(11) FREMLÆGGELSESSKRIFT 132476

DANMARK

(51) Int. Cl.³ G 09 C 1/06

(21) Ansøgning nr. 166/71 (22) Indleveret den 15. jan. 1971

(23) Løbedag 15. jan. 1971

(44) Ansøgningen fremlagt og fremlæggelsesskriftet offentliggjort den 8. dec. 1975

DIREKTORATET FOR PATENT- OG VAREMÆRKEVÆSENET

(30) Prioritet begæret fra den 16. jan. 1970 nr. 524/70, Sverige.

(71) AB TRANSVERTEX, Fittja industriområde, Norsborg, Sverige.

(72) Opfinder: Bengt Florin, ingeniør, Lugntorpsvägen 45, Hägersten, Sverige.

(74) Fuldmægtig under sagens behandling:
Dansk Patent Kontor A/S.

(54) Chiffreringsapparat, især for identitetssignalering.

Opfindelsen angår et chiffreringsapparat, og formålet med opfindelsen er at tilvejebringe et apparat til chiffrering af en klartekst, nærmere betegnet til frembringelse af en kode, som det i praksis er umuligt at dechiffrere.

Et sådant apparat er nærmest tænkt for identitetssignalering, f.eks. mellem to radiostationer, af hvilke hver station har et sådant apparat til disposition. Identitetssignalering foregår på den måde, at hver radiostation på sit apparat (apparaterne forudsættes at have samme grundindstilling) indstiller samme klartekst. Derefter lader begge radiostationer med sine apparater denne klartekst chiffrere og skal da få den samme kode frem (apparaterne er ens indstillede). Udvekslingen af identiteten går derefter hensigtsmæssigt for sig på den måde, at den ene radiostation opgiver den ene halvdel af koden og den anden radio-

station den anden halvdel af koden. Eftersom begge radiostationer har adgang til hele koden, kan begge kontrollere, at den anden station har afgivet rigtig identitet. Det er derfor aldrig nødvendigt at foretage nogen dechiffrering.

Apparatet ifølge opfindelsen er ejendommeligt ved det i patentkrav 1 angivne, hvorved der er tilvejebragt et sådant chiffreringsapparat, som er egnet til identitetssignalering. Ved hjælp af bl.a. de i patentkrav 1 angivne enheders sammenkobling i en endeløs række efter hverandre, vil den mindste ændring i klarteksten medføre en gennemgribende ændring af koden. For hver ny klartekst vil en radikalt ændret ny kode blive frembragt. Det må anses for praktisk umuligt ved hjælp af systematiske studier af sammenhørende klartekster og koder at få kendskab til den nøgle, som apparaterne arbejder efter.

Apparaterne anvendes hensigtsmæssigt med en klartekst, som dannes af en timeangivelse, en minutangivelse og to bogstaver. Ved tidspunktet for en identitetssignalering indstilles herunder dette tidspunkt, f.eks. 09 16, på begge apparater ligesom to bogstaver fra et af de korresponderende radiostationers kaldesignaler, f.eks. F K. Derefter chiffrerer begge apparater denne klartekst, hvorved koden f.eks. bliver D G Y D. Identiteten udveksles da ved, at den ene station sender DG og den anden YD. Ændres klarteksten så lidt som muligt, f.eks. blot til 09 18 F K, ændres koden gennemgribende, f.eks. til K K P B. Ved at anvende tidspunktet for identitetsudveksling som en del af klarteksten elimineres risikoen for, at samme klartekst (og dermed samme kode) anvendes mere end én gang pr. døgn. En gang pr. døgn kan derfor hensigtsmæssigt apparaternes indre indstillinger omstilles, således at der fremkommer stadig nye koder.

Opfindelsen forklares nærmere ved udførelseseksempler under henvisning til tegningen, hvor

fig. 1 viser et rent mekanisk udførelseseksempel på et chiffreringsapparat ifølge opfindelsen,

fig.2 i snit efter linien II-II i fig. 1 hvorledes i apparatet indgående spærrearme påvirker et med stopknaster forsynet hjul, og hvorledes et i apparatet indgående hjul fremføres af et andet hjul,

fig. 3 et med kugler forsynet hjul i perspektiv,

fig. 4 et snit efter linien IV-IV i fig. 1 og

fig. 5 et koblingsdiagram for apparatet i elektronisk udførelse.

