PATENT Nr 61104.

BESKRIVNING

OFFENTLIGGJORD AV

KUNGL. PATENT- OCH REGISTRERINGSVERKET.

AKTIEBOLAGET CRYPTOGRAPH,

STOCKHOLM.

Chiffreringsapparat.

(Uppfinnare: A. G. Damm.)

Klass 42: n.

Patent i Sverige från den 28 september 1923.

Föreliggande uppfinning avser en chiffreringsapparat, som på grund av sin konstruktion lämpar sig såsom portativ apparat och som gentemot hittills konstruerade portativa apparater av jämförlig art uppvisar förenkling av de mekaniska detaljerna med därav följande reduktion av tillverkningskostnad och dimensioner samtidigt med, att den medger ett förenklat handhavande och tillåter framställning av chiffer av mera komplicerad art och med längre mutationsperiod än hittills ernåtts.

Utsträckande så långt praktiskt möjligt av längden av den till grund för chiffreringen liggande serien av olika inställningar mellan chiffreringsorganen, vilken serie bestämmer de successiva möjligheterna till teckensubstitutioner under chiffreringens gång och här liksom vid alla mekaniska apparater måste bliva periodisk, är av största betydelse för chiffersäkerheten, vilken som bekant delvis beror av förhållandet mellan mutationsseriens periodlängd och längden av chiffret resp. den text, som skall chiffreras.

(Med mutationsserie menas här och i det följande den talserie, vars termer successivt angiva avstånden inom en viss normalserie »alfabet» mellan varandra i klar text och chiffer successivt motsvarande tecken.)

Utom av nyssnämnda förhållande beror chiffersäkerheten även av mutationsseriens genom företeelser i chiffret mer eller mindre framträdande regelbundenhet. Som vid begagnande av en normalserie med n tecken endast n olika termer kunna ingå i mutationsserien, måste flera eller färre av dessa i en serie av exempelvis $x \times n$ termers periodlängd upprepas ett antal gånger, och då det tydligen kan inträffa och vid fortsatt chiffrering förr eller senare måste inträffa, att upprepningar av teckenkombinationer i texten sammanfalla med upprepningar av kombinationer av termer i mutationsserien, så kunna upprepningsintervallernas faktoriala och kongruensförhållanden enligt inom cryptologien kända lagar giva vägledning för sannolikhetsslutsatser angående mutationsseriens matematiska byggnad, vilka i sin ordning kunna underlätta ett chiffers tydning av utomstående.

Bortsett från periodlängdens utsträckning är det således ett önskemål vid varje mekanisk chiffreringsapparat att dels så mycket som möjligt hindra uppkomsten av lika upprepningsintervaller, och en likformig fördelning av dessa inom mutationsperioden, dels möjliggöra primtalsintervaller och sådana, vilkas primfaktorer icke äro desamma som de, vilka ingå i apparatens mekaniska organs rörelseperioder eller bestämma nyckelorganens anordning.

Det är dessa önskemål föreliggande uppfinning avser att så långt möjligt nå. Dessutom avser den att underlätta ett snabbt och lätt utbyte av å hela chiffreringsförloppet inverkande organ resp. dessa organs olika anordning och inställning relativt varandra.

Bifogade ritning visar en utföringsform av en chiffreringsapparat enligt uppfinningen i fråga. Fig. 1 är en längdsektion och fig. 2

en vy av apparaten sedd uppifrån, delvis i sektion. Fig. 3 är en tvärsektion genom apparaten visande drivmekanismen och fig. 4 visar anordningen av kedjan, ett av apparatens en godtycklig sifferserie representerande organ.

I ett hölje 1 av till sin grundform fyrkantig tvärsektion är vridbart lagrad en axel 2, på vilken äro fästa tvenne cirkulära skivor 3, fast förbundna med varandra medelst stänger 4. Vid omkretsen av skivorna 3 äro utbytbart fästa i axiell led anordnade stavar eller lameller 5, var och en på yttersidan försedd med en teckennormalserie (ett alfabet). Det av skivorna 3 och lamellerna 5 bildade organet benämnes här nedan »cylinder».

På axeln 2 är vidare fastsatt ett tandhjul 6, i vilket ingriper en av en fjäder 7 påverkad klinka 8, vridbart lagrad å den ena armen av en tvåarmad, å axeln 2 vridbart lagrad hävstång 9, vars andra arm påverkas av en vid höljet 1 fäst fjäder 10, som strävar att hålla hävstången 9 i det i fig. 3 visade läget. Tandhjulet 6 har samma antal tänder som antalet lameller 5 å »cylindern».

