

STUDIEBLAD

TECHNISCH BLAD VOOR
PTT PERSONEEL

In dit nummer:

Beveiliging van informatie

Technisch Engels

Digitale audio

Van volgordediagram tot functiediagram (2)

Verbindingswegen

Speurtocht langs Nederlandse musea

Nr. 7, 38e jaargang

juli 1983

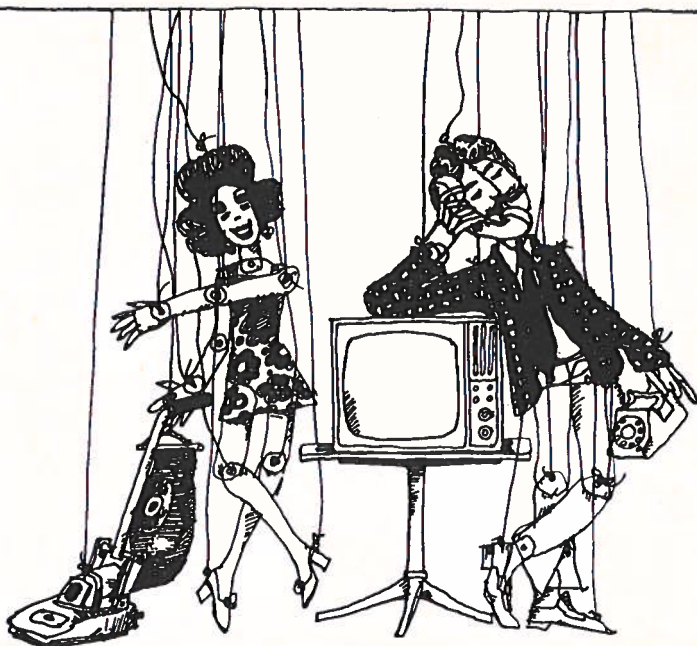


Een staaf zuiver silicium voor de produktie van halfgeleiders. Hiervan worden schijven met een dikte van 1 mm gezaagd. Het soortelijk gewicht van het zilverachtig glanzende materiaal is 2,4.

(Siemens Persfoto)

STUDIEBLAD technisch blad voor PTT personeel

uitgave AbvaKabo en CFO.
redactie Hoofdred. ing. B. Kieboom. Red. ing. P. A. de Boer, P. J. Boomgaard.
redactiesecr. J. P. v. d. Broek. Redactiesecretariaat H. A. Dekkinga, Distelweide 29, 2272 VP Voorburg,
telefoon 070 - 75 64 20 na 18.00 uur 070 - 27 63 61.
administratie AbvaKabo, Bredewater 16, 2715 CA Zoetermeer, giro 4073, telefoon 079 - 51 12 11,
voor verzending, administratie e.d.
abbonement f 18,- per jaar. Voor niet-PTT-ers f 30,- per jaar. Verschijnt maandelijks.
advertenties Uitgeverij en Drukkerij Smits B.V., Westeinde 135, 2512 GW Den Haag,
telefoon 070 - 89 53 90.



Bewegingloos - zonder kabels.

NKF maakt kabels.

Voor energie-overdracht en voor telecommunicatie.

Al meer dan 60 jaar. Lang genoeg voor veel ervaring. Genoeg ook om te weten
wat cliënten wensen. Van eenvoudige lokale kabels tot Bamboe-kabels
voor CATV-systemen toe.

NKF KABEL 

Beveiliging van informatie

Ir. M. R. Oberman

Een nieuwe artikelenreeks

De redactie van het Studieblad heeft aan enkele medewerkers van het Dr. Neher Laboratorium gevraagd of zij voor ons tijdschrift een artikel wilden schrijven. Aan dit verzoek is gehoor gegeven, zodat de lezers in deze jaargang een aantal bijdragen kunnen verwachten, geschreven door onderzoekers uit het PTT-bedrijf „where the future is made”. Op deze manier kunnen zij iets meer te weten komen over het werk en de projecten waarmee de laboratoriummedewerkers zich bezighouden.

Natuurlijk heeft de redactie de auteurs uitdrukkelijk verzocht het niveau van de artikelen niet te ver te laten uitstijgen boven hetgeen de gemiddelde lezer gewend is. Het moet worden gezegd, dat de auteurs zich bijzonder goed van hun taak hebben gekwetten.

Het eerste artikel, dat in dit nummer verschijnt, is van de heer M. R. Oberman en handelt over het beveiligen van informatie. De auteur heeft aan zijn artikel een tweetal opgaven toegevoegd, zodat iedereen kan beproeven of hij het gelezene heeft begrepen.

Voor hen die niet zo vertrouwd zijn met het PTT-laboratorium volgt hier in enkele zinnen een korte introductie.

Het Dr. Neher Laboratorium is gevestigd in Leidschendam en ressorteert onder de hoofddirectie Technische Zaken. In dit bedrijf werken ongeveer 600 mensen, waarvan meer dan de helft speur- en ontwikkelingswerk verricht. Deze onderzoekers zijn verdeeld over vijf sectoren met elk zijn eigen specialisme. De vijf sectoren zijn: werktuigbouwkunde, informatica, natuurwetenschappelijk onderzoek, schakeltechniek en transmissie. De overige personeelsleden werken op ondersteunende afdelingen, zoals de personeelsdienst, de boekhouding, het secretariaat, enz.

Het meeste werk verrichten de onderzoekers voor de operationele dienst Telecommunicatie. Op dit moment wordt er bijvoorbeeld intensief geëxperimenteerd met de glasvezel. Onlangs werd in Geldrop een proefopstelling geopend, waar de mogelijkheden van dit nieuwe transmissiemiddel grondig zullen worden getest.

Ook voor de andere diensten van PTT verrichten de ingenieurs onderzoek en ontwikkelen zij nieuwe systemen. Zo werd voor de post de automatische sorteermachine ontwikkeld en is men thans voor de giro bezig met het vervaardigen van een apparaat dat handgeschreven betalingsopdrachten kan lezen. Het jongste project, waar hard aan wordt gewerkt, is sprekersverificatie.

Aan dit laatste onderwerp zal ook in ons tijdschrift aandacht worden geschonken. Door de bijdragen uit het laboratorium blijven onze abonnees op de hoogte van de technische ontwikkelingen, die van vitaal belang zijn voor ons bedrijf.

de Redactie

Inleiding

Beveiliging van schriftelijke informatie werd voor zover bekend al in de oudheid toegepast door bijvoorbeeld de Egyptenaren en later de Grieken en Romeinen.

Was het in de tijd van de farao's nog de onbekendheid van de gebruikte hiërogliefen voor de niet ingewijdene, in de Romeinse tijd werd al voor een meer mathematische aanpak gekozen.

Hoewel een zeer beperkt deel van de bevolking kon lezen en schrijven, was er toch behoefte aan een betere mogelijkheid tot beveiliging van informatie.

Uit de geschetste situatie is een parallel door te trekken naar een meer recent verleden.

In de begintijd van de computer waren er maar weinig mensen die een computer konden programmeren. De behoefte aan beveiliging van informatie was in die tijd beperkt, immers alleen een kleine groep kon met deze machines omgaan.

Naarmate er meer computers kwamen, waren er meer mensen die deze machines konden bedienen. De noodzaak tot beveiliging van informatie groeide dan ook; zeker wanneer men bedenkt dat over het algemeen meer gebruikers één computer gingen delen. Andere factoren die invloed hebben op de noodzaak tot beveiliging van informatie in computer-communicatienetwerken worden gevonden in het gebruik van mini- en microcomputers in gespreide (decentrale) opstellingen.

Naast het toenemend gebruik van computersystemen is ook de communicatie tussen computersystemen op verschillende plaatsen sterk vergroot. De toename in telecommunicatie faciliteiten maakt een beïnvloeding van berichten eenvoudiger. Gezien de toename van telecommunicatie-faciliteiten ligt het voor de hand dat men ook belangrijkere berichten via deze transportmedia gaat verzenden.

Afhankelijk van de mate van belangrijkheid van een bericht kan al dan niet worden overwogen het tegen bepaalde mogelijkheden te beschermen. Een groep berichten die in computer-communicatiesystemen kunnen worden verzonden en een bepaald „gewicht" hebben, zijn bijvoorbeeld financiële berichten of transacties.

Wanneer in een financieel bericht, dat met behulp van een computer-commu-

nicatiesysteem kan worden verzonden, mogelijkheden zijn tot bewust veranderen van informatie van bijvoorbeeld afzender, geadresseerde of overgemaakt bedrag, dan zijn er potentiële fraudemogelijkheden aanwezig. Een effectief middel om deze en soortgelijke belangrijke berichten te beveiligen, is door middel van versluiering van de berichtinhoud.

Deze techniek wordt ook wel cryptografie genoemd.

In een beknopt overzicht zullen enkele mogelijkheden en beperkingen die deze techniek biedt, worden toegelicht.

