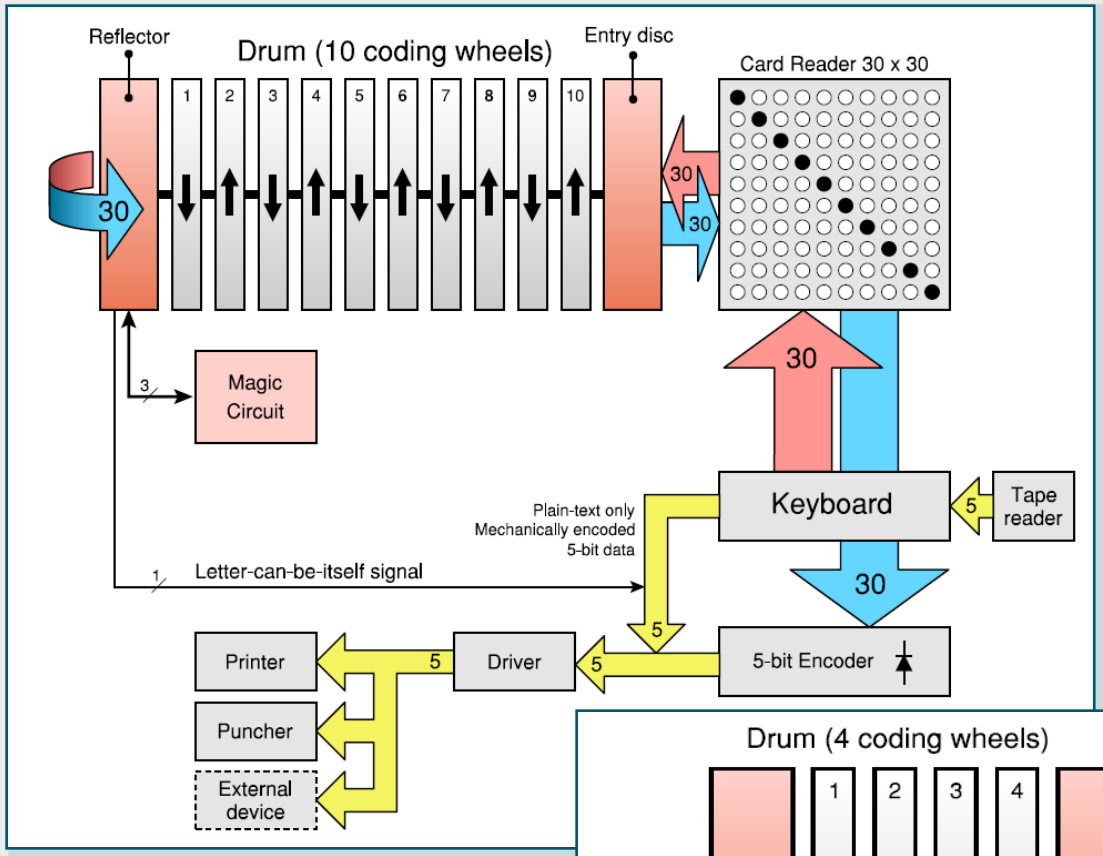
Fialka holkort



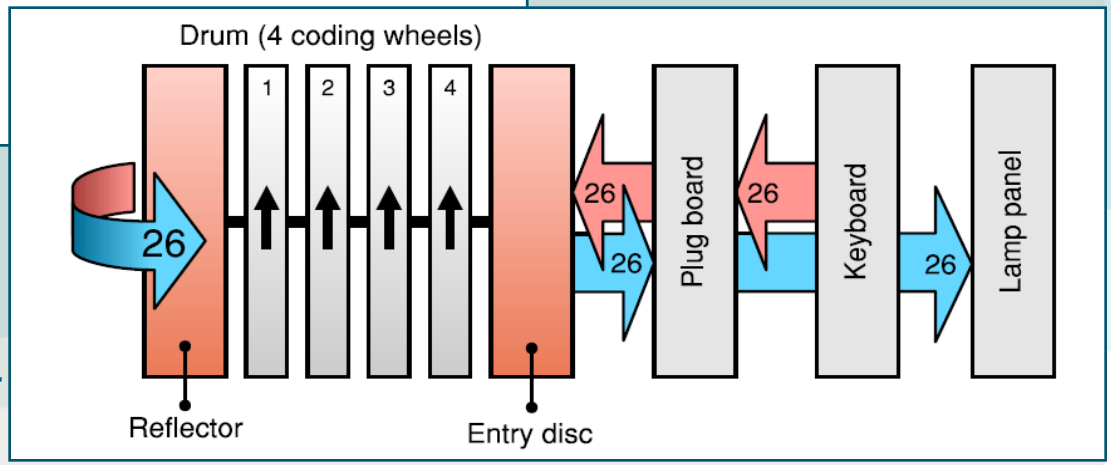
Fialka blokkdiagram



Oppsummering



Fialka



Enigma

Newton

NRK1, sundag 25.11. kl. 18.30.

”Verdens mest kjente kodemaskin, Enigma, testes.”