NORGE [B] (11) **UTLEGNINGSSKRIFT** Nr. 129373

STYRET
FOR DET INDUSTRIELLE
RETTSVERN

(51) Int. Cl. H 04 1 9/02

(52) Kl. 21a[1]-21

(21) Patentsøknad nr. 3006/68
(22) Inngitt 31.7.1968
(23) Løpedag 31.7.1968
(41) Søknaden alment tilgjengelig fra 3.2.1969
(44) Søknaden utlagt og utlegningsskrift utgitt 1.4.1974
(30) Prioritet begjært fra: 2.8.1967 Sveits, nr. 10913/67

(71)(73) Anstalt Europäische Handelsgesellschaft, Vaduz, Liechtenstein.

(72) Sture Nyberg, Weinbergstr. 14, Zug, Sveits.

(74) Bryns Patentkontor A/S

(54) Innretning for automatisk sifrering og/eller desifrering av en tekst som består av flersifrede binært kodede tegn.

Oppfinnelsen angår en innretning for automatisk sifrering og/eller desifrering av en tekst som består av flersifrede binært kodede tegn, ved hjelp av flersifrede binært kodede kodetegn som leveres fra en kodetegngenerator.

Automatisk arbeidende sifrerings- og desifreringsinnretninger benytter idag for det meste siffersignalrekker, hvor såvel klarteksttegnene resp. kryptoteksttegnene likesom kodetegnene er tilordnet et antall toverdige signalverdier, som regel fem. Sifreringen skjer som oftest på en av følgende to måter: Enten blir de stedvis motsvarende toverdige informasjoner knyttet sammen i en

eksklusiv-Eller-kombinasjon (fortegnsmultiplikasjon), eller adderes de toverdige verdier i modul-2^n-form hvor n er antallet toverdige verdier av tegnene (som regel som ovenfor nevnt fem, hvor $2^n = 32$).

Et eksempel på den første kodingsart:
(Eksklusiv-Eller-kombinasjon)

Teksttegn	0 L 0 L L
Kodetegn	L 0 0 L 0
Resultat	0 0 L L 0

Et eksempel på den andre kodingsart:
(Binær addisjon)

Teksttegn	0 L 0 L L
Kodetegn	L 0 0 L 0
Resultat	L L 0 0 0 (L)

Vanligvis bortfaller den i klammer stående overføring.

Kodeinformasjonen tas kontinuerlig fra en kodetegninnretning som kan være utformet som en selvstendig generator eller f.eks. som hullbåndavleser eller lignende. Det er innlysende at for desifrering er det nødvendig med synkronisering av den der anvendte kodetegngenerator. Kodetegngeneratoren frembringer en kodetegnrekke som bare er underlagt kodetegngeneratorens lovmessighet. Minst to slike generatorer må altså arbeide nøyaktig likt. I et fjernmeldenett benyttes imidlertid et større antall generatorer, idet hver stasjon er tildelt en slik generator fordi hver stasjon må kunne samarbeide med enhver av de andre. I praktisk bruk er det imidlertid umulig å hindre en av en stasjon benyttet tegnrekke i sin tildelte kodegenerator å bli anvendt av en annen stasjon. Det oppstår da såkalte kodelike tekster som kan desifreres ved språklig sammenligning.

Hensikten med oppfinnelsen er å tilveiebringe en framgangsmåte hvorved opptreden av kodelike tekster hindres. Dette oppnås ifølge oppfinnelsen ved et adderingsverk for binær addering av teksttegn og kodetegn med en første inngang for tilførsel av teksttegn, en andre inngang som er forbundet med kodetegngeneratoren for tilførsel av kodetegn, en utgang for uttak av tegn som resultat av hver addisjon, og en overføringsutgang som avgir et overføringssignal når det ved addisjonen av tegnene i siste siffer

opptrer en overføring, samt en med overføringsutgangen forbundet databehandlingsanordning for siffersignalrekker, som er koplet foran den første eller andre inngangen av adderingsverket, eller etter utgangen av dette, for ifølge et overføringssignal å modifisere på bestemt måte de i databehandlingsanordningen innmatede tegn.

