

NORGE



**STYRET
FOR DET INDUSTRIELLE
RETTSVERN**

Utlegningskrift nr. 121284

Int. Cl. H 04 1 9/00 Kl. 21a¹-21

Patentsøknad nr. 163.526 Inngitt 17.VI 1966

Løpedag -

Søknaden alment tilgjengelig fra 1.VII 1968

Søknaden utlagt og utlegningskrift utgitt 8.II 1971

Prioritet begjært fra: -

Standard Telefon og Kabelfabrik A/S,
Ulvenveien, Økern, Oslo.

Oppfinnere: Per Reidar Abrahamsen, Vildvinveien 1D, Kjeller og
Kåre Ragnar Meisingset, Ringsveien 16, Stabekk.

Fremgangsmåte for chifring/dechifring, samt
chifreringsenhet for utførelse av fremgangsmåten.

Oppfinnelsen vedrører kryptografisk fjernskriverutstyr og spesielt en fremgangsmåte til chifring og dechifring. Oppfinnelsen vedrører også en chifreringsenhet for utførelse av fremgangsmåten.

I kryptografisk utstyr behandles en klartekst med et nøkkelmateriale på sendersiden slik at en chifrert tekst fremkommer, og klarteksten reproduseres på mottakersiden ved at den chifrerte teksten behandles med et duplikat av nøkkelmaterialet brukt på sendersiden.

Nøkkelmaterialet kan være i form av et engangs nøkkelbånd eller det kan være i form av en "pseudo-random" serie med nøkkeltegn eller elementer som er laget mekanisk eller elektrisk.

I de fleste konvensjonelle chifreringsystemer er chifrerings/dechifreringsprosessen basert på enkel modulo-2 addisjon slik at hvert klarteksttegn blir modulo-2 addert med et nøkkeltegn.

Målet med den foreliggende oppfinnelse er å fremskaffe en chifreringsenhet som kan brukes i samband med "pseudo-random" nøkkelmateriinalgeneratoren for øket sikkerhet.

Det særegne ved oppfinnelsen fremgår av de nedenfor fremsatte krav.

Det ovenfor nevnte formål samt de i kravene angitte særtrekk ved oppfinnelsen fremgår klart av den følgende detaljerte beskrivelse av utførelse sett i sammenheng med tegningene, hvor

Fig. 1a viser et funksjonelt blokkskjema for en utførelse av oppfinnelsen,

Fig. 1b viser et blokkskjema med de viktigste forbindelser mellom blokkene,

Fig. 1c-i og 2a-h viser et detaljert blokkskjema over oppfinnelsens utførelse,

Fig. 3 viser et detaljert diagram over blokk 6 i Fig. 2a, en monostabil pulsgenerator (OS),

Fig. 4 viser et detaljert diagram over blokk 5 i Fig. 2a, en tilbakestillingskrets (RES) og tidspulsgenerator (25 kHz OSC),

Fig. 5 viser et detaljert diagram over blokk 14 i Fig. 2a, en fjernskriverdrivforsterker (DA) og en avlesningskrets (RC), og

Fig. 6 viser de forskjellige logiske symboler som er brukt i Fig. 1c-i og 2a-h,

Fig. 7 viser hvordan Fig. 1c-i og 2a-h skal settes sammen for å danne et fullstendig skjema.

Funksjonelt blokkskjema

I figur 1a er vist et funksjonelt blokkskjema som har nær tilknytning til det detaljerte blokkskjema. Følgende hoveddeler av blokkskjemaet vil bli omtalt i noen detalj: Generator for pseudorandom nøkkel-tegn. - Generator for 5-elements tall "P". - Teller "C(P)". - Inngangsregister "Reg X". - Pluggbord. - Plugg A. Deretter vil også startprosedyren såvel som chifrerings- og dechifreringsprosessen og telex-tilkobling bli omtalt i forbindelse med det funksjonelle blokkskjema.

Generator for pseudo-random nøkkel-tegn

Nøkkelgeneratoren omfatter to ikke-lineære tilbakekoblende skyveregistre REG I og REG II. Begge registre har 15 trinn, 12 trinn henholdsvis i blokk 10 og 11 og 3 trinn i blokk 12 som også inneholder de ikke-lineære tilbakekoblingskretser. De to utganger fra registerne adderes modulo-2 og resultatet lagres i REG Z i blokk 9. Under chifring og dechifring vil de to registre bli påvirket slik at det alltid er et nytt nøkkeltegn tilstede i REG Z. Alle utganger fra de to registre er tilkoblet individuelle kolonner på et pluggbord. Hvilke utganger som skal brukes for de ikke-lineære tilbakekoblingsfunksjoner, velges ved hjelp av plugger på pluggbordet, idet radene F, G, H og K er bestemmende for REG I og radene S, T, V og W er bestemmende for REG II.

Generator for 5-elements tall "P"

"P" er et 5-elements pseudo-random tall som frembringes av de to hovedregistre REG I og REG II ved hjelp av 5 utganger fra hvert register, valgt ved hjelp av plugger på pluggbordet. Pluggbordradene A - E og M,N,P,Q,R tilføres blokk 8 og innstillingskretsene for binærtelleren "C(P)". Hver av de fem innstillings-signaler er en modulo-2 addisjon av et utgangssignal fra REG I og et utgangssignal fra REG II. Disse kombinerte signaler er også pseudo-random.

Teller "(P)"

Binærtelleren i blokk 7 vil alltid telle "nedover". Tellerens funksjon er å styre antall skyvepulser som tilføres inngangsregisteret REG X. Ved chifring settes til å begynne med tallet "P" inn i binærtelleren, og dette betyr at REG X tilføres "P" skyvepulser, men ved dechifring settes tallet $31 - "P"$ inn i telleren til å begynne med. Ved dechifring vil forøvrig telleren stoppe når den inneholder tallet 1, i stedet for 0, slik at telleren i dette tilfelle teller $31 - "P" - 1$ trinn, d.v.s. $30 - "P"$ trinn. Betydningen av dette vil fremgå av beskrivelsen av dechifringsprosessen.

Inngangsregister REG X

Reg X i blokk 2 inneholder 5 like trinn hvorav ett er vist i fig. 1a. I tillegg har dette register et sjette trinn som virker som buffertrinn. REG X har to virkemåter:

- Det virker som et normalt 5-elements skyveregister som mottar skyvepulser fra inngangstelleren i blokk 4. Inngangen til det første trinn kommer fra fjernskriveren via lesekreten i blokk 14. (Denne forbindelse er ikke vist i det funksjonelle blokkskjema).
- Det virker som et tilbakekoblet skyveregister hvor hvert trinn omfatter en modulo-2 addisjonskrets og en flip-flop, hvor en hvilken som helst utgang kan kobles til en hvilken som helst inngang ved hjelp av loddeforbindelser på den kodeplugg som er vist til venstre på tegningen, og begge disse forbindelser er gjort slik at det fremkommer en maksimal sekvens $2^5 - 1 = 31$. Dette er symbolisert i Fig. 1a ved en X som kommer via plugg A gjennom modulo-2 addisjonskretsen i blokk 1 og gjennom inngangslogikken i blokk 2 frem til flip-floppen.

Det er også mulig å innstille hvert element i 5-elements registeret REG X til resultatet av en modulo-2 addisjon av ett element i selve REG X og et tilsvarende element i REG Z. Dette er symbolisert i figur 1a ved den nedre modulo-2 addisjonskrets i blokk 1 med innganger x og z.

Pluggbord

Pluggbordet er et bord med 10 horisontale rader og 30 vertikale kolonner som utgjør en matrix med 300 krysspunkter. De vertikale kolonner er forbundet

med de 30 utganger fra de to hovedregistre. Tilfeldig valgte utganger fra de to registre kan kobles til de horisontale rader ved hjelp av pluggen innsatt i krysspunktene i pluggbordet. Disse tilfeldige utganger vil bli tilført de ikke-lineære tilbakekoblingskretser og innstillingskretsene for tallet "P". Det vil også være mulig, ved hjelp av raden L på pluggbordet, å forhåndsinnstille de to registre med et startinnhold.

Plugg A

Når REG X virker som et tilbakekoblet skyveregister, vil de fem tilbakekoblings-signaler bli ført tilbake til de fem innganger via plugg A. Når krysskoblingene på denne plugg er riktig gjort, vil REG X gjennomløpe en maksimal sekvens, d.v.s. en syklus på 31 tegn.

Andre deler som er vist i det funksjonelle skjema

REG Z kan eventuelt innstilles ved hjelp av en nøkkelbåndleser (TAPE RDR) via inngangslogikken i blokk 9. Denne virkemåten kan benyttes dersom større sikkerhet ønskes. Hovedregisterne REG I og REG II funksjonerer ikke i slike tilfelle, slik at inngangen til REG Z er null.

REG Y i blokk 9 brukes bare i startfasen og da som bufferregister i chifreringsenheten.

Blokk 3 omfatter følgende tre kretser:

- 1) HUK FF er en flip-flop som husker om et VOGN TILBAKE tegn er detektert eller ikke.
- 2) INNS./TILB. brukes under startfasen for å tilbakestille inngangsregisteret og hovedregisterne.
- 3) Blokken $K_1 - K_5$ er et normalt skyveregister koblet som en ringteller og brukes for styring av chifrerings- og dechifreringsprosessene. Tellerens funksjoner er følgende: Ved K_1 leses fjernskrivertegnet inn i registeret REG X. Ved K_2 blir innholdet av dette register testet for å finne ut om det inneholder TALL SKIFT eller VOGN TILBAKE. Dersom et TALL SKIFT detekteres, blir dette tegn omformet til VOGN TILBAKE. Dersom imidlertid VOGN TILBAKE detekteres omformes dette til NY LINJE. Årsaken til dette vil klart fremgå når telex-virkemåten beskrives. Ved K_3 blir et pseudo-random 5-elements tall "P" matet inn i binærtelleren "C(P)". Ved K_4 blir inngangsregisteret REG X koblet som et tilbakekoblet skyveregister. Telleren "C(P)" teller ned til null og pulsene fra denne teller føres via FF_{S1} i blokk 4 til inngangsregisteret i blokk 2. Ved K_5 blir innholdet av REG I og REG II addert modulo-2 og resultatet ført tilbake til REG X. Deretter blir innholdet testet for å finne ut om det resulterende tegn er et tegn som er tillatt i telex eller ikke. Hvis ikke, blir modulo-2 addisjonen utført en gang til. Det resulterende tegn vil da alltid være et tillatt tegn.

Blokk 7 inneholder to ringtellere, $i_1 - i_4$ og $j_1 - j_3$. Disse tellere styrer startfasen. Hovedregisterne skal alltid starte fra et tilfeldig startpunkt for hver ny melding som skal sendes. Dette betyr at de må tilføres seks tegn. De første tre tilføres REG I og de neste tre tilføres REG II ved hjelp av de to ringtellere.

I blokk 5 finnes en oscillator med frekvens 25 kHz som trigger en monostabil multivibrator i blokk 6 og denne trigger igjen inngangstelleren i blokk 5. Den monostabile kretsen kan innstilles på forskjellige tidsforsinkelser ved hjelp av en velger og forskjellige fjernskriverhastigheter kan således realiseres.

TILB. i blokk 5 brukes til tilbakestilling av hovedregisterne ved sending av klartekst eller ved chifring med nøkkelbånd.

TP.LOG. i blokk 4 bestemmer det signal som leveres til fjernskrivers mottagerspole. Dette signal består av en start- og en stopp-puls som tilføres fra inngangstelleren, og fem informasjonselementer som leveres fra REG X. I KLARstilling kommer denne informasjon fra registertrinn 1 og i SEND- eller MOTTAstilling fra buffertrinnet i REG X. Disse to innganger er symbolisert med X_1 og X_6 .

Chifreringsprosess

Chifreringsprosessen starter når avlesekretsene mottar en startpuls fra et klarteksttegn ved betjening av tastatur-senderen eller automatsenderen på en fjernskriver. Avlesekretsen starter inngangstelleren, som igjen leverer skiftpulser til REG X, REG I og II og REG Z via flip-flop FF_{S2}. I denne første fase av chifreringsprosessen er REG X koblet som et normalt skyveregister med informasjonsinngang til det første trinn, hvorved klartekst-tegnet innføres i REG X, mens det foregående chifrede tegn er sendt til fjernskriveren fra registertrinnet X_6 via fjernskrivers drivforsterker (DR.FORST.) Når nå REG X inneholder de fem informasjonselementer, inneholder REG Z fem nye nøkkelementer, og "C(P)" er innstilt på et nytt P-tall. Deretter er REG X koblet som et tilbakekoblet skyveregister med periode 31, og pulser fra 25 kHz (oscillatoren) tilføres "C(P)" og REG X. Tilførselen av disse 25 kHz skyvepulser avskjæres når "C(P)" = 0, d.v.s. etter P pulser. REG X har da blitt fremmatet gjennom P tilstander og den nåværende tilstand er derfor en funksjon av "P" som kan symboliseres ved uttrykket $X(P)$. Til slutt innstilles REG X til resultatet av addisjonen $X(P) \oplus Z$, hvor Z er den lagrede utgang fra nøkkelgeneratoren. Dersom resultatet av denne addisjon gir et av de to tegn som ikke er tillatt, blir addisjonen utført en gang til, hvorved $X(P)$ igjen fremkommer $X(P) \oplus Z \oplus Z = X(P)$. I dette tilfelle brukes $X(P)$ som chifret tegn.

Dechifreringsprosess

Dechifreringsprosessen starter når avlesekretsen mottar en start puls fra det chifrede tegn $X(P) \oplus Z$, som da forskyves inn i REG X, mens det foregående dechifrede tegn leses av fjernskriveren via dennes drivforsterker. Innholdet av REG X og REG Z adderes så modulo-2 og resultatet, $X(P) \oplus Z \oplus Z = X(P)$, settes inn i

REG X. Klarteksttegnet X kan nå teoretisk gjenvinnes ved å fremmate REG X "P" trinn bakover i syklusen, eller ved å forskyve REG X 30-"P" trinn forover. Sistnevnte metode utføres ved å innstille C(P) til 31-"P" og telle ned til 1. På mottagersiden utføres selvfølgelig også addisjonen $\text{REG X} \oplus \text{REG Z}$ to ganger dersom et uønsket tegn detekteres.

Startprosedyre

Som tidligere nevnt trengs 6 tegn for å utstyre hovedregisterne med start-informasjon. Disse 6 tegn innføres først i hver melding som skal chifreres og velges enten tilfeldig eller i henhold til en liste over lange sykluser i nøkkelgenerator-en. Disse tegn chifreres for sending ved å benytte en fra pluggbordet bestemt innstilling av hovedregisterne.

Telex-tilkobling

Chifferteksten må ikke inneholde tegn som ikke kan trykkes av en vanlig fjernskriver i telex-installasjon eller tegn som vil forstyrre overføring på en telex-kanal, som f.eks. HVEM DER. Slike tegn unngås ved å ikke bruke tegnene ALL SPACE og TALL SKIFT som chiffertekst. Chiffertekstalfabetet inneholder derved 30 tegn mens der er 31 tillatelige klarteksttegn. En ren chifring av disse 31 tegn er derfor ikke mulig. Problemet er løst ved å innføre restriksjoner ved chifring av VOGN TILBAKE og NY LINJE.

Ikke-tillatte tegn unngås meget enkelt ved å utelate de to kritiske tegn i inngangsregisteret REG X når dette arbeider som et normalt lineært tilbakekoblet skyverregister. REG X fremmates således langs en 30-syklus som inneholder alle mulige 5-elements kombinasjoner unntatt de to som svarer til fjernskrivertegnene ALL SPACE og TALL SKIFT.

Blokk-skjema

I figur 1b er vist et blokkskjema som omfatter de viktigste styretråder, for å gi en bedre forståelse av det detaljerte skjema.

Generell beskrivelse

På fig. 1c-i og 2a-h er det vist en detaljert blokktegning over oppfinnelsens utførelse. Den viste kretsen representerer et "off-line" kryptografisk utstyr hvor nøkkelmaterialet ikke er anbragt på en strimmel, hvilket utstyr er istand til å chifrere og dechifrere normale fjernskrivermeldinger på en måte som kan sammenlignes med standard telex operasjoner.