På axeln 2 är därjämte roterbart lagrat ett tandhjul 11, på vars nav är fäst ett stifthjul 12, som kvarhålles av en kordongmutter 13 med låsmutter 14. I stifthjulet 12, som lämpligen kan vara sammansatt av tvenne skivor, finnas på lika avstånd anbragta, radiella urborrningar, i vilka kunna placeras stift 15. Stifthjulet är försett med en cylindrisk fläns 16, på vilken finnas tecken, ett för varje stifthål i stifthjulet 12, vars tillfälliga läge kan avläsas medelst dessa tecken genom en liten öppning 17 i höljet 1. Tandhjulet 11, som liksom tandhjulet 6 påverkas av klinkan 8, har samma antal tänder som antalet stifthål i stifthjulet 12 och detta antal är mindre än antalet tänder å tandhjulet 6. De båda tandantalen äro så avpassade i förhållande till varandra och till hävstångens 9 rörelser, att denna hävstång vid full nedtryckning från det i fig. 3 visade läget vrider tandhjulet 6 två tandlängder men tandhjulet 11 endast en tandlängd. Hävstångens 9 nedåtvridning begränsas därigenom, att klinkan 8 stöter emot ett stoppstift 18. De båda tandhjulen 6 och 11 fasthållas i sina lägen medelst en spärrfjäder 19.

Medelst stiften 15 i stifthjulet 12 påverkas ett vid omkretsen med urtagningar för stiften försett drivhjul 20, vilket är roterbart lagrat å en i ett lager 21 infäst tapp 22. På nämnda drivhjuls nav är fäst ett åttasidigt prisma 23, som tjänar till att överföra drivhjulets 20 rörelse till en kedja, sammansatt av länkar 24a och 24b av olika höjd, ordnade i enlighet med en godtyckligt vald sifferserie. Denna kedja löper kring en ställbar ledrulle 25. För varje gång ett stift 15 påverkar drivhjulet 20, vrides detta $^1/_8$ varv, varvid kedjan frammatas ett stycke lika med längden av en kedjelänk. Mot kedjan anligger mitt för prismat 23 en rulle 26, lagrad på en tapp å änden av en arm 27, som är fäst på den ena änden av en axel 28, vilken är vridbart anbragt i ett utsprång å lagret 21. Vid axelns 28 andra ände är i 90° vinkel mot armen 27 fäst en arm 29, som medelst en länk 30 är förbunden med en å axeln 2 vridbart lagrad bygel 31, vilken påverkas av en fjäder 32 på sådant sätt, att rullen 26 hålles tryckt mot kedjan 24a, 24b. När rullen 26 anligger mot en låg länk 24b, intager bygeln 31 det med heldragna linjer i fig. 3 visade läget, under det att den tvingas att intaga det med streckprickade linjer i samma figur visade läget, då rullen 26 påverkas av en hög kedjelänk 24a. I översidan av apparatens hölje finnes en långsträckt avläsningsöppning 34, som till sina dimensioner motsvarar tvenne närliggande lameller i cylindern, och bygeln 31 är så anordnad relativt nämnda avläsningsöppning, att den allt efter sitt tillfälliga läge täcker den ena eller den andra av de mitt för avläsningsöppningen befintliga lamellerna. Bygeln är på yttersidan försedd med ett alfabet (se fig. 2).

När den nu beskrivna apparaten skall användas för chiffrering, inställes »cylindern» 3, 5 medelst en på axeln 2 utanför höljet sittande kordongskiva 33 i ett överenskommet utgångsläge. Allt efter överenskommelse uppsökes före eller efter det att hävstången 9 nedtryckts en eller flera gånger den mot den första bokstaven i den givna texten svarande bokstaven i det å bygeln 31 befintliga alfabetet. Den mitt för denna bokstav befintliga bokstaven i det genom avläsningsöppningen 34 synliga cylinderalfabetet sättes såsom första tecknet i chiffret. Därefter trycker man ned hävstången 9 och söker upp det mot den andra bokstaven i den givna texten svarande bokstaven i bygelalfabetet och sätter den mitt emot denna bokstav stående bokstaven i det genom avläsningsöppningen 34 synliga cylinderalfabetet såsom andra tecknet i chiffret samt upprepar därpå samma manipulationer för varje följande tecken i den givna texten.