Når databehandlingsanordningen f.eks. er tilsluttet foran inngangene for kodetegn, dvs. mellom kodetegngeneratoren og adderingsverket, og når addisjonen av et teksttegn og et modifisert eller ikke modifisert kodetegn resulterer i et overføringssignal over adderingsverkets overføringsutgang, modifiseres det etterfølgende kodesignal som mates inn av databehandlingsanordningens kodetegngenerator på grunn av overføringssignalet, og innføres som et modifisert kodetegn i adderingsverket.

Når databehandlingsanordningen er tilsluttet foran inngangene for teksttegn, overføres hvert teksttegn som innkommer til databehandlingsanordningen etterat et overføringssignal har opptrått over overføringsutgangen i modifisert tilstand til adderingsverket, og adderes der til motsvarende kodetegn.

Når databehandlingsanordningen er tilsluttet adderingsverkets utganger frembringes et utgangstegn, dvs. et hemmelig teksttegn i modifisert tilstand, f.eks. til et telexnett, når i løpet av foregående operasjon addisjonen av delene i et teksttegn og et kodetegn resulterer i et overføringssiffer.

Ved en forholdsvis lang tekst vil gjennomsnittlig 50% av de forskjellige addisjoner resultere i et overføringssiffer, slik at ved en sifreringsoperasjon vil omtrent halvparten av tegnene (klartekst- eller kodetegn eller tegn i den hemmelige tekst) bli modifisert, men den andre halvdel vil bli sendt ut uten modifisering.

På denne måte oppnås det resultat at ved hver tekst som gjennomgår sifrering eller desifrering (klartekst eller hemmelig tekst) vil noen av de kodetegn som frembringes av kodetegngeneratoren modifiseres automatisk og individuelt. Hver tekst sifreres således med sin egen individuelle kode.

Det er klart at ved anvendelse av kodetegnmodifisering vil de enkelte koder som tilføres adderingsverket ved to forskjellige kommunikasjonstilfeller være ulike selv om kodetegnrekkene som leveres av kodetegngeneratorene er identiske. Der er således

umulig ved bare en sammenligning av språket i de to tekster som sifreres på denne måte, å desfirere dem, fordi de kodetegn som adderes til den opprinnelige tekst må være identiske for at en slik desifreringsmåte skal kunne anvendes. Databehandlingsanordningen kan være slik konstruert at den som svar på et inngangssignal overfører gruppene av inngangssignaldeler til utgangene i syklisk permutering med et siffer. Slike databehandlingsanordninger er kjente og bygges f.eks. opp av logiske kretselementer.

Databehandlingsanordningen kan også konstrueres slik at overføringssignalet i modul-2^n adderes til inngangssignaldelene. Det er meget lett å konstruere en slik anordning. I dette tilfelle kan det oppnås en enda mere effektiv sifrering ved hjelp av egnede kretser som er innrettet slik at databehandlingsanordningen påvirker addisjonen bare når et forutbestemt logisk signal, fortrinnsvis logisk "1" tilføres den siste dataposisjon for kodetegninngangene.

Et utførelseseksempel på oppfinnelsen skal forklares nærmere under henvisning til tegningen.

Fig. 1 viser skjematisk de enkelte trinn ved sifreringen.

Fig. 2 viser skjematisk de enkelte trinn ved desifreringen.

For bedre forståelse av utførelseseksemplet skal bemerkes:

Det benyttes en toverdig (binær) addisjonsmodul 32 for den idag ved fjernskriveranlegg vanlige 5er kode, men denne brukes ikke direkte til kodingen. Fremgangsmåten er naturligvis ikke begrenset til 5-plass-koding og er her bare nevnt som eksempel. En ved denne addisjon eventuelt opptredende overføring (som vanligvis vil falle bort som ovenfor nevnt) blir avlest og anvendt for modifikasjon av det etterfølgende kodetegn som er tildelt det etterfølgende teksttegn, hvorved i første rekke den egentlige koding dvs. sammenknytning av teksttegn og kodetegn, ikke skal tas i betraktning.