Hovedblokkene er antydnet med brutte linjer, og terminalene for hver hovedblokk er nummerert med individuelle nummere. Terminalene er videre utstyrt med betegnelser slik at deres sammenkoblinger er lett forståelige.

I omtrent alle hovedblokkene er det antydnet passende testpunkter. Disse punktene har betegnelsen TP1, TP2 ... TP5 og vil ikke bli ytterligere beskrevet.

I hovedblokkene er det brukt logiske symboler som er beskrevet i detalj i forbindelse med diagrammet over symbolene, Fig. 6. Alle de logiske blokkene er utstyrt med koder som er individuelle for hver hovedblokk. Flip-flop kretsene er i tillegg utstyrt med funksjonalistiske betegnelser plassert omtrent i midten av det logiske symbolet.

Blokk 1 i Fig. 1c, d inneholder fem par modulo-2 addisjonskretser. Alle addisjonskretsene bortsett fra den nederste, består av en NAND-port og en EXCLUSIVE-OR-port. Den nederste kretsen består av tre NAND-porter A1, A2, A3. Utgangene fra hvert par er koblet til inngangene til en individuell EXCLUSIVE-OR-port. Ved hjelp av to portsignaler K5 og K4 kan enten den nedre eller øvre addisjonskretsen hos hvert par ha sin utgang koblet til utgangen fra de fem EXCLUSIVE-OR-portene E1, E2, K1, K2, B2.

Blokk 2 i Fig. 1c, d inneholder seks flip-flops, $X_1 - X_6$, med sine respektive kretser. Flip-flop kretsene $X_1 - X_5$, utgjør et tilbakekoblet skyveregister (register X) som brukes til å oppbevare og behandle informasjonselementene bestående av fjernskrivertegn. Flip-flop kretsen X_6 brukes til forsinkelser. I tillegg til inngangskretsene for flip-flop kretsene $X_1 - X_6$ inneholder også blokk 2 fire NAND-porter A2, D2, A1, D1 for å detektere om innholdet av flip-flop kretsene $X_1 - X_5$ henholdsvis tilsvarende ett av fjernskrivertegnene TALLSKIFT (1 ...), VOGN TILBAKE ($\Leftarrow$), NY LINJE ($\equiv$) eller ALL SPACE (B1).

Blokk 3 i Fig. 2d, f inneholder forskjellige port- og flip-flop-kretser hvorav de viktigste er hukommelsesflip-floppen som er brukt til oppbevaring av tegnet NY LINJE under dechifreringen, innstillingsflip-floppen som er brukt til å frembringe de nødvendige signaler for startinnstillingen av nøkkel generator-registrene, og hovedprogramtelleren (teller K) som består av fem tellertrinn $k_1 - k_5$.

Blokk 4 i Fig. 2c, b inneholder inngangs-telleren $\overline{FF}_0$, FFe, FFa, FFb, FFc, FFd og FF_{s2} med tilhørende kretser. Dette er en binær teller som brukes til å styre innmatningen av fjernskrivertegnene inn og ut av utstyret.

Blokk 5, Fig. 2a som inneholder blokkene 25 kHz OSC (tidspulsgenerator) og RES (tilbakestillingskrets) er vist i detalj på Fig. 4. Tilbakestillingskretsen brukes til å gi likestrømsignaler til hovedregisteret i generatoren for nøkkelmaterialet.

Blokk 6 i Fig. 2a som inneholder blokken OS er vist i detalj på Fig. 3. Denne kretsen brukes til tidsstyring av inngangstelleren.

Blokk 7 i Fig. 2d, e, f, g, h inneholder en ring-teller (teller 1) med tre trinn i2 - i4 og en annen ring-teller (teller 3) også med tre trinn j1 - j3. Disse to tellerene brukes til å regulere startprosessen til utstyret. Blokk 7 inneholder også en binær teller (teller P) med fem trinn $C_1 - C_5$. Den sistnevnte er en binærteller som er brukt til telling nedover fra et startpunkt mottatt som likestrøms-signaler fra blokk 8.

Blokk 8 på Fig. 2e,g,h inneholder forskjellige port-kretser. Port-kretsene brukes til å forsyne telleren $C_1 - C_5$ i blokk 7 med nødvendig opplysninger fra generatoren for nøkkelmaterialet i henholdsvis chifrerings- og dechifreringsfasen.

Blokk 9 på Fig. 1e,f inneholder et nøkkel-tegn register (register Z) med fem trinn $Z_1 - Z_5$. Dette register mottar normalt på terminalene J, K, I trinn Z sine opplysninger i serie form fra nøkkelgeneratoren. Opplysninger kan imidlertid også komme parallelt fra en utvendig båndleser med betegnelsen TR. Blokk 9 inneholder også en hovedforsterker for skyvøpulsene hvilken forsterker består av portene C2, C3, C4, og F, G, H1 og H2. Den inneholder også et skyveregister (register Y) $Y_1 - Y_5$ som brukes som et mellomliggende oppbevaringsregister under startfasen.

Blokkene 10, 11 og 12 på Fig. 1e,f,g,h,i utgjør nøkkelgeneratoren, som igjen inneholder to 15-elementers ikke-lineære tilbakekoplete skyveregistere, REG I₁ - REG I₁₅ - REG II₁ - REG II₁₅, med triggerflip-flops og tilhørende utgangs- og inngangs-port-kretser.

Blokk 14 på Fig. 2a inneholder blokkene RC (Innlesningskrets) og DA (Driverforsterker) som er vist i detalj på Fig. 5.

Plug A på Fig. 1c,d inneholder sammenkoplede forbindelser mellom dens terminaler som bestemmer mønsteret av tilbakekoplingen på tilbakekoplingsskyveregisteret $X_1 - X_5$, blokk 2, som igjen er brukt i chifrerings- og dechifreringsprosessen.

Blokk TR på Fig. 1f er en strimmelavleser. Denne innretningen er normalt ikke tilkople, men kan koples inn for å muliggjøre bruken av engangs nøkkelstrimmel som nøkkelmateriale.

Gitterene med betegnelsen PB på Fig. 1g,h,i viser skjematisk et pluggbord som brukes for innsetting av informasjoner angående nøkkelmaterialet i utstyret. Sirklene rundt krysningspunktene mellom horisontale og vertikale linjer antyder at det er elektrisk forbindelse ved hjelp av en kortslutningskontakt.

På Fig. 1e,h,2b er det vist flere veksel-kontakter med betegnelsen enten S eller $\bar{S}$. Disse er kontakter på en bryter med tre stillinger. Bryterens midtstilling tilsvarer at utstyret er i ro eller i klarstilling. De andre to stillinger tilsvarer sending og mottaking eller henholdsvis chifring og dechifring.

Blokk TP på Fig. 1f antyder en fjernskriver med dens sendekontakt og mottakerspole. Dette er også vist på Fig. 5.

Blokk TB1 (Fig. 2a) er en terminal-stripe. S4 (Fig. 2a) er en bryter med to stillinger som tilsvarer enkelt-strøms og dobbelt-strøms drift av fjernskriveren. S3 (Fig. 2a) er en bryter med to stillinger som tilsvarer tyve og tredve mA dobbelt-strøm eller førti og seksti mA enkeltstrøm til fjernskriverens mottakermagnet. Flerstillingsbryteren JB (Fig. 2a) brukes for valg av riktig tidskonstant for den monostabile kretsen i blokk 6 (Fig. 2a).

BESKRIVELSE AV VIRKEMÅTEN

Innledning

Som nevnt kan ikke chiffterteksten inneholde tegn som ikke kan punches av en vanlig fjernskriver i en telex-installasjon, eller tegn som kan forstyrre overføringen i en telexkanal, slik som tegnet HVEM DER.

Chifreringsprosessen starter når avlesningskretsen mottar startpulsene fra tegn X i en klar tekst som betjenes fra nøkkelbordet eller den automatiske senderen hos en fjernskriver. Avlesningskretsen starter en oscillator, som igjen gir skyvepulser til registerene X (Fig. 2c,d), I (Fig. 1g,i), II (Fig. 1h,i) og X (Fig. 1e). På den måten sendes det foregående chifrerte tegn til fjernskriveren fra register X via fjernskriverens driv-forsterker. Når register X inneholder de 5 informasjons-elementene, inneholder register Z 5 "nye" nøkkelelementer og teller P (Fig. 2g,h) innstilles på et nytt P-nummer. Nå er register X koplet som et tilbakekoplings-skyveregister med maksimal lengde, og skyve-pulsene tilføres til teller P og register X. Tilførselen av 25 kHz skyve-pulser stoppes når teller P = 0, d.v.s. etter P pulser. Deretter koples X som et vanlig skyveregister og innstilles for informasjonsregister $X \oplus$ register Z. Dette er den chifrerte formen på den klare teksten som sendes ut når det neste klare teksttegnet skyves inn i register X. Dette er den vanlige chifreringsprosessen. For å unngå visse vanskeligheter i samband med telexkanalene brukes ikke chiffer-teksttegnene ALL SPACE og TALLSKIFT. Den førstnevnte fordi noen fjernskrivere ikke kan perforere ALL SPACE. TALLSKIFT unngås fordi forstyrrelser i overføringen kan oppstå for visse "tall"-tegn.

Nå når en av disse to kombinasjonene er oppdaget som chifrert tekst, blir ikke register X innstilt til register $X \oplus$ register Z, men det forblir i ro. På denne måten sendes den forskjøvnede klarteksten i register X ut som chifrert tekst.

Denne prosessen er reverserbar, og dette muliggjør dechifreringsprosessen.

Chifreringsfasen

La det først være antatt at startprosess som vil bli forklart senere er blitt utført, og at normal chifreringsprosessen skal finne sted. Tegnet som skal chifrerer, går inn i utstyret seriemessig fra fjernskriverens overføringskontakt TP (Fig. 2a) som har krafttilførsel fra avlesningskretsen RC i blokk 14. (Fig. 2a). I avlesningskretsen RC blir strømmen som går igjennom eller ikke gjør det, til overføringskontakten forandret til logiske nivåer som passer for resten av utstyret. Utgangs-signalet fra avlesningskretsen går til blokk 4 (port A1) (Fig. 2a) som inneholder inngangstetteren $\overline{FF_0}$, $\overline{FF_e}$, $\overline{FF_a}$, $\overline{FF_b}$, $\overline{FF_c}$, $\overline{FF_d}$ og de tilhørende kretser. Ved mottakelsen av startpulsene fra det tegnet som skal chifrerer vil denne inngangs-telleren gjennomgå en komplett syklus med en hastighet som er bestemt av den monostabile kretsen OS

i blokk 6, Fig. 2a. Signaler som skriver seg fra inngangstelleren brukes til å styre innmatningen av tegnet inn i inngangsregisteret i blokk 2, Fig. 1c,d og også til å fremmate nøkkelgeneratorregisterene i blokkene 10, 11 og 12. Når inngangstelleren har gjennomløpet sin syklus, vil de fem informasjonselementene som er av fjernskrivertype, bli lagret i inngangsregisteret $X_1 - X_5$ i blokk 2.

Chifreringsprosessen vil så starte. Denne prosessen styres av en ringteller $k_1 - k_5$ i blokk 3 Fig. 2f kalt telleren K. Telleren K forblir i sin hvilestilling under inngangs-tellerens syklus. På slutten av inngangstellerens syklus, d.v.s. når det siste informasjonselementet av fjernskriverkarakter er matet inn i register X, vil telleren K gå til stilling K2.

I denne stillingen K2 vil en vurdering og mulig modifikasjon av klartekst i register X finne sted. Dette er nødvendig fordi chifferteksten som tilslutt dannes fra chifreringsprosessen ikke må inneholde tegn som ikke uten vanskeligheter kan overføres gjennom en telex-kanal. I dette utstyret må ikke tegnene ALL SPACE og TALLSKIFT forekomme i den chifrede teksten. Det førstnevnte er ikke tilstede i den klare teksten, men det sistnevnte er det. For å få TALLSKIFT fjernet fra den chifrede teksten vil dette tegnet i den enkle teksten bli forandret til VOGN TILBAKE. For å forhindre forvirring må VOGN TILBAKE i den klare teksten forandres til NY LINJE. Dette er mulig fordi det antas at i den klare teksten opptrer de to tegnene VOGN TILBAKE og NY LINJE alltid parvis. Hvis nødvendig utføres forandringene av den klare teksten som er beskrevet ovenfor i programtellerstillingen K2 ved å benytte en skyvepuls i inngangsregistertrinnene $X_1 - X_5$. Programtelleren K går deretter til stilling K3. I denne stillingen K3 finner det første skritt i chifreringsprosessen sted. Inngangsregisteret X er nå koplet som et tilbakekopplingsregister med maksimal lengde. Det vil motta et antall skyvepulser bestemt av innholdet i teller P, Fig. 2g,h, som utgjøres av flip-flop $C_1 - C_5$ i blokk 7, Fig. 2g,h. Denne teller teller nedover fra sin startposisjon og til null ved hjelp av signalet fra hoveduret. Startposisjonen er bestemt av et "pseudo-random" tall P som er overført fra nøkkelgeneratoren REG I, REG II, Fig. 1g,h,i til teller P, Fig. 2g,h, i parallell når hovedprogramtelleren K, Fig. 2f, er i posisjon K2. Når telleren P har nådd nullstillingen, vil programtelleren K gå fra K3 til K4, og trinn to i chifreringsprosessen vil finne sted.

Denne andre chifreringsoperasjonen består av modulo-2 addisjon i blokk 1 av innholdet i inngangsregister X og et vilkårlig nummer som kommer inn i parallell fra register Z i blokk 9, Fig. 1e. Som det fremgår av tegningen, inneholder registeret Z fem trinn Z_1 til Z_5 som er koplet som et vanlig skyveregister. Informasjonen som går inn i register Z, kommer fra utgangen til de to nøkkelgeneratorregisterene, REG I, REG II ved port D3 i blokk 12, Fig. 1i. Register Z skyves sammen med de to nøkkelgenerator-registerene REG I, REG II under innmatningen av klarteksttegnet

med programtelleren i posisjon K1. Modulo-2 addisjonen av innholdet i inngangsregisteret X og i nøkkeltegnregisteret Z foretas som nevnt ovenfor i parallell uten noen overføring av mente-informasjon fra trinn til trinn. Før programtelleren K slås over til K5, sjekkes innholdet i register X for å kontrollere om det kan overføres til linjen. Portene D1 og A2 i blokk 2, Fig. 1 sjekkes om registeret inneholder henholdsvis tegnene ALL SPACE eller TALLSKIFT, og modulo-2 addisjonene vil så bli gjentatt.

Innholdet i register X vil således være som det var etter trinn én i chifreringsprosessen. Fordi ALL SPACE aldri vil være tilstede under normalsyklusen hos et tilbakekopplingsregister med maksimal lengde, og fordi stillingen TALLSKIFT automatisk unngås i dette utstyret, kan innholdet i register X etter chifreringsprosessens trinn én alltid overføres til linjen. Som en kan se brukes ikke annet trinn i chifreringsprosessen når det resulterer i et tegn som ikke kan overføres til linjen.

Det chifrerte tegnet som nå er i register X, overføres til fjernskriverens mottakermagnet TP, Fig. 2a, under innmatningen av det neste enkle tekst-tegnet i register X, hvorpå den ovennevnte prosessen gjentas.

Startprosessen som er nevnt tidligere, er nødvendig for å sikre at nøkkelgenerator registerene REG I, REG II har forskjellige startpunkter fra melding til melding. Under chifreringsfasen består denne startprosessen av innmatningen av 6 fjernskriver-tegn, d.v.s. 30 elementer inn i nøkkelgenerator registerene. Samtidig chifrerer og overføres disse 6 tegnene til fjernskriverens mottakermagnet TP (og deretter til linjen). På mottaker- eller dechifreringsiden vil de 6 tegnene bli dechifrert og overført inn i dechifreringsutstyrets nøkkelgenerator registre. På denne måten er en sikret samme startpunkt både for chifrerings- og dechifreringsutstyret. De 6 tegnene som gir et startpunkt, tas under vanlig drift fra en startpunktstabell som på forhånd er forberedt for et spesielt tilbakekopplingsmønster i nøkkelgenerator registerene. Under chifreringen overføres ikke startpunkttegnene direkte fra avlesningskretsen til nøkkelgenerator registerene, men de går gjennom et mellomliggende lager-register, register Y i blokk 9, Fig. 1e. Register Y mottar skiftpulser samtidig med nøkkelgenerator registerene REG I, REG II, og det ovenfor nevnte nøkkeltegnregisteret Z.

