SVERIGE

PATENT- OCH
REGISTRERINGSVERKET

UTLÄGGNINGSSKRIFT nr 348 067
Int Cl G 09 c 1/06

P.ans. nr 524/70 Inkom den 16 I 1970
Giltighetsdag den 16 I 1970
Ans. allmänt tillgänglig den 17 VII 1971
Ans. utlagd och utläggningsskriften publicerad den 21 VIII 1972
Prioritet ej begärd

AB TRANSVERTEX, VÅRBY
Uppfinnare: B Florin, Hägersten
Ombud: N Larfeldt

Chiffreringsapparat särskilt för lösensignalering

Uppfinningens ändamål är att åstadkomma en apparat för chiffrering av en klartext, vilket chiffer är praktiskt omöjligt att dechiffrera.

En sådan apparat är närmast tänkt för lösensignalering, exempelvis mellan två radiostationer, varvid vardera radiostationen förfogar över en apparat. Lösensignaleringen går till så, att vardera radiostationen på sin resp. apparat - apparaterna förutsätts vara lika grundinställda - ställer in samma klartext; därefter låter båda radiostationerna med sina apparater chiffrera denna klartext och skall då få fram samma chiffer - apparaterna är lika inställda. Utväxlingen av lösen går sedan lämpligen till så, att den ena radiostationen uppger den ena hälften av chiffret och den andra radiostationen den andra hälften av chiffret. Eftersom båda radiostationerna har tillgång till hela chiffret kan bägge kontrollera att motstationen avgivit rätt lösen. Någon dechiffrering behöver således aldrig göras.

Genom att apparaten enligt uppfinningen erhållit de i patentkrav 1 angivna kännetecknen, har erhållits en sådan särskilt för lösensignalering lämpad chiffreringsapparat. Genom bl.a. de i patentkravet 1 angivna enheternas koppling i ändlös serie med varandra kommer minsta ändring av klartexten att medföra en genomgripande ändring av chiffret. För varje ny klartext kommer ett radikalt ändrat nytt chiffer att er-

hållas. Det torde även vara praktiskt omöjligt att genom systematiska studier av samhörande klartexter och chiffer få kännedom om den nyckel apparaten arbetar efter.

Lämpligen används vid apparaten en klartext, som utgörs av en timangivelse, en minutangivelse och två bokstäver. Vid tidpunkten för lösensignaleringen ställs härvid denna tidpunkt, exempelvis 09 16 in på bägge apparaterna liksom två bokstäver ur någon av de korresponderande radiostationernas anropssignaler, exempelvis F K. Därefter låts bägge apparaterna chiffrera denna klartext, varvid chiffret exempelvis blir D G Y D. Lösen utväxlas härvid genom att ena stationen säger DG och den andra YD. Ändras klartexten så litet det går, exempelvis bara till 09 18 F K ändras chiffret genomgripande, exempelvis till K K P B. Genom att använda tidpunkten för lösenutväxlingen som del av klartexten elimineras risken att samma klartext (och därmed samma chiffer) används mer än en gång per dygn. En gång per dygn ställs därför lämpligen apparaternas inre inställningar om så att ständigt nya chiffer erhålls.

På ritningen visas utföringsexempel på uppfinningen.

Fig. 1 visar en vy av ett rent mekaniskt utföringsexempel på chiffreringsapparaten och fig. 2 visar i snitt II-II av fig. 1 hur i apparaten ingående spärrarmar påverkar ett stoppklacksförsett hjul och hur ett i apparaten ingående hjul fås att matas fram av ett annat hjul. Fig. 3 visar i perspektiv ett kulförsett hjul och fig. 4 snitt IV-IV av fig. 1. Fig. 5 visar ett kopplingsschema för apparaten i elektronikutförande.

På en axel 32 är 4 inställningshjul 19-22 och 4 påverkningshjul 2-5 anordnade. På varje inställningshjul, som kan ställas in i 26 olika jämnt fördelade vinkellägen 40 (fig. 3) med vinkeln $\alpha = 360^{\circ}:26$ mellan vinkellägena är sammanlagt 26 stycken kulor 18 anordnade i 6 stycken kransar 41 på så sätt att det alltid finns en kula i varje vinkelläge. Kulorna kan flyttas om axiellt inom samma vinkelläge 40 från en krans 41 till en annan på det sätt man önskar.

