NORGE

STYRET
FOR DET INDUSTRIELLE
RETTSVERN

Utlegningsskrift nr. 127884

Int. Cl. G 09 c 1/06 Kl. 42n-14

Patentsøknad nr. 104/71 Inngitt 12.1.1971
Løpedag -
Søknaden alment tilgjengelig fra 19.7.1971
Søknaden utlagt og utlegningsskrift utgitt 27.8.1973
Prioritet begjært fra: 16.1.1970 Sverige, nr. 524/70

AB TRANSVERTEX,
Fittja industriområde, Norsborg, Sverige.

Oppfinner: Bengt Florin,
Lugntorpsvägen 45,
Hägersten, Sverige.

Fullmektig: Siv.ing. Rolf Larsen.

Chiffreringsapparat.

Denne oppfinnelse har til formål å tilveiebringe et apparat for chiffrering av en klartekst, nærmere bestemt et chiffer som det i praksis er umulig å dechiffrere.

Et slikt apparat er nærmest tenkt for løsensignalering, f. eks. mellom to radiostasjoner av hvilke hver stasjon har til disposisjon et slikt apparat. Løsensignaleringen foregår slik at hver radiostasjon på sitt apparat (apparatene forutsettes å ha samme grunninnstilling) innstiller samme klartekst. Derefter lar begge radiostasjoner med sine apparater denne klartekst chiffrere og skal da få frem det samme chiffer (apparatene er likt innstilt). Utvekslingen av løsen går siden hensiktsmessig for seg på den måte at den ene radiostasjon oppgir den ene halvdel av chifferet og den annen

radiostasjon den annen halvdel av chifferet. Eftersom begge radiostasjoner har adgang til hele chifferet, kan begge kontrollere at motstasjonen har avgitt riktig løsen. Noen dechiffrering er det derfor aldri nødvendig å foreta.

Ved at apparatet ifølge oppfinnelsen har de trekk som er angitt i patentkrav 1, er det tilveiebragt et slikt spesielt chiffreringsapparat som er egnet for løsensignalering. Ved hjelp av bl.a. de i patentkrav 1 angitte enheters sammenkobling i en endeløs rekke med hverandre vil den minste endring i klarteksten medføre en gjennomgripende endring av chifferet. For hver ny klartekst vil et radikalt endret nytt chiffer bli frembragt. Det ansees praktisk umulig ved hjelp av systematiske studier av sammenhørende klartekster og chiffer å få kjennskap til den nøkkel som apparatene arbeider efter.

Apparatene anvendes hensiktsmessig med en klartekst som dannes av en timeangivelse, en minuttangivelse og to bokstaver. Ved tidspunktet for en løsensignalering innstilles herunder dette tidspunkt, f.eks. 09 16 på begge apparater likesom to bokstaver fra ett av de korresponderende radiostasjoners anropssignaler, f.eks. F K. Derefter tillates begge apparater å chiffrere denne klartekst, hvorved chifferet f.eks. blir D G Y D. Løsen utveksles da ved at den ene stasjon sender DG og den annen YD. Endres klarteksten så lite som det er mulig, f.eks. bare til 09 18 F K, endres chifferet gjennomgripende, f.eks. til K K P B. Ved å anvende tidspunktet for løsenutveksling som en del av klarteksten elimineres risikoen for at samme klartekst (og dermed samme chiffer) anvendes mer enn en gang pr. døgn. En gang pr. døgn omstilles derfor hensiktsmessig apparatenes indre innstillinger slik at stadig nye chiffer fremkommer.

På tegningen vises utførelseseksemplet på oppfinnelsen.