De nødvendige portfunksjoner under startprosessen blir holdt rede på av to tretrinns ringtellerer I og J i blokk 7, Fig. 2f,h. Teller I som inneholder trinnene $i_2 - i_4$ slås over en gang for hver komplette syklus telleren K, Fig. 2f, gjør. Telleren J som inneholder trinnene $j_1 - j_3$ fremmates en gang for hver fullstendige syklus telleren I gjør.

Pluggbordet PB, Fig. 1g,h,i, lagrer opplysninger om hvordan utgangsstillingen skal være for registerene REG I og REG II, Fig. 1e,f,g,h,i. Det er $2^{30} \cdot 10^9$ mulige innstillinger. Startinnstillingene brukes til chifrerer av de 6 tegnene som er valgt for å gi tilstrekkelige lengder på syklusene i de ovennevnte registerene. Teller-

ene $i_2 - i_4$ og $j_1 - j_3$ i blokk 7 holder greie på startprosedyren og bestemmer når registerene skal mates med startinformasjoner.

Signalet fra hoveduret som styrer alle funksjonene i utstyret skriver seg fra en 25 kHz oscillator i blokk 5, Fig. 2a, som gir firkant-bølger. Blokk 5, inneholder også en tilbakestillingskrets som gir den strømmen som er nødvendig for å innstille alle flip-flop kretsene i nøkkelgenerator registerene til nullstilling når utstyret er i klar eller hvilestilling.

Dechifreringsfasen

Dechifreringen av et tegn starter med en overføring av et tegn fra fjernskriverens overføringskontakt TP og inn i utstyret slik som i chifreringsfasen. Startpulsene fra tegnet som skal chifreres vil også i dette tilfellet starte opp en syklus i inngangstelleren i blokk 4, Fig. 2c. På samme tid mates chifferetekst-tegnenes informasjonselementer, som skal dechifreres, inn i inngangsregisteret X. Dette skjer mens programtelleren K er i sin hvilestilling K1. De to trinnene i chifreringsprosessen må nå utføres i omvendt rekkefølge. Derfor utføres i programteller K's stilling K2 modulo-2 addisjon av innholdet i register X og Z. Hvis innholdet i register X etter modulo-2 addisjonen er lik ALL SPACE eller TALLSKIFT, er det tydelig at modulo-2 addisjonen er blitt utført to ganger i løpet av chifreringsprosessen. Av denne grunn gjentas det også her, og dette betyr at bare den motsatte prosess av trinn 1 i chifreringsprosessen vil bli utført. Et fem trinns tilbakekopplingsregister med maksimal lengde har en syklus på 31. I dette utstyret passerer automatisk stillingen som tilsvarende TALLSKIFT. Derfor har dette registeret en effektiv lengde på 30 stillinger. For å reproducere den opprinnelige klare teksten under dechifreringsprosessen er det nødvendig å fremmate register X 30-P trinn. Dette gjøres, som tidligere nevnt under forklaringen av chifreringsprosessen, ved å innstille P riktig. Skyvingen av register X i løpet av dechifreringsprosessen foretas med programtelleren i stilling K3. Tilslutt må det med programtelleren i stilling K4 utføres en modifisering som opphever den som foretas under chifreringsprosessen. Som det er forklart ovenfor, ble tegnet TALLSKIFT forandret til VOGN TILBAKE, og tegnet VOGN TILBAKE ble forandret til NY LINJE. Hvis derfor det chifrerte tegnet som inneholdes i register X, er lik VOGN TILBAKE må det forandres til NY LINJE. Dette foretas ved å tilføre en skyvepuls til trinnene i register X med programtelleren i posisjon K4. Hvis innholdet i register X etter å ha mottatt tilbakekoppling er likt NY LINJE, kan dette skyldes enten et NY LINJE tegn under chifreringsprosessen eller et omforandret VOGN TILBAKE under chifreringsprosessen. Som nevnt ovenfor antas det at tegnene VOGN TILBAKE og NY LINJE opptre parvis og i samme rekkefølge som akkurat nevnt. Når tegnet NY LINJE først fremgår etter tilbakekopplings-skift operasjonen, blir det øyeblikkelig forandret til VOGN TILBAKE med programtelleren i posisjon K4. Denne forandringen oppbevares også ved å innstille hukommelses-flip-floppen i blokk 3, Fig. 2d. Såfremt VOGN TILBAKE og NY LINJE

alltid overføres parvis, vil det neste tegnet som dannes fra tilbakekoplingsskyveoperasjonen under dechifreringen, igjen være NY LINJE. I og med at hukommelsesflip-floppen nå er innstillet, sløyfes forandringen av tegnet NY LINJE med programtelleren i stilling K4. Dette betyr at NY LINJE vil være det chifrerte tegnet som skal overføres til fjernskriverens mottakermagnet TP, Fig. 2a, i løpet av den neste innmatingsprosessen. Som en forstår er tegnet VOGN TILBAKE på denne måten blitt overflødiggjort, og den fjernskriverkombinasjonen som vanligvis brukes for overføring av dette tegnet, brukes isteden til å overføre TALLSKIFT. Denne unngåelsen av fjernskriverkombinasjonen TALLSKIFT fra den chifrerte teksten er innført for å hindre talltegn i alfabetet for chiffterteksten. Dette er nødvendig fordi det i en ubetjent telex-stasjon ikke kan tillates at svarenheten utløses, mens chiffterteksten er i ferd med å komme inn. Som kjent utløses svarenheten ved hjelp av HVEM DER. Ved å unngå tegnet TALLSKIFT fullstendig i chiffterteksten, vil aldri fjernskriveren settes i "upper case" når den mottar en chiftert beskjed.

BESKRIVELSE AV HOVEDKRETSENE

Nøkkelgenerator

Nøkkelgeneratoren inneholder to ikke-lineære tilbakekoplingsskyveregistere, REG I og REG II (Blokkene 10, 11, 12, Fig. 1g,h,i), hver med 15 trinn, henholdsvis REG I₁₋₁₅ og REG II₁₋₁₅, og med et tilbakekoplingssignal $F(A_1, A_j, A_k, A_l)$ A_{15} , der $F(A_1, A_j, A_k, A_l)$ er en ikke-lineær funksjon hvis kombinasjonstabell over de binære variable A_1, A_j, A_k og A_l dannes av utgangssignalene fra fire av registertrinnene. i, j, k og l er alle forskjellig og ellers tilfeldig valgt ved hjelp av plugger på et pluggbord.

Dette er vist på Fig. 1g,h,i der tilbakekoplingssignalet fra REG I tas fra trinnene Nr. 4, 14, 10 og 9, slik at i, j, k og l i dette tilfellet er lik henholdsvis 4, 14, 10 og 9. Disse fire utgangssignalene mates inn på portene B4, C1, B3 og C2 i blokk 12, Fig. 1i, og det kombinerte signalet fra porten C2 er modulo-2 addert i portene E4, F1 med utgangssignalet A_{15} fra det siste trinnet REG I₁₅. Tilbakekoplingssignalet tilføres registeret REG I ved port D1, blokk 10, Fig. 1e,g.

Tilbakekoplingssignalet til registeret REG II tas på samme måte fra trinnene Nr. 7, 10, 3 og 6, kombinert i portene B1, A1, B2 og A2, blokk 12, Fig. 1i. Dette kombinerte signalet modulo-2 adderes til utgangssignalet A_{15} fra det siste registertrinnet REG II₁₅ i portene E3, F2 og overføres til registerinngangen i port D2, blokk 11, Fig. 1f,h.

Dette er en registertype som enda ikke er helt matematisk forklart i litteraturen, men det er klart at en lang syklus fra et slikt register alltid gir et "pseudorandom" mønster. Videre har sekvensene vanligvis forskjellige lengder som betyr at nøkkelgeneratorregisterenes fysiske lengder kan være like. Det er likevel visse

muligheter for at en sekvens kan være meget kort. Derfor er ikke startpunktene i dette systemet fullstendig vilkårlig, men de er valgt for å gi tilstrekkelige lengder på syklusene. I det nuværende utstyret som har to 15-elementers registre, må 6 tegn velges for hver melding som skal sendes. Utgangs-signalene fra de to registerene er modulo-2 addert i portene D1, D2, D3 og D4, Fig. 1i, for å gi den ønskede rekkefølgen av "pseudo-random" nøkkelementer. Slike sekvenser oppbevares i et 5-elementersregister $Z_1 - Z_5$, blokk 9, Fig. 1e. Antallet forskjellige koplinger er

$$\binom{15}{4} \times \left(\binom{15}{4} - 1 \right) \approx 1.86 \times 10^6$$

I de to registerene REG I og REG II er det brukt "trigger" flip-flops. I en "trigger" flip-flop er innholdet etter en tidspuls avhengig av inngangs-signalet såvel som av det signalet som er tilstede i selve flip-flopkretsen. Det følgende likningssettet beskriver derfor registerets yteevne:

$$A_1' = F(A_i, A_j, A_k, A_l) \oplus A_{15} \oplus A_1$$

$$A_2' = A_1 \oplus A_2$$

$$A_3' = A_2 \oplus A_3$$

$$A_{15}' = A_{14} \oplus A_{15}$$

A_1 er signalet som befinner seg i registertrinn Nr. 1 før en tidspuls, og A_1' er signalet som er i det samme trinnet etter tidspulsen. På samme måte er det for de andre trinnene, og yteevnen er lik for de to registerene.

Generator for "P"

P er et 5-elementers "pseudo-random" tall tatt fra de to registerene REG I og REG II, Fig. 1g, h, i, på den måten som er vist i blokk 8, Fig. 2e,g,h. Hvert element er resultatet av en modulo-2 addisjon av utgangs-signalene fra tilfeldig valgte elementer i begge registre. Blokk 8, Fig. 2e,g,h inneholder 5 portkretser som det til hver tilføres to signaler fra pluggbordet PB. Til det første portkomplekset som består av portene C1, C2, C3, C4, B1, B2, B3 og D2, blokk 8, Fig. 2e tilføres det signaler fra pluggbordmultiplene PB/A og PB/M. Som det fremkommer fra Fig. 1g,h, er PB/A tilknyttet REG I, mens PB/M er tilknyttet REG II. En liknende sammenheng er tillagt de andre fire portkretser. Antall forskjellige brukbare koplinger er:

$$\binom{15}{5} \times \binom{15}{5} \approx 9 \times 10^6$$

Utgangen fra hver av portkretsene som tilsammen utgjør tallet P overføres til en teller $C_1 - C_5$, blokk 7, Fig. 2g,h.

Under chifreringen mates tallet P inn i den binære telleren $C_1 - C_5$, men under dechifreringen mottar denne telleren tallet $31 - P$. I begge tilfellene teller telleren ned til null samtidig som den teller pulsene fra 25 kHz-tilførselen.

Inngangsregister

Reg X (Blokk 2, Fig. 1c,d) som består av trinnene $X_1 - X_5$ har to operasjonsfaser.

- Det virker som et normalt 5-elements skyveregister og mottar skyve-pulser med 50 Hz (for 50 Bauds fjernskriverhastighet).
- Det virker som et tilbakekoplings-skyve-register der hvert trinn inneholder en modulo-2 addisjonskrets, d.v.s. porten H1, og en flip-flop, d.v.s. X_1 . En hvilken som helst utgang kan koples til en hvilken som helst inngang ved hjelp av koplinger loddede til en plugg, PLUG A, og disse koplingene utføres i henhold til et polynom, og de resulterer i en sekvens med maksimal lengde $2^5 - 1 = 31$. 5-elements-kombinasjonen som danner tegnet TALLSKIFT, fjernes fra syklusen. På denne måten gjennomgår REG X en 30-syklus som inneholder alle mulige 5-elementskombinasjoner bortsett fra ALL SPACE og TALLSKIFT. Det er tilnærmet 15 000 forskjellige sykluser å velge mellom. Skyvepulsene i dette tilfellet kommer fra 25 kHz-kilden, og antallet pulser er likt det antall trinn som telleren $C_1 - C_5$, blokk 7 teller.

Pluggbordet

Pluggbordet (PB), Fig. 1g,h,i, er en tavle med "horisontale" og "vertikale" terminal-rekker arrangert i matrisseform med tilnærmet 300 krysspunkter (hull). En plugg som settes inn i et krysspunkt vil sammenkople de horisontale og vertikale terminal-rekkene i dette spesielle krysspunktet. Pluggen på pluggbordet bestemmer hvilke utganger som bør brukes for tilbakekoplingsfunksjonene, og hvilke utganger som bør brukes til å fremskaffe tallet P, og hvilke flip-flop-kretser som innstilles først.

Monostabil Multivibrator

Fig. 3 viser det detaljerte skjematiske diagrammet over blokk 6 på Fig. 2a. Denne kretsen OS gir tidsreferansen for fjernskrivers inngangs- og utgangssignaler. Definerte tidsintervaller oppnås ved hjelp av en monostabil multivibrator som inneholder transistorene Ts1 og Ts2 med de tilhørende komponenter. I hvile-fasen leder transistor Ts1 mens Ts2 er koplet fra. En "trigger"-puls som tilføres gjennom en diode D3 vil kutte ut transistor Ts1. Ved regenerativ virkning av kretsen vil igjen transistor Ts2 lede. Denne tilstanden vil vare inntil kondensatoren C1 er utladet gjennom motstand R3. Transistor Ts1 vil begynne å lede igjen og Ts2 vil koples ut.

Transistor Ts4 leder en kort stund når kretsen kobles tilbake igjen til hviletilstanden. På denne måten lades tidsstillings-kondensatoren C1 raskt opp. Herav oppnås en meget kort tilbakestillingstid. Kretsens pulslengde er upåvirket av høy belastning. Transistorene Ts3 - 4 og Ts5 - 6 danner inngangs-kretsen. Utløsningen av kretsen inntreffer hver gang transistor Ts3 koples inn. Motstanden R8 som er koplet til basis av Ts3, brukes til å forhindre mulige utløserpulser når kretsen er i sin tilsynelatende stabile tilstand. Utgangs-signalet tas fra transistor Ts7's kollektor. I hvilefasen er som tidligere fastslått, transistor Ts2 ikke strømførende. Ts7 vil da heller ikke være strømførende, og utgangen vil være kraftig. Når kretsen innstilles til sin tilsynelatende stabile tilstand er Ts2 strømførende, og på samme måte Ts7. Utgangs-signalet vil da være lavt, d.v.s. nesten likt jordingspotensialet. Tidsstillings-kondensatoren C1 inneholder fire elementer med betegnelsen C1a - C1d. Hensikten med dette arrangementet er å oppnå forskjellige puls-lengder ved hjelp av utvendige forbindelser, slik at kretsen kan tilpasses forskjellige fjernskriverhastigheter. Sammenkopling av terminalene 3 - 4 gir en hastighet på 75 Bauds, 6 - 4 tilsvarende 50 Bauds, og 5 - 4 tilsvarende 45 Bauds.

Transistorene kan være av følgende typer:

Ts1: 2S 201; Ts2 - 3; 2S 302; Ts4; 2N 1711; Ts5 - 7; BSY 95A eller tilsvarende komponenter, og alle diodene kan være av typen 1S 920 eller liknende.

Tids-puls generator

Fig. 4 viser en detaljert skisse over to forskjellige kretser i blokk 5, Fig. 2a. Den øvre er tids-puls generatoren, 25 kHz OSC. Dette er en astabil multivibrator som inneholder transistorene Ts1 og Ts2 pluss tilhørende komponenter. Transistorene Ts3 og Ts4 er kretsens utgangsforsterkere. Hensikten med diodene D1, D2 og utjevningsskondensatoren C3 er å unngå en stabil tilstand der begge transistorene er ledende på samme tid, hvilket kan inntreffe med en konvensjonell astabil multivibrator.

Tilbakestillingskretsen

På nedre del av Fig. 4 er det vist en tilbakestillingskrets RES som har til oppgave å tilføre et likestrøms-signal til tilbakekoblings-registerenes nøkkelgenerator. Når en av inngangstransistorene Ts6 eller Ts7 er strømførende vil også utgangstransistoren Ts5 være strømførende og tilføre strøm til belastningen. Hvis begge transistorene er i en frakoplet tilstand vil heller ikke utgangstransistoren Ts5 være strømførende. Transistorene kan være av følgende typer: Ts5; 2S 302; Ts1-4, 6-7; BSY 27 eller tilsvarende komponenter, og diodene D1-2 kan være av typen 1S 920 eller liknende.

