NORGE

(12) **PATENT**

(19) NO (11) **300950** (13) B1

(51) Int Cl[6] H 04 L 12/22, 9/00, H 04 M 11/08

Patentstyret

(21) Søknadsnr	885046	(86) Int. inng. dag og søknadsnummer	
(22) Inng. dag	11.11.88		
(24) Løpedag	11.11.88	(85) Videreføringsdag	
(41) Alm. tilgj.	16.05.89	(30) Prioritet	13.11.87, FR, 8715718
(45) Meddelt dato	18.08.97		

(73) Patenthaver Jean-Pierre Boule, 12 rue de la Résistance, F-14540 Soliers, FR
Dominique Hamel, 37 rue Lanfranc, F-14000 Caen, FR
Martial Menconi, 8 Résidence Olympia, F-14000 Caen, FR

(72) Oppfinner Innehaverne

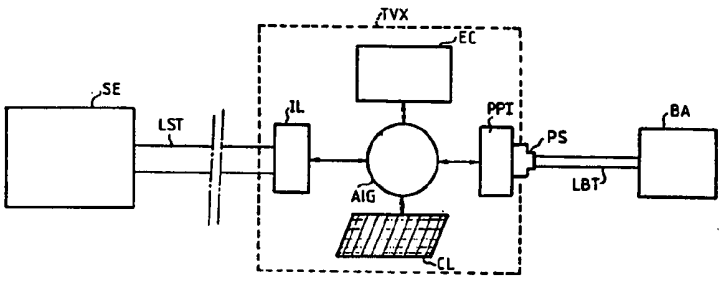
(74) Fullmektig Onsagers Patentkontor AS, 0103 OSLO

(54) Benevnelse **Innretning og fremgangsmåte til å sikre dataoverføringen mellom en videoterminal og en tjener**

(56) Anførte publikasjoner Nachrichtentechnische Zeitschrift NTZ,vol.36,nr.8. august 1983, Berlin, DE, W. Bosch:"Bildschirmtext .... s. 500-504

(57) Sammendrag

Beskyttelsen av dataoverføringen mellom videoterminal (TVX) og en tjener (SE) utføres ved hjelp av en ekstra pakke (BA) forbundet med et videoadapterstøpsel (PPI) på en terminal (TVX). I en forsesjonsutførelse virker pakken på svitsjeinnretningen (AIG) til terminalen ved å overvåke enhver annen handling på svitsjeutstyret. Svitsjekabinettet og tjeneren foretar en dialog i henhold til en bestemt sekvens av operasjoner som omfatter definisjonen av en overført sesjonsnøkkel enkryptert i samsvar med en basisnøkkel. En anomali som forekommer under denne dialogen avbryter for sesjonsmoden.



Oppfinnelsen angår en innretning og en fremgangsmåte for beskyttelse av overføring av data mellom en videotexterminal og en tjener. Disse data angår både styringen av aksessen til tjeneren og overføringen av meldinger straks sesjonen er etablert. Oppfinnelsen angår alle videotexterminaler, spesielt, men ikke utelukkende, de kjent under det franske handelsnavn "Minitel".

For å styre aksessen til videotexsystemer utsatt for problemer lik de ved fjerndatabehandlingssystemer, kan tre fremgangsmåter benyttes. En første fremgangsmåte er basert på gjenkjennelse av et element som er kjent av brukeren og som generelt er et passord. Imidlertid er dette passord temmelig utsatt for avlytting og ingen standardterminal gir noen beskyttelse mot denne trussel. En annen fremgangsmåte er basert på gjenkjennelsen av et element som angår dette individ, såsom f.eks. en biometrisk karakteristikk (stemme, fingeravtrykk). Imidlertid har slike metoder, selv om de synes ganske fordelaktige, inntil nå ikke blitt benyttet av tekniske og økonomiske årsaker. En tredje fremgangsmåte er endelig basert på gjenkjennelsen av et element som besittes av individet. I denne kategori er "smarte" kort og autentiseringsinnretninger de mest pålitelige verktøy, da de implementerer en beregningsalgoritme som gjør dem istand til helt å identifiseres. Imidlertid synes ikke disse systemene av økonomiske årsaker til å ha oppnådd den suksess man håpet på.

Flertjeneste-smartkortet krever implementering av utstyr som kan betraktes som tungt og kostbart innenfor rammen av en enkelt logisk aksesskontroll. I realiteten krever denne teknikken at kortlesere forbindes med videotexterminalene for brukerkort, sikkerhetsprosessorer for kortene til tjeneren og endelig en dialog-programvare mellom en parsammensetning (leser-kort) på den ene side og en parsammensetning (sikkerhetsprosessor-kort) på den annen side.

Autentiseringsinnretningene gjør det mulig å redusere kostnaden for logisk aksesskontroll, men krever bruk av utlesningsinnret-

ninger og tastaturer eller optiske sensorer. Da det i tillegg ikke er noen forbindelse med videotexterminalen, er brukeren nødt til å spille rollen som et grensesnitt mellom autentiseringsinnretningen og terminalen. Dernest benytter disse innretningene generelt en ekstern strømforsyning som gjør deres bruk enda mer komplisert.

Den foreliggende oppfinnelse eliminerer disse ulemper ved å foreslå å beskytte aksesskontrollen til en tjener ved autentisering av videotexterminalen og beskyttelse av meldingene som utveksles mellom tjeneren og videotexterminalen ved hjelp av en enkel innretning som ikke krever at det skal utføres noen materiell tilpasning, hverken til terminalen eller tjeneren og som er mindre kostbar enn hva som for tiden er tilfellet.

Hensikten med oppfinnelsen er også å frakoble videotexterminalene i tilfelle det gjøres forsøk på å modifisere dataene som overføres på transmisjonslinjen.

En annen hensikt med oppfinnelsen er å benytte en ekstra pakke som kan plugges direkte inn i videoadapterstøpselet til videotexterminalen uten en selvstendig strømforsyning.

En annen hensikt med oppfinnelsen er å tillate beskyttelse under sesjonen, ved hjelp av kryptering eller ved signatur, av overføringen meldinger mellom denne tjener og videotexterminalen slik at hemmeligholdelse og/eller integriteten til disse meldingene sikres.

Oppfinnelsen søker også å skaffe en innretning hvis karakteristikker gjør det mulig å utvide bruken av videotexanvendelser i stand til å nå en meget vid sektor av offentligheten (hva angår kostnaden), mens tjenesten skreddersys.

Disse og ytterligere hensikter og fordeler oppnås ved hjelp av de trekk som er beskrevet i patentkravene.

Oppfinnelsen vil lettere forstås ved lesning av den følgende

beskrivelse med henvisning til den vedføyde tegning.

Fig. 1 viser et diagram av en innretning i henhold til oppfinnelsen,

fig. 2 viser et diagram som representerer en utførelsesmåte for en ekstra pakke i innretningen på fig. 1,

fig. 3 viser et koblingsdiagram som gjengir hovedelementene i den ekstra pakke på fig. 2,

fig. 4 viser et flytkart som beskriver starten av forsesjonsmoden for den ekstra pakke i henhold til oppfinnelsen,

fig. 5 viser et flytkart som beskriver en første variantutførelse av slutten av pakkens forsesjonsmode,

fig. 6 viser et flytkart som beskriver en annen variant av slutten av forsesjonsmoden til pakken,

fig. 7 viser et flytkart som beskriver den første del av virkemåten til en spesiell mode av pakken i henhold til oppfinnelsen,

fig. 8 viser et flytkart som beskriver en annen del av virkemåten til den særskilte mode for pakken i henhold til oppfinnelsen.

Den ledsagende tegning som hovedsakelig omfatter elementer av en bestemt art kunne om nødvendig ikke bare benyttes for lettere å forstå den etterfølgende detaljerte beskrivelse, men også til definisjonen av oppfinnelsen.

I henhold til oppfinnelsen omfatter innretningen vist på fig. 1 en tjener SE forbundet ved hjelp av en telematikklinje LST til en videotexterminal TVX. I resten av beskrivelsen skal begrepet "videotexterminal" erstattes av ordet "terminal". Terminalen

TVX omfatter konvensjonelt et linjegrensesnitt IL, en skjerm EC, et tastatur CL og et videoadapterstøpsel PPI plassert nedstrøms på linjen LST. Disse terminalelementene styres av en svitsjekontrollinnretning AIG som inneholder terminalens protokollprogramvare. I henhold til oppfinnelsen omfatter innretningen en ekstra pakke BA koblet ved hjelp av en spesialsokkel PS av en linje LPT til videoadapterstøpselet PPI. Pakken BA er derfor forbundet nedstrøms for terminalen i motsetning til en kobling oppstrøms for terminalen, nemlig mellom linjegrensesnittet IL og tjeneren SE.

Pakken BA er vist skjematisk på fig. 2. Denne pakken er omtrent 8 cm lang, 3 cm bred og 2 cm dyp. Den omfatter to lysemitterende dioder LED 1 og LED 2 anordnet på en slik måte at det er synlig for brukeren når pakken er plugget inn i videoadapterstøpselet ved hjelp av en spesialplugg PS. Denne spesialsokkel PS omfatter fem stifter P1-P5 hvis funksjon skal angis i det følgende. PS-sokkelen gjør det mulig å forsyne pakken BA med strøm slik at det ikke er nødvendig å utstyre den med en ekstern strømforsyning.