Fig. 1 viser et riss av et rent mekanisk utførelseseksempel av chiffreringsapparatet, og fig. 2 viser i snitt efter linjen II-II på fig. 1 hvordan sperrearmer som inngår i apparatet påvirker et hjul som er forsynt med stoppeknaster og hvordan et hjul som inngår i apparatet bringes til å mates frem av et annet hjul. Fig. 3 viser i perspektiv et hjul forsynt med kuler, og

fig. 4 viser et snitt etter linjen IV-IV på fig. 2. Fig. 5 viser et koplingsskjema for apparatet i elektronikk-utførelse.

På en aksel 32 er det anordnet fire innstillingshjul 19-22 og fire påvirkningshjul 2-5. På hvert innstillingshjul som kan stilles i 26 forskjellige, jevnt fordelte vinkelstillinger 40 (fig. 3) med en vinkel $\alpha = 360^{\circ}:26$ mellom vinkelstillingene, er det tilsammen anordnet 26 kuler 18 i seks kranser 41 på en slik måte at det alltid finnes en kule i hver vinkelstilling. Kulene kan forskyves aksielt innenfor samme vinkelstilling 40 fra en krans 41 til en annen på ønsket måte.

Kulene i hver krans 41 avføles av en sperrearm 12-17. Den annen ende av sperrearmene samvirker med et av påvirkningshjulene som hver for seg har seks aksielt fordelte partier, som hvert er forsynt med en stoppeknast 6-11. Hver kulekrans på innstillingshjulet samvirker gjennom en sperrearm med et parti forsynt med stoppeknast på påvirkningshjulet. Sperrearmene er dreibart opplagret på en aksel 34.

På hvert av innstillingshjulene 21 og 20 er det anordnet en sifferkrans 24, henholdsvis 25, for tidsnummer og en bokstavkrans 28, henholdsvis 29, med et uordnet alfabet. På innstillingshjulet 19 er det anordnet to bokstavkranser, nemlig en med et ordnet og en med et uordnet alfabet 26, henholdsvis 30. Til innstillingshjulet 22 hører bokstavkranser 27, 31 som er anordnet på den høyre ende av akselen 32 og som gjennom tannhjulene 36 og 37, akselen 24' og tannhjulene 38, 39 er koplet slik til innstillingshjulet 22 at ved dreining av bokstavkransene 27 og 31, vil innstillingshjulet 22 dreise seg like meget. Bokstavkransen 27 har et ordnet alfabet, og bokstavkransen 31 et uordnet alfabet.

Utgangsinnstillingen utføres ved at innstillingshjulene 19 og 22 ved hjelp av de ordnete alfabeter 26 og 27 innstilles på det ønskete stasjonssignal, og innstillingshjulene 21 og 20 på tidsnummeret ved hjelp av sifferkransene 24 og 25. Løsenet består av to bigrammer som avleses på innstillingshjulenes uordnete alfabeter 28-31 etter et forutbestemt antall frem- og tilbakegående dreininger av rattet 1 mellom vinkelstillinger bestemt av en stoppeinnretning 42 (fig. 4) og en arm 43 på akselen 32.

Påvirkningshjulene 2-5 er anordnet slik på akselen 32 at de ved dreining av rattet 1 med urviserretningen følger med på grunn av friksjonen (kulen 44 som av en fjær 45 trykkes mot akselen 32) mot akselen 32, som rattet 1 er festet på. Den vinkel som

f.eks. hjulet 5 tillates å følge med akselen bestemmes av stoppeknastene 6-11 og en gruppe sperrearmer 12-17. De tre øvrige påvirkningshjul 2-4 har tilsvarende egne stoppeknaster og sperrearm-grupper. I hver gruppe sperrearmer blir bare én arm påvirket av en kule på slik måte at armens annen ende kommer inn i virkeområdet for den tilhørende stoppeknast.