Ved denne fremgangsmåte oppnås at enhver tekst som bringes til koding på individuell måte endrer de av kodegeneratoren vanligvis til rådighet stilte kodetegn. Enhver melding får således sin egen individuelle kode.

Det skal uttrykkelig fastholdes at koden for to meldinger også kan være forskjellig hvis de primære fra kodegeneratoren leverte kodetegnrekker til å begynne med har samme karakteristikk. For

språklig desifrering av to meldinger er det imidlertid ubetinget nødvendig at den kode som adderes i begge tilfeller er fullstendig overensstemmende.

Dermed oppnås at slike meldinger ikke lenger blir kodelike og derfor ikke kan desifreres hvis det ikke ved sifreringen opprinnelig ble anvendt samme kodetegnrekke.

I følgende eksempler blir endringen av vedkommende kodetegn som tas fra den av kodegeneratoren leverte rekke, oppnådd på den måte at det cyklisk foretas en permutering en plass. I prinsippet kan også andre lovmessige endringer av kodetegnene utføres. Arten og måten er irrelevant for oppfinnelsesprinsippet i seg selv.

Det følgende eksempel beror på følgende operasjoner:

Tekstsignalfølgen, i det følgende betegnet som tekstbokstaver, blir ifølge prinsippet om fortegnmultiplikasjon sammenknyttet med den tilhørende kodesignalrekke, i det følgende betegnet kodebokstaver, hvorved disse kodebokstaver - som ovenfor nevnt- på forhånd eventuelt er permutert cyklisk en plass.

Sammenknytningsregelen skal rekapituleres (Eksklusiv-Eller-kombinasjon).

LxO = O OxL = O LxL = L OxO = L

For frembringelse av modifikasjonssignalet som altså skal innvirke på de etterfølgende kodebokstaver utføres en addisjon, hvorved følgende grunnsetning skal bringes i erindring:

O+O = O O+L = L L+O = L L+L = O (+L)
O+O+L = L O+L+L = O (+L) L+O+L = O (+L)
L+L+L = L (+L)

På fig. 1 er vist en tabellarisk fremstilling av fem etter hverandre følgende kodetrinn. I kolonne A er vist klartekstbokstavene på toverdig skrivemåte i 5er kode - som er vanlig i fjernskriveranlegg idag -. I kolonne B er vist kodebokstavene slik de i dette tilfelle leveres fra kodegeneratoren. Kolonne C inneholder den modifiserte kode slik de til enhver tid frembringes etter inntreffen av et modifikasjonssignal fra det foregående trinn ved cyklisk permutering. I kolonne D er resultatet av regneoperasjonen "tekst ganger modifisert kode" angitt og i kolonne E er sluttelig resultatene for signalfrembringelsen som er dannet ved regneoperasjonen "opprinnelig kode plus kryptobokstav".

Det er klart at på linje 1 som første operasjon frembringes kryptobokstaven i kolonnen D ved multiplikasjon av bokstaven i kolonne A med kodebokstaven i kolonne C.

Denne kryptobokstav blir som resultat stilt til rådighet for videreføring og dessuten blir den slik som pilen oppover antydet, trukket inn for utførelse av regneoperasjonen: Koden fra kolonne B pluss kryptobokstaven er lik signalresultatet i kolonne E.

Det er videre klart at det skjer en overføring til plass 6 som her trekkes inn som signal for modifikasjon av kodebokstaven B i linje 2.

I linje 2 blir således kodebokstaven i kolonne B cyklisk permutert og dens nye form er vist i kolonne C, og multiplikasjon med tekstbokstaven fra kolonne A gir resultat i kolonne D.

Den opprinnelige kryptobokstav i kolonne B i linje 2 blir så addert med det nettopp frembragte resultat i kolonnen D og gir i kolonne E en signalbokstav idet det igjen på plass 6 skjer en overføring som griper inn i linje 3.

Av linje 3 fremgår at i kolonnen E dannes et resultat som ikke har noen overføring til plass 6 og således blir i linje 4 kryptobokstaven i kolonne B overført uforandret for blanding i kolonne C.

Sammenfattet må altså alltid følgende to operasjoner utføres:

1. Egentlig kodeoperasjon:

Tekstbokstaven ganger modifisert kodebokstav = resultat D.