Toepassingsmogelijkheden in computer-communicatie-omgeving

Cryptografie is een techniek die de mogelijkheid biedt informatie tijdens transport of gedurende opslag te beschermen tegen doelgerichte wijziging, kopiëren of meelesen van informatie.

Deze techniek biedt dan ook bij juiste toepassing mogelijkheden om begrippen zoals privacy van informatie (= ongeautoriseerde inspectie van informatie) en integriteit van informatie (= ongeautoriseerde modificatie van informatie) kracht bij te zetten.

In een computer-communicatiesysteem is een aantal aspecten te onderscheiden:

- Toe-/uitgangscntrole
- Informatieverwerking
- Informatie-uitwisseling
- Transport

Elk aspect kan toepassingsmogelijkheden op cryptografisch gebied hebben. Een beperkt aantal toepassingen wordt in dit artikel behandeld.

Toe-/uitgangscntrole

Een correcte toegangscontrole tot een computer-communicatiesysteem is van belang voor zowel de rechtmatige gebruiker als de systeembeheerder. Wanneer een systeem faciliteiten verleent, die identiteitafhankelijk zijn, wordt de noodzaak van een *beveiligd* toegangsverleningssysteem alleen maar groter. De toegangsverlening is in vele gevallen als volgt: vele systemen maken gebruik van wachtwoorden die door de gebruiker aan het systeem worden afgegeven. Het systeem onderzoekt of het afgegeven wachtwoord overeenkomt met de opgeslagen referentie. Wanneer dit overeenstemt wordt toegang verleend, zo niet, dan kan een nieuwe poging worden toegestaan. Gezien het feit dat in het systeem, zoals genoemd een referentie is opgeslagen, kan het mogelijk zijn deze referenties uit het systeem te lichten. Dit is in principe ongewenst, omdat daarmee de toegangsverlening kan worden beïnvloed.

Dit probleem kan worden opgelost door de referenties versluierd in het

systeem op te slaan.

Ontcijfering van de referentie is in principe niet nodig, omdat de vergelijking van het afgegeven wachtwoord en de opgeslagen referentie moeten overeenstemmen. Dit kan ook als ze beide zijn versluierd (zie fig. 1.). Het resultaat van de versluiering van het afgegeven wachtwoord moet overeenstemmen met de opgeslagen, versluierde referentie.

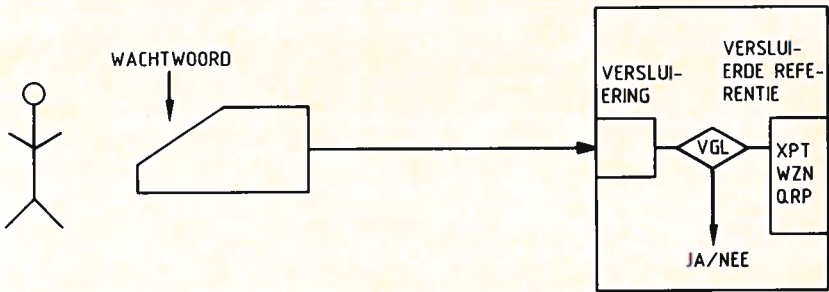


fig. 1.

Wanneer nu de versluierde wachtwoorden uit het systeem worden gelicht, dan zijn deze voor derden niet bruikbaar. De referentie die in het systeem wordt bewaard, is versluierd, en dus is de oorspronkelijke tekst er niet uit terug te vinden.

Informatieverwerking

Toepassing van vercijferingsmethoden op informatie die moet worden bewerkt, is niet mogelijk. Wanneer in een vercijferde tekst één of meer karakters worden bewerkt, is ontcijfering tot de oorspronkelijke klare tekst niet meer mogelijk.

Wel is het mogelijk (en kan het afhankelijk van het gewenste beschermingsniveau zinvol zijn) de informatie die ligt opgeslagen door middel van vercijfering te beveiligen. De informatie is dan niet meer leesbaar voor diegenen die de sleutel niet hebben. Gedacht kan worden aan informatie op computerschijven.

Informatie-uitwisseling

Beveiliging van informatie tijdens de uitwisseling met andere systemen ondervindt de laatste jaren een sterk toenemende belangstelling en behoefte. Discussie over privacy van informatie en integriteit van informatie dragen daar sterk toe bij.

Het is mogelijk de privacy van informatie te beschermen door een bericht te vercijferen (fig. 2a.). Het is mogelijk de integriteit van een bericht te beschermen door de berichtinhoud te waarmerken (= van een echtheidsgarantie

voorzien) door het toevoegen van een code aan het bericht. Naar aanleiding van deze berichtwaarmmerking is te controleren of de ontvangen berichtinhoud nog overeenstemt met de oorspronkelijke berichtinhoud.

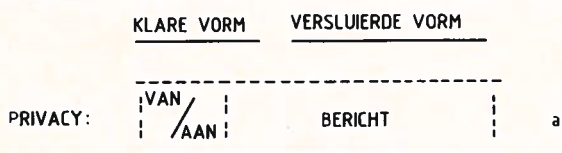


fig. 2a.

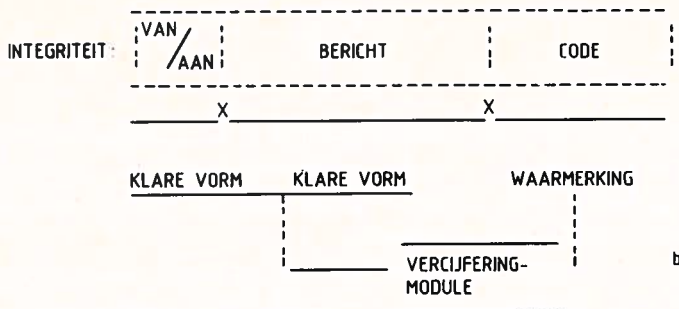


fig. 2b. (geheime sleutel).

Naast de waarmmerking van berichten zijn er ontwikkelingen die het misschien mogelijk kunnen maken handtekeningen in elektronische vorm aan berichten of transacties te „plakken”. Cryptografie zal bij deze ontwikkelingen een belangrijke rol gaan spelen, omdat vercijfering van informatie de mogelijkheid biedt een uniek kenmerk achter te laten. Naar aanleiding van dit kenmerk is de oorspronkelijke gebruiker vast te stellen.

Transport

Het transport van berichten in een systeem kan worden beveiligd, indien een gebruiker dat wenst.

Versluiting van berichten kan bescherming bieden tegen mogelijke ongewenste beïnvloeding van berichten onderweg, maar ook wanneer een bericht (per ongeluk) verkeerd wordt afgeleverd. Degene die het dan ontvangt zal niet in staat zijn het (niet voor hem bestemde) bericht te ontcijferen, omdat hij niet de bijbehorende ontcijfersleutel bezit.

Versluiting van informatie in een bericht biedt geen bescherming tegen vernietiging of verloren gaan van het bericht.

Cryptografie, terminologie

Cryptografie is het versluieren van informatie met behulp van een algoritme. Dit algoritme kan dan onder besturing van een sleutel een cryptogram produceren, zodat de geboden klare tekst kan worden omgezet in een cryptogram (fig. 3.).

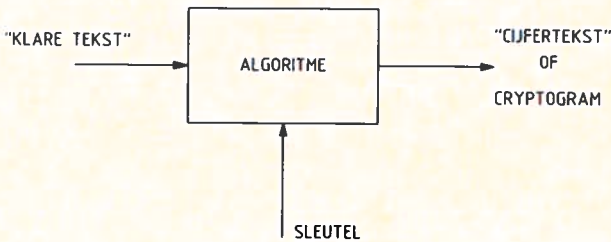


fig. 3.

De werkwijze om een boodschap geheim te maken, is gebaseerd op de vertaling van de klare tekst via een algoritme, onder besturing van een sleutel in de cijfertekst. Een algoritme is een rekenschema, dat aangeeft hoe een bepaalde berekening moet worden uitgevoerd.

Een andere, verschillende, sleutel voor hetzelfde algoritme geeft een andere, verschillende, uitkomst voor dezelfde oorspronkelijke klare tekst.

De werkwijze om een klare tekst in een cijfertekst of cryptogram te transformeren, wordt versleutelen of vercijferen genoemd. De omgekeerde bewerking, van cijfertekst naar klare tekst, wordt ontsleutelen of ontcijferen genoemd.

Er zijn algoritmen waarvoor geldt dat voor vercijferen een andere sleutel nodig is dan voor ontcijferen. Dit worden wel asymmetrische systemen genoemd. Bij deze groep systemen bestaat er een relatie tussen de vercijfer- en ontcijfer-sleutel, die voor „anderen” niet uit één van de twee sleutels is af te leiden. Hierop wordt later teruggekomen.

Het algoritme en de sleutel in een cryptografisch systeem is te vergelijken met het slot en de sleutel van een kluisdeur. Met de sleutel kan de kluis worden gesloten (het bericht is vercijferd), met de sleutel kan ook de kluis weer worden geopend (het bericht is ontcijferd). Zonder bezit of „kennis” van de sleutel is één en ander niet mogelijk.