Att dechiffrering av med tillhjälp av den ovan beskrivna apparaten framställda chiffer kan ske, framgår därav, att de olika alfabeten vid deschiffrering komma att successivt intaga samma relativa lägen som vid chiffreringen varit fallet.

Om bygelalfabetets och cylinderalfabetens tecken hava omkastad ordningsföljd, eller om de äro godtyckligt parvis reciproka, alltså enligt någon av typerna:

I. abcdefghijklmnopqrstuvwxyz
II. zyxwvutsrqponmlkjihgfedcba
edcbazyxwvutsrqponmlkjihgf
jihgfedcbazyxwvutsrqponmlk
o. s. v.

eller:

I. abcdefghijklmnopqrstuvwxyz
II. jmkxygfplacibvzhswqutnrdeo
psjwihlfecmgkzuatvbqordnzy
o. s. v.

där I betecknar bygelalfabetet och II cylinder-

alfabeten, så kunna teckensubstitutionerna ske på alldeles samma sätt vid chiffrering och vid dechiffrering.

Äro däremot bygel- och cylinderalfabet regellöst olika varandra, måste, om vid chiffreringen teckensubstitutioner skett från bygel- till cylinderalfabet, motsvarande dechiffreringssubstitution ske från cylinder- till bygelalfabet, och vice versa.

För att kunna klargöra apparatens verkningssätt i anseende till den till grund för chiffreringen liggande mutationsserien antages i det följande för enkelhets skull, att alla cylinderalfabeten uppvisa omvänd teckenföljd mot bygelalfabetet i inbördes förskjutningar motsvarande alfabetens ordningsföljd runt om cylindern mot dennas rörelseriktning räknat.

Vid den ovan beskrivna apparaten kan naturligtvis tillämpas vilken delning som helst av cylindermanteln i olika antal alfabetlameller, men ett udda antal bör av lätt insedda skäl väljas. Vissa av dessa lameller kunna på godtyckliga ställen utelämnas eller icke vara försedda med alfabet. Är så fallet, kan det vid vissa tillfällen inträffa, att avläsningsöppningen frånsett bygelalfabetet blir tom, varvid hävstången 9 måste nedtryckas två eller flera gånger efter varandra, innan någon teckensubstitution kan äga rum.

Här antages nu t. ex. att cylindern har 29 lameller och att alfabeten nr 7 och 12 äro utelämnade, så att vid vila av bygeln 31 och cylinderns stegvisa matning 2 steg åt gången alfabeten med början vid 1 skulle successivt visa sig i avläsningsöppningen i ordningsföljden:

1, 3, 5, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 2, 4, 6, 8, 10, 14, 16, 18, 20, 22, 24, 26, 28, 1, 3, 5, 9 .....

och under de gjorda antagandena giva upphov till en mutationsserie lika med denna talserie.

Om emellertid bygeln 31, som antages från början hava befunnit sig i det i fig. 2 med heldragna linjer visade läget, ändrar läge t. ex. vid första cylinderrörelsen, så kommer icke alfabetet n:r 3 utan i stället n:r 4 att bliva synligt i öppningen. Stode bygeln vid nästa manipulation stilla, skulle följaktligen alfabetet n:r 6 bliva synligt, under det att vid bygelns ombyte av läge, detta bleve fallet med alfabetet n:r 5. Bygelns rörelse tjänar således normalt att åstadkomma alldeles samma verkan i avseende på de relativa förflyttningarna mellan bygel- och cylinderalfabet, som om cylindern vrede sig omväxlande 2, 3 eller 1 steg. Men som ju dessutom tomrum å cylindern kunna nödvändiggöra en eller flera extra minapulationer, och denna (tomrummens) effekt icke är konstant utan beroende på bygelns tillfälliga läge, d. v. s. på sammansättningen och det tillfälliga läget av kedjan 24a, 24b, vilket läge i sin ordning beror av anordningen och det tillfälliga läget av stifthjulet 16, så inses, att en oerhört komplicerad alfabetväxlingsserie vid utnyttjande av dessa förhållanden kan uppstå, vars beskaffenhet icke kan uttryckas genom någon allmängiltig, analytiskt användbar formel, emedan samma verkan kan hava flera olika orsaker.