Innstillingshjulene 19-22 er anordnet slik på akselen 32 at når rattet 1 dreies med urviserne vil hjulene bli stående stille. En av stoppeknastene på hvert enkelt av de fire påvirkningshjul vil stoppe mot fire av de 24 sperrearmer. Til hvert påvirkningshjul hører det en matningshake 23 som arbeider mot en 26-delt matningsskive 33 (fig. 2) som er fast forbundet med et innstillingshjul. Når et påvirkningshjul dreies med urviserne av akselen 32, følger matningshaken 23 med og henter eller beveger seg like mange trinn på den tilhørende matningsskive 33. På denne måte vil hjulene komme til å arbeide parvis slik at f.eks. matningshaken svarende til påvirkningshjulet 5 vil samvirke med matningsskiven for innstillingshjulet 21. Andre slike hjulpar er 4, 20; 3, 19 henholdsvis 2, 22.

I neste funksjonstrinn dreies rattet 1 mot urviserne. Derved følger påvirkningshjulet med på grunn av friksjonen mot akselen, hvorved matningshaken 23 bringer med innstillingshjulet like mange trinn som stoppeknastene i forutgående arbeidstrinn kunne bevege seg før de ble stoppet av sperrearmene.

Fremmatningen av innstillingshjulene gjør at fire nye kuler kommer til å påvirke 4 av de 24 sperrearmer som føres frem i sine respektive stoppeknasters virkeområder.

Ved derpå følgende dreining med urviserne avsøkes disse sperrearmer og matningshakene 23 henter like mange trinn på innstillingshjulene som stoppeknastene har dreiet seg før de treffer sperrearmene.

Under det følgende arbeidstrinn dreies rattet 1 mot urviserne og innstillingshjulene mates frem til en ny posisjon med den følge at fire nye kuler 18 kommer til å påvirke sperrearmene.

Som det fremgår bygger løseapparatets prinsipp på at dettes fremmatende deler hele tiden påvirker forutsetningene (innstillingshjulets innstilling) for fremmatningen under neste arbeidstrinn. For at alle hjul skal få samme uregelmessige fremmatning er hjulene sammenkoplet til en ring ved hjelp av over-

føringsakselen 24. Påvirkningshjulet 2 vil således mate frem innstillingshjulet 22. Et tilstrekkelig antall dreininger av rattet 1 forårsaker således at de utgangsstillinger som gjøres av innstillingshjulene for hver løseutveksling kommer til å påvirke samtlige innstillingshjuls fremmatning.

Selv om hjulene i utførelseseksempelet er vist anordnet ved siden av hverandre på én eneste aksel, så kan det også tenkes andre arrangementer av hjulene innenfor rammen av oppfinnelsestanken. Eksempelvis kan det være fordelaktig å anordne hjulene på parallelle, jevnt fordelte aksler anordnet langs en sirkel med et påvirkningshjul på hver aksel og et funksjonsmessig efterfølgende innstillingshjul og rattets aksel er anordnet i sirkelens sentrum.

Såvel innstillingshjul som påvirkningshjul og deres innbyrdes forbindelser og driften av hele anordningen kan utføres elektronisk, dvs. erstattes med elektroniske elementer og koplinger.

Et eksempel på apparatet i elektronikkutførelse er vist på fig. 5. Her er hver hjulsats 2,19; 3,20; 4,21 henholdsvis 5,22 erstattet med innbyrdes likt oppbygde elektronikkenheter 51, 61, 71 henholdsvis 81. Enhetene har hver et skiftregister 52, 62, 72 henholdsvis 82, som hvert hensiktsmessig på kjent måte er oppbygget av en rekke bistabile vipper betegnet nr. 1 - 26. Hvert skiftregister er tilforordnet en lamperekke 53, 63, 73 henholdsvis 83. Primærinnstillingen av tid og stasjonssignal bevirkes ved hjelp av strømbrytere 54, 64, 74 henholdsvis 84. Skiftregistrene som har et trinn polvendt, mates frem trinn for trinn ved lukning av de respektive strømbrytere 54, 64, 74 henholdsvis 84. Skiftregistrene fungerer altså som ringtellere. En ring teller er et tilbakekoplet skiftregister hvor samtlige trinn unntatt ett er nullstilt. Når det innmates trinnpulser til en ringteller, flyttes 1-tilstanden ett trinn fremad for hver puls. Lamperekkene som styres av de respektive skiftregistere, vil på grunn av det polvendte skiftregistertrinn bare ha en eneste lampe tent, og ved manøvrering av de respektive strømbrytere kan den nevnte posisjon flyttes. På venstre side av lamperekken 53 er det anordnet timeangivelser og på høyre side det uordnete alfabet. Ved primærinnstillingen av enheten 51 fremføres den tente posisjon til det ønskete timetall (som er 04 ifølge eksemplet på fig. 5, dvs. lampen ved 04 er tent) med strømbryteren 54. På