2. Hjelpeoperasjon:

Resultat pluss original kodebokstav = signal E.

Signalet er et tegn som modifiserer de etterfølgende kodebokstaver hvis det på plass 6 skjer en overføring.

Det er klart at denne modifikasjonsordre i gjennomsnitt dukker opp i ca. 50% av tilfellene. Den andre halvdel av kodebokstavene kan overtas uforandret.

Det er naturligvis også uten videre mulig i stedet for fortegnmultiplikasjon for den egentlige koding å anvende addisjon modul-2 resp. modul-32, slik at hjelpeoperasjonen faller bort, ved

at resultatet samtidig anvendes som signal. Det kan i dette tilfelle også forutsettes en ytterligere variasjon: Overføringssignalordren gjøres bare virksom når det for frembringelse av signalbokstaven tilførte kodetegn på et eller annet sted, f.eks. på siste plass, har en L.

Desifreringen utføres på samme måte og er vist på fig. 2. I kolonne F er vist kryptotekstbokstavene, i kolonne G kodebokstavene, i kolonne H den modifiserte kode, i kolonne I resultat av multiplikasjonen (klarteksten frembragt ved desifreringen), i kolonne K sluttelig igjen signalbokstavene som kan utløse modifikasjonen av koden.

I linje 1 er i kolonne F vist kryptobokstaven slik den fremgår av fig. 1, kolonne D, linje 1. Dens addisjon med koden i kolonne G (opprinnelig for sifrering av kolonne B) gir i kolonne K signalbokstavene som igjen har en overføring til plass 6.

Den samme kryptobokstav i kolonne F, linje 1 blir imidlertid også multiplisert med den modifiserte kode i kolonnen H (ved første tegn igjen identisk med den opprinnelige kode fra kodegeneratoren) og gir i kolonne I det desifrerte tegn som resultatbokstav.

I linje 2 er igjen vist den samme operasjon og det er nå klart at kryptobokstaven i kolonne G ved modifikasjonsordre fra den foregående linje omdannes ved cyklisk permutering til en ny bokstav som er angitt i kolonne H. Multiplikasjonen gir igjen den opprinnelige klartekstbokstav i linje 2.

Det er uten videre klart for fagmannen at i stedet for vedkommende påvirkning av kodebokstaven kunne også tekstbokstaven påvirkes. Således består også den mulighet å utføre en påvirkning av de dannede resultatbokstaver. Hele operasjonen reduseres således til en påvirkning av kodeoperasjonen i øyeblikket.

Beskrivelsen ovenfor av en cyklisk permutering av toverdige elementer av kodebokstaven ved modifikasjon, er bare en av de realiserbare muligheter. Ved en addisjonssifrering kunne det f.eks. også tenkes at det toverdige overføringselement adderes til neste kodetegn for å tilveiebringe modifikasjonen.

129373

Patentkrav

1. Innretning for automatisk sifrering og/eller desifrering av en tekst som består av flersifrede binært kodede tegn, ved hjelp av flersifrede binært kodede kodetegn som leveres fra en kodetegngenerator, karakterisert ved et adderingsverk for binær addering av teksttegn og kodetegn med en første inngang for tilførsel av teksttegn, en andre inngang som er forbundet med kodetegngeneratoren for tilførsel av kodetegn, en utgang for uttak av tegn som resultat av hver addisjon, og en overføringsutgang som avgir et overføringssignal når det ved addisjonen av tegnene i siste siffer opptrer en overføring, samt en med overføringsutgangen forbundet databehandlingsanordning for siffersignalrekker, som er koplet foran den første eller andre inngangen av adderingsverket, eller etter utgangen av dette, for ifølge et overføringssignal å modifisere på bestemt måte de i databehandlingsanordningen innmatede tegn.

2. Innretning ifølge krav 1, karakterisert ved at databehandlingsanordningen er en anordning som syklisk permuterer de innmatede tegn en plass.

3. Innretning ifølge krav 1, karakterisert ved at databehandlingsanordningen er en adderingsanordning som adderer overføringssignalet i modul-2^n-form til det innmatede tegn.