Hovedelementene til pakken BA er vist på fig. 3. Stiften P1 til sokkelen PS på pakken BA leverer polarisasjonsspenninger på 5 volt. Den er koblet i jord ved hjelp av en kondensator C2 med en verdi på 0,1 mikrofarad og ved hjelp av en elektrolytisk kondensator C1 med en verdi på 10 mikrofarad. Stiften P2 til sokkelen på pakken BA leverer referansejord. Stiften P5 er også forbundet til jord, men er ikke vist på denne figur.

Pakken BA omfatter en dialoganordning MDI bestående av en sentral prosessorenhet ICI klokket av klokken Q1. Sentralprosessorenheten ICI omfatter en lese-skrivehukommelse eller -lager MV og en lesehukommelse eller leselager MM. Denne lesehukommelse er en fast hukommelse, dvs. ikke programmerbar. Sentralprosessorenheten er en mikrokontroller av typen som kan fås med referansen 8051 fra av "INTEL", et firma i USA. Frekvensen til klokken Q1 er 10 Mhz. Bena 18,19 i sentralprosessorenheten ICI er forbundet med henholdsvis kontaktene på

klokken Q1 og jord ved hjelp av to kondensatorer C6 og C7 med en verdi på 22 pikofarad. Bena 32-39 på sentralprosessorenheten ICI er henholdsvis forbundet til bena 8-1 på en låshukommelse IC2. Denne låshukommelse IC2 er av den type som kan fås med nummeret 8282 fra firmaet "INTEL". Bena 1-8 på låshukommelsen IC2 er også forbundet til polarisasjonsspenningen på 5 volt ved hjelp av en krets L91 som har en høy impedans bestående av motstander med en verdi på 10 kiloohm. Benet 31 på sentralprosessorenheten IC1 er forbundet til en polarisasjonsspenning på +5 volt såvel som til jord via en kondensator C4 med en verdi på 10 nanofarad. Benet 30 på sentralprosessorenheten IC1 er forbundet til bena 9 og 11 på låshukommelsen IC2.

Benet 9 på sentralprosessorenheten IC1 er forbundet til polarisasjonsspenningen ved hjelp av en elektrolytisk kondensator C3 med en verdi på 10 mikrofarad og til jord ved hjelp av en motstand R1 (5,6 kiloohm) i parallell med en diode D1 av den type som kan fås med typenummer IN4148 fra det franske firma "SILEC". De andre diodene som heretter omtales i teksten skal være identiske med dioden D1. Bena 10 og 11 på sentralprosessorenheten IC1 er henholdsvis forbundet til stiftene P3 og P4 på utgangssokkelen på pakken BA. Stiften P3 utgjør overføringsstiften, mens stiften P4 utgjør mottagertilkoblingskontakten. Stiften 10 er forbundet med polarisasjonsspenningen ved hjelp av en motstand R2 med en verdi på 5,2 kiloohm og en sikkerhetsdiode D2. Benet 10 er også forbundet til jord ved hjelp av en annen sikkerhetsdiode D3. Tilsvarende er benet 11 koblet til polarisasjonsspenningen ved hjelp av en 5,6 kiloohms motstand R3 og en sikkerhetsdiode D4 så lenge som den er koblet til jord ved hjelp av sikkerhetsdioden D5.

Pakken BA omfatter også et leselager IC3 og et sett av logiske OG-porter IC4. IC3-hukommelsen er av typen som kan fås med nummer 2864 fra firmaet "INTEL" og IC4-settet er av typen som kan fås med nummeret 7408 fra firmaet "TEXAS INSTRUMENTS" i USA. Bena 12-19 på låshukommelsen IC2 er henholdsvis forbundet til bena 3-10 på hukommelsen IC3. Bena 2,11-13,15-19 og 21-25 på hukommelsen IC3 er henholdsvis forbundet til bena 25, 39-37,

36-32, 23, 24, 22 og 21 på sentralprosessorenheten IC1. Benet 28 på hukommelsen IC3 er først forbundet med polarisasjonsspenningen og dernest til jord gjennom en 10 nanofarads kondensator C9. Bena 14 og 27 på hukommelsen IC3 er henholdsvis forbundet til jord og til bena 16 på sentralprosessorenheten IC1.

Sett av logiske porter IC4 styrer den lysemitterende diode LED1 ved hjelp av en motstand R4 med en verdi på 470 ohm forbundet til dens ben 6 og den annen lysemitterende diode LED2 ved hjelp av en motstand 5 med en tilsvarende verdi på 470 ohm forbundet med benet 8. Dioden LED 1 er rød og utgjør en første displayinnretning, mens dioden LED 2 er grønn og utgjør en annen displayinnretning. Benet 14 på IC4 er forbundet til polarisasjonsspenningen på 5 volt og jord gjennom en kondensator C8 med en verdi på 10 nanofarad. Bena 1,2 og 7 er forbundet med jord, bena 4 og 5 til benet 8 på sentralprosessorenheten IC1, bena 9 og 10 til henholdsvis bena 7 på sentralprosessorenheten IC1 og tilkoblingskontaktene 12 og 13 henholdsvis til bena 29 og 17 på sentralprosessorenheten.

Sentralprosessorenheten IC1 omfatter to krypterings/dekrypteringsalgoritmer som hva den første angår er en DES-(DATA ENCRYPTION STANDARD)algoritme og hva den andre angår en RSA-(RIVEST SHAMIR ADLEMAN)algoritme. Disse to krypteringsalgoritmene utgjør en del av den første kryptering/dekrypteringsanordning for pakken BA. DES og RSA-algoritmene er henholdsvis lagret i leselagret MM i sentralprosessorenheten IC1 og i en seksjon IC30 av hukommelsen IC3.

Det bør nevnes her at DES-krypterings/dekrypteringsalgoritmen benytter en basisnøkkel KB. For at pakken BA og tjeneren SE dessuten kan kommunisere ved hjelp av DES-algoritmen, er det nødvendig at nøkkelen KB er lagret både i pakken BA og tjeneren SE. RSA-algoritmen arbeider ved hjelp av en basisnøkkel som i realiteten er kombinasjonen av to nøkler avhengig av hverandre, en offentlig nøkkel KPB lagret i tjeneren og den annen en hemmelig nøkkel KBS lagret i pakken.

Leselageret MM i den sentrale prosessorenheten IC1 omfatter dessuten basisnøkkelen KB som er nødvendig for DES-algoritmen og den hemmelige nøkkel som er nødvendig for RSA-algoritmen. En annen seksjon IC31 av denne hukommelse IC3 omfatter på kryptert form ved hjelp av DES-algoritmen og lagringsnøkkelen KST, en autentiseringskode i pakken BA og en hemmelig kode CC som er spesifikk for en gitt bruker.

Leselageret MM, skrive-leselageret MV og hukommelsen IC3 utgjør en første lagringsanordning for pakken. Seksjonen IC31 av hukommelsen IC3 utgjør en programmerbar leselageranordning for pakken BA. Leselageret MM utgjør en fast lesehukommelsesanordning for pakken BA.

Naturligvis er valget av mikrokontrolleren på ingen måte restriktivt. F.eks. er det mulig å velge en mikrokontroller av den type som kan fås med typenummer 8052 fra INTEL. I dette tilfelle vil autentiseringskoden I og den hemmelige kode lagres i en liten EPROM hukommelse utenfor mikrokontrolleren 8052 og innholdet av den ovennevnte seksjon IC30 vil bli samlet i den faste ROM til mikrokontrolleren 8052.

Tilsvarende vil det være mulig å velge en mikrokontroller av den type som kan fås med typenummer 68JC11 fra USA-bedriften MOTOROLA. I dette tilfelle vil en ekstern hukommelse ikke lenger være nødvendig for å lagre den hemmelige kode CC og autentiseringskoden I, da den siste vil være lagret i mikrokontrollerens EPROM.

Tilsvarende omfatter tjeneren en annen dialoganordning og en annen krypterings/dekrypteringsanordning bestående enten av DES-algoritmen eller RSA-algoritmen. Basisnøkkelen KB for DES-algoritmen er også lagret i den annen lagringsanordning. Disse andre lagringsanordninger omfatter også den offentlige nøkkel KBP benyttet i RSA-algoritmen.

I henhold til oppfinnelsen, vil den således beskrevne innret-

ning være istand til å arbeide enten ved hjelp av DES-algoritmen eller ved hjelp av RSA-algoritmen i henhold til kravene, idet valget av algoritmen kan skje ved hjelp av informasjon inneholdt i autentiseringskoden I.

Virkemåten til den ovennevnte innretning skal nå forklares ved spesielt å henvise til fig. 4-8.

Alment omfatter virkemåten til pakken to hovedmoder:

- En forsesjonsmode hvor pakken vil autentiseres,

- en sesjonsmode som kan implementeres etter forsesjonsmoden for å beskytte overføringen av meldinger mellom pakken og tjeneren via terminalen.