Kulorna i varje krans 41 avkänns av en spärrarm 12-17. Med spärrarmarnas andra ände samverkar ett av påverkningshjulen, som vart och ett har 6 stycken axiellt fördelade, vardera med en stoppklack 6-11 försedda partier. Varje kulkrans på inställningshjulet samverkar via en spärrarm med ett stoppklackförsett parti på påverkningshjulet. Spärrarmarna är vridbart lagrade på en axel 34.

På vartdera av inställningshjulen 21 och 20 är anordnad en sifferkrans 24 resp. 25 för tidsnummer och en bokstavskrans 28 resp. 29 med ett

oordnat alfabet. På inställningshjulet 19 finns två bokstavskransar, en med ett ordnat och en med ett oordnat alfabet 26 resp 30. Till inställningshjulet 22 hör på axelns 32 högra ände anordnade bokstavskransar 27, 31, som via kugghjulen 36, 37, axeln 24' och kugghjulen 38, 39 är så kopplade till inställningshjulet 22, att vid vridning av bokstavskransarna 27, 31 inställningshjulet 22 kommer att vrida sig lika mycket. Bokstavskransen 27 har ett ordnat och bokstavskransen 31 ett oordnat alfabet.

Initialinställningen utförs genom att inställningshjulen 19 och 22 med tillhjälp av de ordnade alfabeten 26 och 27 inställs på den önskade stationssignalen och inställningshjulen 21 och 20 på tidsnumret med tillhjälp av sifferkransarna 24 och 25. Lösen består av två bigram, som avläses på inställningshjulens oordnade alfabet 28-31 efter ett förutbestämt antal fram- och återgående vridningar på vredet 1 mellan av stopp 42 (fig 4) och en arm 43 på axeln 32 bestämda vinkellägen.

Påverkningshjulen 2-5 är så anordnade på axeln 32 att de när vredet 1 vrids medurs följer med på grund av friktionen (kulan 44 som av en fjäder 45 trycks mot axeln 32) mot axeln 32, som vredet 1 är fastsatt på. Den vinkel som exempelvis hjulet 5 tillåts följa med axeln bestäms av stoppklackarna 6-11 och en grupp spärrarmar 12-17. De tre övriga påverkningshjulen 2-4 har motsvarande egna stoppklackar och spärrarmsgrupper. I varje grupp spärrarmar är endast en arm påverkad av en kula på så sätt att armens andra ände kommer in i sin stoppklacks verksamhetsområde.

Inställningshjulen 19-22 är så anordnade på axeln 32 att de när vredet 1 vrids medurs kommer att stå stilla. En av stoppklackarna på vart och ett av de 4 påverkningshjulen kommer att stoppa mot 4 av de 24 spärrarmarna. Till varje påverkningshjul hör en matarhake 23, som arbetar mot en med ett inställningshjul fast förbunden 26-delad matarskiva 33 (fig 2). När ett påverkningshjul av axeln 32 vrids medurs, följer matarhaken 23 med och hämtar lika många steg på tillhörande inställningshjuls matarskiva 33. På detta sätt kommer hjulen att arbeta i par, så att exempelvis påverkningshjulets 5 matarhake kommer att samarbeta med inställningshjulets 21 matarskiva. Övriga sådana hjulpar är 4, 20; 3, 19 resp 2, 22.

I nästa moment av operationen vrids vredet 1 moturs. Därvid följer på grund av friktionen mot axeln, påverkningshjulet med, varvid matarhaken 23 medbringar inställningshjulet lika många steg som stoppklackarna vid förra momentet kunde röra sig innan de stoppades av spärrarmarna.

Frammatningen av inställningshjulen gör att 4 nya kulor kommer att påverka 4 av de 24 spärrarmarna som förs fram i sina resp stoppklackars verksamhetsområde.