På en aksel 32 er anbragt fire indstillingshjul 19 til 22 og fire påvirkningshjul 2 til 5. På hvert indstillingshjul, som kan stilles i 26 forskellige, jævnt fordelte vinkelstillinger 40 (fig. 3) med vinklen $\alpha = 360^{\circ}:26$ mellem vinkelstillingerne, er anbragt sammenlagt 26 kugler 18 i seks kredse 41 på en sådan måde, at der altid findes en kugle i hver vinkelstilling. Kuglerne 18 kan flyttes aksialt inden for samme vinkelstilling 40 fra én kreds 41 til en anden alt efter ønske.

Kuglerne i hver kreds 41 afføles af en spærrearm 12 til 17. Spærrearmenes anden ende samvirker med et af påvirkningshjulene, som hver har seks aksialt fordelte, hvert med en stopknast 6 til 11 forsynede partier. Hver kuglekreds på indstillingshjulet samvirker over en spærrearm med et med stopknaster forsynet parti på påvirkningshjulet. Spærrearmene er drejeligt lejret på en aksel 34.

På hvert af indstillingshjulene 21 og 20 er anbragt en talkrans 24 henholdsvis 25 for tidsangivelse og en bogstavkrans 28 henholdsvis 29 med et vilkårligt ordnet alfabet. På indstillingshjulet 19 findes to bogstavkranse, én med et i og én med et ikke i bogstavorden ordnet alfabet 26 henholdsvis 30. Til indstillingshjulet 22 hører i højre ende af akselen 32 anbragte bogstavkranse 27, 31, som over tandhjul 36, 37, akselen 24' og tandhjul 38, 39 er koblet til indstillingshjulet 22, således at indstillingshjulet 22 ved drejning af bogstavkransene 27, 31 bliver drejet lige så meget. Bogstavkransen 27 har et ordnet og bogstavkransen 31 et ikke ordnet alfabet.

Begyndelsesindstilingen udføres ved, at indstillingshjulene 19 og 22 ved hjælp af de ordnede alfabeter 26 og 27 indstilles på det ønskede stationssignal og indstillingshjulene 21 og 20 på tidsangivelsen ved hjælp af talkransene 24 og 25. Identiteten består af to dobbelttegn, som aflæses på indstillingshjulenes ikke ordnede alfabeter 28 til 31 efter et forudbestemt antal frem- og tilbagegående drejninger på håndtaget 1 mellem af et stop 42 (fig. 4) og en arm 43 på akselen 32 bestemte vinkelstillinger.

Påvirkningshjulene 2 til 5 er anbragt sådan på akselen 32, at de, når håndtaget 1 drejes med uret, følger med på grund af friktionen (kuglen 44, som af en fjeder 45 trykkes mod akselen 32) mod akselen 32 , som håndtaget er sat fast på. Den vinkel, som f. eks. hjulet 5 får lov til at følge med akselen, bestemmes af stopknasterne 6 til 11 og en gruppe spærrearme 12 til 17. De øvrige tre påvirkningshjul 2 til 4 har tilsvarende egne stopknaster og spærrearmsgrupper. I hver gruppe spærrearme er kun én arm påvirket af en kugle på en sådan måde,

at armens anden ende kommer ind i virkeområdet for dens stopknast.

Indstillingshjulene 19 til 22 er anbragt sådan på akselen 32, at de, når håndtaget 1 drejes med uret,kommer til at stå stille.En af stopknasterne på hver af de fire påvirkningshjul vil stoppe mod fire af de fireogtyve spærrearme.Til hvert påvirkningshjul hører en fremføringshage 23, som arbejder mod en med et indstillingshjul fast forbundet, 26-delt fremføringsskive 33 (fig. 2). Når et påvirkningshjul af akselen 32 drejes med uret, følger fremføringshagen 23 med og bevæger sig lige så mange trin på det tilhørende indstillingshjuls fremføringsskive 33. På denne måde arbejder hjulene parvis, således at f.eks. fremføringshagen på påvirkningshjulet 5 samarbejder med fremføringsskiven på indstillingshjulet 21. De øvrige sådanne hjulpar er 4 og 20, 3 og 19 henholdsvis 2 og 22.

I operationens næste punkt drejes håndtaget 1 mod uret. Derved følger på grund af friktionen mod akselen påvirkningshjulet med, hvorved fremføringshagen 23 medbringer indstillingshjulet lige så mange trin, som stopknasterne ved forrige punkt kunne bevæge sig, inden de standsedes af spærrearmene.

Fremføringen af indstillingshjulene gør, at fire nye kugler kommer til at påvirke fire af de fireogtyve spærrearme, som føres frem i deres respektive stopknasters virkeområde.