4. Innretning ifølge krav 3, karakterisert ved at den adderende databehandlingsanordning gjennom en av inngangene er styrt av kodetegnene fra adderingsverket, idet databehandlingsanordningen da bare utfører addisjonen når den nevnte inngang har et logisk L - signal.

(56) Anførte publikasjoner: Ingen.

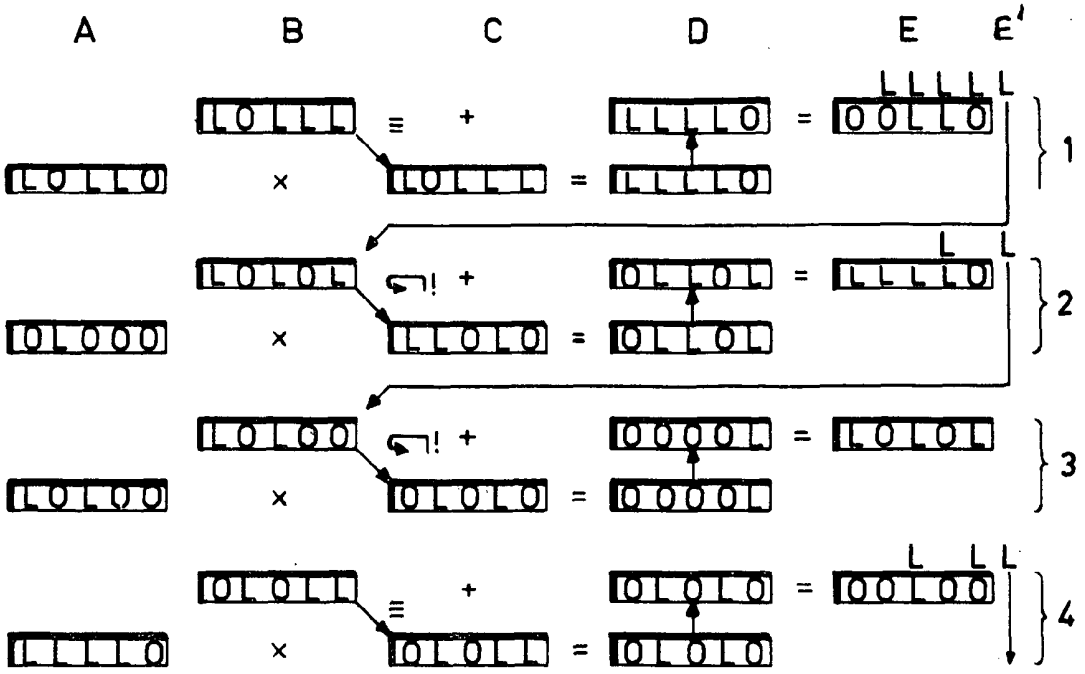

Fig. 1

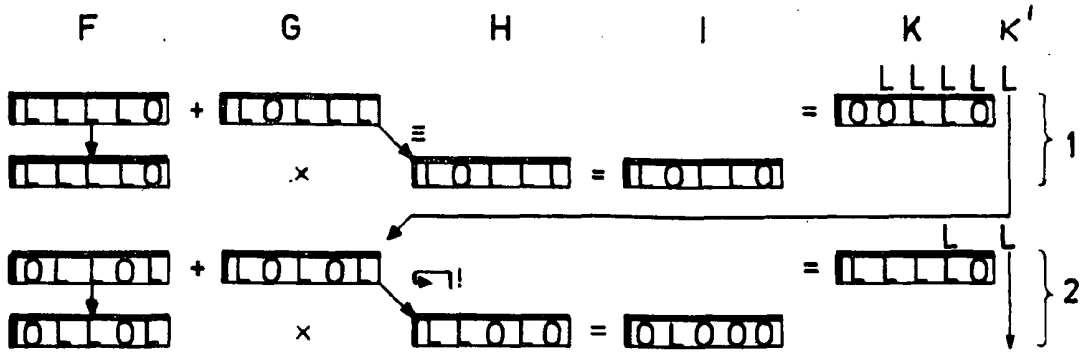

Fig. 2