Vid därpå följande vridning medurs avsöks dessa spärrarmar och matarhakarna 23 hämtar lika många steg på inställningshjulen som stoppklackarna har att vrida sig innan de träffar spärrarmarna.

Under nästa moment vrids vredet 1 moturs och inställningshjulen matas fram till en ny position med följd att fyra nya kulor 18 kommer att påverka spärrarmarna.

Som synes bygger lösenapparatens princip på att dess frammatande delar hela tiden påverkar förutsättningarna (inställningshjulets inställning) för nästa moments frammatning. För att alla hjulen skall få samma oregelbundna frammatning har hjulen sammankopplats till en ring genom överföring saxeln 24. Påverkningshjulet 2 kommer alltså att mata fram inställningshjulet 22. Ett tillräckligt antal vridningar på vredet 1 förorsakar således att de initialinställningar som görs av inställningshjulen före varje lösenutväxling kommer att påverka samtliga inställningshjuls frammatning.

Såväl inställningshjul som påverkningshjul och deras inbördes förbindelser och drivningen av hela anordningen kan givetvis elektroniseras, dvs ersättas med elektroniska element och kopplingar.

Ett exempel på apparaten i elektronikutförande visas på fig 5.Här är varje hjulsats 2,19;3,20;4,21 resp 5,22 ersatt av inbördes lika uppbyggda elektronikenheter 51,61,71 resp. 81. Enheterna uppvisar vardera ett skiftregister 52,62,72 resp 82, vartdera lämpligen på känt sätt uppbyggt av en serie bistabila vippor nr 1-26. Varje skiftregister är tillordnat en lamprad 53,63 ,73 resp 83. Primärinställningen av tid och stationssignal verkställs med tillhjälp av strömbrytare 54,64 ,74 resp 84. Skiftregisterna, som har ett steg polvänt, matas fram steg för steg genom slutning av resp strömbrytare 54,64,74 och 84. Lampraderna, som styrs av resp. skiftregister, kommer på grund av det polvända skiftregistret att ha endast en lampa tänd och genom manövrering av resp strömbrytare kan den tända positionen flyttas. På vänster sida om lampraden 53 finns timangivelserna och på höger sida det oordnade alfabetet. Vid primärinställningen av enheten 51 stegas den tända positionen fram till önskat timtal (som är 04 enligt exemplet på fig 5, dvs lampan vid 04 är tänd) med strömbrytaren 54. På samma sätt sker primärinställning medelst övriga skiftregister 62,72, och 82. Lampraden 63 anger minuter och lampraderna 73 och 83 anger tillsammans bigrammet för stationssignalen. Efter avslutad primärinställning skall denna krypteras, vilket utförs genom slutning av en för alla enheterna gemensam strömbrytare 91 ett på förhand bestämt antal gånger, som vid appa-

raten enligt fig 1 motsvarar vridningen av vredet 1 ett bestämt antal gånger. Vid varje slutning av strömbrytaren 91 matas skiftregisterna 52, 62,72 och 82 enligt exemplet i fig 5 fram lika många steg som de av de polvända skiftregisterna nr 5,7,10 och 25 utvalda räknarna 106,110,113 och 120 anger. Under skiftregistrens frammatning får inga nya räknare väljas ut, varför samtliga räknare är spärrade då strömbrytaren 91 sluts, men när strömbrytaren 91 öppnas igen, blir det möjligt för de polvända skiftregisterna att ånyo välja ut fyra räknare analogt med den första vridningsrörelsen med vredet, som vid nästa slutning av strömbrytaren 91 ger frammatning av skiftregisterna 52,62,72 och 82. Räknarnas 101-124 funktion motsvaras vid apparaten enligt fig 1 av stoppklackarnas 6-11 funktion.

Efter tryckning ett på förhand bestämt antal gånger på strömbrytaren 91 har de fyra tända positionerna på lampraderna 53,63,73 resp. 83 förskjutits ett antal steg, och de bokstäver i de oordnade alfabeten, som nu kan avläsas intill de tända positionerna, utgör lösen.