samme måte skjer primærinnstillingen ved hjelp av de øvrige skiftregistre 62, 72 og 82. Lamperekken 63 angir minutter, og lamperekkene 73 og 83 angir tilsammen bigrammet for stasjonssignalet. Etter avsluttet primærinnstilling skal denne kodes, hvilket utføres ved slutning av en felles strømbryter 91 et antall ganger som er bestemt på forhånd, som ved apparatet på fig. 1 tilsvarer dreiningen av rattet 1 et bestemt antall ganger. Ved hver slutning av strømbryteren 91 mates skiftregistrene 52, 62, 72 og 82 ifølge eksemplet på fig. 5 frem like mange trinn som de av de polvendte skiftregistertrinn nr. 5, 7, 10 og 25 utvalgte tellere 106, 110, 113 og 120 angir. Under fremmatningen av skiftregistrene kan ingen nye tellere velges ut, og derfor er samtlige tellere sperret når strømbryteren 91 lukkes, men når strømbryteren 91 igjen åpnes, blir det mulig for de polvendte skiftregistertrinn på ny å velge ut fire tellere analogt med den første dreiebevegelse av rattet, som ved neste lukning av strømbryteren 91 gir fremmatning av skiftregistrene 52, 62, 72 og 82. Funksjonen av tellerne 101-124 tilsvarer i apparatet på fig. 1 funksjonen av stoppeknastene 6-11.

Etter trykking på strømbryteren 91 et forhåndsbestemt antall ganger, har de fire tente posisjoner på lamperekkene 53, 63, 73 henholdsvis 83 forskjøvet seg et antall trinn, og de bokstaver i de uordnete alfabeter som nå kan avleses inntil de tente posisjoner, utgjør løsenet.

P a t e n t k r a v:

1. Chiffreringsapparat spesielt for løsensignalering, k a r a k t e r i s e r t ved minst to enheter (2,19; 3,20; 4,21; 5,22 henholdsvis 51; 61; 71; 81) som hver omfatter en trinnvis bevegbar innstillingsanordning (19-22 henholdsvis 52; 62; 72; 82) og et flertall tellere (6-11 henholdsvis 101-124) hvor hvert innstillingstrinn på innstillingsanordningen er koplet til en teller og enhetene er koplet i en endeløs rekke med hverandre gjennom overføringsorganer mellom tellerne for en enhet og innstillingsanordningen for den etterfølgende enhet, gjennom hvilke overføringsorganer ved aktivering av særskilte aktiveringsorganer (1 resp. 91) etter begynnelsesinnstilling av de respektive enheters innstillingsanordninger, det kan overføres en trinnvis fremføring av de respektive innstillingsanordninger med det antall trinn som bestemmes av den for anledningen virksomme teller i den

nærmest foregående enhet i rekken.