Forsesjonsmoden kan effektueres enten ved å benytte DES-algoritmen eller ved å benytte RSA-algoritmen. Fordelaktig skal sesjonsmoden eksekveres med DES-algoritmen. I tilfelle DES-algoritmen benyttes i forsesjonsmoden finner gjensidig autentisering sted mellom tjeneren og pakken og basisnøkkelen KB er lagringsnøkkelen KST.

Starten på forsesjonsmoden er representert av flytkartet på fig. 4 som benyttes på to algoritmer. Flytkartene på henholdsvis figurene 5 og 6 angår DES- og RSA-algoritmen og representerer to varianter av slutten på forsesjonsmoden.

I denne forsesjonsmode virker pakken på svitsjeinnretningen AIG slik at de forskjellige koblinger for terminalen konfigureres. Samtidig overvåker pakken enhver handling på denne svitsjeinnretning, nemlig enhver handling hvis opphav er eksternt for pakken (tjeneren eller en tredjeparts forulempende handling som forsøker å modifisere koblingene). Enhver annen handling, f.eks. en anmodning om å modifisere svitsjingen som ikke kreves av pakken, vil resultere i at forsesjonsmoden avbrytes.

Tilsvarende skal pakken i denne forsesjonsmode sperre forbin-

delsen mellom tastaturet og terminalen og linjegrunnsnittet slik at ikke noe informasjon som mates inn av brukeren, er i stand til å overføres klart til LST-linjen. Hver gang denne sperringen blir effektivt utført, slås den første displayanordning på.

Nå følger en beskrivelse av bruken av starten av forsesjonsmoden ved hjelp av DES-algoritmen DES.

Etter at brukeren på sin terminal har tastet inn koden for aksess til den valgte tjener, sender tjeneren en identifikasjonsanmodning til pakken i trinn 10. Denne identifikasjonen består i å sjekke at adressen for pakken er gyldig. Pakken mottar anmodningen i trinn 11, verifiserer i trinn 12 gyldigheten av adressen og sender i trinn 13 om den siste er gyldig en identifikasjonsbekreftelse til tjeneren. Den siste mottar denne bekreftelsen på trinn 14 som markerer starten på en forhåndsbestemt sekvens av operasjoner mellom første dialoganordning i pakken og den annen dialoganordning i tjeneren.

Alment kan en melding utvekslet mellom tjeneren og pakken bestå av en serie 8-bits ord TVL hvor hvert ord T angir typen av operasjon, biten V angir feltet for de virkelige data og biten L spesifiserer lengden i byter av datafeltet V.

Etter å ha mottatt bekreftelsen i trinn 14, sender tjeneren en autentiseringsanmodning til pakken. Denne autentiseringsanmodning svarer til en bit T lik 01 og mottas av pakken i trinn 15 og etter å ha virket på svitsjeinnretningen AIG slik at forbindelsen linjegrensesnitt/tastatur sperres, initialiserer pakken i trinn 16 en melding på skjermen EC som anmoder brukeren om å mate inn sin fortrolige kode CC. Brukeren mater deretter inn sin fortrolige kode på tastaturet.
Etter at denne fortrolige kode er blitt matet inn, verifiserer pakken i trinn 17 hvorvidt eller ikke den svarer til dataene lagret i EPROM-anordningen i pakken. For å foreta denne sammenligningen dekrypterer en krypterings/dekrypteringsan-

ordningen en fortrolig kode ved hjelp av lagringsnøkkelen KST. Når samsvaret er korrekt, sender pakken sin identifikasjonskode I i trinn 18 til tjeneren. Tjeneren mottar den i trinn 19 og byten 3 har da verdi 02. Ved hjelp av en algoritme for å generere et passende randomtall, velger tjeneren deretter i trinn 20 et randomtall X'. Ved hjelp av dette tall X' for autentiseringskoden I og basisnøkkelen KB til DES-algoritmen, beregner den annen krypterings/dekrypteringsanordning til tjeneren et element av de kryptografiske data Y' ved hjelp av DES-algoritmen (21). Tallet X' utgjør den første primærnøkkel hvis betydning skal forklares i det følgende.

I resten av beskrivelsen skal seriene av trinn 10-21 betegnes med henvisningen 1. Resten av flytkartet som angår slutten av forsesjonsmoden er vist på fig. 5.

Etter å ha beregnet de kryptografiske data Y', sender tjeneren sin autentiseringskode S i trinn 22 til pakken. Den siste motta den i trinn 23, idet byten 3 også har verdi 02. Ved mottagelse av autentifiseringskoden S velger den første dialoganordning i pakken (trinn 24) et annet randomtall X og en første krypterings/dekrypteringsanordning beregner et element av de kryptografiske data Y ved hjelp av DES-algoritmen, basisnøkkelen KB, det annet randomtall X og autentiseringskoden S (trinn 25).

Dette annet randomtall som X som utgjør primærnøkkelen, genereres av den første dialoganordning fra tiden som medgår mellom det øyeblikk da pakken har anmodet brukeren om å mate inn sin fortrolige kode og det øyeblikk hvor den siste effektivt har matet det inn på tastaturet.

Etter å ha bestemt de kryptografiske data Y, sender pakken dem i trinn 26 til tjeneren, idet byten T da har verdien 03. Tjeneren mottar Y i trinn 27 og krypterer dem i trinn 34 ved hjelp av DES-algoritmen og bruk av basisnøkkelen KB. Denne krypteringen tillater tjeneren å hente sin autentiseringskode S og verifisere den. Om denne verifikasjon er positiv, får

tjeneren deretter det annet randomtall X og sammenføringen av det første randomtall X' og det annet randomtall X skal utgjøre den definitive sesjonsnøkkel KSS som kan benyttes av DES-algoritmen i sesjonsmoden (trinn 36). Sesjonsnøkkelen KSS skal lagres i lese-skrivelageret MV.

Før dekrypteringen av de kryptografiske data Y i trinn 34, sender tjeneren de kryptografiske data Y som ble beregnet i trinn 21. Pakken mottar disse kryptografiske data i trinn 29 og dekrypterer dem ved hjelp av basisnøkkelen KB til DES-algoritmen. I trinn 31 henter pakken således sin autentiseringskode I såvel som det første randomtall X'. Verifikasjonen av I utføres i trinn 32 og om denne sjekken er positiv, sender pakken en bekreftelse som tjeneren mottar i trinn 37. Etterpå beregner pakken (i trinn 3) den definitive sesjonsnøkkel KSS av DES-algoritmen som er sammenføringen av randomtallene X og X'. I resten av beskrivelsen skal trinnene 31 og 32 betegnes med henvisningen 30.

Trinn 37 markerer slutten på forsesjonsmoden for pakken BA. Denne modeslutt er markert ved aktivering av den annen displayanordning LED2. I denne forsesjonsmode, vil en anomali vedrørende innmatingen av den fortrolige kode i trinn 17 på skjermen fremkalle visningen av en melding som angir at den fortrolige kode er gal. Brukeren kan mate inn tre ukorrekte meldinger. Hvis den fortrolige kode fremdeles er gal etter disse tre meldinger, avbrytes forsesjonesmoden i trinn 38. Tilsvarende er det under hele denne forsesjonsmoden viktig at sekvensen av de forhåndsbestemte operasjoner utføres i den nødvendige orden. Denne orden er representert av de stigende verdier 01,02,03 for byten 3. Hvis pakken eller tjeneren mottar en byte med gitt verdi uten å ha mottatt byten med den foregående verdi, avbrytes også forsesjonsmoden i trinn 38. Endelig vil en anomali resultatet av en operasjon gjøre at forsesjonsmoden avbrytes. En slik anomali kan være feiltilpasningen mellom autentiseringskoden I som mottas, og den lagrede (trinn 32).

Hvis forsesjonsmoden er utført korrekt, vil tjeneren og pakken gjensidig identifisere seg selv og pakken kan gå over til sin sesjonsmode. Brukeren kan derfor sende tjeneren (og omvendt) krypterte eller signerte meldinger. Disse meldingene skal være kryptert eller signert ved hjelp av DES-algoritmen ved bruk av sesjonsnøkkelen KSS.

I det tilfelle hvor brukeren eller tjeneren ikke ønsker å overføre noen krypterte eller signerte meldinger, blir disse meldingene derfor overført i klartekst på linjen LST og pakken BA er da "gjennomsiktig" i relasjon til terminalen så lenge som krypteringen eller signaturen ikke behøves.

På den annen side kan sesjonsmoden tjeneren anmode pakken om å foreta en kryptert datainnmating av data tastet inn på tastaturet av brukeren. I dette tilfelle vil pakken ved mottagelse av en slik melding, karakterisert av en byte T lik 04 og en byte L lik 01, virke på svitsjeinnretningen AIG slik at den siste i klartekst sperrer utgangen på linjen LST av data matet inn på tastaturet av brukeren. Disse data skal på forhånd krypteres av DES-algoritmen før de sendes på linjen LST. Et eksempel på et dataelement som skal mates inn kryptert, kan være transaksjonsstørrelsen i tilfelle av en hjemmebank-tjeneste. Således bevares denne transaksjonens fortrolighet. Tjeneren kan også sende kryptert informasjon (f.eks. en bankkontoutskrift) på linjen LST og denne informasjonen skal dekrypteres ved hjelp av DES-algoritmen og sesjonsnøkkelen KSS.