Het effect van de toepassing van cryptografie is, dat een bericht voor diegene die de sleutel niet bezit, onleesbaar is geworden.

Het spreekt voor zich dat als een sleutel zoek of verminkt raakt het vercijferde bericht ook niet meer te reconstrueren is voor de oorspronkelijke sleutelbezitter.

Het zal dan ook duidelijk zijn, dat een doeltreffend beheer van sleutels die in cryptografische systemen worden gebruikt, noodzakelijk is.

Het is gebleken dat niet elk bekend cryptografisch algoritme even sterk is. Hiermee wordt bedoeld dat er mogelijkheden zijn om zonder kennis van de sleutel een gegeven cryptogram op te lossen.

Om hier iets dieper op in te gaan zal iets over het begrip „breekbaarheid” moet worden gezegd. Wanneer op de breekbaarheid van een cryptografisch systeem wordt gelet, is de volgende verdeling mogelijk: – theoretisch onbreekbaar of – theoretisch breekbaar.

Een systeem is onbreekbaar als er gebruik wordt gemaakt van een sleutel die tenminste even lang is als het te verzenden bericht, volledig willekeurig is samengesteld en slechts eenmaal wordt gebruikt. Dit wil zeggen dat alle andere systemen die een kortere sleutel gebruiken breekbaar zouden zijn.

Systemen waarvan is gesteld dat ze theoretisch gesproken breekbaar zijn, kunnen worden onderverdeeld in: praktisch onbreekbaar en praktisch breekbaar.

Systemen die praktisch onbreekbaar zijn, hebben de eigenschap dat de tijd om deze systemen op te lossen langer is dan de geldigheidsduur van het gecijferde bericht. Deze categorie systemen is technisch gezien interessant. Helaas is het echter zeer moeilijk een ondergrens te geven in de oplossingsduur. Een bovengrens in de oplossingsduur is meestal wel mogelijk. Bijvoorbeeld de tijd die nodig is om alle mogelijke sleutels van een algoritme uit te proberen.

Methoden

De methoden die door de eeuwen heen zijn gebruikt, zijn gebaseerd op logische en/of rekenkundige bewerkingen.

Een voorbeeld van een methode die in de tijd van de Romeinen gebruikelijk was, is gegeven in fig. 4. Deze methode is vernoemd naar de bekende romeinse keizer Julius Caesar.

Klare tekst :	D E	G E H E I M E	T E K S T
Sleutel :	J J	J J J J J J J	J J J J J
<hr/>			
Cryptogram:	M N	P N Q N R V N	C N T B C

fig 4.

De substitutie heeft plaats door, na nummering van de letters van het alfabet (A=0, B=1, C=2, . . . Z=25) tekst en sleutel modulo 26 op te tellen. Modulo (mod) is een rekenkundige bewerking met twee getallen, waarvan het resultaat gelijk is aan de rest die ontstaat bij de deling van het eerste getal door het tweede getal.

Rekenen met „modulo” gaat als volgt: $X \text{ modulo } Y = \text{rest}$, bij deling van X door Y . X , Y , rest zijn gehele getallen, groter of gelijk aan 0.

Bijvoorbeeld $5 \text{ mod(ulo) } 4 = 1$, $12 \text{ mod } 14 = 12$ etc. Als X kleiner is dan 0, dan wordt het geheel aantal malen Y bij X opgeteld. Voor fig. 4. kan aldus worden gevonden:

$$\begin{aligned} (D+J) \text{ mod } 26 &= 3+9=12=M \\ (E+J) \text{ mod } 26 &= 4+9=13=N \\ (G+J) \text{ mod } 26 &= 6+9=15=P \\ (H+J) \text{ mod } 26 &= 7+9=16=Q \\ (T+J) \text{ mod } 26 &= 19+9=28 \text{ mod } 26=2=C \end{aligned}$$

Ontcijfering volgens:

$$\begin{aligned} (M-J) \text{ mod } 26 &= 12-9=3=D \\ (N-J) \text{ mod } 26 &= 13-9=4=E \\ (P-J) \text{ mod } 26 &= 15-9=6=G \\ (Q-J) \text{ mod } 26 &= 16-9=7=H \\ (C-J) \text{ mod } 26 &= 2-9=-7 \text{ mod } 26=19=T \end{aligned}$$

Wanneer een cryptogram wordt opgelost zonder dat de sleutel en/of het vercijferingsalgoritme bekend is, dan is het cryptogram gebroken.

Het bovenstaande cryptogram is op statistische gronden eenvoudig te breken, zeker wanneer de tekst wat langer is. Het opstellen van de frequentiestatistiek van het voorkomen van de letters in het cryptogram, vergeleken met de bekende frequentiestatistiek van voorkomen van letters in de Nederlandse taal geeft al snel de oplossing. De letter E komt in het Nederlands het meeste voor (gevolgd door T, O, A, N). Dit betekent dat in de cijfertekst de letter die het meeste voorkomt, waarschijnlijk in de klare tekst een E moet zijn.

Een andere methode is het uitproberen van de mogelijke sleutels. Er is over het algemeen maar één methode die de goede oplossing geeft en dus een leesbare tekst geeft. Een probleem om zelf op te lossen is aan het slot van dit artikel toegevoegd.

Het systeem van fig. 4. heeft op een aantal punten ongewenste beperkingen, bijvoorbeeld op het aantal sleutel mogelijkheden. In principe zijn er 26 mogelijke sleutels. Dit soort systemen wordt mono (één) alfabet systemen genoemd. Het ligt voor de hand dat er ook poly (meer) alfabet systemen zijn. Een voorbeeld is in fig. 5. gegeven.

Klare tekst :	D E	G E H E I M E	T E K S T	
Sleutel tekst :	M R	M R M R M R M	R M R M R	
				+ mod 26
Cijfer tekst :	P V	S V T V U D Q	K Q B E K	

fig. 5.

Soortgelijke methoden als genoemd voor de „Ceasar” maken het ook mogelijk dit soort cryptogrammen op te lossen zonder kennis van de sleutel. Dit soort methoden zijn met behulp van een computer snel oplosbaar.

Inmiddels zijn er de laatste jaren meer complexe vercijferingsmethoden door publicatie bekend geworden.

Hiervan dient o.a. te worden genoemd de „Data Encryption Standard” (DES) en het „Openbaar sleutel algoritme volgens het RSA” (Rivest, Shamir, Adleman) algoritme.

Het DES algoritme is op verzoek van de Amerikaanse overheid ontwikkeld en is beschikbaar in een geïntegreerd circuit.

De bewerkingen die in het algoritme worden uitgevoerd bestaan uit:

- transpositie;
- substitutie;
- logische bewerkingen.

Het algoritme vercijfert 64 bit data (klare tekst) in 64 bit cijfertekst met behulp van een sleutel van 56 bit. Verrijfering is mogelijk met een snelheid van 600 bit/sec, afhankelijk van de toegepaste chip.

Dit algoritme gebruikt voor verrijferen dezelfde sleutel als voor ontcijferen. Het algoritme wordt alleen in omgekeerde volgorde doorlopen.

Het „RSA algoritme” gebruikt verschillende sleutels voor ontcijferen en verrijferen. Deze sleutels hebben een onderlinge relatie. Echter uit de ene sleutel is de andere niet af te leiden. De verrijfer- en ontcijfersleutel worden sleutelparen genoemd.

Het „RSA algoritme” is gebaseerd op het feit dat het eenvoudiger is twee priemgetallen te kiezen en deze met elkaar te vermenigvuldigen, dan dat het mogelijk is dit produkt in factoren te ontbinden.

Bijvoorbeeld 518940557 is te ontbinden in factoren: 15107 en 34351, maar sneller is het produkt van deze twee getallen te berekenen.

Het effect van een verrijfersleutel en een ontcijfersleutel is, dat de verrijfersleutel hierdoor bekend kan worden gemaakt zonder dat de ontcijfersleutel hierdoor bekend raakt. De gedachte hierbij is dat iedereen berichten mag ontcijferen. Het ontcijferen mag echter alleen door diegene gebeuren voor wie het bericht bestemd is. Dit kan gebeuren door het geheimhouden van de ontcijfersleutel!

De procedure die bij het sleutelsysteem volgens het „RSA algoritme” hoort, is als volgt:

Kies 2 priemgetallen p en q
bereken $F=(p-1)(q-1)$
bereken $n=p.q$

b.v. $p=5$ $q=11$
 $F=(5-1)(11-1)=40$
 $n=5.11=55$

Kies de vercijfersleutel: VC b.v. VC=23
de ontcijfersleutel: OC OC=7

te berekenen uit $VC \cdot OC \bmod F = 1$ $23 \cdot 7 \bmod 40 = 161 \bmod 40 = 1$

Stel bericht 2 (klare tekst), de vercijfertekst is dan 2 tot de macht VC mod n (2 tot de macht 23) mod 55=8. De ontcijfering heeft plaats volgens: (cijfer tekst) tot de macht OC mod n =(8 tot de macht 7) mod 55 =2.

