Octrooiraad

(10) A **Terinzagelegging** (11) **8000675**

Nederland (19) **NL**

(54) **Werkwijze voor het coderen en decoderen van berichten.**

(51) Int.Cl³.: H04L 9/02.

(71) Aanvrager: N.V. Philips' Gloeilampenfabrieken te Eindhoven.

(74) Gem.: Ir. R.A. Bijl c.s.
Internationaal Octrooibureau B.V.
Prof. Holstlaan 6
5656 AA Eindhoven.

(21) Aanvrage Nr. 8000675.

(22) Ingediend 4 februari 1980.

(32) - -

(33) - -

(31) - -

(62) - -

(43) Ter inzage gelegd 1 september 1981.

De aan dit blad gehechte stukken zijn een afdruk van de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekening(en).

Werkwijze voor het coderen en decoderen van berichten.

De uitvinding heeft betrekking op een werkwijze voor het coderen en decoderen van berichten, volgens welke in een zendstation klare bericht impulsen en code impulsen worden gemengd, voor het vormen van een gecodeerd bericht en waarin in een ontvangstation de gecodeerde bericht impulsen en identieke code impulsen worden gemengd voor het verkrijgen van de klare bericht impulsen, waarbij de code impulsen in het zendstation en het ontvangstation worden opgewekt door een code generator waarvan de aanvangstoestand de code impuls opeenvolging bepaalt, waarbij het aantal mogelijke aanvangstoestanden zeer groot is en in het zendstation en in het ontvangstation de aanvangstoestand wordt bepaald door een in het zendstation en het ontvangstation opgeslagen eerste toestandsinformatie, aangeduid als basissleutel en door een tweede toestandsinformatie, aangeduid als berichtsleutel, welke in één van de stations willekeurig wordt gekozen en naar het andere station wordt overgedragen.

Een dergelijke werkwijze is bekend uit het US octrooischrift 3.291.908.

In telecommunicatienetten waarin voor de geheimhouding van de berichten van bovengenoemde werkwijze wordt gebruik gemaakt, bestaat vaak de behoefte om een aantal basissleutels toe te passen. Bijvoorbeeld om de stations in groepen met ieder een eigen basissleutel te kunnen indelen of om berichten in groepen met ieder een eigen basissleutel te kunnen classificeren. Het aantal basissleutels welke om klaarblijkelijke redenen ook dagsleutels worden genoemd, kan enkele tientallen bedragen. De dagsleutels worden gevoonlijk opgeslagen in beveiligde geheugencompartimenten van de codeerapparatuur, in welk verband de benaming : sleutelcompartimentatie ingang heeft gevonden.

Het gebruik van een meervoudigheid van dagsleutels vergt in een ontvangstation de instelling van de juiste dagsleutel, welke afhankelijk kan zijn van het tegenstation en/of de aard van het bericht. Deze instelling geschiedt tot dusver met de hand hetgeen een actie van een bedieningspersoon vergt en tevens vatbaar is voor vergissingen.

De uitvinding beoogt een werkwijze van het aangegeven type te verschaffen volgens welke in het ontvangstation de juiste dagsleutel (basissleutel) automatisch wordt ingesteld.