Undertiden er det ikke nødvendig å kryptere en melding, men på den annen side kan det være nødvendig å verifisere helheten av meldingen når den mottas. Dette er grunnen til at tjeneren og pakken er istand til å signere de overførte meldinger.

En melding som inneholder en rekke blokker med åtte byter av data signeres på følgende måte. Den første blokken sendes først i klartekst på linjen LST og krypteres deretter ved hjelp av DES-algoritmen, den andre blokken sendes først i klartekst på

linjen LST etterfølgende den første blokk og deretter sammenlignes den f.eks. i en logisk EKSKLUSIV ELLER-port med den første krypterte blokk, idet resultatet av denne sammenligningen i sin tur krypteres av DES-algoritmen. Denne prosessen gjentas inntil alle meldingsblokkene er sendt. Den endelige signatur sendes deretter på linjen LST. Ved mottagelse av meldingen, verifiserer tjenerne eller pakken signaturen mot bruk av samme metode, og sikrer således at meldingen i sin helhet blir mottatt. Bekjentgjørelsen av en signert melding er karakterisert ved det faktum at byten T antar verdien 05.

I sesjonsmoden kan pakken uten videre motta en melding betegnet av en byte T lik 4 eller en melding betegnet av en byte T lik 5. I denne sesjonsmoden av pakken vil et hvert forsøk av en datahacker på å interferere med svitsjekontrollen til terminalen resultere i at sesjonsmoden avbrytes og pakken kobles ut. Denne utkobling kan også vil av en anmodning for utkobling fra brukeren eller tjeneren. Sesjonsnøkkelen blir deretter slettet og skal erstattes av en annen nøkkel under en fremtidig sesjon.

Med henvisning nå til fig. 6, viser denne et flytkart for hvordan slutten av forsesjonsmoden til pakken virker med bruk av en RSA-krypteringsalgoritme. Starten på moden kan ses av fig. 4. På fig. 6 skal de analoge elementene eller de analoge funksjoner med henvisning til de vist på fig. 4 og 5 betegnes ved hjelp av henvisningstall økt med 100 med hensyn til elementene på fig. 4 og 5. Bare forskjellene mellom fig. 6 og fig. 4 og 5 skal beskrives i det følgende.

Selv om RSA-algoritmen benyttes, er de personlige data CC og I fremdeles dekryptert av DES-algoritmen ved bruk av lagringsnøkkelen KST.

Etter å ha utført serien av trinn 101 på fig. 4, har tjeneren således i trinn 121 bestemt de kryptografiske data Y' ved hjelp av RSA-algoritmen, den offentlige nøkkel KBP, pakke-autentiseringskoden I og randomtallet X'. I RSA-algoritmeversjonen

benyttet av søkerne, er de kryptografiske data kodet på 40 byter. Da transmisjonen på linje LST i denne utførelsesform bare muliggjør en 8 byters transmisjon, er det derfor nødvendig å dele dataene Y' i fem kryptografiske dataelementer Y'1, Y'2, Y'3, Y'4, Y'5. De fem kryptografiske dataelementene Y'1 til Y'5 blir suksessivt sendt i rekkefølge til pakken i trinn 40. Pakken mottar henholdsvis disse under trinnene 41,43,45 og 49 og sender tjeneren bekreftelse når den siste mottar i trinnene 42,44,46 og 48. Etter mottagelse av dataene Y'5 i trinn 49, begynner den første krypterings/dekrypteringsanordningen i serien av trinn 130 å dekryptere de kryptografiske data Y' ved hjelp av RSA-algoritmen og den hemmelige nøkkel KBS forbundet med den offentlige nøkkel KPB.

Naturligvis vil det være mulig å benytte en kodemode slik at dataene Y' overføres på en gang.

Etter å ha verifisert at autentifiseringskoden I var korrekt, fås således randomtallet X' og en bekreftelse sendes til tjeneren som den siste mottager i trinn 137. Da randomtallet X' er på 32 byter (da autentiseringskoden I er på 8 byter), er det nødvendig å utføre kompresjon av tallet X' i trinn 50 slik at det reduseres til 8 byter. Dette komprimerte tall X' skal utgjøre sesjonsnøkkelen KSS for DES-algoritmen som deretter eventuelt skal benyttes under sesjonsmoden.

Nå følger en beskrivelse som angår den spesielle mode for å benytte innretningen i henhold til oppfinnelsen med spesiell henvisning til fig. 7 og 8.

Som tidligere nevnt var det nødvendig at pakkeautentiserings-koden I, såvel som brukerens fortrolige kode var lagret i EPROM-hukommelsen IC31. Det er derfor foretrukket å ha et første lasteprogram for dataene i sentralprosessorenheten IC1. Dette første program starter automatisk straks pakken først får tilkoblet strøm ved en passende terminal utstyrt med en skjerm. En melding skal vises på skjermen for å be om at både pakke-autentiseringskoden I og den fortrolige kode for den mulige

bruker mates inn. Dette skal utføres i trinn 200. Trinn 201 omfatter mottagelse av dataene og lagrer deretter i trinn 202 de data som på forhånd er krypterte av DES-algoritmen som befinner seg utenfor pakken, i hukommelsen. Når trinn 202 er avsluttet, følger et trinn 203 hvor en ny lasting av autentiserings- og fortrolige koder er sperret. I trinn 204 blir således slutten på dataoverføringen angitt ved aktivering av de lysemitterende dioder LED 1 og LED 2 og trinnene 205 ender avslutter det første lasteprogram.

Det annet lasteprogram, hvis flytkart er vist på fig. 8, er et program som tillater data å legges inn eller at spesifikke programvarer innføres i pakken. Dataene og programvaren kan f.eks. være personlige telefonbeskjeder med automatisk kobling til et valgt nummer eller lokale teksteditor. Det annet program skal starte automatisk straks pakken kobles til strøm for annen gang.

Selv om dette annet lasteprogram omfatter en rekke blokker, utføres lagringen av en blokk i hukommelsen IC3 i trinn 302. Det sendes derfor en bekreftelse som angir at denne blokken er korrekt lagret og operasjonen fortsetter inntil alle blokkene i det annet lasteprogram er lagret i hukommelsen. Når antallet mottatte blokker er lik antallet blokker som skal mottas, fremkommer i trinn 303 et trinn 305 som er identisk med trinn 203 og sperrer en ny lasting av et annet program og trinn 306 angir slutten på lastingen av blokkene ved aktivering av diodene LED1 og LED2. Trinn 307 avslutter lasteprogrammet. Blokkene som skal lagres kan ledsages av forhåndsbestemt signatur som gjør det mulig å sjekke den effektive lagring av et autorisert program.

Oppfinnelsen kan omfatte varianter, spesielt de følgende:

- Det har tidligere blitt vist at forsesjonsmoden ble initialisert av tjeneren. Imidlertid kan det f.eks. være mulig å sikre at moden initialiseres på en ordre som mates inn av brukeren på terminalens tastatur.

- Med det henblikk å skaffe ytterligere beskyttelse av de utvekslede data og oppfinnelsens personlige natur, er det mulig å forestille seg at lagringsnøkkelen KST benyttet av DES-algoritmen, er kombinasjonen av minst to nøkler. Den første nøkkel eller initialen nøkkel KF vil maskeres i det faste leselager MM i mikrokontrolleren når den dannes. Den eksterne hukommelse IC31 i mikrokontrolleren vil deretter inneholde kryptogrammet for en mellomnøkkel KI. Endelig vil den eksterne hukommelse inneholde de personlige data (CC, I) kryptert av DES-algoritmen og lagringsnøkkelen KST.

Således vil mellomnøkkelen KI på det tidspunkt pakken benyttes, være dekryptert ved hjelp av sitt kryptogram og den initiale nøkkel KF. Lagringsnøkkelen KST skal deretter dekrypteres av sitt kryptogram og mellomnøkkelen mens de personlige data skal dekrypteres av lagringsnøkkelen. I det tilfelle hvor DES--algoritmen benyttes i forsesjonsmoden, er lagringsnøkkelen KST, basisnøkkelen KB og sesjonsnøkkelen KSS skal overføres kryptert i henhold til basisnøkkelen KB, idet basisnøkkelen også lagres i den annen lagringsanordning i tjeneren. I det tilfelle hvor RSA-algoritmen benyttes, er basisnøkkelen fremdeles kombinasjonen av den offentlige nøkkel KPB og den hemmelige nøkkel KBS.

Denne varianten tillater en større grad av personliggjørelse av pakken, da det er mulig å forsyne forskjellige brukere med pakker som har den samme nøkkel KF, men som har egne mellomnøkler KI og lagringsnøkler KST for hver bruker. Dessuten gjør det faktum at lagringsnøkkelen foreligger i form av et kryptogram, det mulig å lagre den i et eksternt programmerbart leselager og ikke lenger i et fast leselager i mikrokontrolleren.

- Sekvensiering av fortsettelsen av operasjoner utføres ved bruk av byten T. Denne bruk avhenger av transmisjonsprotokollen. Generelt behøver bare hver operasjon å forsynes med et karakteristisk element som gjør det mulig å identifisere den.