Avlesningskretsen

Fig. 5 viser en detaljert skisse av kretsene som finnes i blokk 14 på Fig. 2a. På øvre del av Fig. 5 er avlesningskretsen RC vist. En strøm på omtrent 40 mA til-

føres avlesningskretsen RC fra + 50 V kilden gjennom motstandene R17 via terminalene 6 og 3 gjennom fjernskriverens kontakt TP og tilbake. Hvis fjernskriverkontakten er lukket, vil inngangstransistoren Ts9 bli strømførende. Hvis fjernskriverkontakten er åpen, vil Ts9 ikke være strømførende. Utgangssignalet som tas fra kollektoren på Ts9, vil være lavt når fjernskriverkontakten er lukket, hvilket tilsvarende MARK, og det vil være høyt når fjernskriverkontakten er åpen, hvilket tilsvarende SPACE. For å ha utgangssignalet tilgjengelig i motsatt fase er et inverteringsstrinn som består av Ts8 og tilhørende komponenter, lagt til avlesningskretsen.

Drivforsterkeren.

På den nedre del av Fig. 5 er det vist en detaljert skisse av fjernskriverens drivforsterker DA. Denne kretsen inneholder inngangstransistorene Ts1, Ts2 og Ts3 med tilhørende komponenter, to generatorer med konstant strøm, Ts6 og Ts7 med tilhørende komponenter og to fjernskrivertransistorer Ts4 og Ts5 for strømkopling og de tilhørende komponenter. Ved hjelp av ytre koplinger, S3, kan kretsen tilpasses til å virke for enkel- eller dobbelstrøm og på to forskjellige strømnivåer. Ved drift med enkelstrøm er de to generatorene med konstant strøm koplet i parallell. I MARK tilstand leder derfor transistor Ts5, mens Ts4 er ikke-strømførende. Strømmen fra konstantstrømsgeneratorene går således gjennom fjernskriverens mottakermagnet M. I SPACE tilstand leder transistoren Ts4, mens Ts5 er ikke-strømførende. Ingen strøm går derfor gjennom fjernskriverens mottakermagnet M. På inngangssiden tilsvarende MARK et høyt inngangssignal og SPACE et lavt inngangssignal. Transistorene kan være av de følgende typer Ts1, Ts2, Ts3, Ts8, Ts9: BSY 95A; Ts4, Ts5: 2N 1893; Ts6, Ts7: 2N 2904A eller tilsvarende komponenter, mens diodene D1, D2 kan være av typen ZF 5.6 eller liknende.

Logiske Symboler

På Fig. 6 er vist de forskjellige symbolene som representerer de forskjellige logiske funksjonene i hoveddiagrammet. Disse er: Inverter, 2-inngangs NAND-port, 3-inngangs NAND-port, 5-inngangs-NAND-port, JK flip-flop med forhåndsinnstilling og en EXCLUSIVE-OR-port.

Disse logiske symbolene og deres funksjon er beskrevet i detalj i folderen "Series 73 Solid Circuit Semiconductor Networks", Bulletin No. DL-S 567650, July 1965, som er utgitt av Texas Instruments Incorporated. Symbolene vist fra toppen i Fig. 6 tilsvarende det følgende TI nettverk: 1/4 SN 7350, 1/4 SN 7360, 1/3 SN 7331, 1/2 SN 7311, 1/2 SN 7302 og 1/2 SN 7370. Symbolene som tilsvarende 1/4 SN 7350, 1/2 SN 7302 og 1/2 SN 7370 er av enkelhetshensyn tegnet noe forskjellig.

PATENTKRAV:

1. Fremgangsmåte for chifring av en klartekst ved hjelp av et register, karakterisert ved at hvert klarteksttegn X chifres slik at et tilsvarende chiffertegn C fremkommer ved innmating av klarteksttegnet X i registeret hvorpå registeret fremmates fra et startpunkt bestemt av klarteksttegnet X i den bestemte syklusen et antall trinn P , der P er en variabel verdi bestemt av en nøkkelmateri-
generator.
2. Fremgangsmåte for dechifring av en tekst som er chifret i henhold til krav 1 ved å bruke en tilsvarende chifreringsenhet og nøkkelmateri-
generator, karakterisert ved at hvert tegn C dechifres slik at det tilsvarende klartekst-
tegnet X reproduseres ved at ovennevnte chifrede tegn C innmattes i registeret, hvorefter registeret fremmates fra et startpunkt bestemt av det chifrede tegnet C i den bestemte syklusen et antall trinn $\bar{P}$, der $\bar{P} = \text{en full syklus} - P$, og der P er den samme variable verdi som er brukt under chifringen, eller i motsatt retning i ovennevnte syklus et antall trinn P .
3. Fremgangsmåte for å forbedre chifringen/dechifringen i henhold til krav 1 eller 2, karakterisert ved at det chifrede tegnet C i et videre chifreringsstrinn på chifreringsiden, adderes modulo-2 til en annen variabel verdi Z bestemt av nøkkelmateri-
generatoren, slik at det fremkommer et forbedret chifret tegn C^1 og at ovennevnte forbedrede chifrede tegn C^1 på dechifreringsiden adderes modulo-2 til ovennevnte annen variable verdi Z fra en tilsvarende nøkkelmateri-
generator slik at det chifrede tegnet C fremkommer.
4. Chifreringsenhet for utførelse av fremgangsmåten ifølge de foregående krav, hvor en klartekst eller chifret tekst som foreligger i binærkodet form innføres i et flertrinns register og behandles med et nøkkelmateriale for henholdsvis chifring og dechifring, karakterisert ved at flertrinnsregisteret omfatter en modulo-2 addisjonskrets og en flip-flop-krets i hvert trinn, idet chifreringsprosessen (dechifreringsprosessen) foretas i selve registeret ved at enheten omfatter en av nøkkelmateri-
et styrt koblingsanordning for sammenkobling av inngangene og utgangene fra de forskjellige trinn og en av nøkkelmaterialet styrt pulskilde for fremmating av registeret, hvorved registeret ved behandling av teksten følger en definert syklus et definert antall skritt.

Anførte publikasjoner:

Nedrlandsk Alm. tilgjengelig søknad nr. 6.412.505 b

121284

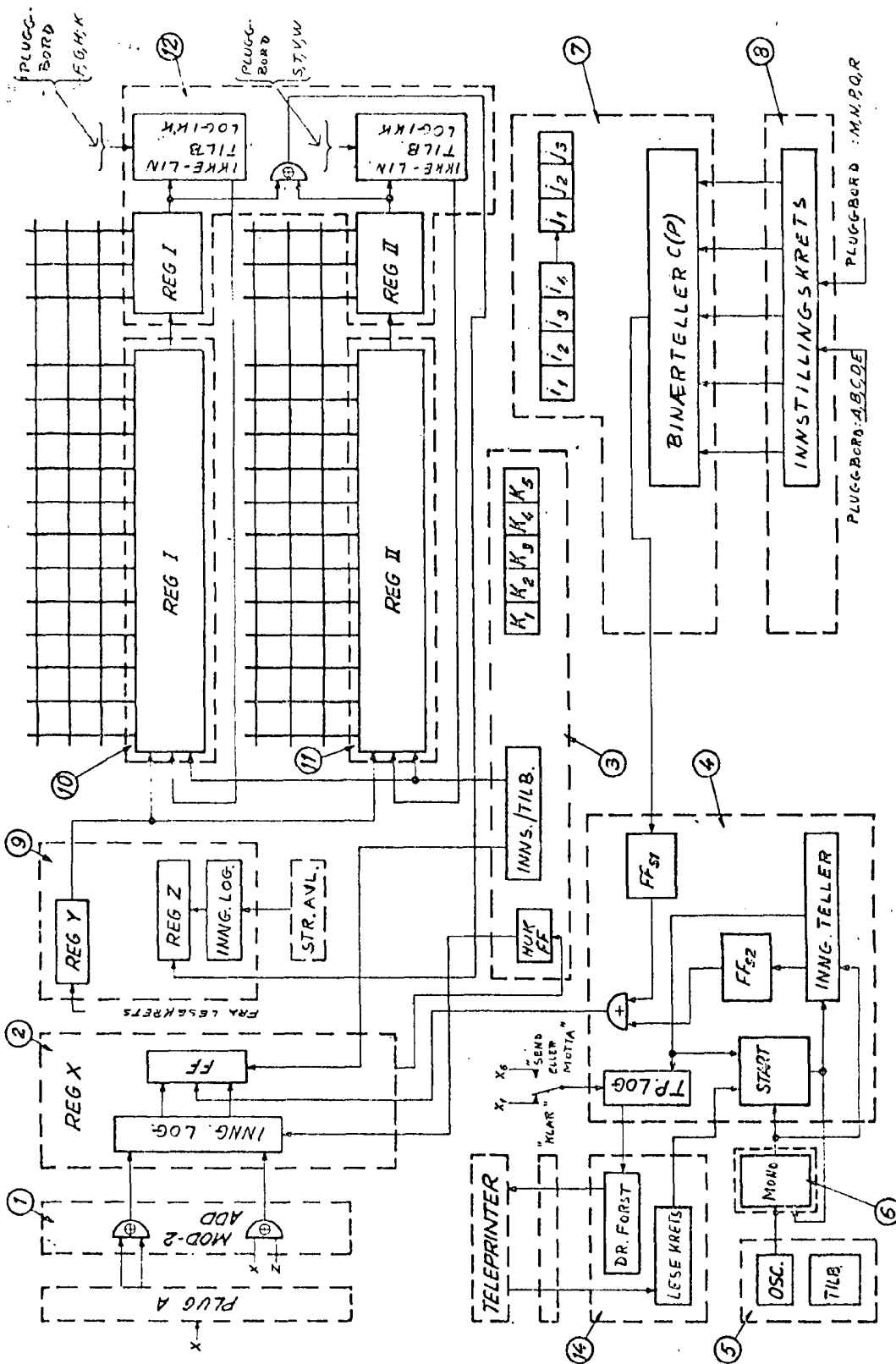


FIG. 1a

121284

Fig. 1b

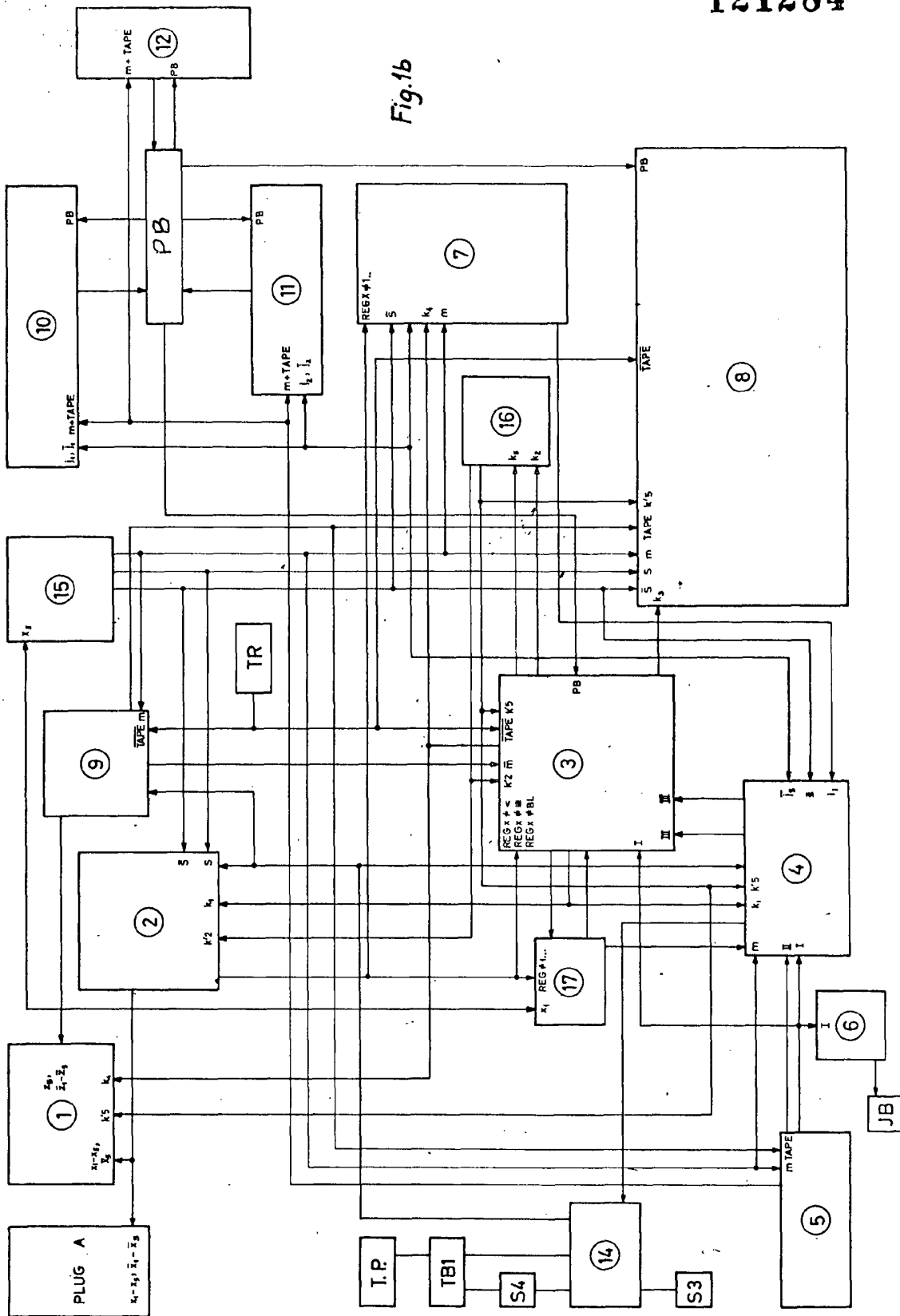
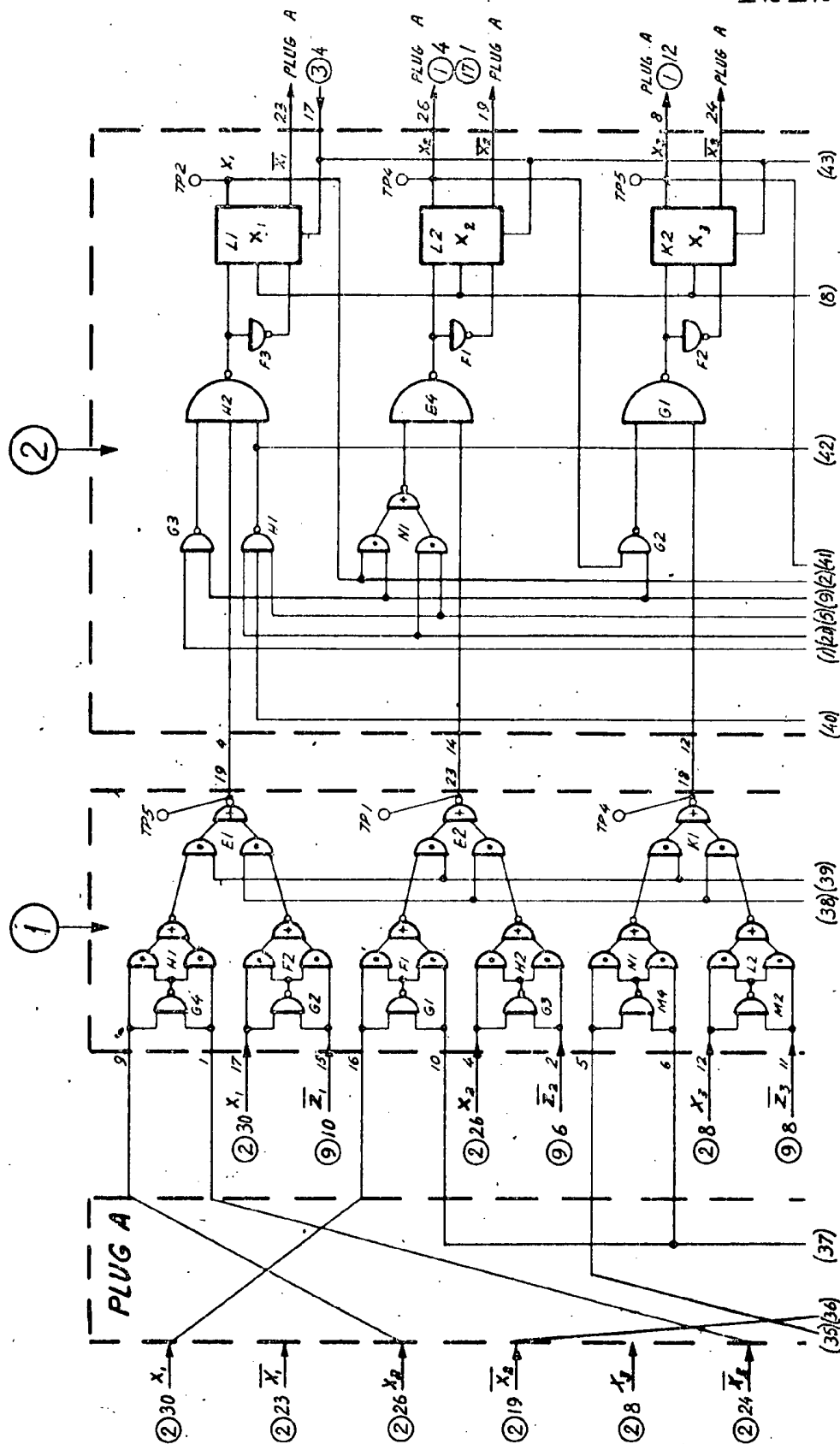


Fig. 1c.