De procedure lijkt betrekkelijk eenvoudig. De vercijferingsmethode wordt in de praktijk uitgevoerd met priemgetallen die ongeveer 100 of meer cijfers lang zijn. De reden hiervoor is, dat de kans dat een gebruikt priemgetal (de vercijfer- of ontcijfersleutel) goed wordt gekocht, verschrikkelijk klein is. De gok is dan ongeveer zo groot als van het reeds genoemde „DES algoritme”.

Probleem

Naar aanleiding van dit artikel zijn twee problemen bijgevoegd, die de lezer na lezing van de tekst zou moeten kunnen oplossen.

Probleem 1

Vindt de klare tekst van onderstaande Ceasar.

FQW E F Q Z P U Q Z U Q F H Q D E X G U Q D P L U V Z
L U V Z Z U Q F M X F U V P P G U P Q X U V W

Probleem 2

Wat is de klare tekst als gegeven is dat de ontcijfersleutel (OC) = 3 en n=55?
Het systeem werkt volgens de beschreven „RSA methode”. Er geldt A=1, B=2, . . ., Z=26. Er dient per karakter te worden ontcijferd.
De cijfertekst is:

R E Y K Y R E I

De redactie van het **STUDIEBLAD** verloot onder de inzenders van de goede oplossingen een boekenbon ter waarde van f 25,— per probleem.

Oplossingen van deze twee problemen kunnen op een briefkaart naar de redactie van het **STUDIEBLAD** worden verzonden.

Adresseren aan: Redactiesecretariaat Studieblad-PTT, CATF-VD 307, Postbus 420, 2260 AK Leidschendam.

Inzendingen worden binnen drie weken na verschijnen ingewacht.

Technisch Engels

bewerkt door mej. C. V. Poolman en W. S. v. Dam

Submerged repeater reliability

Submerged repeater **reliability** must **approach** the **ultimate obtainable**. The **cost of recovering** and replacing a faulty **repeater** in deep water, and the **loss of revenue** during the operation, can be enormous, particularly if bad weather prevents the repair ship **effecting the repair** immediately. Consequently, in the design and choice of repeater components, **well-proven techniques** are preferred to **the latest devices**. Only components the reliability and stability of which can be **predicted with near certainty** for periods **well in excess of 20 years** are used.

Transistors (**in spite of their advantages over valves**) were **not** introduced into main amplifiers of submerged repeaters **until** several years after they had come into general commercial use, and only when **exhaustive life tests** on the particular transistors to be used had indicated their greater reliability than that of valves.

Repeater manufacture is carried out in a dust-free area where temperature and **humidity** are controlled and where operators wear special clothing. **Rigorous** inspection routines are **enforced** right from the **raw material** stage of each component or piece part.

Cable Power Feeding Arrangements

Power is fed to the submerged repeaters over the centre conductor of the cable from a constant **d.c.** source at one terminal (simple-end feeding) or from both terminals (double-end feeding). The power return path is via the sea.

In the double-end feeding case, the power units at the two terminals are in series and, **assuming** that they are set up to supply at **similar** voltages, the mid-point of the cable will be at the same potential as the sea. **Typical values** of feeding current and voltage drop per repeater for valve repeaters are 415 mA and 83 volts respectively. Typical values for a transistorised repeater are 200 mA and 25 volts.

Overgenomen uit: "Telecommunications Pocket Book"

Samengesteld door T. L. Squires uitg. Newnes-Butterworths, Londen

EXPLANATORY NOTES

reliability	betrouwbaarheid
to approach	naderen, benaderen
ultimate	laatste, uiterste
the ultimate obtainable	het maximaal haalbare
recovering a repeater	het naar boven halen, „opvissen”, van een versterker
loss of revenue	het operationele verlies, het derven van opbrengst
effecting the repair	het uitvoeren van de reparatie
well-proven techniques	beproefde technieken
the latest devices	de nieuwste apparaten
predict with near certainty	voorspellen met een aan zekerheid grenzende waarschijnlijkheid
well in excess of	ruimschoots langer dan
in spite of	ondanks
advantages over	voordelen ten opzichte van
valves	buizen
not . . . until	pas
exhaustive life tests	„uitputtende” (grondige) levensduurproeven
repeater manufacture	het vervaardigen van versterkers
humidity	vochtigheid
rigorous	streng
to enforce	verplicht stellen
raw material	grondstof
power feeding arrangements	voorzieningen voor wat betreft de voeding
d.c. (direct current)	gelijkstroom
assuming	aannemende dat, er van uitgaande dat
similar	gelijksoortig
typical values	typerende, representatieve waarden

Digitale audio

Begin maart hebben Philips en Sony de compact disc op de Nederlandse markt geïntroduceerd. Hiermee is een eerste stap gezet in de richting van een digitaal audio systeem voor de huiskamer. Het is duidelijk dat hiermee de digitale opmars in de audio-wereld is begonnen.

Behalve digitale platenspelers, digitale recorders en effect apparatuur zullen ook de andere schakels in het opname proces worden gedigitaliseerd.

Dit alles met als doel een „enorme” kwaliteitswinst voor de consument.

In dit artikel wordt het principe en de globale werking van digitale audio beschreven. De tekst is ontleend aan de cursus „Digitale audio” van Elektronica opleidingen Dirksen.*

Evenals in de telecommunicatietechniek speelt bij digitale audio puls-code-modulatie (PCM) een grote rol. Het verschil met de telefoniesignalen (300-3400 Hz) is echter de hoge kwaliteit welke van het audio-signaal wordt geëist. Genoemd worden: een signaal-ruis verhouding van meer dan 90 dB, een niet-waarneembare wow en flutter, een vervorming van minder dan 0,05% en een uiterst rechte frequentie karakteristiek van 0 tot 20 kHz. Een geluidskwaliteit, die ook bij herhaald kopiëren behouden blijft.



Compact Disc speler CDP-101.

* Dit artikel wordt gepubliceerd met toestemming van Elektronica opleidingen Dirksen te Arnhem.

Basisprincipe digitale audio

Geluid bestaat uit trillingen, die zich voortplanten door een medium. Geluid dat via een medium ons oor bereikt, kunnen we „horen”.

Vaak willen we geluidssignalen bewerken, registreren of transporteren. Daartoe is het nodig het geluidssignaal om te zetten in een elektrisch signaal.

Om geluid om te zetten in een elektrisch signaal gebruiken we een opnemer (b.v. een microfoon).

Om een elektrisch signaal weer om te zetten in een hoorbaar geluidssignaal gebruiken we een weergever (b.v. een luidspreker). Tussen de opnemer en weergever zit het signaalverwerkend deel, waarmee het in een elektrisch signaal omgezette geluidssignaal wordt bewerkt, geregistreerd en/of getransporteerd.

Het opnemen, verwerken en weergeven van geluidssignalen noemen we een audiosysteem. Fig. 1 geeft een eenvoudige voorstelling weer van een audiosysteem.



fig. 1.

In de analoge techniek zet de opnemer een geluidssignaal om in een analogo elektrisch signaal. De weergever zet een analogo elektrisch signaal om in een geluidssignaal.

Een analogo signaalverwerkend deel heeft als voordeel, dat de verwerking eenvoudig en goedkoop kan gebeuren.

De amplitude en de frequentie van het elektrisch signaal blijven evenredig met de sterkte en de frequentie van het geluidssignaal.

De kwaliteit van het uiteindelijke, na verwerking weer te geven geluidssignaal ligt echter beduidend lager dan dat van het signaal vóór verwerking.

Bij toepassing van een digitaal signaalverwerkend deel wordt het analoge signaal van de opnemer zo vlug mogelijk omgezet in digitale grootheden (binaire getallen). Dit gebeurt met behulp van een analogo/digitaal-omzetter (A/D-omzetter).

De frequentie en de sterkte van het oorspronkelijke analoge geluidssignaal is nu slechts moeilijk of helemaal niet in de binaire getallen te herkennen.

Een digitaal signaal kan echter een hoge en constante kwaliteit hebben, zodat in het signaalverwerkend deel praktisch geen afbreuk wordt gedaan aan de kwaliteit van het oorspronkelijke signaal.

Om vervolgens een verwerkt digitaal signaal te kunnen weergeven, moet er

weer een omzetting plaatsvinden van digitaal naar analoog. Dit gebeurt met een digitaal/analoog-omzetter (D/A-omzetter).

Een digitaal audiosysteem heeft dus een digitaal signaalverwerkend deel, waarbij een A/D-omzetter nodig is voor omzetting van analoog naar digitaal, en een D/A-omzetter nodig is voor omzetting van digitaal naar analoog.

Een eenvoudige voorstelling van een digitaal audiosysteem is in fig. 2 weer-gegeven.