Så t. ex. kunna avläsningar å alfabet n:r 1 och 5 omedelbart efter varandra bero på vilket som helst av nedanstående antaganden:

a) cylindermatning från 1 till 3, tomrum å 3, extra manipulation med matning till 5, varvid kedjan antingen kan stå stilla eller hava två lika länkar efter varandra,

b) cylindermatning från 1 till 3, varvid kedjan växlar från hög till låg länk, vilket ger avläsningsläget 4, tomrum å 4, extra manipulation med matning till 5, som blir avläsningsläge, emedan kedjan ånyo växlar från låg till hög länk,

c) cylindermatning från 1 till 3 med avläsningsläget 2 på grund av kedjeväxling från låg till hög länk, tomrum å 2, extramanipulation med matning till 5, som blir avläsningsläge på grund av kedjeväxling från hög till låg länk.

Att rena primtalsintervaller kunna uppkomma inom en på dylikt sätt erhållen mutationsserie, vilken i verkligheten icke behöver vara identisk med alfabetens avläsningsföljd, emedan den beror icke blott av deras godtyckliga förskjutningar sinsemellan utan även av deras eventuellt olika beskaffenhet, torde inses utan utförligt bevis.

Under förutsättning att cylindern har ett udda antal $2N + 1$, lameller, att stiftskivan är anordnad för S stift och att kedjelänkantalet är K samt att dessa tal icke hava någon gemensam faktor, blir periodlängden $P = (2N + 1)$ S.K manipulationer, och om ett visst antal tomrum T förefinnes å cylindern blir $P = (2N + 1 - T)$ S.K teckensubstitutioner, emedan givetvis periodicitet kan uppkomma, först sedan alla chiffreringsorgan återkommit i sina utgångslägen relativt varandra.

De delar i den ovan beskrivna apparaten, som inverka på chiffrets sammansättning, äro lätt och bekvämt åtkomliga för omflyttning eller utbyte. För detta ändamål äro höljets gavlar 34, 36 anordnade som borttagbara lock, varjämte den sida av höljet, som ligger närmast kedjan 24a, 24b, är uppfällbar kring gångjärn 37. När ordningsföljden av cylinderns alfabetlameller skall ändras, borttages kordongskivan 33, varefter gaveln 34 avlägsnas. Därefter borttages ett stift 35, som låser cylindern på axeln 2, varefter cylindern uttages. När stiften 15 i stifthjulet 12 skola omflyttas, bortskruvas muttrarna 14 och 13, varefter gaveln 16 avlägsnas och stifthjulet 12 uttages.

Patentanspråk:

Chiffreringsapparat, vilken är försedd med ett roterbart organ, å vilket finnas flera normalserier med sinsemellan växlande teckenföljd, vilka serier äro anordnade att i oregelbunden följd bringas att bliva synliga, en i

sänder, i en avläsningsöppning utmed en normalserie, från vilken chiffreringen sker, bokstav efter bokstav, kännetecknad därav, att sistnämnda normalserie är anordnad på ett med det roterbara organet (3, 5) koncentriskt anbragt, fram och åter under den med avseende på sin storlek tvenne bredvid varandra liggande normalserier å det roterbara organet (3, 5) svarande avläsningsöppningen (34) rörligt organ (31), som i sina ändlägen täcker den ena eller den andra av de samtidigt under avläsningsöppningen befintliga normalserierna å det roterbara organet, och vars tillfälliga läge är beroende av ett i enlighet med en godtycklig sifferserie anordnat, rörligt organ (24a, 24b), exempelvis en kedja med länkar av olika form, vilket är anordnat att påverkas av ett för hand roterbart, likaledes i enlighet med en godtycklig sifferserie anordnat organ (12, 15), exempelvis ett pinnhjul, som för varje chiffreringsoperation vrides en viss vinkel genom vridningen av det ett flertal normalserier uppbärande roterbara organet (3, 5), som är anordnat att vridas för hand för varje chiffreringsoperation en sådan vinkel, att en ny normalserie å detsamma blir synlig i avläsningsöppningen.

(Härtill en ritning.)

Stockholm 1926. P. A. Norstedt & Söner

Offentliggjord den 6 juli 1926.

Till Patentet N:o 61104.

Fig. 1.