121284

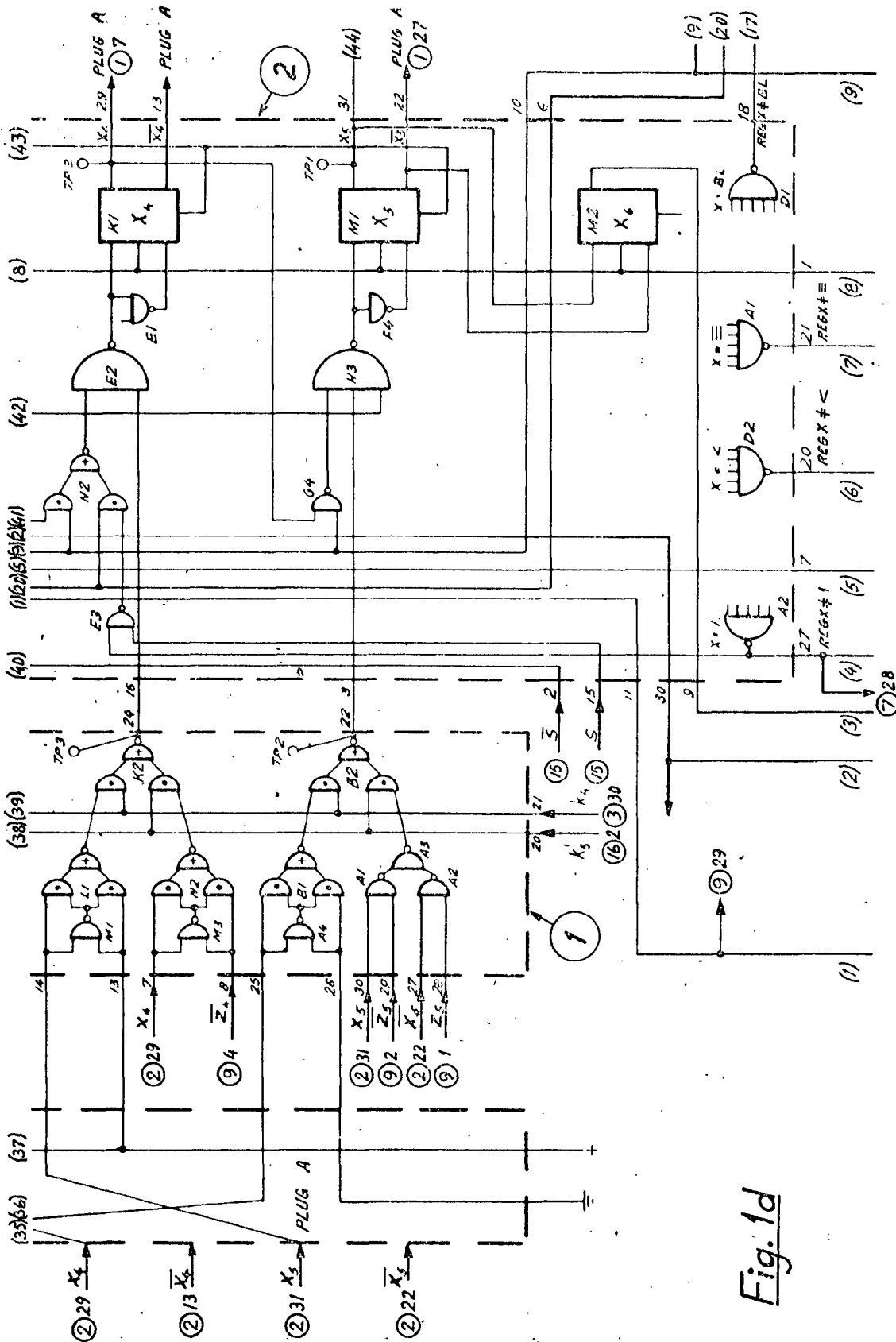
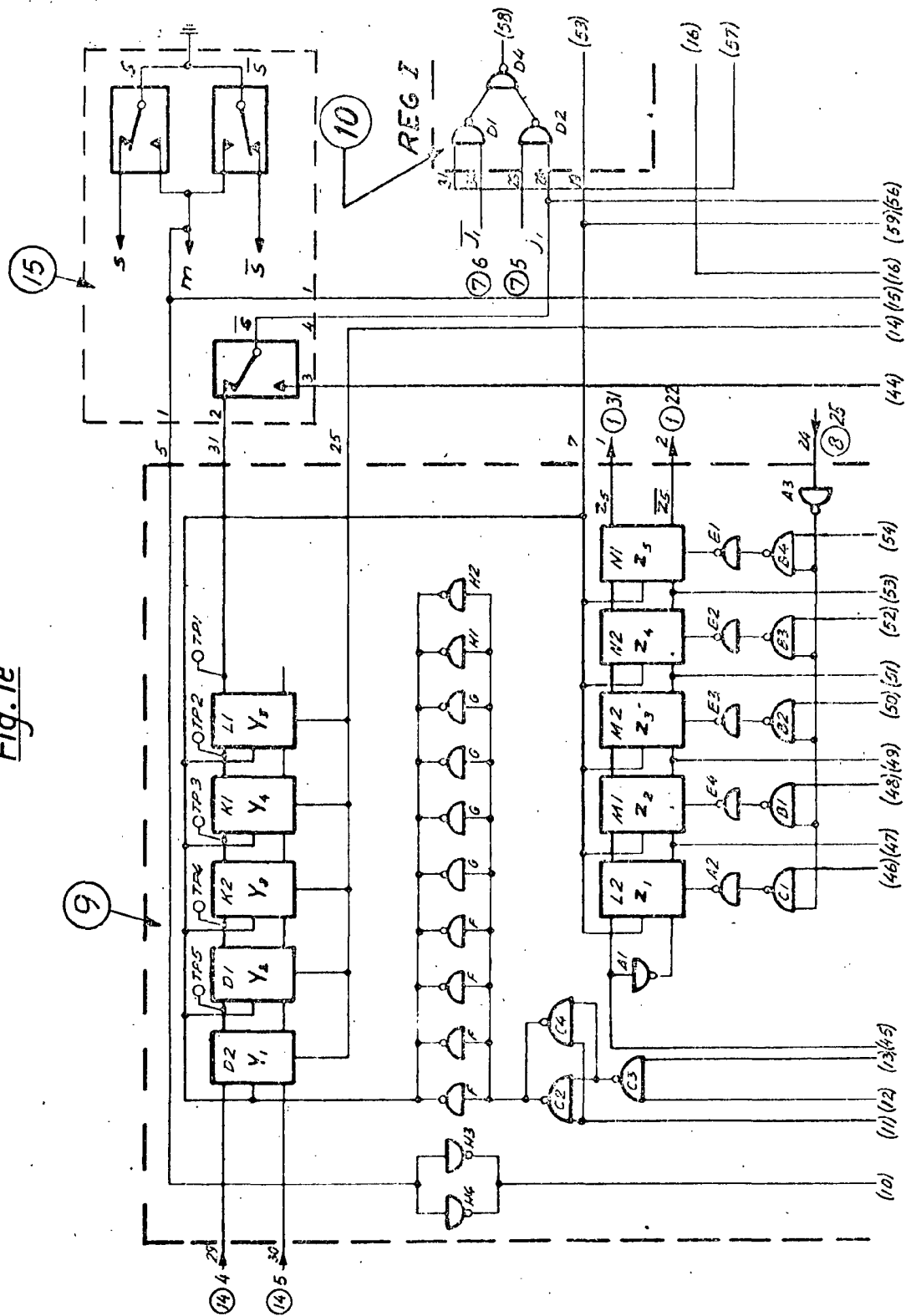
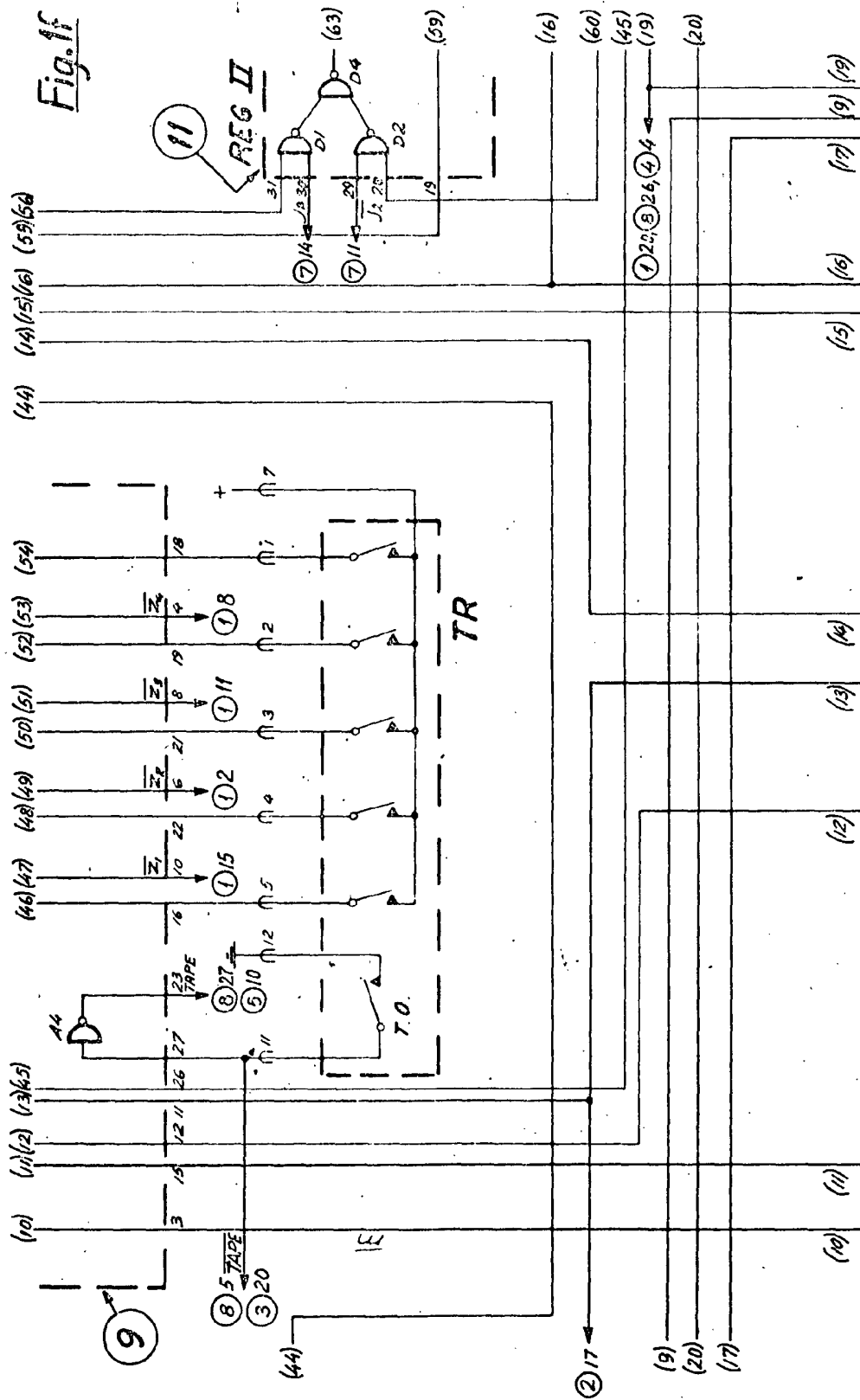
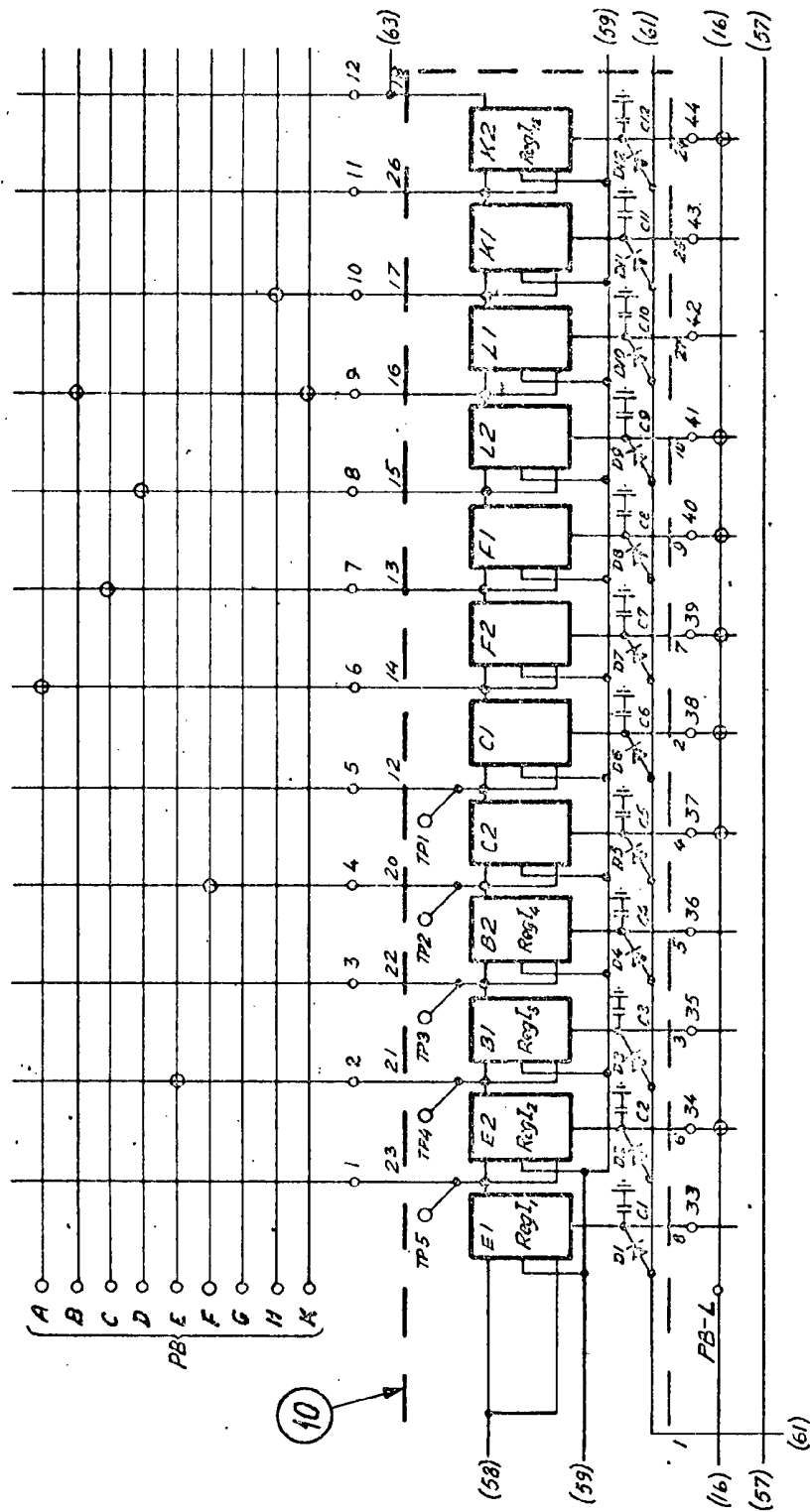