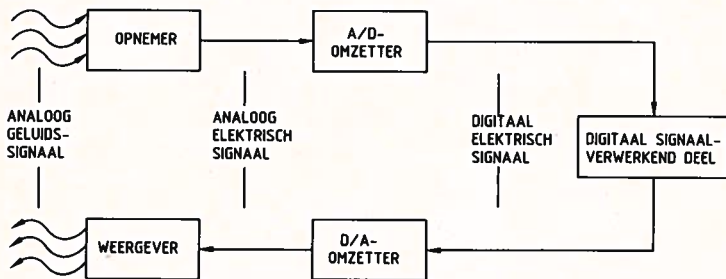


fig. 2.

Omdat in deze keten vooral de omzetting van analoog naar digitaal belangrijk is, zullen wij eerst het principe van A/D- en D/A-omzetting nader bekijken aan de hand van het blokschema van fig. 3.

Analoog/digitaal-omzetting

In fig. 3 zijn de bewerkingen weergegeven, die een analoog signaal achtereenvolgens ondergaat bij de omzetting in binaire getallen.

Fig. 3a geeft een analoog audiosignaal weer, dat moet worden omgezet. Eerst wordt het analoge audiosignaal door een laagdoorlaatfilter gestuurd. Het laagdoorlaatfilter heeft een grensfrequentie van 20 kHz. Frequenties die hoger zijn dan de grensfrequentie van 20 kHz worden door het laagdoorlaatfilter tegengehouden. Dit heeft geen hoorbare invloed op de geluidskwaliteit, want het menselijk oor kan frequenties boven de 20 kHz niet horen. Het nut van dit laagdoorlaatfilter zal in één van de volgende artikelen worden besproken.

Het gefilterde signaal (fig. 3b) wordt toegevoerd aan een z.g. sample/hold-schakeling. Deze schakeling bepaalt op vaste tijdstippen de waarde van het analoge audiosignaal. Dit noemen we *bemonsteren* (to sample). De waarde van een monster wordt vastgehouden (to hold = vasthouden) tot het volgende tijdstip, waarop een nieuw monster wordt genomen.

Door het bemonsteren ontstaat een „trapjeskromme” (fig. 3c).

De hoogte van een „trede” van deze trapjeskromme is nog steeds analoog.

Een analoog signaal kan tussen een bepaald minimum en een bepaald

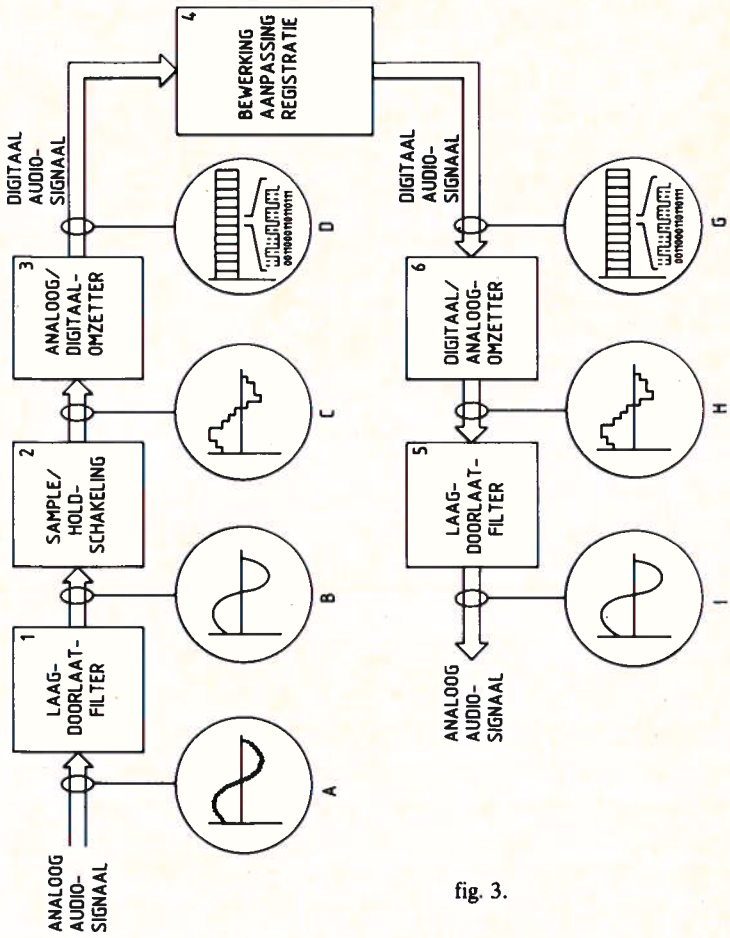
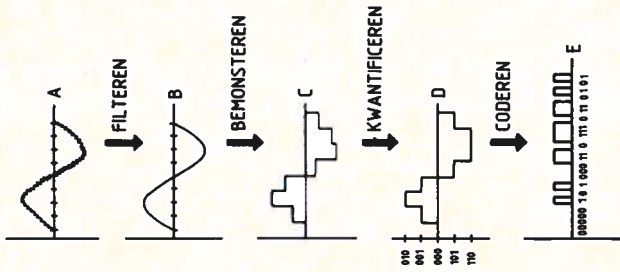


fig. 3.

maximum variëren. Het gebied tussen dit minimum en maximum noemen we het bereik. Dit bereik wordt verdeeld in een aantal gelijke stukken, waardoor er een beperkt aantal niveaus ontstaat.

De hoogte van een trede van het bemonsterde signaal wordt nu afgerond naar het dichtbijzijnde niveau. Dit noemen we *kwantificeren*. Fig. 3c gaat dan over in fig. 3d.

De trapjeskromme in fig. 3d is digitaal, omdat er nu een beperkt aantal niveaus mogelijk is.

De niveaus van de digitale trapjeskromme worden omgezet in binaire getallen m.b.v. een analoog/digitaal-omzetter. Elk niveau van de digitale trapjeskromme komt hierbij overeen met een bepaald-binair getal. Dit omzetten in digitale pulsen noemen we *coderen*.

Het aantal mogelijke niveaus van de digitale trapjeskromme wordt bepaald door het aantal combinaties dat we met een binair getal kunnen weergeven.

Zo kunnen we, als we 10 bits gebruiken, $2^{10} = 1024$ bitcombinaties weergeven. Het bereik van het analoge signaal kunnen we dan in 1024 niveaus verdelen.

Om de binaire getallen aan de uitgang van de analoog/digitaal-omzetter verder te kunnen verwerken, is het vaak nodig dat we de verschillende bits van de binaire getallen één voor één (dus in serie) transporteren. Uit de binaire getallen ontstaat dan het bitpatroon van fig. 3e.

Digitaal/analoog-omzetting

Als een audiosignaal na analoog/digitaal-omzetting is verwerkt, moet het digitale audiosignaal weer hoorbaar worden gemaakt.

Het digitale audiosignaal moet dan in een analoge vorm worden gebracht d.m.v. digitaal/analoog-omzetting.

Het serie-bitpatroon van het digitale audiosignaal wordt eerst weer omgezet in binaire getallen. Deze binaire getallen worden toegevoerd aan een digitaal/analoog-omzetter, die de binaire getallen omzet in een digitale trapjeskromme.

Opmerking: De naam digitaal/analoog-omzetter is enigszins verwarrend, omdat de uitgang van de digitaal/analoog-omzetter nog niet echt analoog is. In de trapjeskromme kan n.l. slechts een beperkt aantal niveaus voorkomen.

De treden van de ontstane digitale trapjeskromme worden „bijgeschaafd” m.b.v. een laagdoorlaatfilter. De treden gaan dan geleidelijk in elkaar over, waardoor er een echt analoog signaal ontstaat.

Dit analoge signaal is, op de gemaakte afrondingsfout bij de analoog/digitaal-omzetting na, praktisch gelijk aan het oorspronkelijke audiosignaal.

(Wordt vervolgd.)

Van volgordediagram tot functiediagram (2)

ir. P. D. C. Reefman
(Vervolg van blz. 169)

Een voorbeeld van een toestandsdiagram

Uit het voorgaande is gebleken dat elke toestandslijn van het volgordediagram kan worden beschreven door middel van een formule in Boole-algebra. Met behulp van deze formules kunnen de toestanden in een bepaalde situatie worden berekend. Het zal duidelijk zijn dat een volgordediagram overzichtelijker is, omdat daar alle toestanden in een bepaalde situatie gelijktijdig kunnen worden afgelezen. De formules zijn echter meer geschikt om in een computer te worden ingevoerd, die dan op zijn beurt wel weer een grafisch volgordediagram kan produceren.

Een andere methode bestaat uit het tekenen van een toestandsdiagram, waarin de in de vorm van mnemotechnische code gedefinieerde toestanden en signalen in volgorde zijn afgebeeld (zie fig. 7). Bij elke toestand is de voorwaarde waaraan voldaan moet worden om vanuit de oude toestand in de nieuwe toestand te komen met een pijltje aangeduid. Bij het vergelijken van fig. 3 en de middelste lijn van fig. 7 valt op dat deze lijn als het ware een ééndimensionale weergave is van fig. 2. Steeds is begin en eind van een bepaalde toestand aangegeven.