Patentkrav:

1. Chiffreringsapparat, särskilt för lösensignalering, k ä n n e t e c k n a d av minst två enheter (2,19; 3,20; 4,21; 5,22 resp. 51; 61; 71; 81), som var och en innefattar en framstegningsbar inställningsanordning (19-22 resp. 52; 62; 72; 82) och ett flertal räknare (6-11 resp. 101-124), varvid varje inställningssteg hos inställningsanordningen är kopplat till en räknare och enheterna är kopplade i en ändlös serie med varandra genom överföringsorgan mellan räknarna hos en enhet och inställningsanordningen hos den efterföljande enheten, vilka överföringsorgan efter inställning av resp. enheters inställningsanordningar är i stånd att överföra en framstegning av resp. inställningsanordning det antal steg, som bestäms av den för tillfället verksamma räknaren i den närmast föregående enheten i serien.

2. Apparat enligt krav 1, k ä n n e t e c k n a d av att för varje enhet (2,19;3,20; 4,21; 5,22) inställningsanordningen utgörs av ett med kulor, stift eller liknande ställbara lyftelement (18) försett, i vridled framstegningsbart inställningshjul (19-22) och räknarna innefattar stoppklackar eller liknande stoppelement (6-11) hos ett vridbart påverkningshjul (2-5), att varje inställningssteg hos inställningshjulet (19-22) direkt eller via spärrarmar (12-17) är tillordnat ett stoppelement (6-11) i enheten, och att överföringsorganen innefattar medbringarorgan (23) mellan påverkningshjulet i en enhet och inställningshjulet i en efterföljande enhet, varvid de i apparaten in-

gående elementen är så kopplade till varandra och ett åt båda håll vridbart vred (1), att vid vridning åt ena hållet samtliga inställningshjul (19-22) kommer att stå stilla och samtliga påverkningshjul (2-5) kommer att vridas en vinkel, som bestäms av de för tillfället verksamma stoppelementen (6-11) och vid vridning åt andra hållet inställningshjulen (19-22) av medbringarorganen (23) kommer att vridas samma vinkel som påverkningshjulen (2-5) vreds i föregående moment.

3. Apparat enligt krav 1 eller 2 med fyra inställningsanordningar resp. inställningshjul, k ä n n e t e c k n a d av att två av inställningsanordningarna resp. inställningshjulen är tillordnade en sifferrad (24,25) med tidsnummer och en bokstavsrad (28,29) med ett oordnat alfabet och de två övriga inställningsanordningarna resp. inställningshjulen vardera är tillordnade en bokstavsrad (26,27) med ett ordnat och en bokstavsrad (30,31) med ett oordnat alfabet.

4. Apparat enligt krav 2 eller 3, k ä n n e t e c k n a d av att samtliga hjul (2-5,19-22) är anordnade på en gemensam axel (32), att vredet (1) står i positiv drivförbindelse med axeln (32) och att påverkningshjulen (2-5) medelst friktion medbringas av axeln till sina av inställningshjulens (19-22) lyftelement (18) bestämda vridningsvinklar.

5. Apparat enligt krav 2 eller 3, k ä n n e t e c k n a d av att hjulen är anordnade på parallella, jämnt fördelade, längs en cirkel anordnade axlar, varvid på varje axel är anordnad påverkningshjulet hos en enhet och inställningshjulet hos en efterföljande enhet och vredets axel är anordnad i cirkelns centrum.

6. Apparat enligt något av krav 2-5, k ä n n e t e c k n a d av att medbringarorganen utgörs av en på inställningshjulen (19-22) anordnad matarskiva (33) och en på påverkningshjulen (2-5) anordnad matarhake (23), som när vredet vrids åt första hållet följer med påverkningshjulet (2-5) och på det stillastående inställningshjulets matarskiva (33) hämtar upp så många steg som motsvarar påverkningshjulets vridning, för att sedan när vredet (1) vrids åt andra hållet medbringa inställningshjulet (19-22) lika många steg som motsvarar påverkningshjulets (2-5) vridning i föregående moment.

