

MEMORANDUM EIGENSCHAPPEN CRYPTAUPHYL

1. De Cryptauphyl is een electronische volledig getransistoriseerde vercijfer/ontcijfer machine. De machine berekent uit een Klare tekst een Crypto tekst of omgekeerd. De Cryptauphyl heeft een sleutelinstelling, is dus "tapeless en rotorless".
2. De Cryptauphyl geeft een Crypto tekst die gecodeerd is in 5 elementen en die voorzien is van start en stop-elementen. De machine werkt "on-line".
3. De statistische eigenschappen van de Cryptauphyl worden nog gemeten. Een serie van 1.000.000 Cryptokarakters verkregen door vijfwerk te vercijferen is uitgeteld voor ieder der 32 mogelijke karakters met tussenresultaten per 10.000 cryptokarakters. De verdeling van de 32 maal 100 telresultaten blijkt Gaussisch te zijn.
4. Hervercijfering van dezelfde Klare tekst is onbeperkt toelaatbaar totdat het aantal Cryptokarakters is bereikt, dat uit veiligheids-overwegingen voor één sleutel-instelling als maximum wordt gesteld.
5. Omdat de Crypto tekst berekend wordt uit de Klare tekst is bij de Cryptauphyl geen sprake van een Sleutel en een Klaar-deel, zodat in het Cryptosignaal geen overgangsverschijnselen optreden die een aanwijzing voor de samenstellende delen zouden kunnen verschaffen.
6. Het Cryptauphyl systeem is gebaseerd op het ononderbroken stappen van vercijfer en ontcijfermachine. Hiertoe wordt in beide gevallen gebruik gemaakt van een eigen impulsbron.
De vercijfermachine berekent continu crypto codegroepen ook als geen codegroep van de Klare tekst wordt aangeboden.
7. De vercijfermachine is geschikt voor samenwerking met een Telexzender. Tevens is de machine voorzien van een eigen toetsenklavier, dat aanzienlijk minder ruimte inneemt dan een Telexzender.
De vercijfermachine is echter in de eerste plaats gebouwd om samen te werken met een bandlezer. Het gebruik van een bandlezer verdient verre de voorkeur boven bovengenoemde directe wijze van invoer.
8. De Cryptauphyl heeft een machinesnelheid van enkele duizenden karakters per minuut. Met een schakelaar zijn direct kiesbaar de snelheden 400 kar/min, 800 kar/min en 1600 kar/min. Naar keuze wordt

- een -

een stopelement met een duur van $1\frac{1}{2}$ element of van 1 element gebruikt.

De nauwkeurigheid van de seinsnelheid is beter dan 0,001%.

9. De machine wordt voorzien van een synchronisatiebeveiliging, die langdurige signaallose perioden kan overbruggen, waardoor de ontcijfermachine kort na terugkeer van het signaal weer slaagt in correcte berekening van de Klare tekst. (*indrukking blok*)
10. De uitgangstrappen van de als vercijfer of als ontcijfermachine gebruikte Cryptauphyl leveren een stroom van 0 tot 40 m A by 60 V.

In de punten 1 t/m 10 worden de basiseigenschappen van de machine genoemd. In een proefmodel zijn daarnaast de volgende mogelijkheden gerealiseerd.

11. De Cryptauphyl is voorzien van een schakeling voor 32 - 26 conversie. Voor réconversie 26 - 32 dient gebruik te worden gemaakt van het onder 7. genoemde Toetsenklavier. Aan het aanloopsynchronisatiesignaal van de vercijfermachine is te zien of deze in de normale mode of in de mode 32-26 werkt.

12. De Cryptauphyl is voorzien van een Onderbreking-Hervatting faciliteit.

Bij gebruik hiervan wordt het Cryptosignaal via een overeengekomen procedure vervangen door één herhaald karakter. Bij Hervatting wordt via een overeengekomen procedure teruggekeerd tot het Cryptosignaal. Voordelen van Onderbreking zijn:

1. Er wordt geen statistisch materieel in handen van een onbevoegde gespeeld als geen bericht wordt vercijferd.
 2. Mogelijkheid van RASkop (zie 13)
 3. Mogelijkheid van E.C.C.M. (zie 14)
13. RASkop is een faciliteit waardoor de mogelijkheid bestaat om (uitsluitend) tijdens een Onderbreking gegevens in niet vercijferde vorm betreffende Routing Adres en Sleutelindicator over te zenden. Er zijn maatregelen genomen om vergissingen te voorkomen. De faciliteit is geblokkeerd bij de 26 mode.
 14. Tijdens Onderbreking bestaat de mogelijkheid de uitzending van het signaal volledig stop te zetten, waarbij echter beide Cryptauphyl

- apparaten -

apparaten blijven stappen. Hierdoor wordt de mogelijkheid geopend om een in ponsband geprepareerd bericht plotseling snel (1600 kar/min) te vertcijferen en te verzenden bij verbreking van de radiostilte.

15. De Cryptauphyl-machine is geschikt om sleutelbanden te vervaardigen met een snelheid van 100.000 karakters per uur.

Physisch Laboratorium 25-11-1960