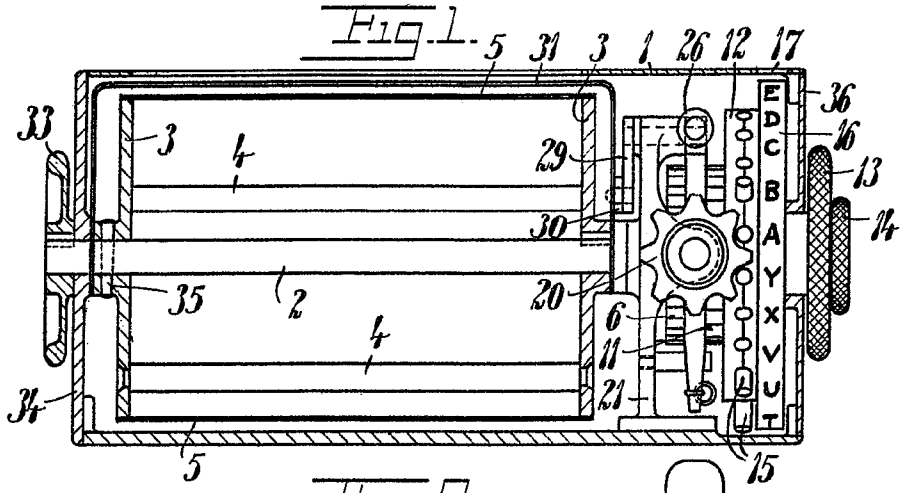


Fig. 2.

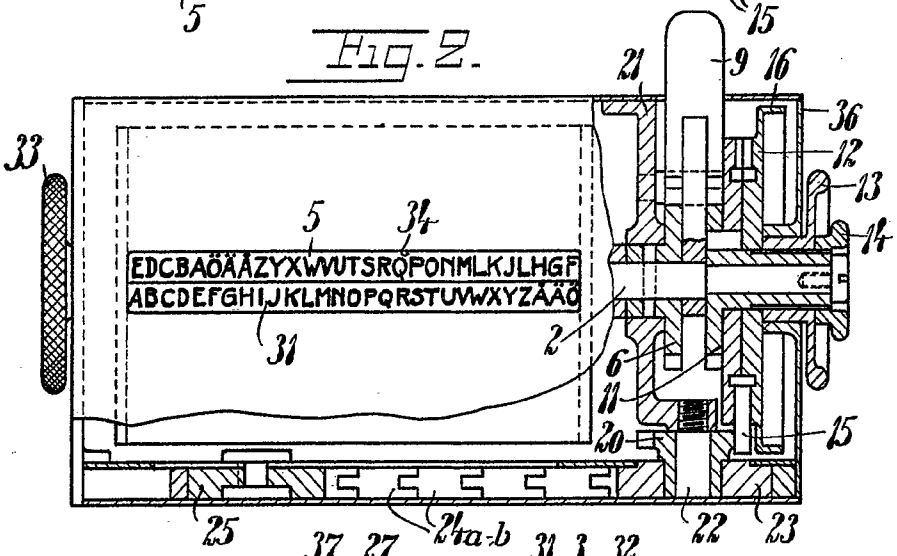


Fig. 3.

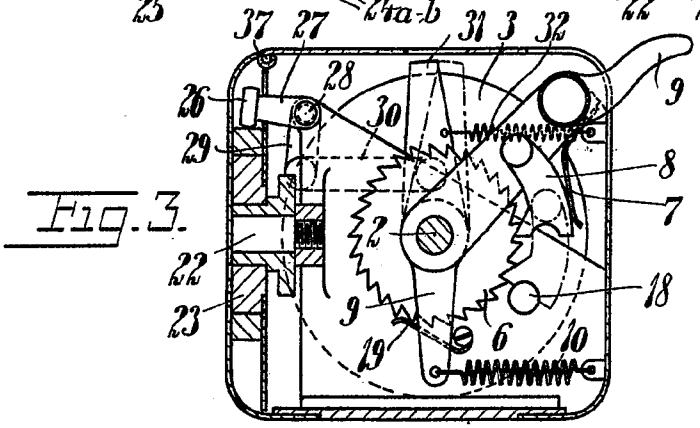
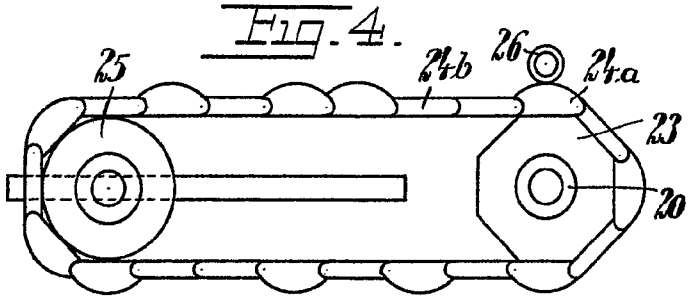


Fig. 4.



Generalstabens Litografiska Anstalt