Faktisk kan noen av de ovenfor nevnte anordninger utelates i de varianter hvor de ikke benyttes, spesielt behøver RSA-algoritmen ikke å settes inn i lagringsanordningen til pakken hvis de gitte applikasjoner utelukkende benytter DES-kryptering.

PATENTKRAV

1. Innretning til utveksling av data mellom på den ene side en videotextterminal (TVX) med et linjegrensesnitt (IL), et tastatur (CL), en skjerm (EC), en nedstrøms videoadapterkobling (PPI), en fordelerinnretning (AIG) mellom disse anordninger og en strømforsyning, og på den annen side en tjener (SE) som innbefatter kryptering/dekrypteringsanordninger og dialoganordninger, hvor innretningen er
k a r a k t e r i s e r t v e d at den også omfatter en ytterligere pakke (BA) forbundet til videoadapterkoblingen (PPI) på videotextterminalen (TVX) og forsynt med strøm fra strømforsyningen til terminalen (TVX), idet den ytterligere pakke (BA) innbefatter krypterings/dekrypteringsanordningene og dialoganordningen (MD1), og at kryptering/dekrypteringsanordningen til den ytterligere pakke og de til tjeneren, såvel som dialoganordningene til den ytterligere pakke og de til tjeneren er innrettet til å samvirke for å danne: først en utvekslingsforsesjon hvorunder de definerer en sesjonsnøkkel (KSS) som overføres i samsvar med en basisnøkkel (KB, KBP, KBS), deretter en utvekslingsesjon hvorunder dialoganordningen til den ytterligere pakke og til tjeneren (SE) samvirker for å tillate utvekslingen av krypterte og/eller signerte meldinger basert på sesjonsnøkkelen (KSS), idet den ytterligere pakke (BA) innbefatter anordninger som er i stand til å virke på fordelerinnretningen (AIG) til videotextterminalen (TVX) for å overvåke en hver annen operasjon på fordeleranordningen (AIG) og for å bevirke avbrudd av forsesjon i tilfellet av en annen operasjon på fordeleranordningen eller en anomali.

2. Innretning i henhold til krav 1,
k a r a k t e r i s e r t v e d at anordningene til den ytterligere pakke,hvilke anordninger er egnet til å virke på fordeleranordningen (AIG), er i stand til å forhindre forbindelsen mellom grensesnittet og tastaturet (CL) ved innføringen av en fortrolig kode (CC) over tastaturet.

3. Innretning i henhold til krav 1 og 2,

k a r a k t e r i s e r t v e d at sesjonsnøkkelen (KSS) genereres fra minst et første randomtall (X').

4. Innretning i henhold til et av kravene 1-3, k a r a k t e r i s e r t v e d at sesjonsnøkkelen (KSS) omfatter en første primærnøkkel (X') generert av dialog-anordningene i tjeneren (SE).

5. Innretning i henhold til krav 4, k a r a k t e r i s e r t v e d at tjeneren (SE) kan levere den første primærnøkkel (X') til videoterminalen (TVX).

6. Innretning i henhold til et av de foregående krav, k a r a k t e r i s e r t v e d at den ytterligere pakke (BA) omfatter en første lagringsanordning (MM, IC3), mens tjeneren (SE) omfatter en annen lagringsanordning, idet de to lagringsanordninger inneholder i det minste en del av basis-nøkkelen.

7. Innretning i henhold til krav 6, k a r a k t e r i s e r t v e d at den første lagringsan-ordning innbefatter faste ROM- og PROM-anordninger (MM; IC31).

8. Innretning i henhold til krav 7, k a r a k t e r i s e r t v e d at PROM-anordningen (IC31) innbefatter spesielle informasjoner kryptert av krypterings/-dekrypteringsanordningene ved hjelp av en lagringsnøkkel (KST).

9. Innretning i henhold til krav 8, k a r a k t e r i s e r t v e d at lagringsnøkkelen er en kombinasjon av minst én initialnøkkel (KF) og én mellomnøkkel (KI), idet initialnøkkelen (KF) er lagret i ROM-anordningen (MM), mens mellomnøkkelen (KI) er lagret i PROM-anordningen (IC31) og krypteres av krypterings/dekrypteringsanordningene ved hjelp av initialnøkkelen (KF).

10. Innretning i henhold til et av kravene 6-9, k a r a k t e r i s e r t v e d at basisnøkkelen er en

enkeltnøkkel (KB) lagret både i de første og andre lagrings-anordninger.

11. Innretning i henhold til krav 4 og 10, k a r a k t e r i s e r t v e d at sesjonsnøkkelen (KSS) er en kombinasjon av den første primærnøkkel (X') og en annen primærnøkkel (X) generert av pakkens første dialoganordning (MD1).

12. Innretning i henhold til krav 11, k a r a k t e r i s e r t v e d at den annen primærnøkkel (X) genereres av et annet randomtall.

13. Innretning i henhold til krav 2 og 12, k a r a k t e r i s e r t v e d at det annet randomtall (X) avhenger av tiden som går mellom anmodningen om å mate inn den fortrolige kode (CC) og den virkelige innmating på tastaturet (CL).

14. Innretning i henhold til krav 11-13, k a r a k t e r i s e r t v e d at den ytterligere pakke (BA) leverer den annen primærnøkkel (X) til tjeneren (SE).

15. Innretning i henhold til krav 8 eller 9 i kombinasjon med et av kravene 10-14, k a r a k t e r i s e r t v e d at basisnøkkelen (KB) er lagringsnøkkelen (KST).

16. Innretning i henhold til et av kravene 6-9, k a r a k t e r i s e r t v e d at basisnøkkelen omfatter en offentlige nøkkel (KBP) lagret i den annen lagringsanordning og en hemmelige nøkkel (KBS) lagret i den første lagringsanordning (MM), idet de offentlige og hemmelige nøkler er komplementære til hverandre.

17. Innretning i henhold til krav 4 og 12, k a r a k t e r i s e r t v e d at sesjonsnøkkelen (KSS) er den første primærnøkkel (X').

18. Innretning i henhold til et av de foregående krav, k a r a k t e r i s e r t v e d at den ytterligere pakke også omfatter anordninger som aktiveres i det minste når videotexterminalen (TVX) først tilkobles strøm for å muliggjøre lagring av personlig informasjon i pakken.

19. Innretning i henhold til et av kravene 2-18, k a r a k t e r i s e r t v e d at den ytterligere pakke (BA) omfatter en første displayanordning (LED1) som indikerer sperring av forbindelsen mellom linjegrensesnittet (IL) og tastaturet (CL).

20. Innretning i henhold til krav 1-19, k a r a k t e r i s e r t v e d at den ytterligere pakke (BA) omfatter en annen displayanordning (LED2) som indikerer etableringen av sesjonsnøkkelen (KSS).

21. Fremgangsmåte til utveksling av data mellom på den ene side en videotextterminal (TVX) og på den annen side en tjener (SE) ved datakryptering og- dekryptering, hvor fremgangsmåten er k a r a k t e r i s e r t v e d at før det etableres en datautvekslingssesjon, blir det i en forsesjon mellom tjeneren og terminalen definert en sesjonsnøkkel som overføres mellom tjeneren (SE) og videotextterminalen (TVX) ved hjelp av en forhåndsbestemt basisnøkkel (KB, KBP, KBS), at denne forsesjon avbrytes hvis det foreligger en anomali i forsesjonen, og at sesjonsnøkkelen (KSS) deretter benyttes til datautvekslingssesjonen.