De werkwijze volgens de uitvinding vertoont daartoe het kenmerk, dat voor het geval een aantal mogelijke basissleutels zijn opgeslagen, in het zendstation en in het ontvangstation, voorafgaande aan de verwerking van de bericht impulsen, een eerste deel van een berichtsleutel wordt gecombineerd met een gekozen basissleutel voor het bepalen van een aanvangstoestand van de codegenerator en in het zendstation de klare berichtsleutel impulsen representerende een opeenvolging van een tweede deel van de berichtsleutel en van een aantal daaruit afgeleide controle tekens worden gemengd met de code impulsen voor het verkrijgen van een gecodeerde berichtsleutel en in het ontvangstation de gecodeerde berichtsleutel impulsen worden gemengd met de code impulsen en deze laatste stap steeds wordt herhaald uitgaande van telkens een andere basissleutel totdat als resultaat van de menging een opeenvolging van een gedecodeerd tweede deel van de berichtsleutel en van een aantal gedecodeerde controle tekens,welke overeenstemmen met de in het ontvangstation uit het gedecodeerde tweede deel van de berichtsleutel afgeleide controle tekens,wordt verkregen, waardoor de juiste aanvangstoestand van de codegenerator in het ontvangstation, welke vereist wordt voor het op juiste wijze decoderen van de gecodeerde bericht impulsen,kan worden bepaald door de laatst gekozen basissleutel en de combinatie van het eerste en het tweede deel van de berichtsleutel.

De uitvinding zal nader worden toegelicht aan de hand van de enkele figuur, welke een blokdiagram toont van een stelsel, omvattende een zendstation en een ontvangstation, voor het uitvoeren van de werkwijze volgens de uitvinding.

In figuur 1 wordt getoond een zendstation S en een ontvangstation R van een stelsel voor de overdracht van berichten met geheimhouding, voor zover als nodig is voor het verklaren van de werkwijze volgens de uitvinding.

Het dient te worden opgemerkt, dat de werkwijze volgens de uitvinding uitsluitend dient om het opsporen van de juiste dagsleutel in het ontvangstation mogelijk te maken. De daarop volgende codering en decodering van de bericht impulsen kan plaats vinden op de wijze zoals is beschreven in US octrooischrift 3.291.908. Het ontvangstation S en het zendstation R zijn alleen getoond in voldoende detail voor het verklaren

van de werkwijze volgens de uitvinding. De configuratie voor het coderen en decoderen van de bericht impulsen is slechts symbolisch aangeduid.

Het zendstation S bevat een zendinrichting 1 voor klare tekst bijvoorbeeld een verreschrijver; het ontvangstation R bevat een ontvanginrichting 2 voor klare tekst bijvoorbeeld eveneens een verreschrijver.

Berichten welke van zendstation S naar ontvangstation R worden overgedragen door transmissiekanaal 3, worden in het zendstation gecodeerd door de bericht impulsen te mengen met een reeks code impulsen in een menginrichting 4. In de ontvanginrichting worden de gecodeerde bericht impulsen gemengd met een identieke reeks code impulsen in een menginrichting 5. De reeks code impulsen, welke een toevalskarakter heeft, wordt in het zendstation opgewekt door code pulsgenerator 6 en in het ontvangstation door de identieke code pulsgenerator 7. Het resultaat is een reeks klare bericht impulsen aan de uitgang van menginrichting 5, wanneer inderdaad de pulsgeneratoren 6 en 7 identieke reeksen code impulsen leveren.

Een reeks code impulsen wordt bepaald door de aanvangstoestand van de code pulsgenerator, waarvan het aantal aanvangstoestanden zeer groot is in vergelijking met 10 exp. 10 (10^{10}).

De aanvangstoestand van pulsgenerator 6 wordt bepaald door een dagsleutel en een berichtsleutel. De berichtsleutel wordt geleverd door een toevalsgenerator 8. De dagsleutel is opgeslagen in een beveiligd geheugen 9. De berichtsleutel wordt door transmissiekanaal 3 overgedragen aan het ontvangstation. In het ontvangstation is de dagsleutel opgeslagen in een beveiligd geheugen 10. De aanvangstoestand van pulsgenerator 7 kan dus bepaald worden door de dagsleutel uit geheugen 10 en de ontvangen berichtsleutel. Het geheim van de bericht overdracht ligt hier in de aanvangstoestand van de pulsgenerator. De informatie over de aanvangstoestand wordt verkregen door de dagsleutel met de berichtsleutel te mengen in de menginrichtingen 11 en 12.