Ved den derpå følgende drejning med uret afsøges disse spærrearme, og fremføringshagerne bevæger sig lige så mange trin på indstillingshjulenes fremføringsskiver, som stopknasterne kan dreje sig, inden de rammer spærrearmene. Under næste punkt drejes håndtaget 1 mod uret, og indstillingshjulene føres frem til en ny position med det resultat, at fire nye kugler 18 kommer til at påvirke spærrearmene.

Som det ses, bygger identitetsapparatet på det princip, at dets fremførende dele hele tiden påvirker forudsætningerne (indstillingshjulets indstilling) for næste punkts fremføring. For at alle hjulene kan få samme uregelmæssige fremføring, er hjulene sammenkoblet til en ring ved overføringsakselen 24'. Påvirkningshjulet 2 kommer altså til at fremføre indstillingshjulet 22. Et tilstrækkeligt antal drejninger på håndtaget 1 forårsager således, at de begyndelsesindstillinger, som udføres af indstillingshjulene før hver identitetsudveksling, kommer til at påvirke samtlige indstillingshjuls fremføring.

Selv om hjulene i udførelseseksemplet er vist anbragt ved siden af hverandre på en enkelt aksel, kan der også tænkes andre arrangementer af hjulene. Eksempelvis kan det være fordelagtigt at anbringe hjulene på parallelle, jævnt fordelte aksler anbragt langs en cirkel med

et påvirkningshjul på hver aksel og et funktionsmæssigt efterfølgende indstillingshjul, idet håndtagets aksel er anbragt i cirklens centrum.

Såvel indstillingshjul som påvirkningshjul og deres indbyrdes forbindelser samt funktionen af hele anordningen kan naturligvis elektroniseres, d.v.s. erstattes af elektroniske elementer og koblinger.

Et eksempel på apparatet i elektronisk udførelse er vist i fig. 5. Her er hvert hjulsæt 2 og 19, 3 og 20, 4 og 21 henholdsvis 5 og 22 erstattet af indbyrdes ens opbyggede elektronikenheder 51, 61, 71 henholdsvis 81. Enhederne udviser hver et koblingsregister 52, 62, 72 henholdsvis 82, hver for sig hensigtsmæssigt på kendt måde opbygget af en række bistabile multivibratorer nr. 1 til 26. Hvert koblingsregister er tilsluttet en lamperække 53, 63, 73 henholdsvis 83. Primærindstillingen tilvejebringes ved hjælp af afbrydere 54, 64, 74 henholdsvis 84. Koblingsregistrene, som har ét trin polvendt, fremføres trin for trin ved betjening af de respektive afbrydere 54, 64, 74 og 84. Lamperækkerne, som styres af de respektive koblingsregistre, kan på grund af det polvendte koblingsregister kun have én lampe tændt, og ved betjening af de respektive afbrydere kan den tændte position forskydes. På venstre side af lamperækken 53 findes timeangivelserne, og på højre side det ikke ordnede alfabet. Ved primærindstillingen af enheden 51 drives den tændte position trinvis frem til det ønskede timetal (som er 04 ifølge eksemplet i fig. 5, d.v.s. lampen ved 04 er tændt) med afbryderen 54. På samme måde sker primærindstillingen ved hjælp af de øvrige koblingsregistre 62, 72 og 82. Lamperækken 63 angiver minutter, og lamperækkerne 73 og 83 angiver tilsammen dobbelttegnet for stationssignalet. Efter afsluttet primærindstilling skal denne omsættes i kryptogram, hvilket udføres ved betjening af en for alle enhederne fælles afbryder 91 et på forhånd bestemt antal gange, som ved apparatet i fig. 1 svarer til drejningen af håndtaget 1 et bestemt antal gange. Hver gang afbryderen 91 sluttes, føres koblingsregistrene 52, 62, 72 og 82 lige så mange trin frem, som de af de polvendte koblingsregistre 5, 7, 10 og 25 (ifølge eksemplet i fig. 5) udvalgte tællere 106, 110, 113 120 angiver. Under koblingsregistrenes fremføring må ingen nye tællere udvælges, hvorfor samtlige tællere er spærrede, når afbryderen 91 sluttes; men når afbryderen 91 atter åbnes, bliver det muligt for de polvendte koblingsregistre pånyt at udvælge fire tællere analogt med den første drejningsbevægelse med håndtaget, som ved næste betjening af afbryderen 91 giver en fremføring af koblingsregistrene 52, 62, 72 og

82. Tællerne 101 til 124's funktion svarer ved apparatet i fig. 1 til stopknasterne 6 til 11's funktion.

Efter nedtrykning et på forhånd bestemt antal gange af afbryderen 91 er de fire tændte positioner i lamperækkerne 53, 63, 73 og 83 forskudt et antal trin, og de bogstaver i de ikke ordnede alfabeter, som nu kan aflæses ud for de tændte positioner, udgør identitetskoden.