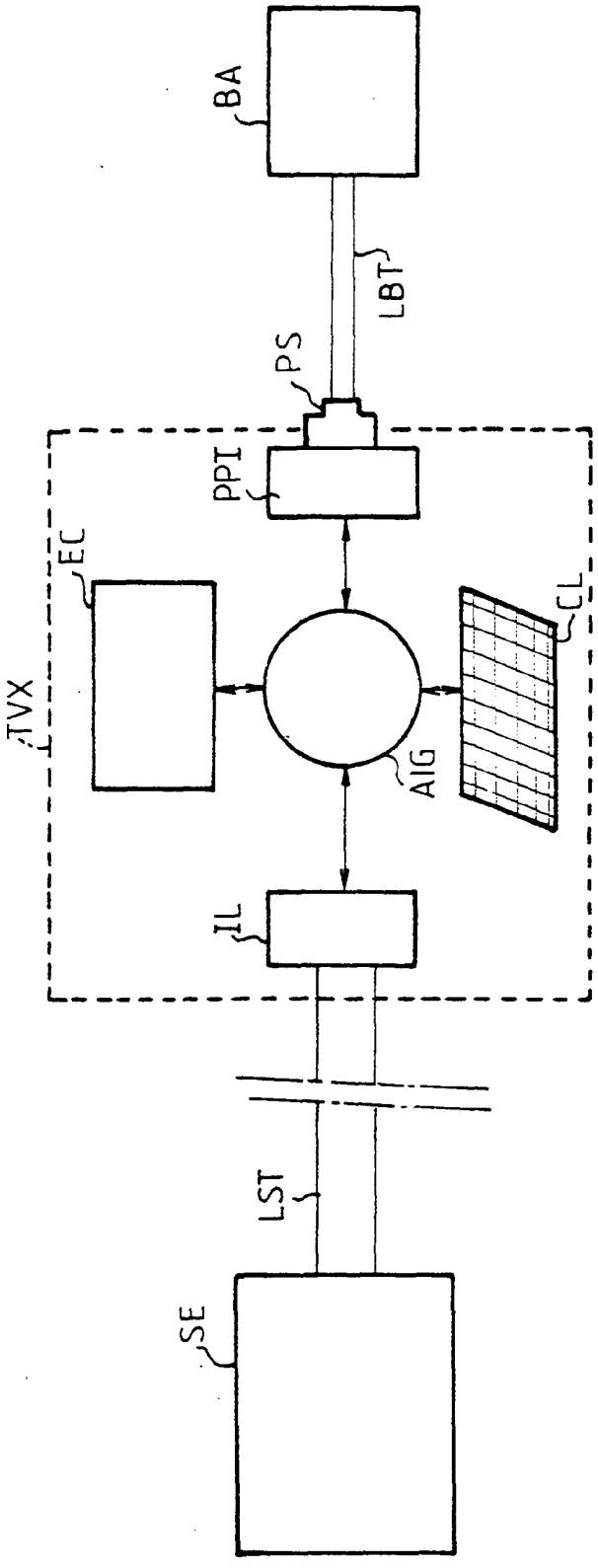


FIG.1

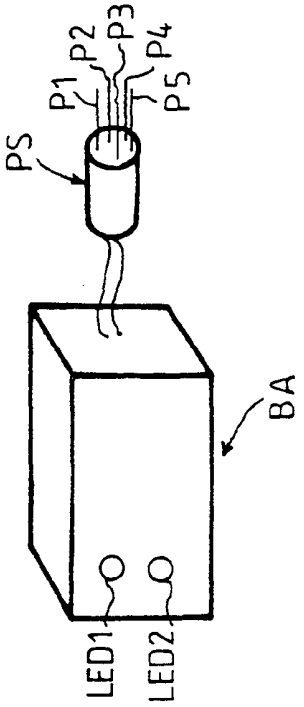


FIG.2

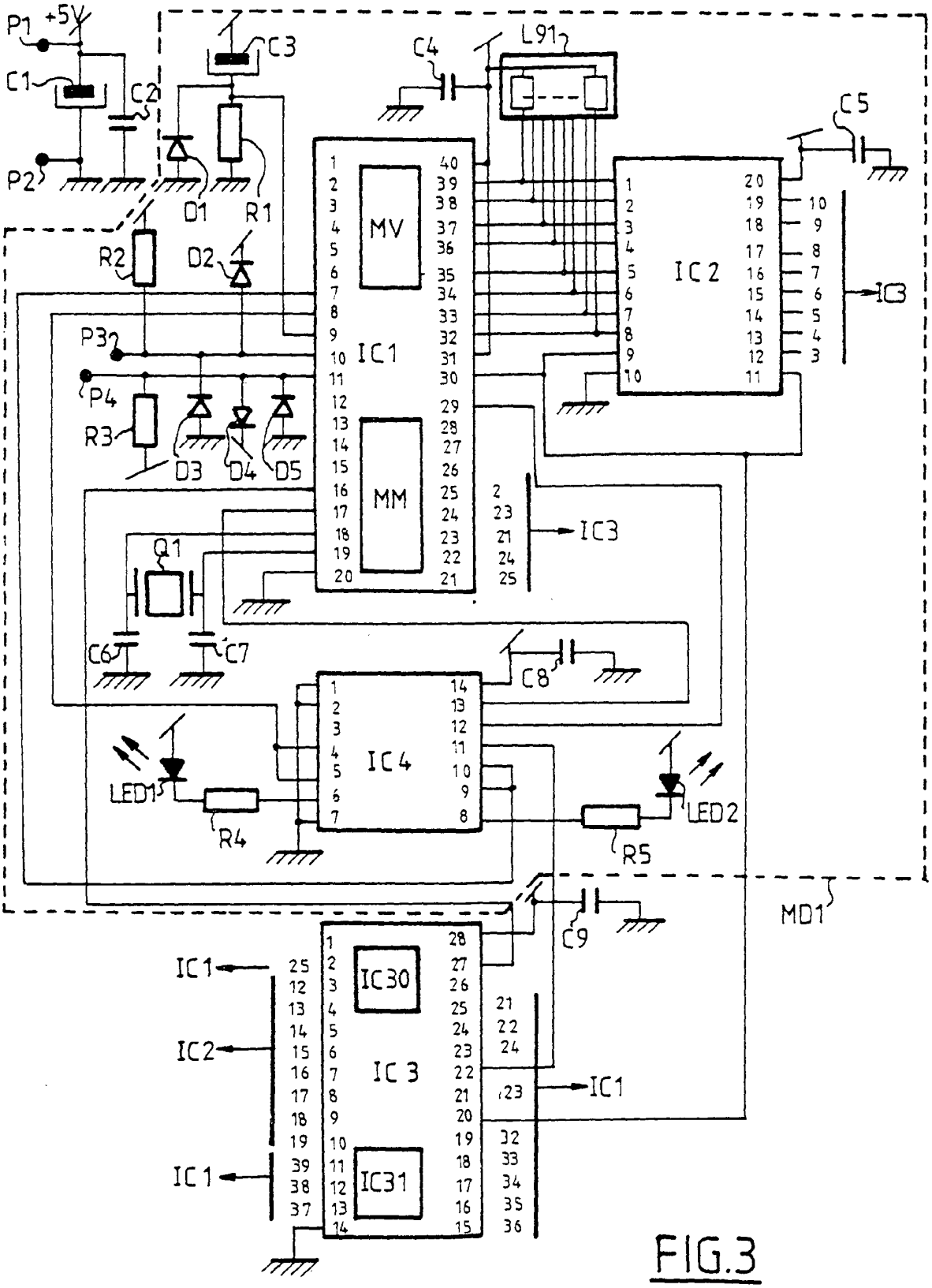

P1
+5V
C1
C2
P2
C3
D1
R1
R2
D2
P3
P4
R3
D3
D4
D5
C4
L91
C5
MV
IC1
MM
IC2
IC3
Q1
C6
C7
C8
IC4
LED1
R4
LED2
R5
MD1
C9
IC30
IC 3
IC31