2. Apparat ifølge krav 1, k a r a k t e r i s e r t ved at for hver enhet (2,19; 3,20; 4,21; 5,22) utgjøres innstillingsanordningen av et innstillingshjul (19-22) som er forsynt med løfteelementer (18), fortrinnsvis i form av kuler, og som er trinnvis bevegbart ved dreining, og tellerne omfatter stoppeknaster eller lignende stoppeelementer (6-11) på et dreibart påvirkningshjul (2-5), at hvert innstillingstrinn av innstillingshjulet (19-22) direkte eller via sperrearmer (12-17) er tilforordnet et stoppeelement (6-11) i enheten og at overføringsorganene omfatter medbringerorganer (23) mellom påvirkningshjulet i en enhet og innstillingshjulet i en etterfølgende enhet, hvorved de i apparatets inngående elementer er slik koplet til hverandre og til et ratt (1) som er dreibart i begge retninger, at ved dreining i den ene retning vil samtlige innstillingshjul (19-22) bli stående stille og samtlige påvirkningshjul (2-5) vil dreies med en vinkel som bestemmes av de for anledningen virksomme stoppeelementer (6-11) og ved vridning i den annen retning vil innstillingshjulene (19-22) av medbringerorganene (23) bli dreiet samme vinkel som påvirkningshjulene (2-5) ble dreiet i foregående arbeidstrinn.

3. Apparat ifølge krav 1 eller 2 med fire innstillingsanordninger, henholdsvis innstillingshjul, k a r a k t e r i s e r t ved at to av innstillingsanordningene henholdsvis innstillingshjulene, er tilforordnet en sifferrekke (24, 25) med tidsnummer og en bokstavrekke (28, 29) med et uordnet alfabet og de to øvrige innstillingsanordninger henholdsvis innstillingshjul, hvert er tilforordnet en bokstavrekke (26, 27) med et ordnet og en bokstavrekke (30, 31) med et uordnet alfabet.

4. Apparat ifølge krav 2 eller 3, k a r a k t e r i s e r t ved at samtlige hjul (2-5, 19-22) er anordnet på en felles aksel (32), at rattet (1) står i positiv drivforbindelse med akselen (32) og at påvirkningshjulene (2-5) ved hjelp av friksjon bringes med av akselen til sine dreievinkler som er bestemt av innstillingshjulenes (19-22) løfteelement (18).

5. Apparat ifølge krav 2 eller 3, k a r a k t e r i s e r t ved at hjulene er anordnet på parallelle, jevnt fordelte aksler anordnet langs en sirkel hvor påvirkningshjulet

på hver enhet er anordnet på hver aksel og innstillingshjulet på en etterfølgende enhet og rattets aksel er anordnet i sirkelens sentrum.

6. Apparat ifølge et av kravene 2-5, k a r a k t e r i s e r t ved at medbringerorganene dannes av en på innstillingshjulene (19-22) anordnet matningsskive (33) og en på påvirkningshjulene (2-5) anordnet matningshake (23) som når rattet dreies i den første retning følger med påvirkningshjulet (2-5) og på det stillestående innstillingshjuls matningsskive (33) henter opp eller beveger seg over så mange trinn som svarer til påvirkningshjulets dreining for så når rattet (1) dreies i den annen retning, å medbringe innstillingshjulet (19-22) like mange trinn som svarende til påvirkningshjulets (2-5) dreining i foregående arbeidstrinn.

Anførte publikasjoner:

Tysk utl. skrift nr. 1175019 (42n-14)