Fig. 1d

Fig. 1e









121284

Fig. 1i

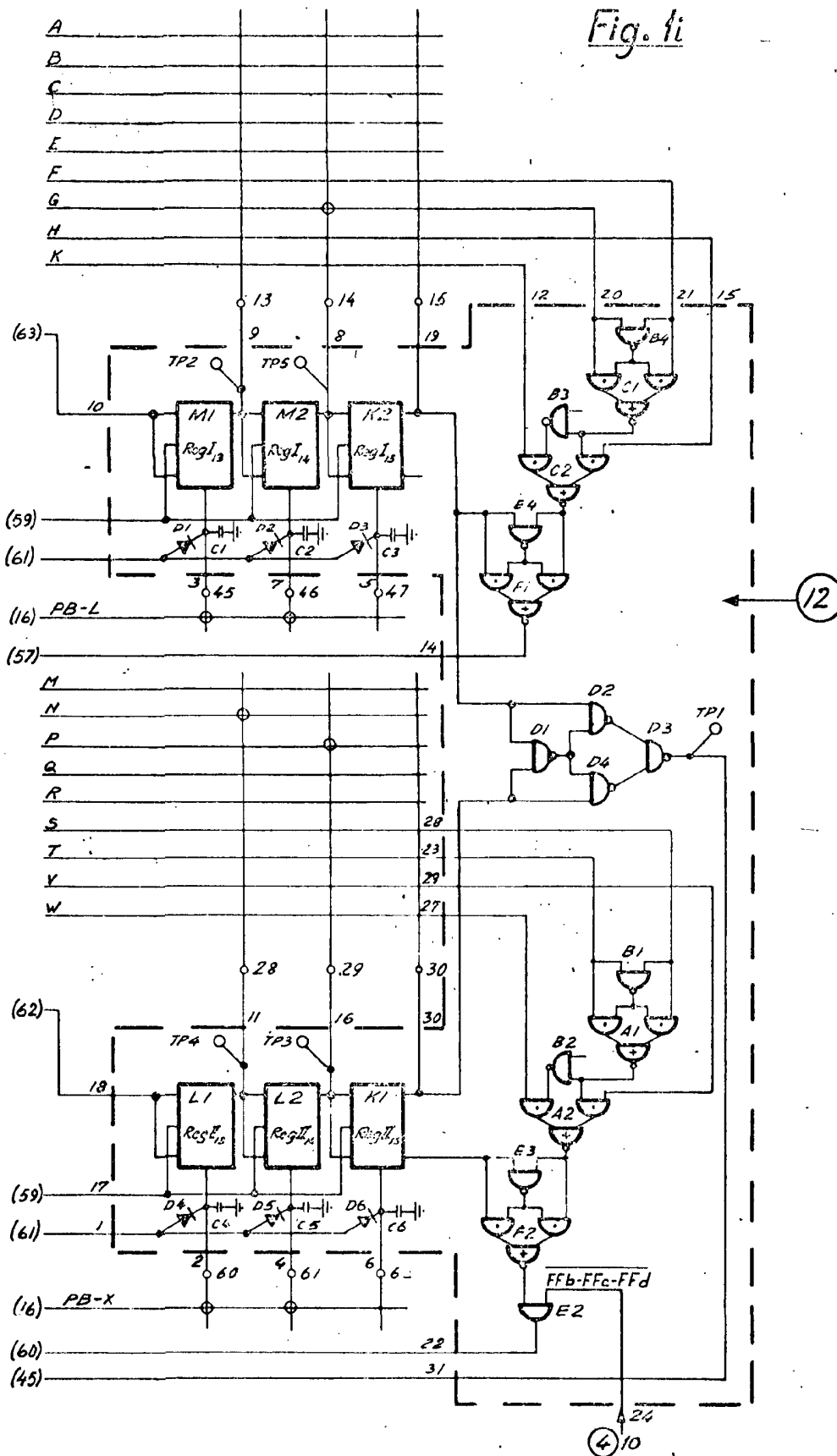
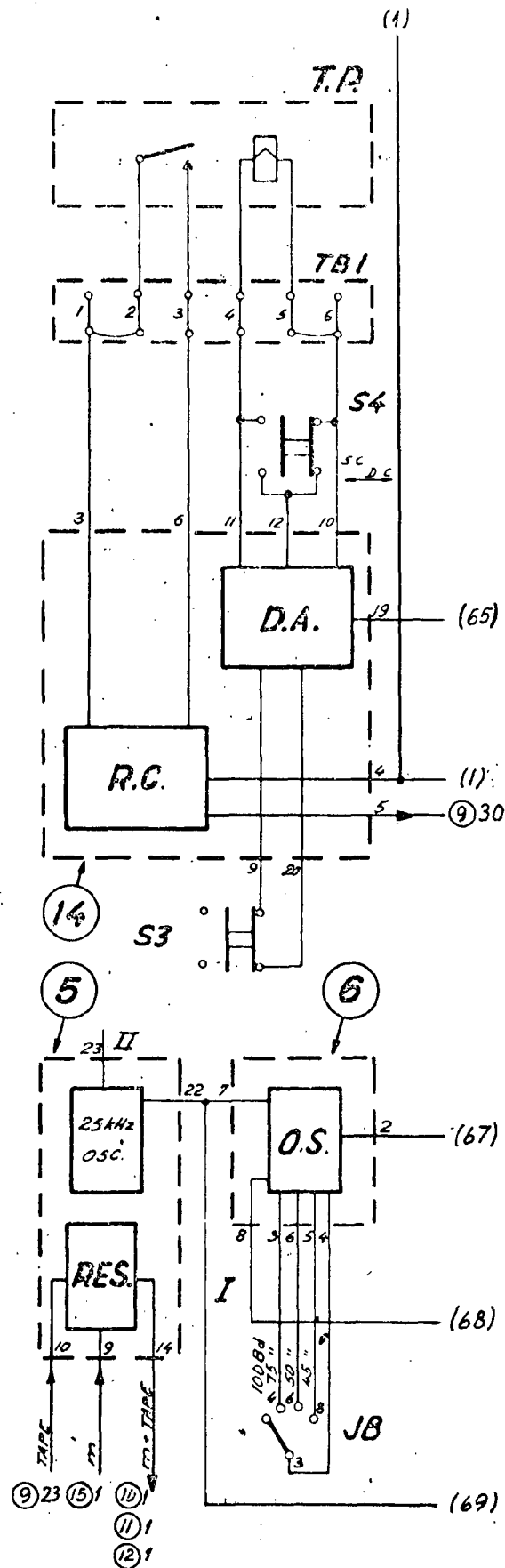


Fig. 2a



121284

Fig. 2b

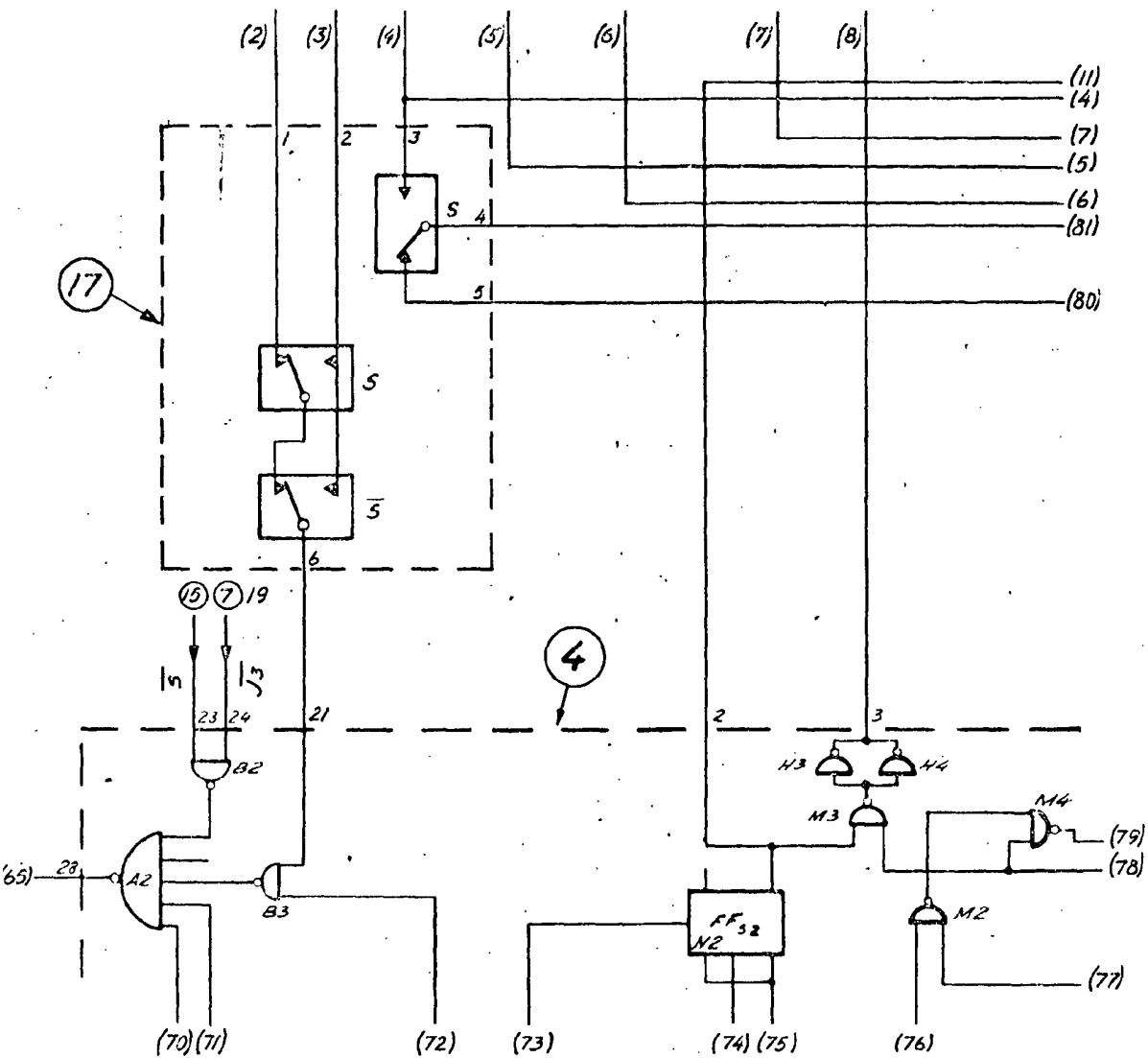


Fig. 2c

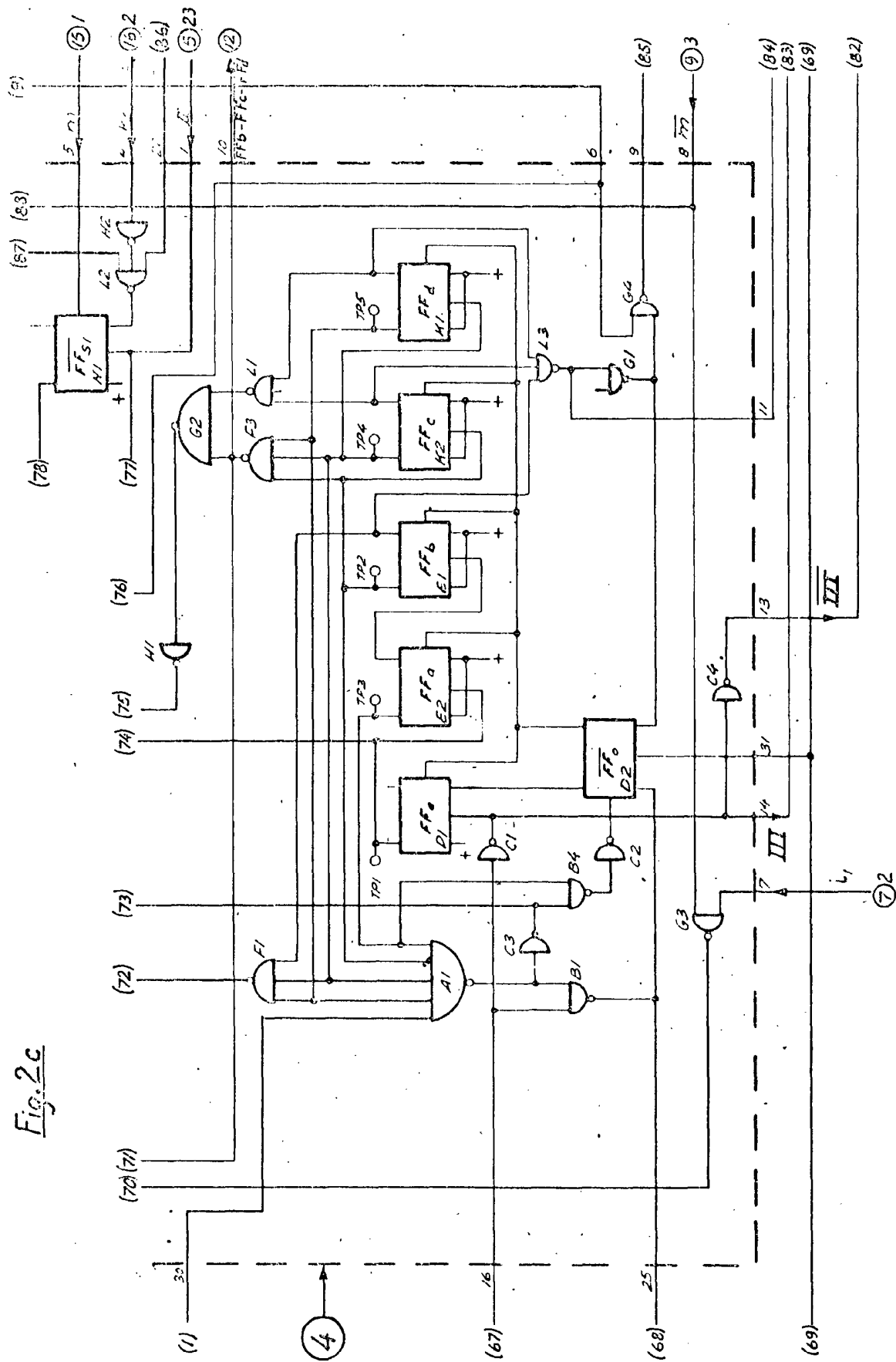
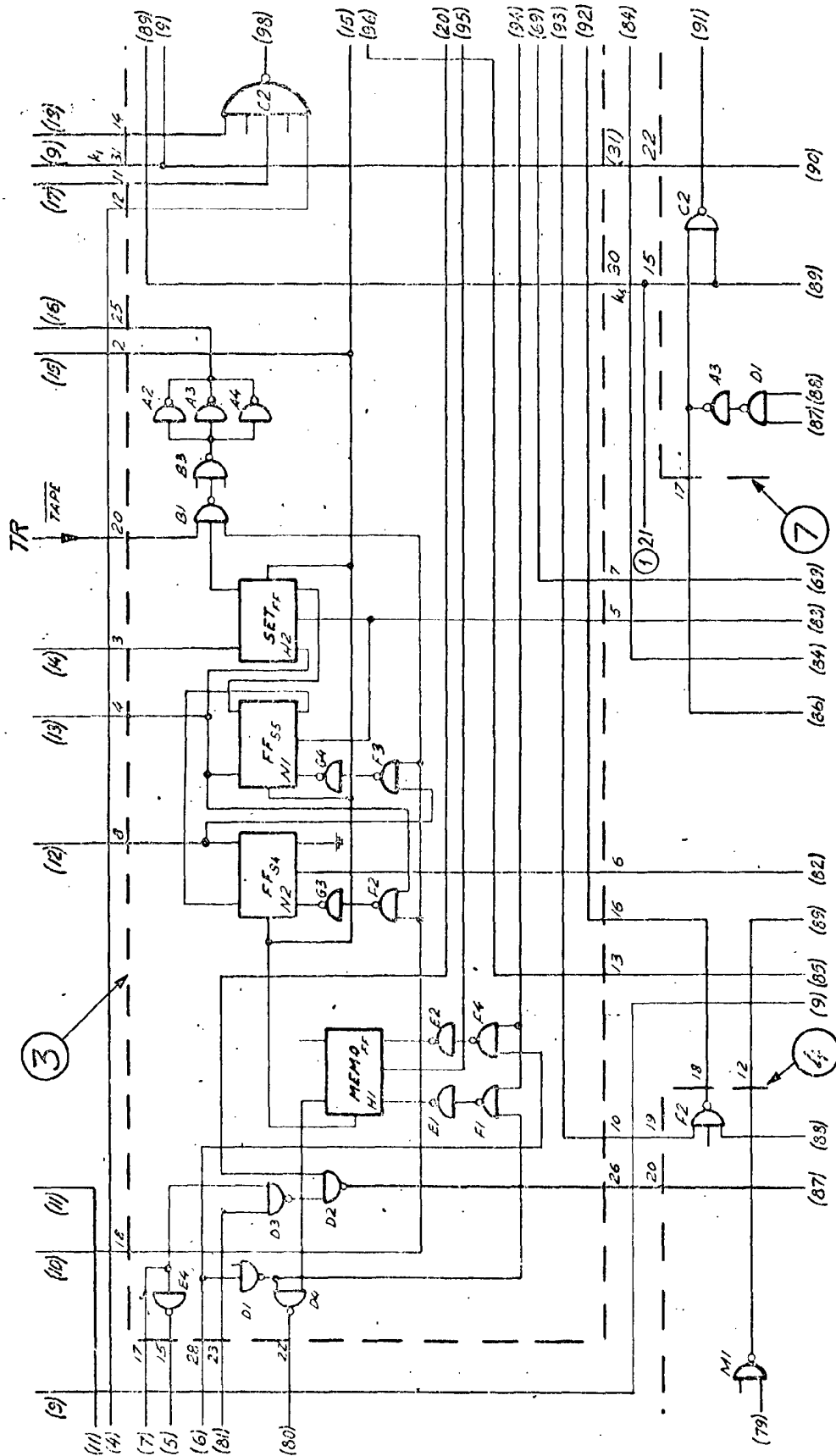