De constructies van de menginrichtingen 4, 5, 11 en 12 en van de pulsgeneratoren 6 en 7 en van de toevalsgenerator 8 zijn in de voorafgaande techniek bekend, zoals bijvoorbeeld wordt aangetoond door het US octrooischrift 3.291.908.

Beschouwd wordt nu het geval, dat een aantal dagsleutels worden toegepast, waarbij het ontvangstation een keus moet maken uit een groep van dagsleutels. De dagsleutels zijn opgeslagen in compartimenten van de geheugens 9 en 10 en kunnen hieruit door afroep worden verkregen. In het

zendstation S wordt een bepaalde dagsleutel gekozen. Er wordt aangenomen dat in het ontvangstation R deze dagsleutel in één van de geheugencompartimenten van geheugen 10 is opgeslagen. Geen à priori kennis wordt verondersteld ten aanzien van het compartiment waarin deze dagsleutel zich bevindt.

De berichtsleutel wordt gegenereerd door toevalsgenerator 8. Een bepaalde werkwijze wordt nu gevolgd welke het mogelijk moet maken om in het ontvangstation de dagsleutel automatisch te bepalen.

De berichtsleutel, welke bijvoorbeeld uit tien tekens bestaat wordt verdeeld in een eerste deel I van vijf tekens en een tweede deel II van vijf tekens. De berichtsleutel wordt opgeslagen in een circulerend geheugen 13. Deel I van de berichtsleutel wordt tevens opgeslagen in een geheugen 14.

Deel I van de berichtsleutel wordt gemengd met de dagsleutel in menginrichting 11. Het resultaat van de menging bepaalt de aanvangstoestand van de code pulsgenerator 6. Verder wordt deel I van de berichtsleutel door transmissiekanaal 3 naar het geheugen 15 van het ontvangstation overgedragen, waartoe de schakelcircuits 16 en 17 in stand (1) staan ingesteld. Deze overdracht kan ter verhoging van de betrouwbaarheid en voor aanduiding van de start van een nieuw bericht een aantal malen, bijvoorbeeld vijf maal, herhaald worden, waartoe het geheugen 13 van een terugvoerleiding is voorzien.

Na de overdracht van deel I van de berichtsleutel wordt een opeenvolging van herhalingen van deel II van de berichtsleutel gecodeerd door menging met de code impulsen van pulsgenerator 6, waarvan de aanvangstoestand door de dagsleutel en deel I van de berichtsleutel is bepaald. Hiertoe wordt deel II van de berichtsleutel een aantal malen, bijvoorbeeld vijf maal, aan menginrichting 4 toegevoerd, waartoe schakelcircuit 18 in stand (2) staat ingesteld. Het resultaat van de menging is een gecodeerde berichtsleutel bestaande uit een gecodeerde opeenvolging van vijf herhalingen van deel II van de klare berichtsleutel. Deze gecodeerde berichtsleutel wordt door transmissiekanaal 3 naar geheugen 19 van het ontvangstation overgedragen, waartoe de schakelcircuits 16 en 17 in stand (2) staan ingesteld.

In het ontvangstation wordt de dagsleutel van een willekeurig compartiment van geheugen 10 gemengd met het deel I van de berichtsleutel in menginrichting 12. Het resultaat van de menging bepaalt de aanvangstoestand van code pulsgenerator 7.

De gecodeerde berichtsleutel, welke in geheugen 19 is opgeslagen, wordt gedecodeerd door menging met de code impulsen van pulsgenerator 7. Hiertoe wordt de gecodeerde berichtsleutel toegevoerd aan menginrichting 5, waartoe schakelcircuit 20 in stand (1) staat ingesteld. Het resultaat van de menging wordt toegevoerd aan testcircuit 21, waartoe schakelcircuit 22 in stand (1) staat ingesteld.