P A T E N T K R A V.

1. Chiffreringsapparat, især for identitetssignalering, k e n d e t e g n e t ved mindst to enheder (2,19; 3,20; 4,21; 5,22 henholdsvis 51; 61; 71; 81), som hver omfatter en trinvis fremførlig indstillingsanordning (19-22 henholdsvis 52; 62; 72; 82) og flere tællere (6-11 henholdsvis 101-124), hvorhos indstillingsanordningen ved hvert indstillingstrin er tilkoblet en tæller, og enhederne er koblet i en endeløs serie gennem et overføringsorgan mellem tællerne i én enhed og indstillingsanordningen i den efterfølgende enhed, hvilket overføringsorgan efter indstilling af de respektive enheders indstillingsanordninger er i stand til at tilvejebringe en fremføring af den respektive indstillingsanordning det antal trin, som bestemmes af den i øjeblikket virksomme tæller i den nærmest foregående enhed i serien.

2. Apparat ifølge krav 1, k e n d e t e g n e t ved, at for hver enhed (2,19; 3,20; 4,21; 5,22) udgøres indstillingsanordningen af et med kugler, stifter eller lignende stilbare kamelementer (18) forsynet, ved drejning trinvis fremførligt indstillingshjul (19-22), og tællerne omfatter stopknaster eller lignende stopelementer (6-11) på et drejeligt påvirkningshjul (2-5), at hvert indstillingstrin på indstillingshjulet (19-22) direkte eller over spærrearme (12-17) hører til et stopelement (6-11) i enheden, og at overføringsorganet omfatter medbringerorganer (23) mellem påvirkningshjulet i én enhed og indstillingshjulet i en efterfølgende enhed, hvorhos de i apparatet indgående elementer er koblet til hverandre og til et i begge retninger drejeligt håndtag (1), således at samtlige indstillingshjul (19-22) ved drejning af håndtaget (1) i den ene retning vil stå stille, og samtlige påvirkningshjul (2-5) vil dreje sig en vinkel, som bestemmes af de i øjeblikket virksomme stopelementer (6-11), medens indstillingshjulene (19-22) ved drejning af håndtaget den anden vej af medbringerorganerne (23) vil blive drejet samme vinkel, som påvirkningshjulene (2-5) blev drejet i den foregående operation.

3. Apparat ifølge krav 1 eller 2, k e n d e t e g n e t ved, at to af indstillingsanordningerne henholdsvis indstillingshjulene er forsynet med en talrække (24,25) med tidsangivelse og en bogstavrække

(28,29) med et alfabet i uorden, og de to øvrige indstillingsanordninger henholdsvis indstillingshjul hver er forsynet med en bogstavrække (26, 27) med et alfabet i orden og en bogstavrække (30,31) med et alfabet i uorden.

4. Apparat ifølge krav 2 eller 3, k e n d e t e g n e t ved, at samtlige hjul (2-5, 19-22) er anbragt på en fælles aksel (32), at håndtaget (1) står i positiv drivforbindelse med akselen (32), og at påvirkningshjulene (2-5) ved friktion medbringes af akselen til deres af indstillingshjulenes (19-22) kamelement (18) bestemte drejningsvinkel.

5. Apparat ifølge krav 2 eller 3, k e n d e t e g n e t ved, at hjulene er anbragt på parallelle, langs en cirkel jævnt fordelte aksler, hvorhos der på hver aksel er anbragt påvirkningshjulet i den ene enhed og indstillingshjulet i den efterfølgende enhed, og håndtagets aksel er anbragt i cirklens centrum.

6. Apparat ifølge ethvert af kravene 2 til 5, k e n d e t e g n e t ved, at medbringerorganet udgøres af en på indstillingshjulet (19-22) anbragt fremføringsskive (33) og en på påvirkningshjulet (2-5) anbragt fremføringshage (23), som, når håndtaget drejes den første vej, følger med påvirkningshjulet (2-5) og på det stillestående indstillingshjuls fremføringsskive (33) samler så mange trin op, som svarer til påvirkningshjulets drejning, for senere, når håndtaget (1) drejes den anden vej, at medbringe indstillingshjulet (19-22) så mange trin, som svarer til påvirkningshjulets (2-5) drejning i foregående operation.