Fig. 2d



121284

Fig. 2e

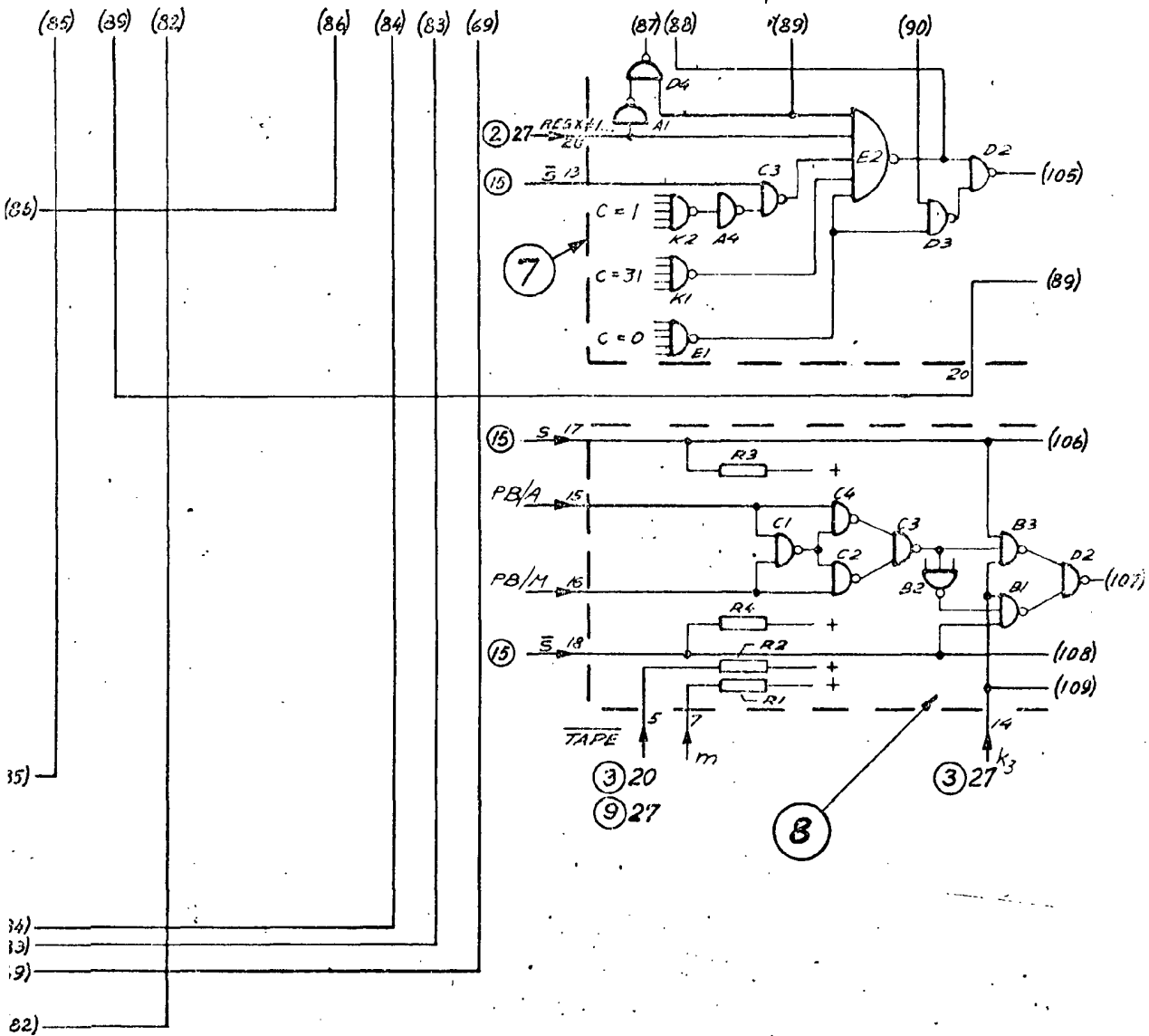


Fig. 2f

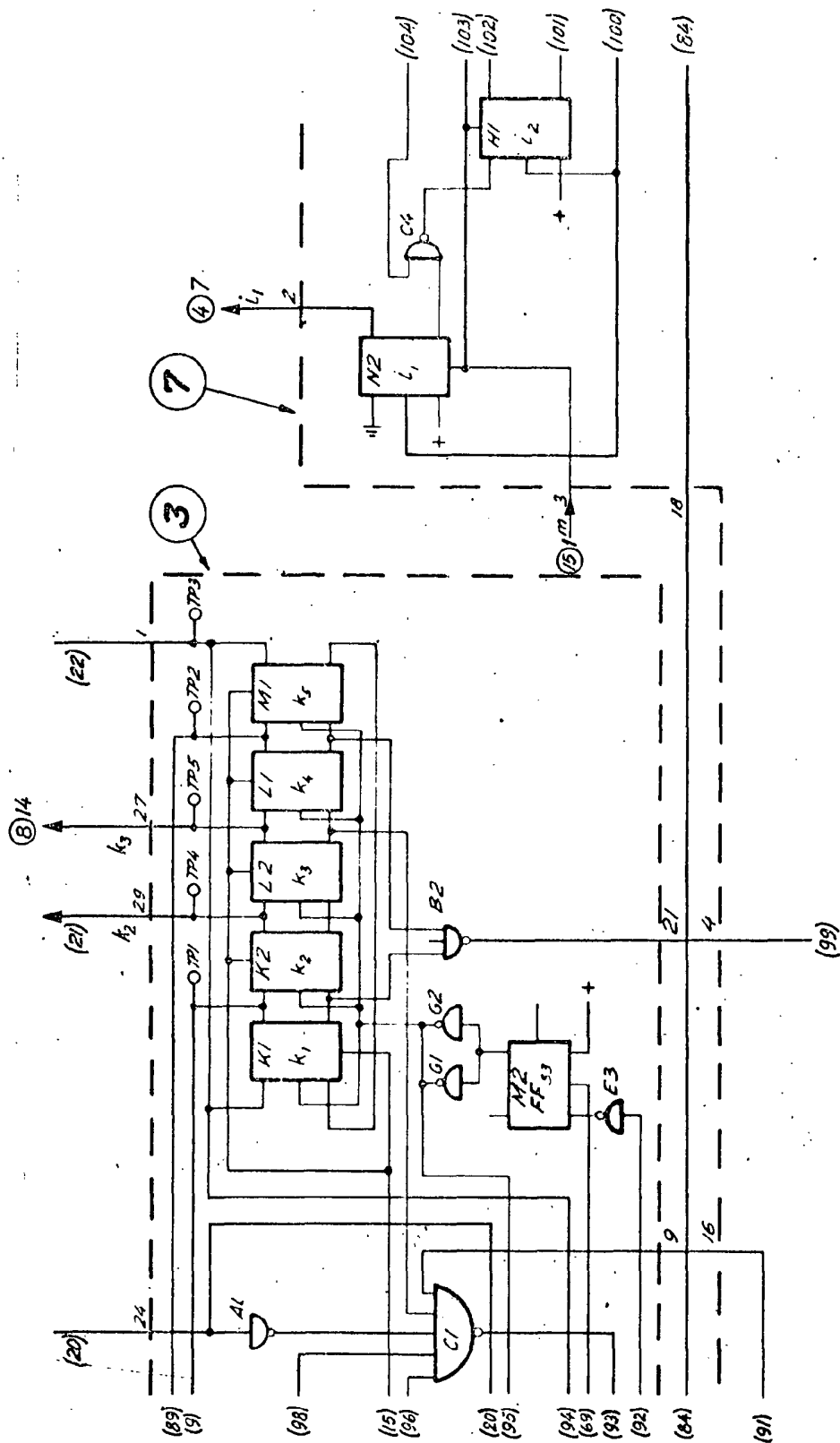
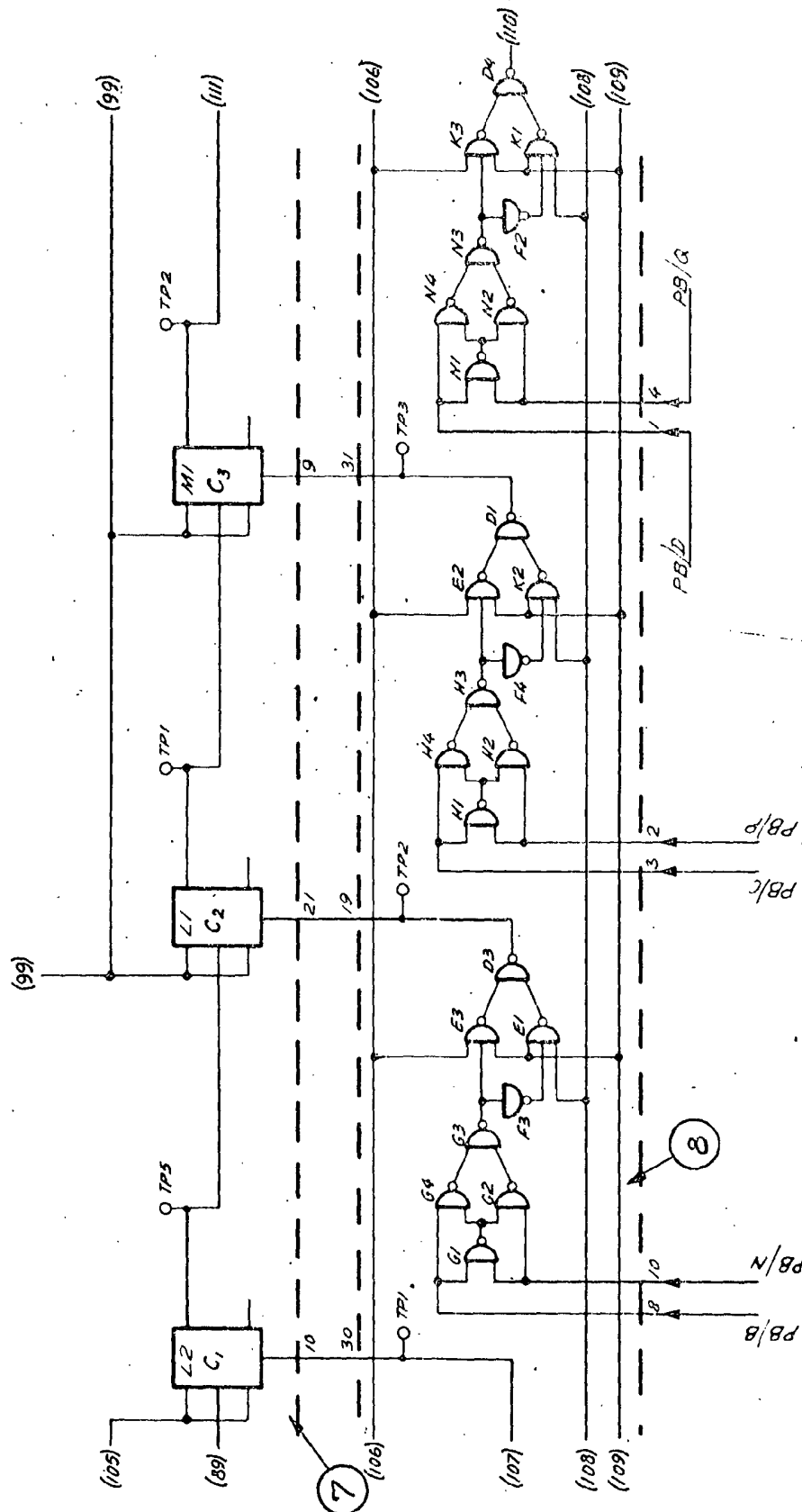
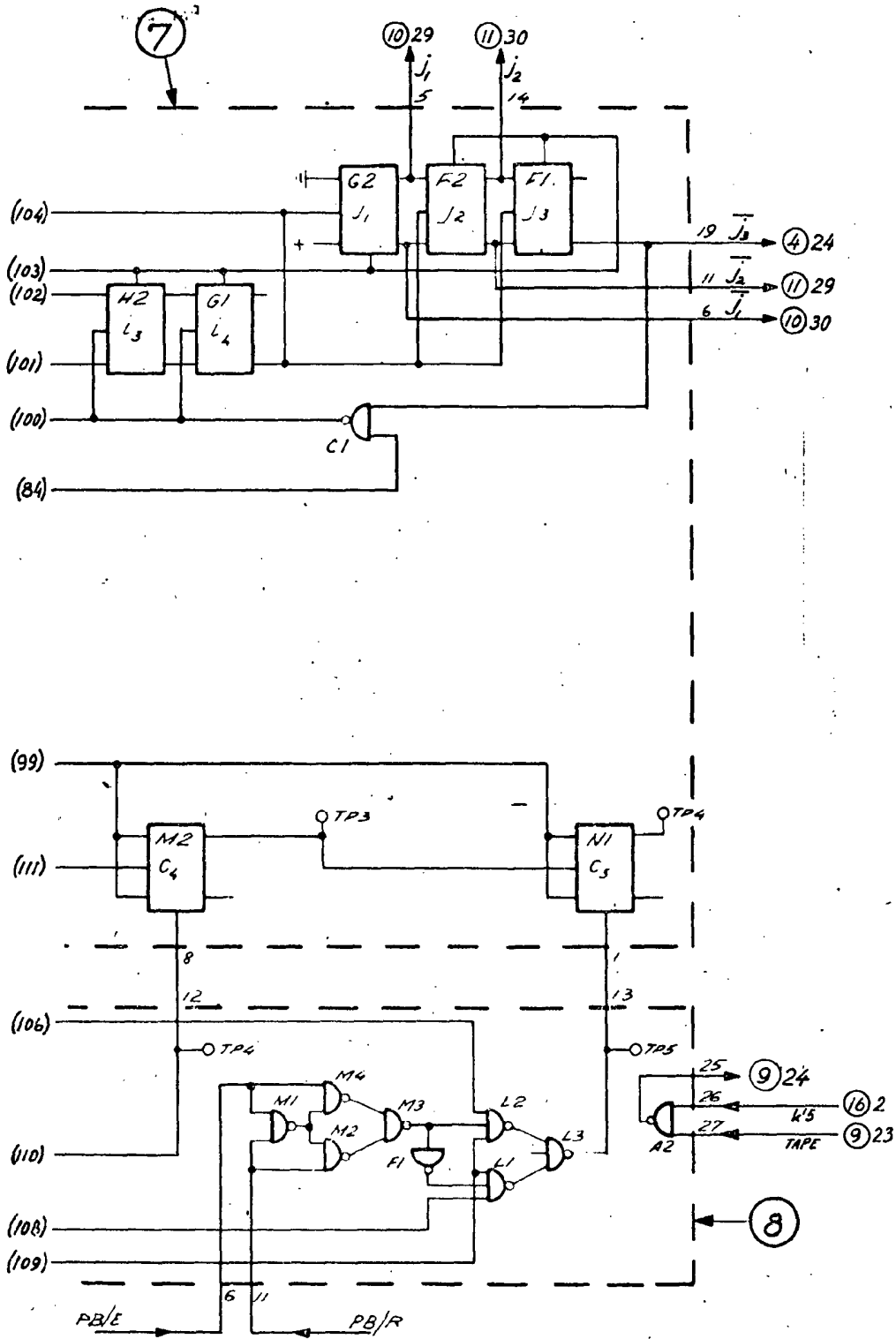