Het is van belang om op te merken dat er een verschil bestaat tussen dit toestandsdiagram en de klassieke vorm van fig. 1 waarin de toestanden elkaar niet kunnen *overlappen*.

Dit opent de mogelijkheid om, in één figuur, meer dan één cyclus van toestanden aan te geven. Zo vindt men bijvoorbeeld in fig. 7 ook fig. 4 terug in „cyclus 2”.

De „lus 1” geeft aan dat de gebeurtenissen bij een telimpuls zich een aantal malen kunnen herhalen.

Verder is aangegeven wat er gebeurt wanneer, vanuit de toestand „beschikbaar” (AVC = Available Condition), de lijn wordt geblokkeerd met het signaal \overline{MBL} (Not Minus to B-wire Line signal). Dit betekent MAL (Minus to A-wire Line signal) of „geen spanning” ($\overline{MAL} \cdot \overline{MBL}$). Symbolisch kan men schrijven: $\overline{MBL} = MAL + \overline{MAL} \cdot \overline{MBL}$.

Ook is aangegeven wat gebeurt bij het signaal \overline{PUX} (Not Power and Unit present).

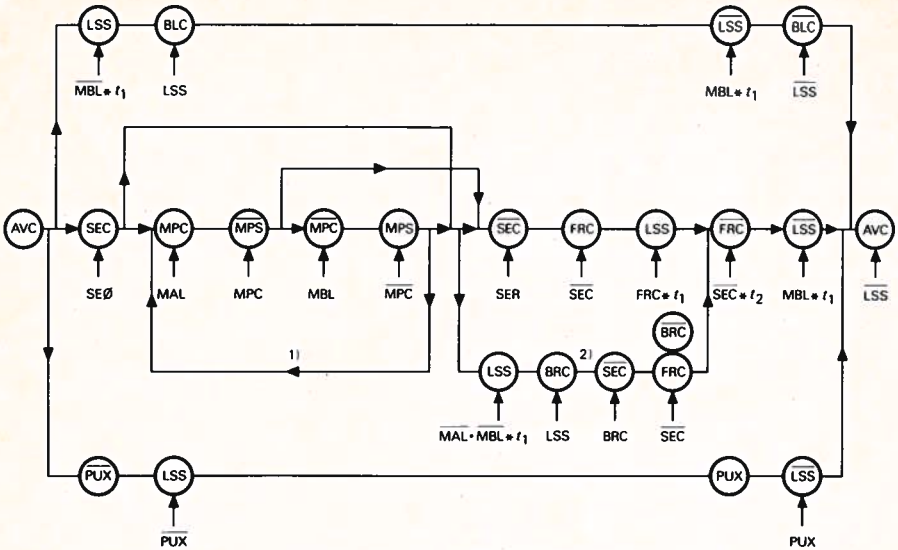


fig. 7. Toestanddiagram van een uitgaande PRX-overdrager voor standaard lijnsignalering.

Uit het voorgaande blijkt, dat een toestanddiagram van dit type meer mogelijkheden biedt dan een volgordediagram. Een bezwaar, dat overigens ook voor het volgordediagram geldt, is dat de argeloze lezer wordt geconfronteerd met een groot aantal, op het eerste gezicht nietszeggende, verkortingen van toestanden. Bij volgordediagrammen zijn dit toestanden van elementen die in het stroomkringschema met dezelfde aanduiding zijn aangegeven. Bij toestanddiagrammen hebben de verkortingen vaak betrekking op complexere situaties dan de toestand van een enkel element en kunnen dus niet altijd in het stroomkringschema worden teruggevonden. Om het geheel leesbaar te houden, is dus in ieder geval een verklarende lijst van de verkortingen noodzakelijk.

Een voorbeeld van een functiediagram

In IEC-verband (IEC = International Electrotechnical Commission) wordt momenteel een functiediagram gestandaardiseerd dat zich uitermate goed leent voor het weergeven van toestanddiagrammen.

Behalve toestanden (blokjes) en condities (streepjes), kunnen ook de situaties of de acties (rechthoekjes) die bij de toestanden horen, worden omschreven en dit opent de mogelijkheid om elke toestand direct op leesbare wijze te verklaren. Fig. 8 geeft aan hoe een gedeelte van fig. 7 er uitziet in de vorm van een functiediagram. Bij de diverse „lussen” kunnen nu, in tegenstelling tot bij fig. 7, ook de condities worden aangegeven die het doorlopen van een „lus” bewerkstelligen. Fig. 9 laat zien hoe logische relaties tussen toestanden gra-

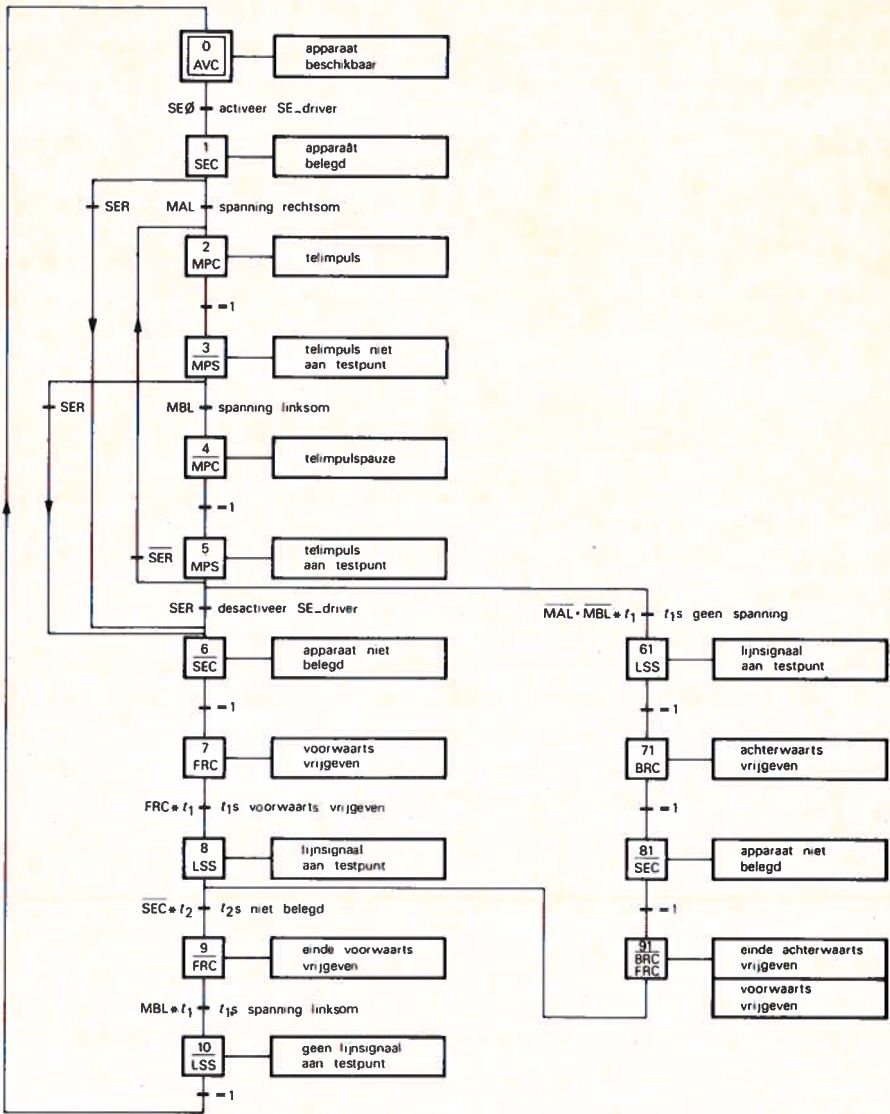


fig. 8. Functiediagram (niveau 1) van een uitgaande PRX-overdrager voor standaard lijnsignalering.

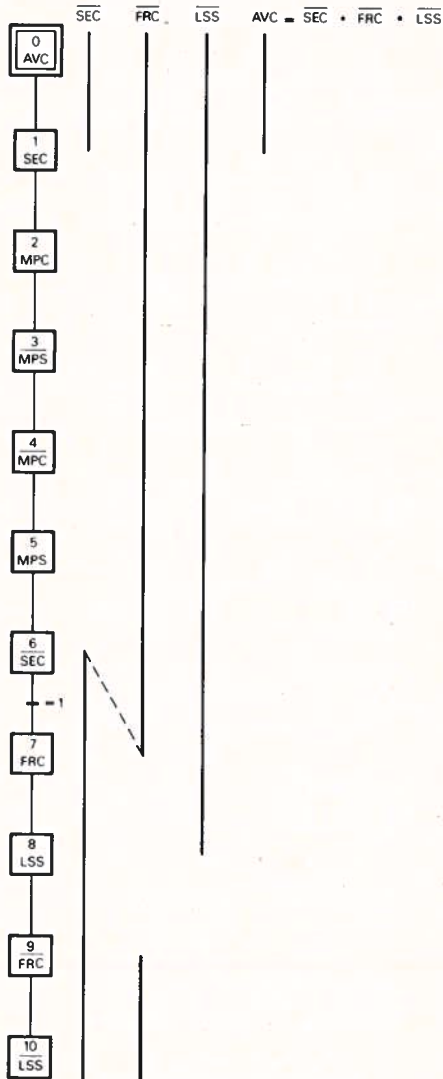


fig. 9. Een grafische methode om logische relaties tussen toestanden af te leiden.