Fremdragne publikationer:

———

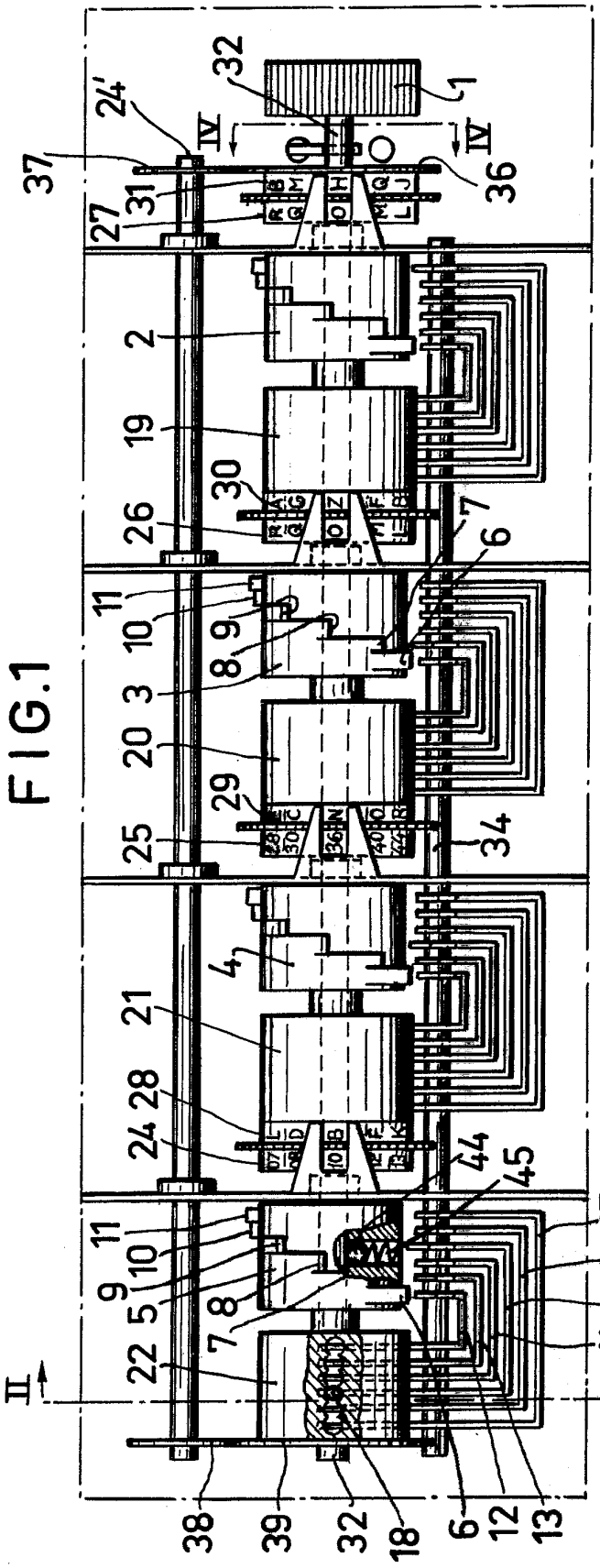

FIG.1

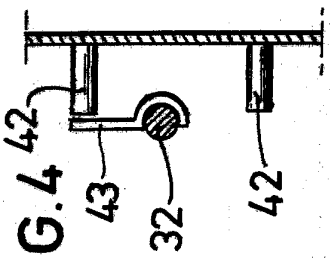

FIG.4

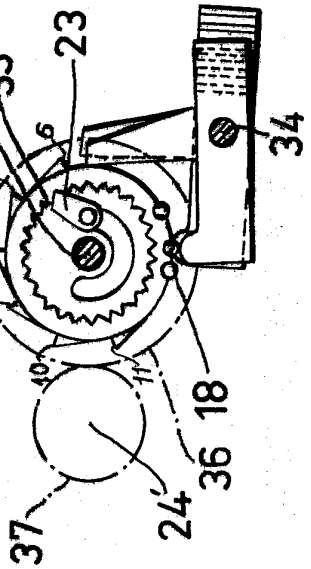

FIG.2