De gecodeerde berichtsleutel bestaat uit een gecodeerde opeenvolging van vijf herhalingen van deel II van de berichtsleutel, dus uit vijf maal vijf of vijfentwintig tekens. Het testcircuit 21 onderzoekt of de vijfentwintig gedecodeerde tekens vijf gelijke groepen van vijf tekens vormen, rekening houdend met een zekere kans op transmissiefouten. Hiertoe wordt onderzocht of de eerste bit van ieder teken overeenkomt met de eerste bits van alle andere tekens. Hetzelfde wordt herhaald voor de tweede bit en de volgende bits van ieder teken. Wanneer het aantal overeenstemmingen kleiner is dan een ingestelde drempelwaarde dan valt de test negatief uit en in het andere geval valt de test positief uit.

Wanneer de door testcircuit 21 uitgevoerde test negatief uitvalt, dan wordt onder besturing van het testcircuit 21 de dagsleutel van een ander compartiment van geheugen 10 gekozen. Verder wordt onder bestuur van testcircuit 21 opnieuw de gecodeerde berichtsleutel van geheugen 19 aan menginrichting 5 toegevoerd. Blijkt hierna dat de test weer negatief uitvalt, dan wordt weer een ander compartiment van geheugen 10 gekozen en wordt het voorgaande herhaald totdat de test positief uitvalt. De gezochte dagsleutel is dan de dagsleutel van het laatst gekozen compartiment van geheugen 10.

Na een positief uitgevallen test kan deel II van de berichtsleutel door de gestreepte verbinding van testcircuit 21 aan het geheugen 15 worden toegevoerd. De aanvangstoestand van pulsgenerator 7 kan dan worden bepaald door de laatst gekozen dagsleutel te mengen met de complete berichtsleutel. Verder kan het ontvangstation in de toestand voor het decoderen van de bericht impulsen gebracht worden, in welke toestand het schakelcircuit 17 in stand (3) en de schakelcircuits 20 en 22 in stand (2) staan ingesteld.

In het zendstation kan na het uitzenden van de gecodeerde berichtsleutel het deel II van de berichtsleutel door de gestreepte verbinding van geheugen 13 aan geheugen 14 worden toegevoerd. De aanvangstoestand van pulsgenerator 6 kan dan worden bepaald door de dagsleutel te mengen

met de complete berichtsleutel. Verder kan het zendstation in de toestand voor het coderen van bericht impulsen gebracht worden, in welke toestand het schakelcircuit 16 in stand (2) en het schakelcircuit 18 in stand (1) staat ingesteld.

Het coderen en het decoderen van de berichten onder gebruikmaking van de in het zendstation gekozen dagsleutel en de in het ontvangstation automatisch opgezochte dagsleutel en de in het zendstation willekeurig gekozen en naar het onvangstation overgedragen berichtsleutel kan nu op de bekende wijze plaats vinden.

Hierboven is beschreven, dat een gecodeerde opeenvolging van herhalingen van deel II van de berichtsleutel door het zendstation naar het ontvangstation wordt overgedragen. Wanneer deze opeenvolging met de juiste dagsleutel wordt gedecodeerd, dan wordt een opeenvolging van herhalingen van deel II van de berichtsleutel verkregen. Wordt echter een andere dagsleutel gebruikt, dan ontstaat een opeenvolging van betrekkelijk willekeurige tekens, welke niet de karakteristieke herhalingen van een groep van tekens omvat, zoals bij gebruik van de juiste dagsleutel het geval zou zijn. Een criterium kan worden vastgelegd, waarmede een opeenvolging van betrekkelijk willekeurige tekens kan worden onderscheiden van een opeenvolging waarin herhalingen van een groep van tekens voorkomen. Deze functie wordt verricht door testcircuit 21.