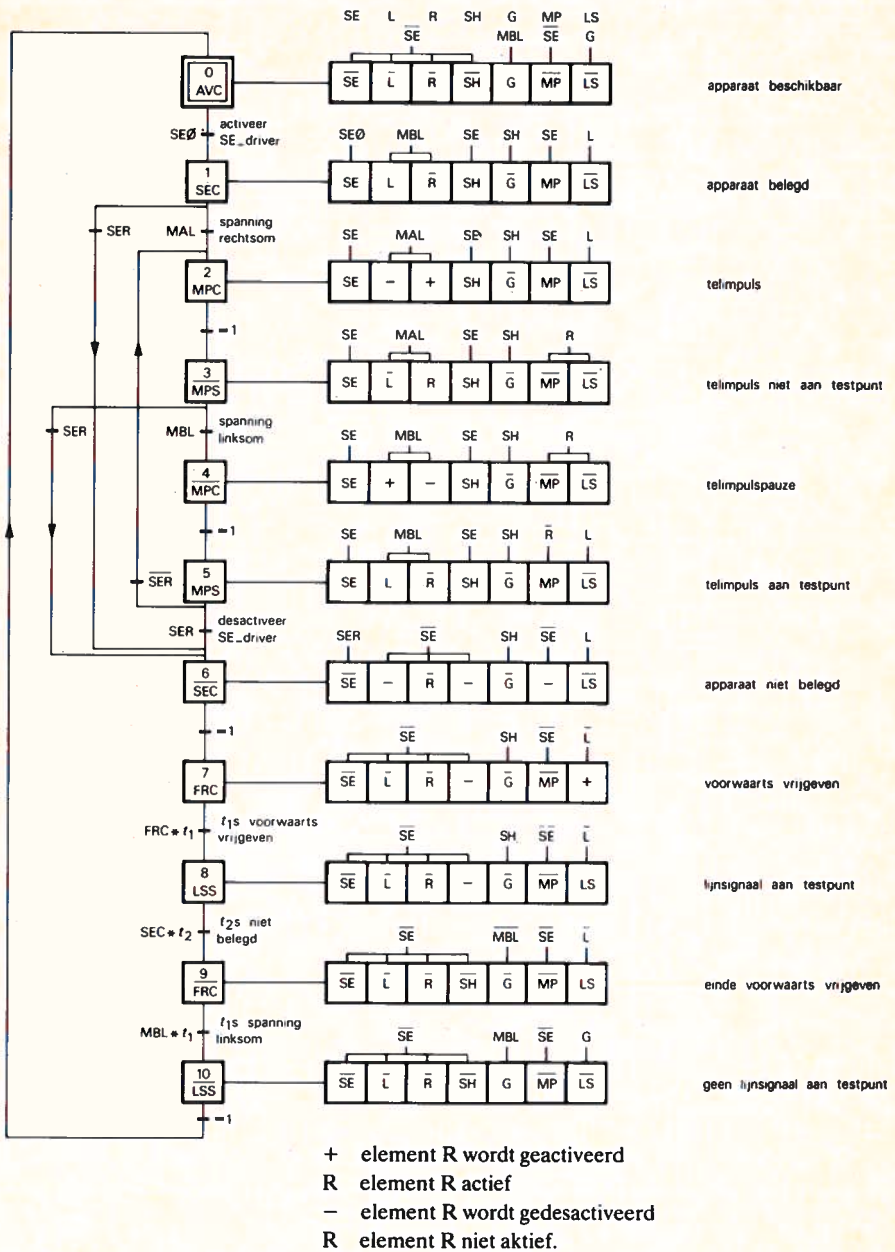


fig. 10. Functiediagram (niveau 2) van een uitgaande PRX-overdrager voor standaard lijnsignalering.

fisch kunnen worden afgeleid door het functiediagram in een twee-dimensionaal volgordediagram te transformeren.

Omdat de overgang tussen toestand 6 en toestand 7 autonoom is, zullen de toestandlijnen van \overline{SEC} en \overline{FRC} elkaar niet overlappen tussen 6 en 7. Uit de toestandlijnen blijkt dat: $AVC = \overline{SEC} \cdot \overline{FRC} \cdot \overline{LSS}$. Het blijkt ook mogelijk te zijn om met behulp van een functiediagram, net als bij een volgordediagram, gedetailleerde informatie te geven over de elementen van het stroomkringschema. Hiervoor is dan wel een ander functiediagram (niveau 2) nodig, dat in fig. 10 wordt getoond. Dit diagram geeft een gedeelte weer van fig. 8. Vaak is het mogelijk om bij een dergelijk diagram ook functionele informatie te verstrekken, waardoor wordt voorkomen dat men twee diagrammen moet raadplegen. Een aantal van de gedefinieerde toestanden (blokjes), komen overeen met stabiele toestanden van de elementen in de schakeling.

Er zijn echter ook gevallen waarin een gedefinieerde toestand overeenkomt met een niet-stabiele toestand van één of meer elementen. Om een dergelijke niet-stabiele toestand aan te kunnen geven, wordt gebruik gemaakt van de tekens + en -.

Het teken + geeft aan dat een element wordt geactiveerd, maar nog niet actief is en het teken - geeft aan dat een element wordt gedesactiveerd, maar nog actief is. Deze mogelijkheden zijn onontbeerlijk in situaties waarin opzettelijk vertragingstijden zijn ingebouwd. Bij elke toestand van een element (blokje in rechthoekje) wordt tevens via een verticaal streepje de oorzaak van die toestand aangegeven. Vaak ontstaat daarbij binnen een rechthoekje een kettingreactie. Bijvoorbeeld in toestand 1 (SEC) $SE \rightarrow SH$ en $SH \rightarrow \overline{C}$. Met behulp van een dergelijk diagram kan men exact de gebeurtenissen in een stroomkringschema (fig. 2) volgen tijdens een bepaalde cyclus van toestanden.

Functiediagrammen kunnen eveneens worden toegepast voor het verklaren van de werking van een processor. Men kan namelijk de inhoud van één of meer registers weergeven als functie van de ingangscmando's tijdens een bepaalde programmacyclus. In dit geval gaat het echter niet om de processorwerking, maar om het gedrag van een autonoom apparaat onder besturing van de processorsignalen $SE\emptyset$ en SER en de lijnsignalen MAL en $\overline{MAL} \cdot \overline{MBL}$.

Verantwoording

Door het complexer worden van de toegepaste technische apparatuur ontstaat er een groeiende behoefte aan compacte en exacte documentatie van systemen. In internationaal verband wordt getracht om hiervoor, via CCITT en IEC, een oplossing te vinden. In tegenstelling tot vroeger is de benadering top-down, d.w.z. eerst wordt een overzicht gegeven van de verschillende acties die een systeem onder invloed van de voorkomende besturingscondities moet

kunnen uitvoeren (niveau 1). Hierna kan eventueel ten behoeve van ontwerpers en onderhoudstechnici gedetailleerde informatie op elementniveau worden gegeven (niveau 2). Het bij de Nederlandse PTT toegepaste (tijd)volgordediagram is een goed voorbeeld van het laatstgenoemde niveau. Er ontstaan echter problemen wanneer wordt getracht om alle mogelijke bedrijfscycli in één figuur weer te geven of om informatie op functioneel niveau te verschaffen. Ook binnen de Nederlandse telecommunicatiewereld zijn al enige pogingen ondernomen om te komen tot een meer functionele weergave van telecommunicatieprocessen o.a. door F. Pakker (PTT) en de helaas te vroeg overleden M. Koeman (PTI). Het is opmerkelijk dat zijn reeds in 1973 in Philips Telecommunication Review gepubliceerde artikel zo aansluit bij de huidige internationale ontwikkelingen (dit wordt duidelijk wanneer men de fig. 7 en 8 vergelijkt). Om deze reden is zijn artikel, met enkele kleine wijzigingen, dan ook als basis genomen voor deze publicatie. Het door CCITT voorgestelde systeem SDL (System Descriptive Language) heeft een vergelijkbare strekking, maar maakt gebruik van symbolen met verschillende contouren die geen optimale tekstruimte opleveren. Via de Joint Working Group CCI/IEC wordt getracht om tot harmonisatie van diverse systemen te komen. Algemeen wordt aangenomen dat voor de exploitatie van systemen diagrammen van niveau 1 voldoende informatie verschaffen, wanneer de systemen zijn voorzien van foutzoekprocedures, die overigens ook met behulp van dezelfde diagrammen kunnen worden weergegeven. Het gebruik van diagrammen van niveau 2 kan daarmee worden beperkt tot systemen zonder foutzoekprocedures en het ontwerpen van systemen.