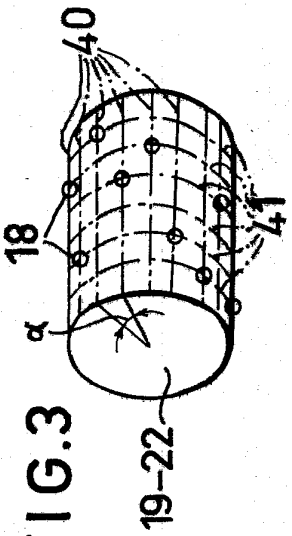

FIG.3

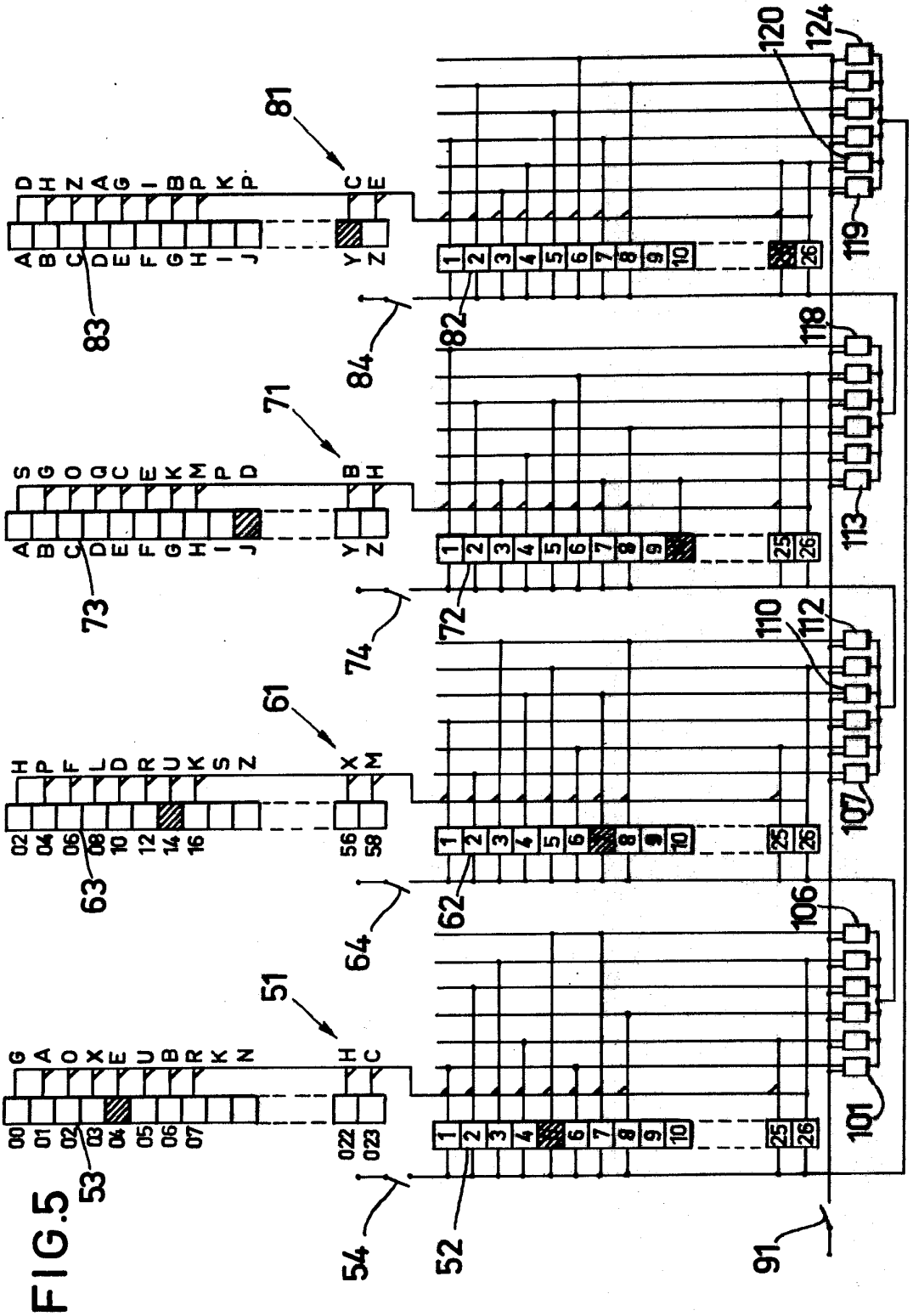
81
83
84
82
71
73
74
72
61
63
64
62
51
53
54
52
91
120
124
119
118
113
110
112
107
106
101

FIG.5