Fig. 2g

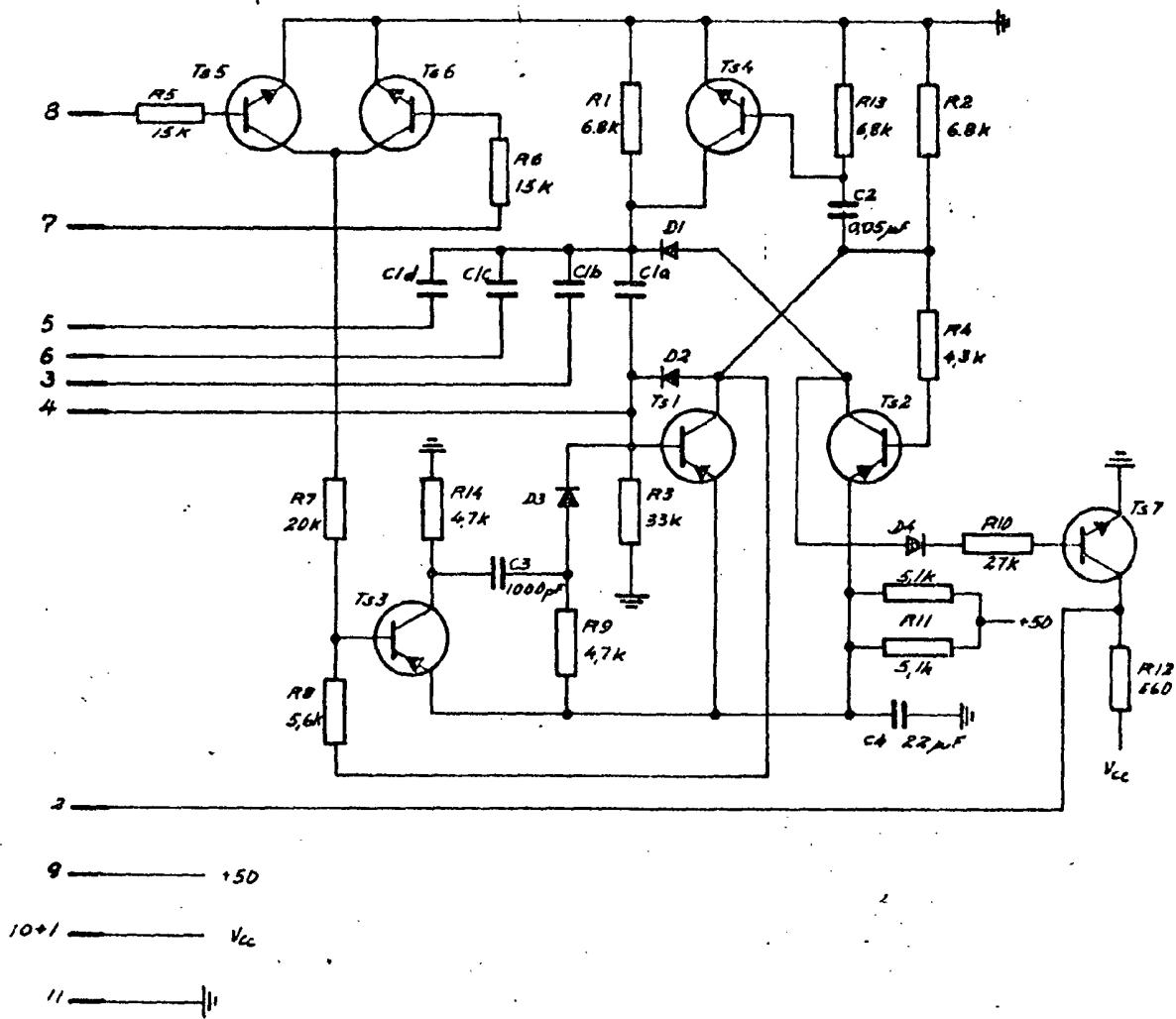


121284

Fig. 2h



121284



O.S.

Fig.3

6

121284

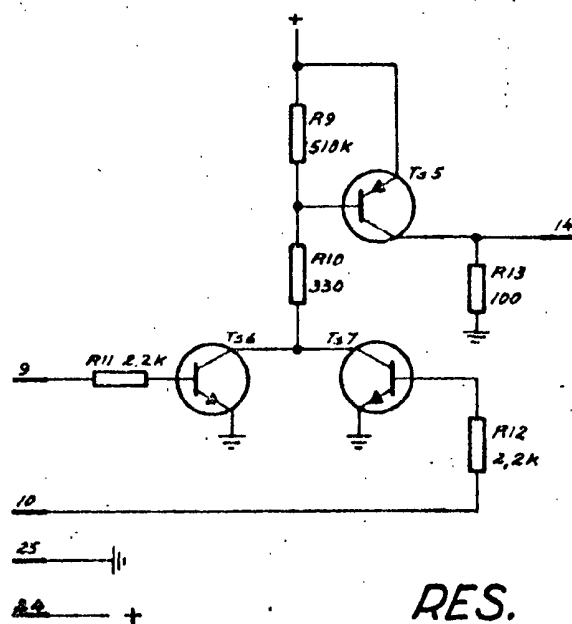
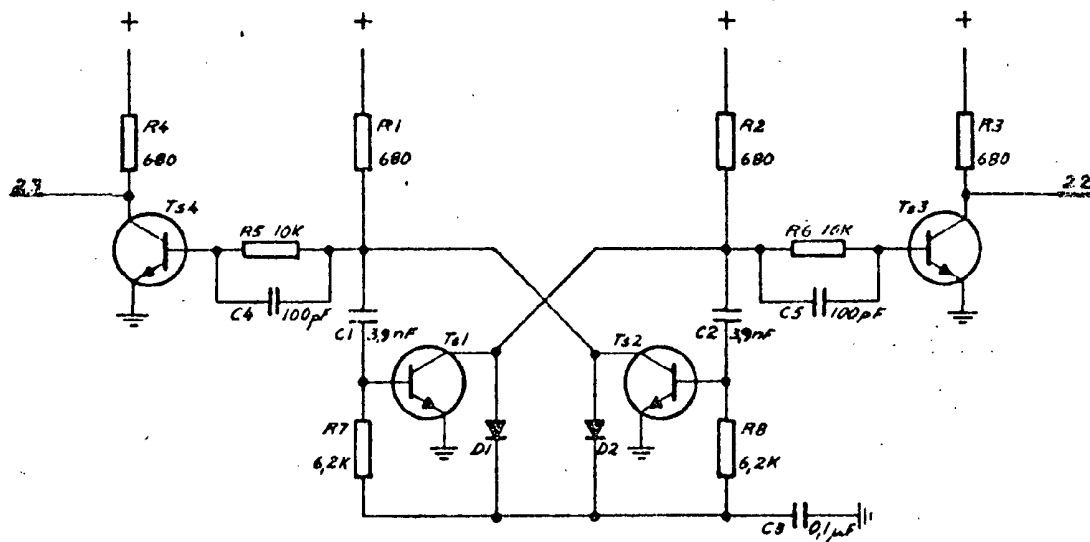
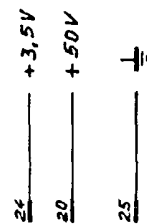
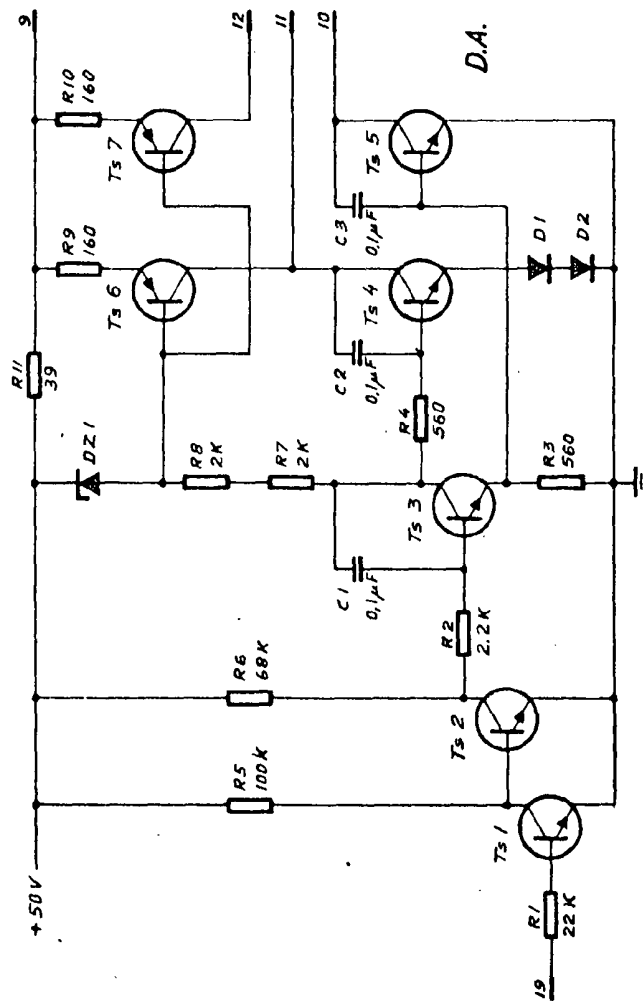
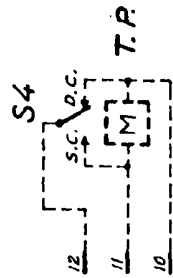
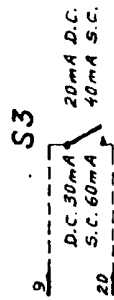
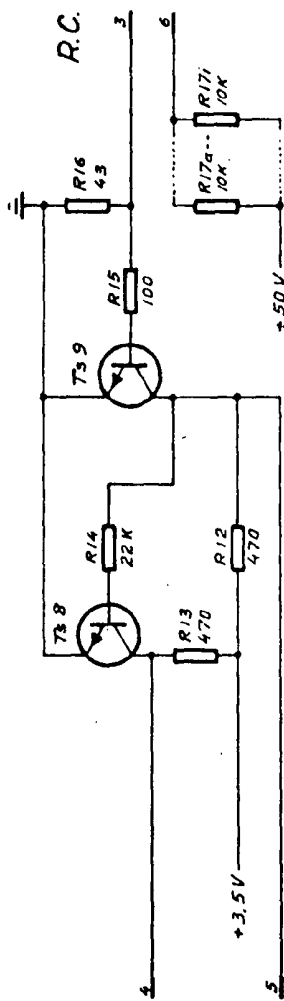


Fig. 4

5

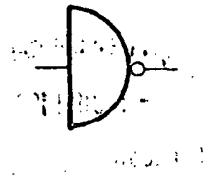


121284

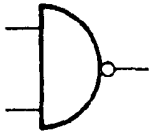
Fig. 5

14

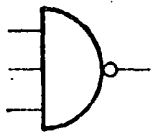
121284



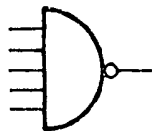
INVERTER



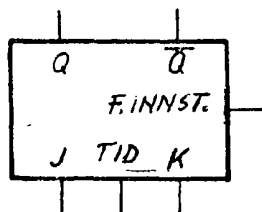
2-INNG. NAND



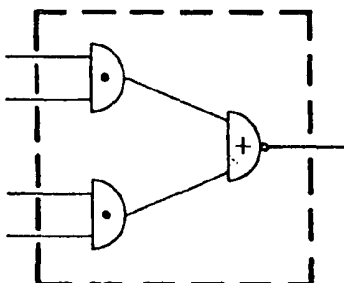
3-INNG. NAND



5-INNG. NAND



JK-FLIPFLOP



EXCLUSIVE - OR

Fig. 6

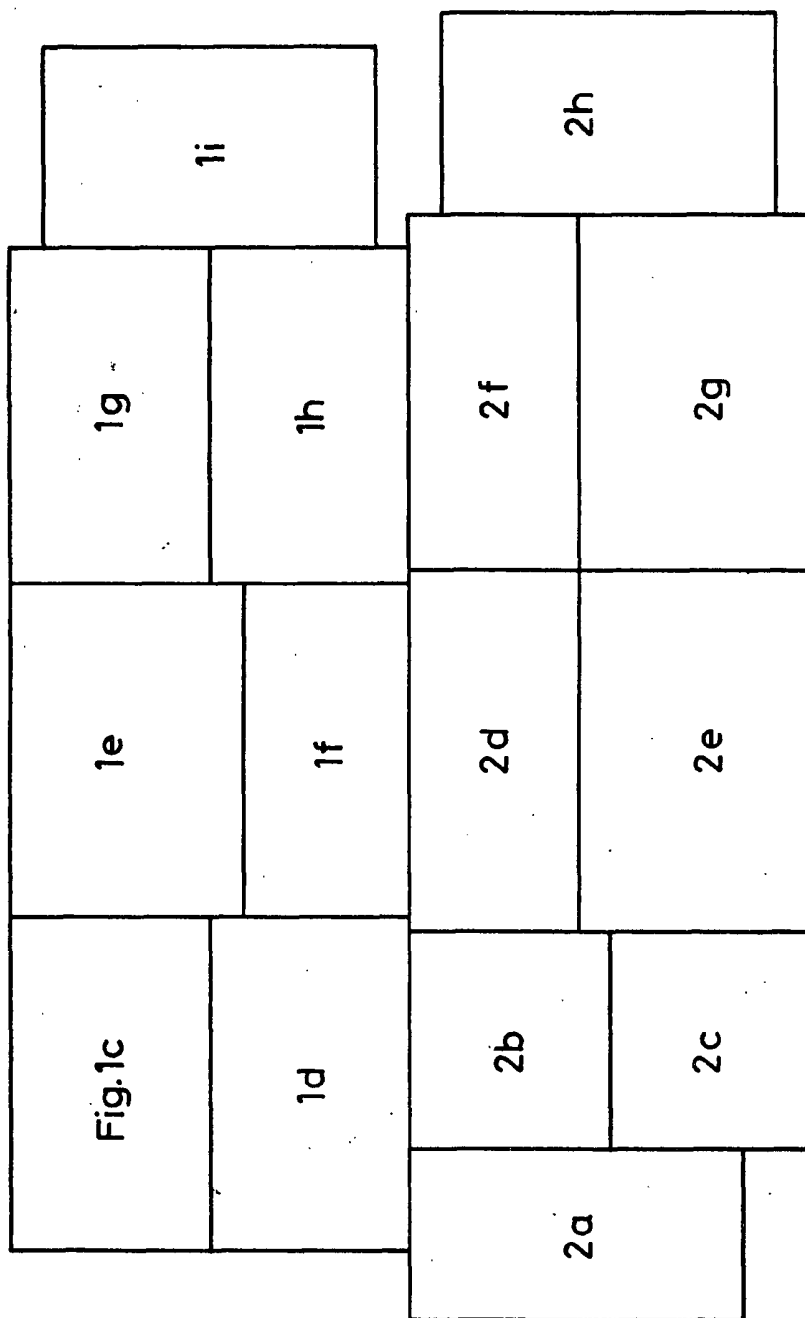


Fig. 7

121284