FIG.3

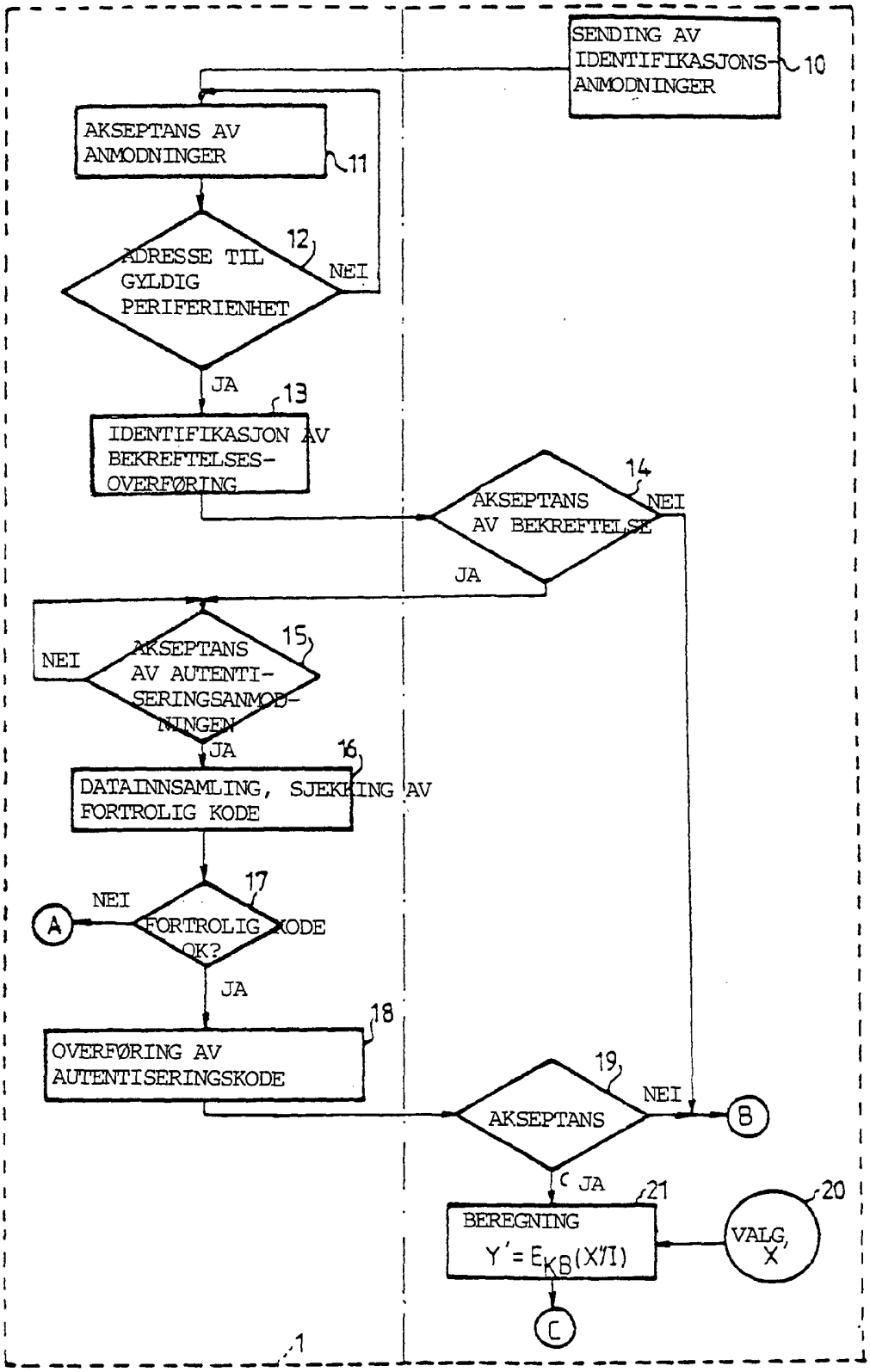

SENDING AV IDENTIFIKASJONS-ANMODNINGER
10
AKSEPTANS AV ANMODNINGER
11
ADRESSE TIL GYLDIG PERIFERIENHET
12
NEI
JA
IDENTIFIKASJON AV BEKREFTELSES-OVERFØRING
13
AKSEPTANS AV BEKREFTELSE
14
NEI
JA
NEI
AKSEPTANS AV AUTENTI-SERINGSANMOD-NINGEN
15
JA
DATAINNSAMLING, SJEKKING AV FORTROLIG KODE
16
NEI
A
FORTROLIG KODE OK?
17
JA
OVERFØRING AV AUTENTISERINGSKODE
18
AKSEPTANS
19
NEI
B
JA
BEREGNING
$Y' = E_{KB}(X'I)$
21
VALG, X'
20
C
1

FIG.4

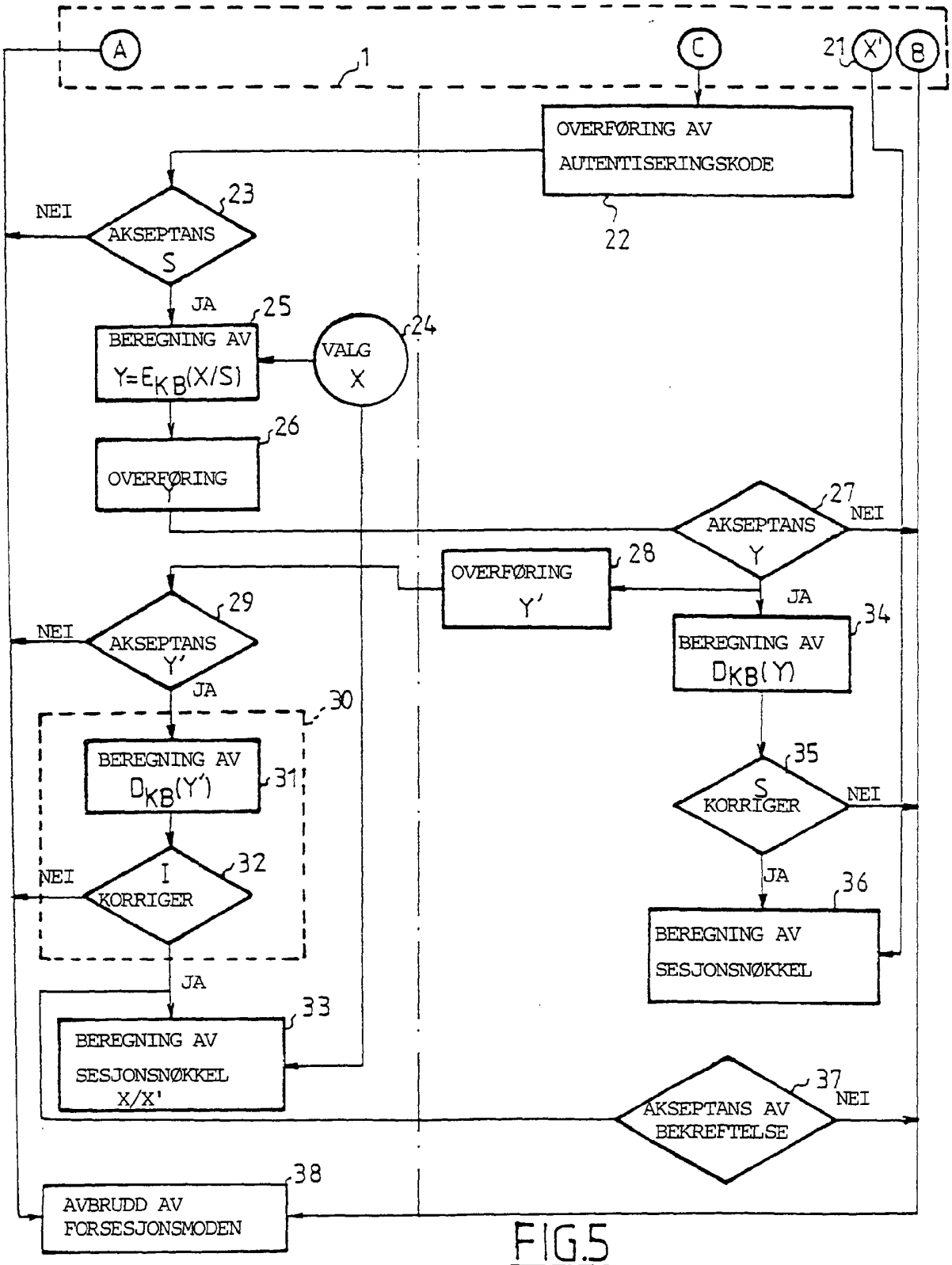

A
1
C
21
X'
B
OVERFØRING AV AUTENTISERINGSKODE
22
23
AKSEPTANS S
NEI
JA
25
BEREGNING AV Y=E_KB(X/S)
24
VALG X
26
OVERFØRING Y
27
AKSEPTANS Y
NEI
28
OVERFØRING Y'
JA
29
AKSEPTANS Y'
NEI
JA
34
BEREGNING AV D_KB(Y)
30
BEREGNING AV D_KB(Y')
31
35
S KORRIGER
NEI
JA
I KORRIGER
32
NEI
JA
36
BEREGNING AV SESJONSNØKKEL
33
BEREGNING AV SESJONSNØKKEL X/X'
37
AKSEPTANS AV BEKREFTELSE
NEI
38
AVBRUDD AV FORSESJONSMODEN