ANFÖRDA PUBLIKATIONER:

Tyskland 1 175 019 (42 n:14)

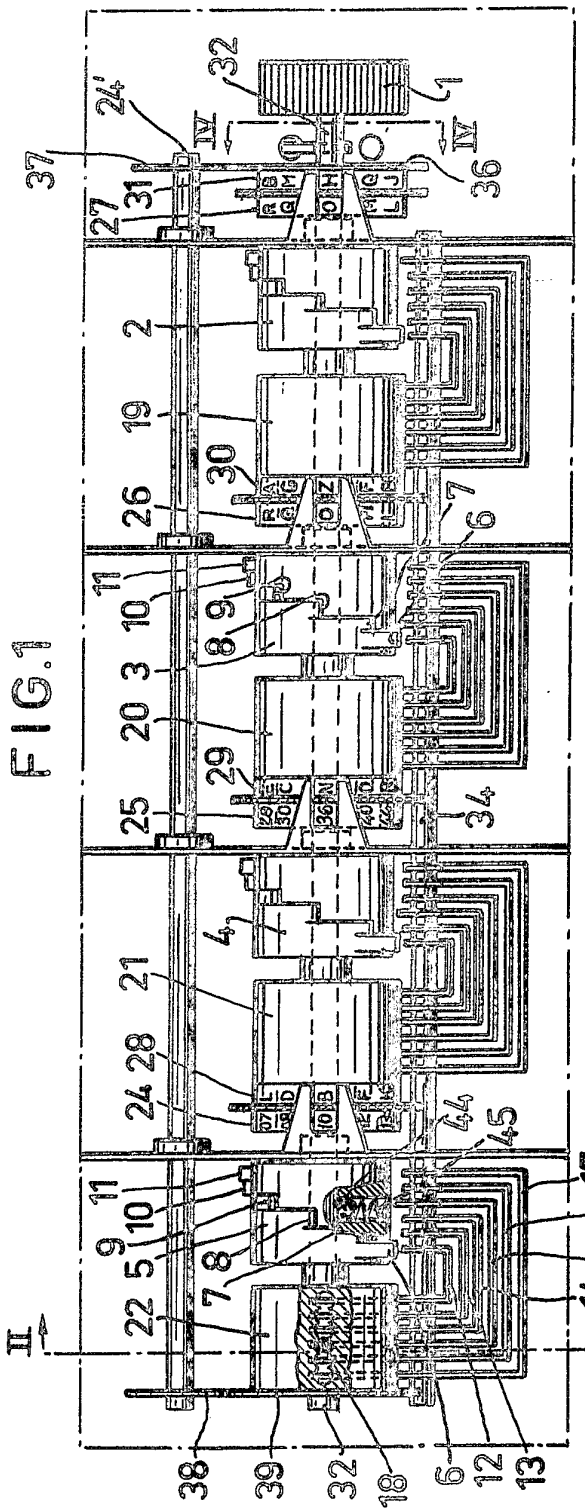

FIG.1

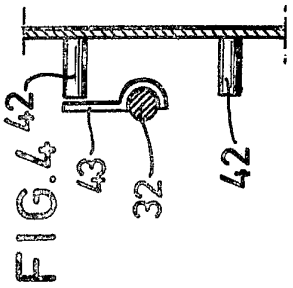