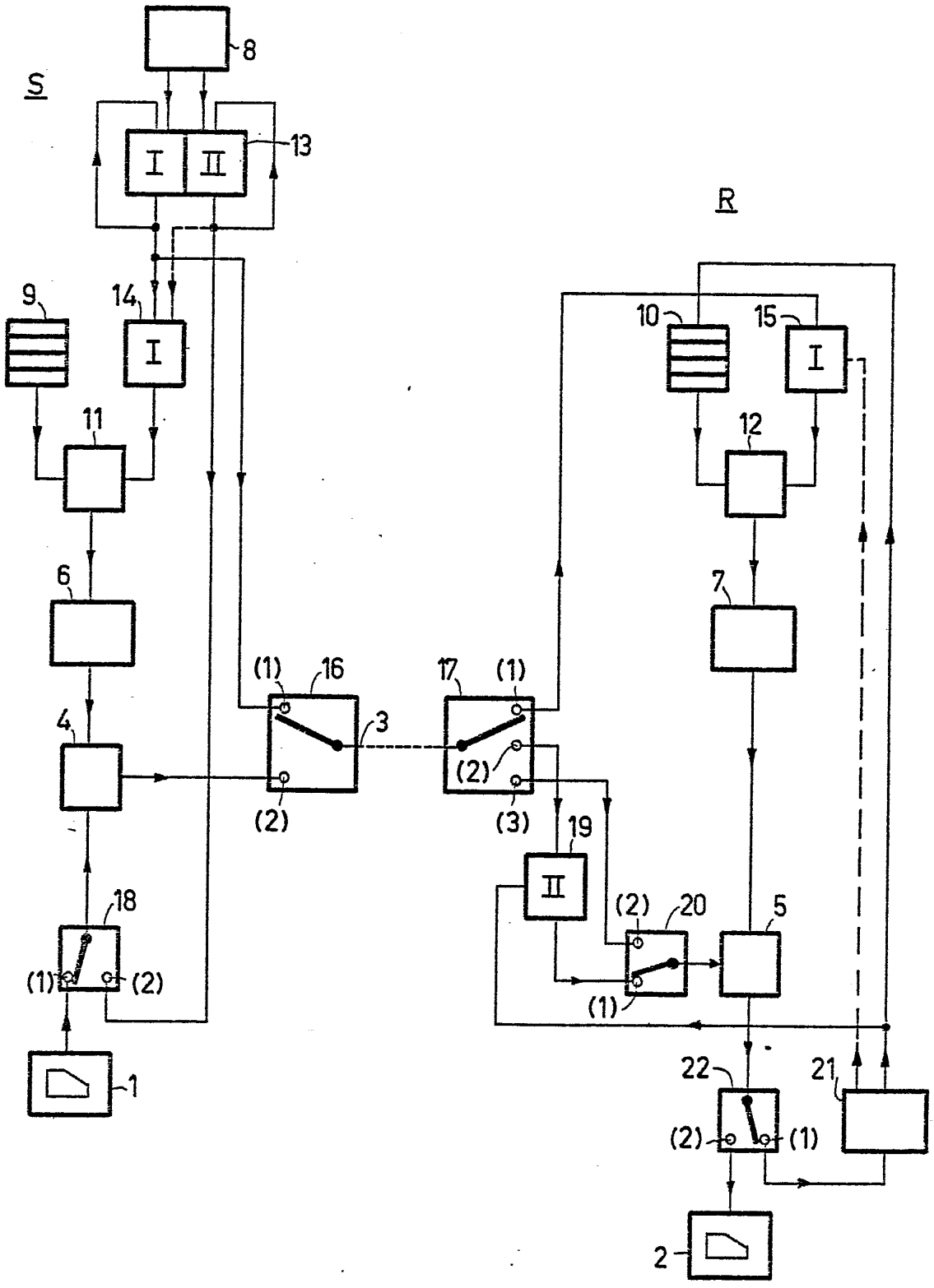
In de plaats van de overdracht van een gecodeerde opeenvolging van een aantal herhalingen van deel II van de berichtsleutel, kan in de hierboven beschreven werkwijze de overdracht van een gecodeerde opeenvolging van deel II van de berichtsleutel en van een aantal daaruit berekende controle tekens worden toegepast. In het ontvangstation worden, na decodering van deze opeenvolging, uit het gedecodeerde deel II van de berichtsleutel controle tekens berekend, op dezelfde wijze als in het zendstation. Deze in het ontvangstation gegenereerde controle tekens worden vergeleken met de gedecodeerde controle tekens. Wanneer hierbij het aantal overeenstemmingen kleiner is dan een ingestelde drempelwaarde dan valt de test negatief uit en is bij de decodering blijkbaar uitgegaan van de verkeerde dagsleutel. De decodering wordt dan nogmaals uitgevoerd maar met een andere dagsleutel. Dit wordt eventueel herhaald, telkens met een andere dagsleutel, totdat de in het ontvangstation gegenereerde controle tekens (in hoofdzaak) overeenstemmen met de gedecodeerde controle tekens. Op