FIG.1

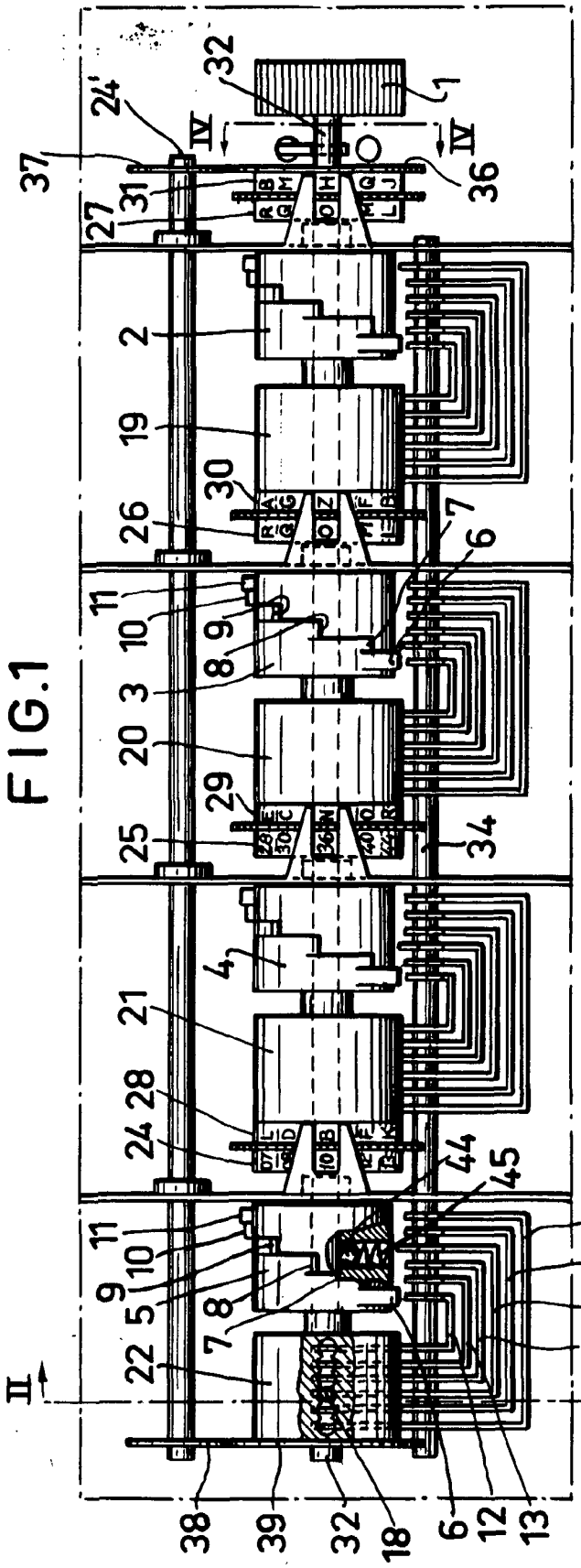


FIG.4

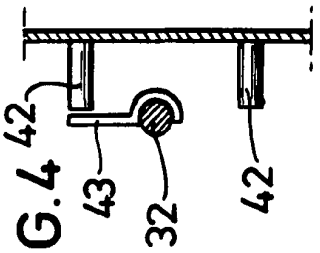


FIG.2

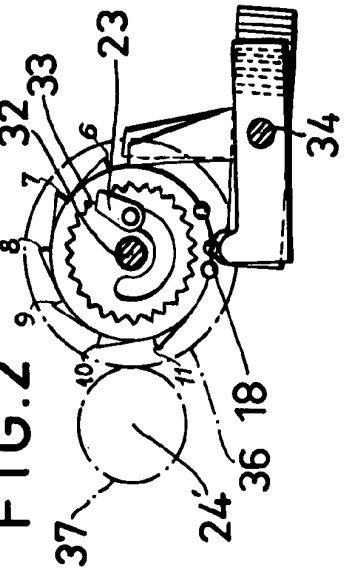
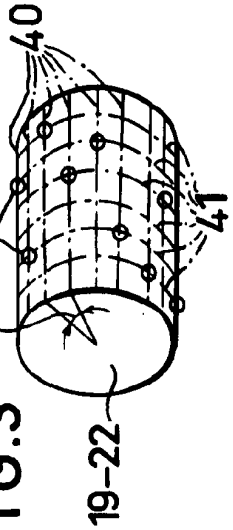