FIG.5

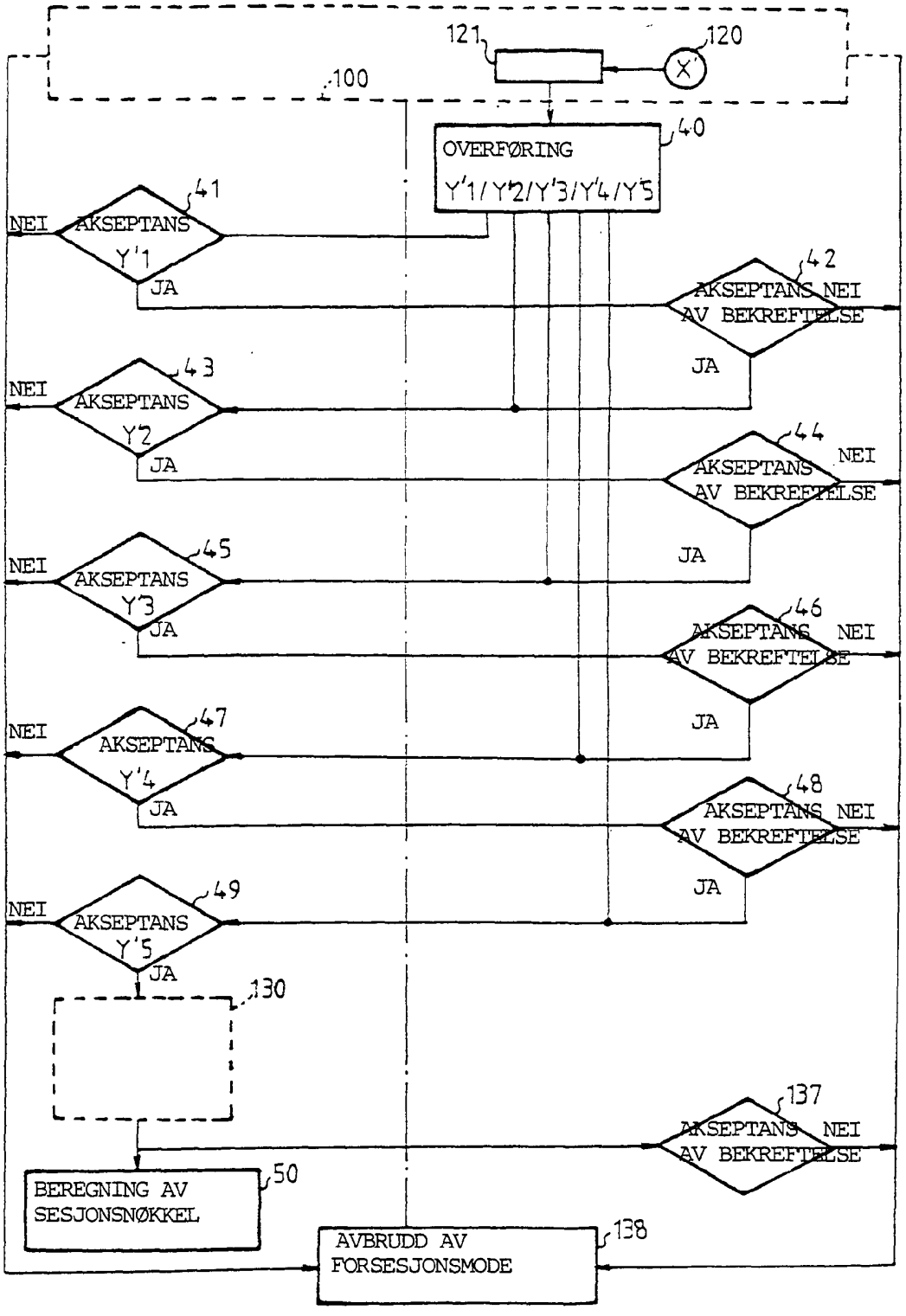

121
120
X'
100
OVERFØRING
Y'1/Y'2/Y'3/Y'4/Y'5
40
41
AKSEPTANS
Y'1
NEI
JA
42
AKSEPTANS NEI
AV BEKREFTELSE
JA
43
AKSEPTANS
Y2
NEI
JA
44
AKSEPTANS
AV BEKREFTELSE
NEI
JA
45
AKSEPTANS
Y3
NEI
JA
46
AKSEPTANS
AV BEKREFTELSE
NEI
JA
47
AKSEPTANS
Y'4
NEI
JA
48
AKSEPTANS
AV BEKREFTELSE
NEI
JA
49
AKSEPTANS
Y'5
NEI
JA
130
137
AKSEPTANS
AV BEKREFTELSE
NEI
BEREGNING AV
SESJONSNØKKEL
50
AVBRUDD AV
FORSESJONSMODE
138

FIG.6

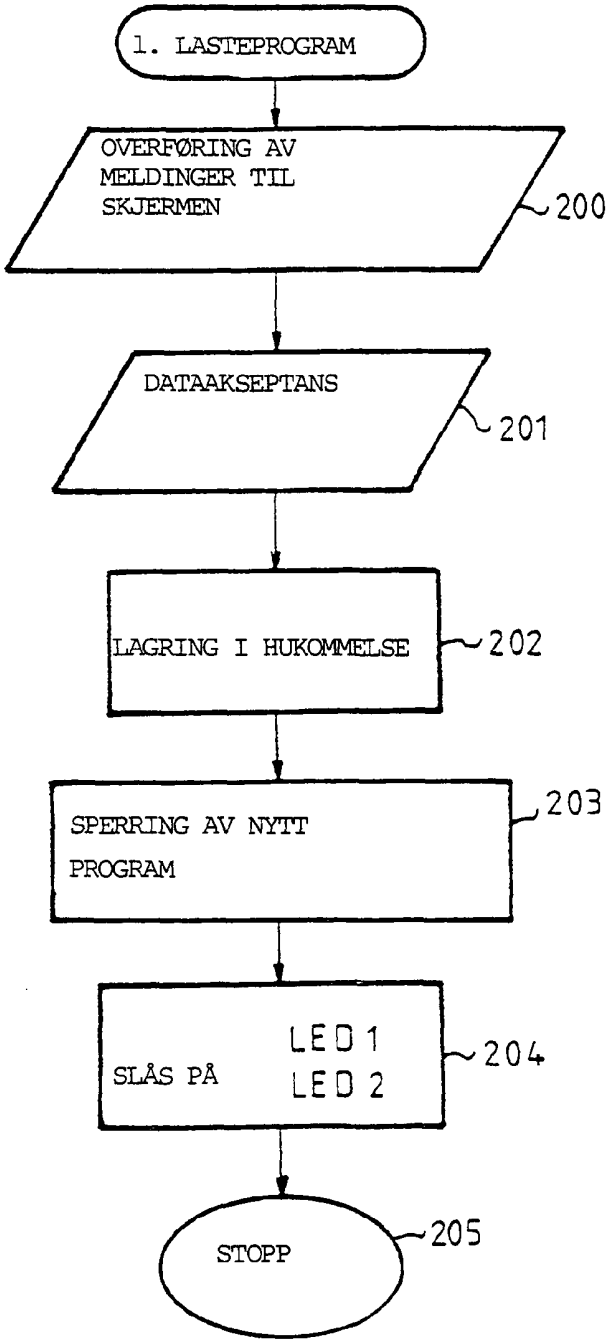

1. LASTEPROGRAM
OVERFØRING AV MELDINGER TIL SKJERMEN
200
DATAAKSEPTANS
201
LAGRING I HUKOMMELSE
202
SPERRING AV NYTT PROGRAM
203
SLÅS PÅ
LED 1
LED 2
204
STOPP
205

FIG.7

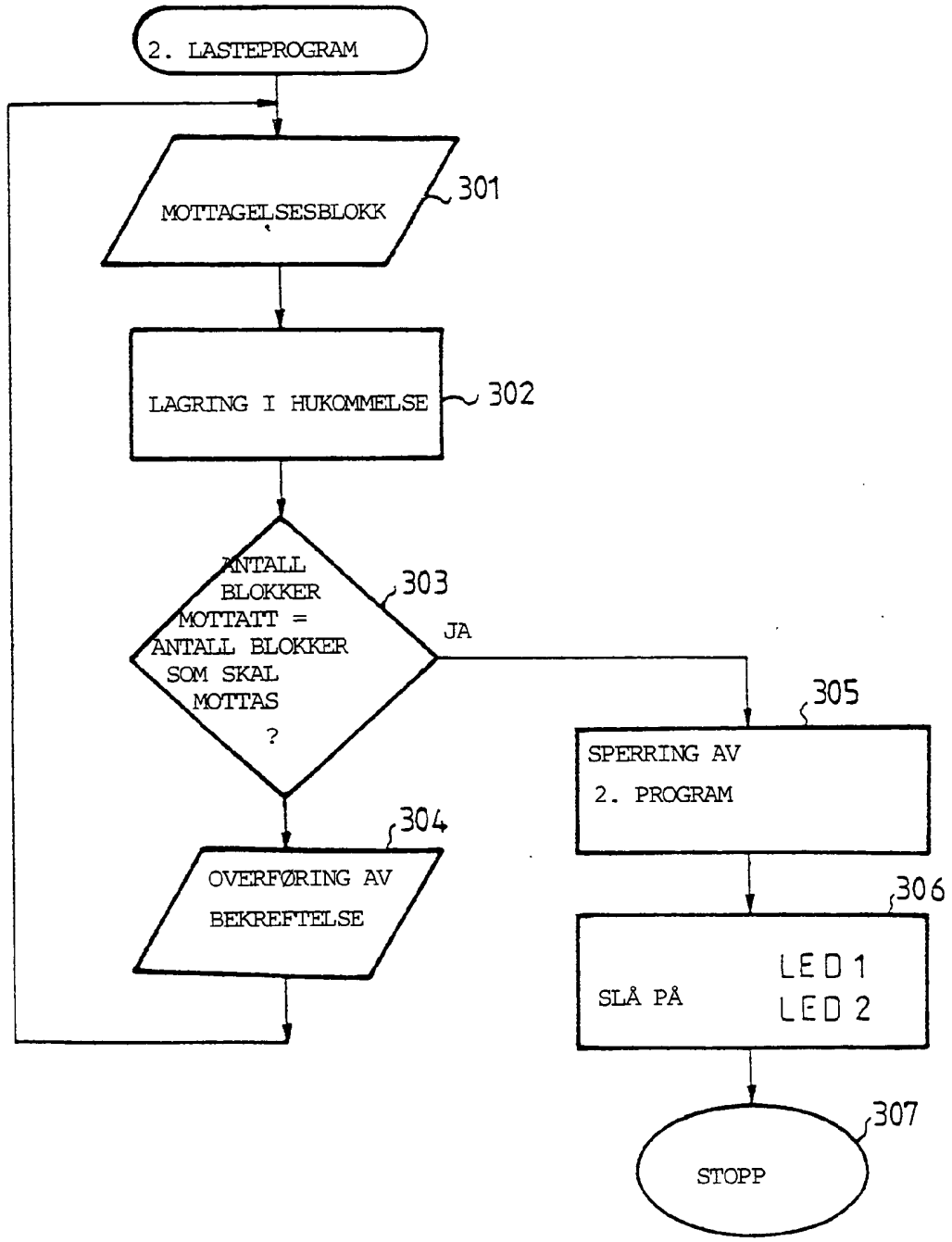

2. LASTEPROGRAM
MOTTAGELSESBLOKK
301
LAGRING I HUKOMMELSE
302
ANTALL BLOKKER MOTTATT = ANTALL BLOKKER SOM SKAL MOTTAS ?
303
JA
OVERFØRING AV BEKREFTELSE
304
SPERRING AV 2. PROGRAM
305
SLÅ PÅ LED 1 LED 2
306
STOPP
307

FIG.8