deze wijze wordt met de overdracht van controle tekens hetzelfde effect bereikt als met de overdracht van de herhalingen van deel II van de berichtsleutel.

Het berekenen van de controle tekens kan plaats vinden op een wijze zoals bekend is voor foutendetecterende of foutencorrigerende codes. Hierbij wordt opgemerkt, dat een eenvoudige herhaling van een berichtteken reeds een controle teken vormt in de zin dat daarmede een fout in het bericht teken kan worden gedetecteerd. Door het begrip controle teken wordt zowel het geval van een tekenherhaling als van een uit de bericht tekens op meer ingewikkelde wijze berekend controle teken omvat.

CONCLUSIE

1. Werkwijze voor het coderen en decoderen van berichten, volgens welke in een zendstation klare bericht impulsen en code impulsen worden gemengd, voor het vormen van een gecodeerd bericht en waarin in een ontvangstation de gecodeerde bericht impulsen en identieke code impulsen worden gemengd voor het verkrijgen van de klare bericht impulsen, waarbij de code impulsen in het zendstation en het ontvangstation worden opgewekt door een code generator waarvan de aanvangstoestand de code impuls opeenvolging bepaalt, waarbij het aantal mogelijke aanvangstoestanden zeer groot is en in het zendstation en in het ontvangstation de aanvangstoestand wordt bepaald door een in het zendstation en het ontvangstation opgeslagen eerste toestandsinformatie, aangeduid als basissleutel en door een tweede toestandsinformatie, aangeduid als berichtsleutel, welke in één van de stations willekeurig wordt gekozen en naar het andere station wordt overgedragen, met het kenmerk, dat voor het geval een aantal mogelijke basissleutels zijn opgeslagen, in het zendstation en in het ontvangstation, voorafgaande aan de verwerking van de bericht impulsen, een eerste deel van een berichtsleutel wordt gecombineerd met een gekozen basissleutel voor het bepalen van een aanvangstoestand van de codegenerator en in het zendstation de klare bericht sleutel impulsen representerende een opeenvolging van een tweede deel van de berichtsleutel en van een aantal daaruit afgeleide controle tekens worden gemengd met de code impulsen voor het verkrijgen van een gecodeerde berichtsleutel en in het ontvangstation de gecodeerde berichtsleutel impulsen worden gemengd met de code impulsen en deze laatste stap steeds wordt herhaald uitgaande van telkens een andere basissleutel totdat als resultaat van de menging een opeenvolging van een gedecodeerd tweede deel van de berichtsleutel en van een aantal gedecodeerde controle tekens, welke overeenstemmen met de in het ontvangstation uit het gedecodeerde tweede deel van de berichtsleutel afgeleide controle tekens, wordt verkregen, waardoor de juiste aanvangstoestand van de code generator in het ontvangstation, welke vereist wordt voor het op de juiste wijze decoderen van de gecodeerde bericht impulsen, kan worden bepaald door de laatst gekozen basissleutel en de combinatie van het eerste en het tweede deel van de berichtsleutel.



8000675

PHN 9680