FIG.4

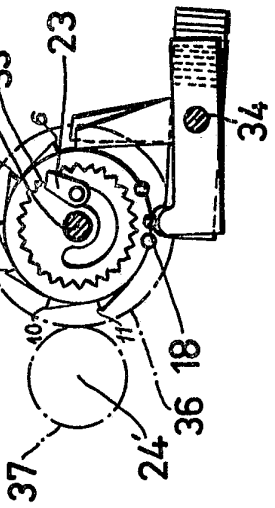

FIG.2

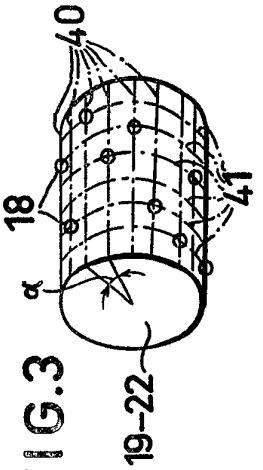

FIG.3

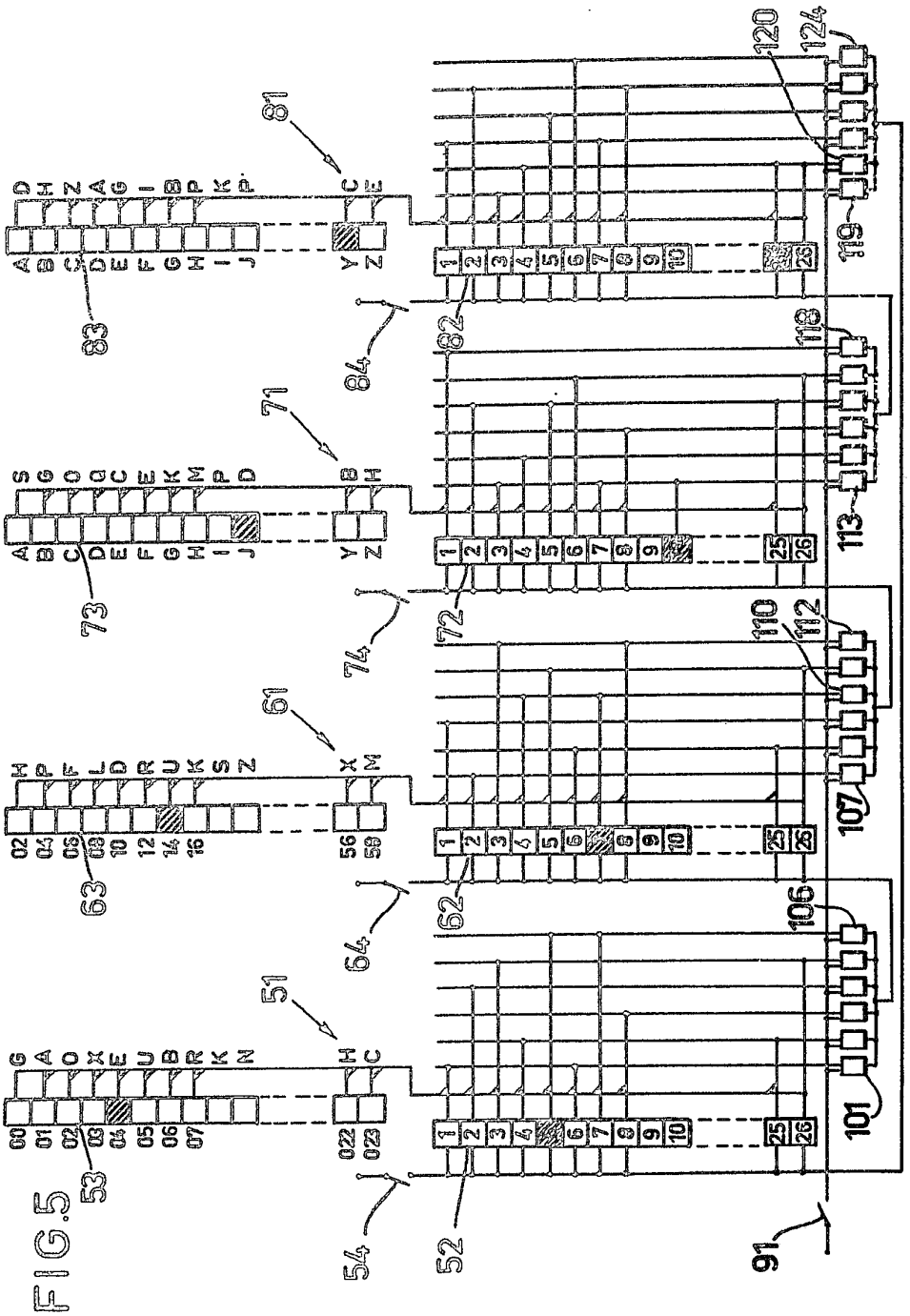

FIG 5