FIG.3



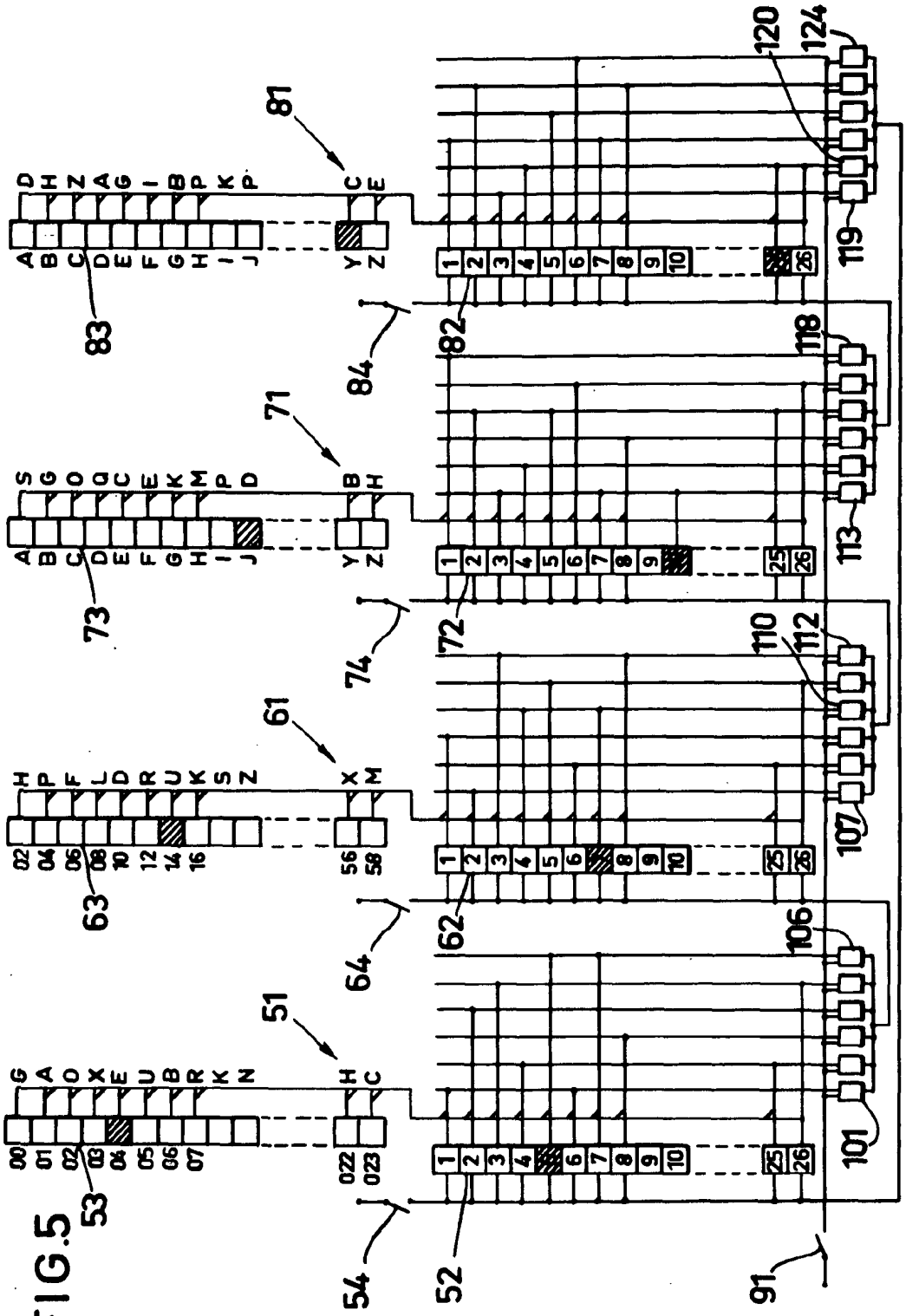

81
71
61
51
83
73
63
53
84
74
64
54
82
72
62
52
91
120
124
119
118
113
110
112
107
106
101

FIG.5