Studieblad PTT
**KENNIS
MAKEN
IS KENNIS
VERRIJKEN**

Verbindingswegen

ing. B. Kieboom
(Vervolg van blz. 125.)

Demping

In het voorgaande is geen rekening gehouden met de demping van de glasvezel. Het licht wordt daarin namelijk verzwakt. Hiervoor zijn twee oorzaken aan te wijzen.

De *eerste oorzaak* is gelegen in de *absorptie* van het licht door het glas. De energie wordt omgezet in warmte en gaat voor de informatieoverdracht verloren.

De *andere oorzaak* is gelegen in de aanwezigheid van *strooicentra* in de vezel. Deze verstrooien het licht zodanig dat de „stralen” (eigenlijk moet hier van trillingswijzen worden gesproken) van richting veranderen (de energie komt in een andere trillingswijze).

Dit verschijnsel vergroot de mode-dispersie in een vezel (zie Studieblad april '83, blz. 123) terwijl ook het licht dermate van richting kan zijn veranderd dat het niet meer in voorwaartse richting wordt geleid; het gaat zijwaarts uit de vezel of plant zich zelfs in terugwaartse richting voort. Van dit laatste verschijnsel kan, zoals hierna blijkt, nog een nuttig gebruik worden gemaakt.

Aanvullend kan worden gesteld dat wanneer het licht vrij vaak van de ene naar de andere trillingswijze gaat, een zeer groot gedeelte van het licht onderweg veel trillingswijzen „heeft gehad”. Dit en het genoemde effect werken tegengesteld. In de praktijk oefenen lassen, bochten en onregelmatigheden in de vezel ook een grote invloed uit op de grootte van de uiteindelijke mode-dispersie.

Beide verschijnselen die tot de demping van het glas bijdragen bestaan uit een *intrinsiek* deel en een *extrinsiek* deel.

Het *intrinsieke deel* van de demping is een grootheid behorende bij het zuivere, niet verontreinigde uitgangsmateriaal. Dit deel is laag te houden door een *juiste materiaalkeuze*.

Het *extrinsieke deel* is een gevolg van *onzuiverheden* en *inhomogeniteiten in het materiaal*. Door zuiver te fabriceren is dit nog te verkleinen (zie verder). Als tussen twee repeaters 45 dB moet worden overbrugd is het duidelijk dat de juiste glassoort van de juiste zuiverheid dient te worden gekozen. Onderstaande tabel geeft een indruk van de dempingen van de glassoorten:

Vensterglas in gebruik bij glasbouw	≈ 20.000 dB/km
Optisch glas voor lenzen	1.000 dB/km
Glas voor glasvezel	4 dB/km

De zuiverheid van glas voor de vezelfabricage dient zo te zijn dat slechts *één vreemd atoom* voorkomt op de 10^9 atomen in het glas. Om een indruk te geven van $1 : 10^9$. Dit is de verhouding van de inhoud van een vingerhoed tot twee maal die van een eengezinswoning.

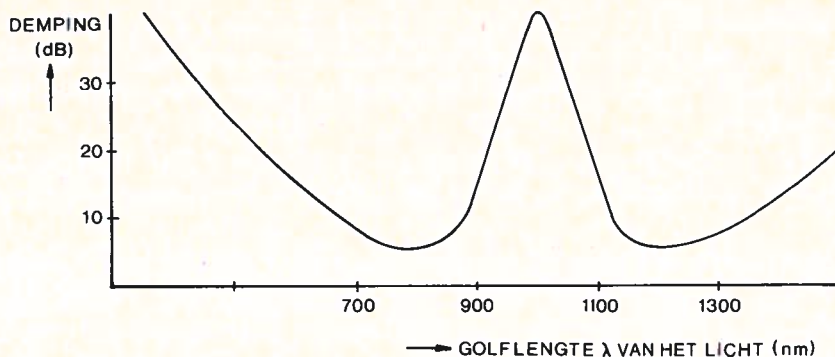


fig. 14. Dempingen van een glasvezel als functie van de golflengte van het gebruikte licht.

Tenslotte nog het verloop van de demping als functie van de *golflengte*. Deze is ruw geschetst in fig. 14 weergegeven.

Het overwegend dalen van de grafiek is een gevolg van de rayleigh-verstrooiing. Deze is evenredig met $1/\lambda^4$.

De piek bij 950 nm is een gevolg van OH-ionen in het glas. Door een zuiverder bereiding kan de concentratie hiervan worden teruggedrongen.

Het weer stijgen bij grotere golflengten is een gevolg van lagere harmonischen van de OH-piek (de grondharmonische ligt bij $\lambda = 2,8$ nm).

Hieruit blijkt dat er twee gebieden zijn die optisch „open” zijn. Dit zijn de gebieden met een golflengte tussen 700 nm en 900 nm en tussen 1100 en 1300 nm.

De fabricage van vezels

Voor het fabriceren van glasvezels zijn globaal twee typen werkwijzen in zwang:

- de dubbele kroes (voor andere glassoorten dan silicumdioxide) en
- de preform- (= voorvorm) methode.

De laatste methode betreft de vervaardiging van de silicumdioxide vezels en kent een aantal uitvoeringen waarvan de Outside Vapour Phase Oxidation (OVPO)- en de Plasma Chemical Vapour Deposition (PCVD)-methode de belangrijkste zijn.

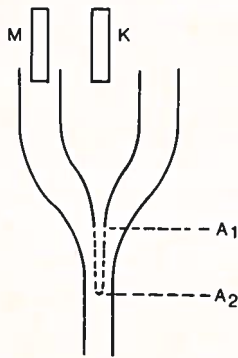
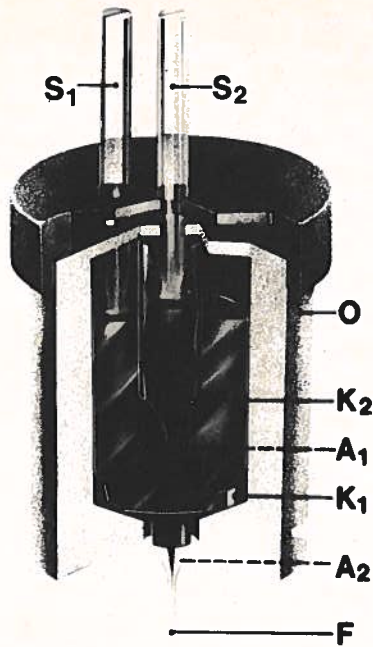


fig. 15. De dubbele kroes.

Dubbele-kroes-installatie voor het trekken van zachtglasvezels (schematisch). K_1 en K_2 zijn concentrische kroezen van zuiver platina. Zij zijn geplaatst in een weerstandsoven O , die het glas op de juiste temperatuur smelt. Het glas wordt toegevoerd door twee voorgevormde staven zuiver zachtglas S_1 en S_2 met verschillende brekingsindex. Bij de uitstroming over traject A_1 A_2 heeft een geringe vermenging van beide glazen plaats waardoor het gewenste brekingsindexprofiel in de glasvezel ontstaat.

De methode van de dubbele kroes

Fig. 15 is een afbeelding van een coaxiale dubbele kroes.

In de binnenste kroes bevindt zich het kernmateriaal, in de buitenste het mantelmateriaal in vloeibare vorm bij een temperatuur van 800°C.

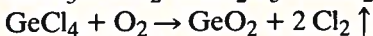
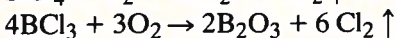
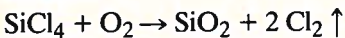
Onder uit deze kroezencombinatie wordt dan de vezel getrokken, terwijl bovenin de voorraad wordt aangevuld vanuit de staven K en M.

De vezel zoals die uit dit apparaat komt is zeer teer. Door de geringste aanraking met de apparatuur, een mensenhand of zelfs stof, kunnen zeer kleine haarscheurtjes worden gemaakt, waardoor de kwaliteit zeer nadelig wordt beïnvloed. Om deze reden wordt de vezel, onmiddellijk na het trekken, van een coating voorzien. De vezel wordt hiertoe door een pijpje met een smalle opening gevoerd. Hierin bevindt zich een plastic dat op deze wijze met een laagdikte van enkele micron wordt gebracht. Hoewel het plastic tamelijk hard is, is het toch raadzaam voorzichtig met de vezel om te gaan daar deze anders toch nog zijn sterkte kan verliezen. De zaak is echter minder kwetsbaar dan voorheen. Met de methode van de dubbele kroes is het mogelijk zowel stepindex-vezels te fabriceren als die met een parabolisch verlopend brekings-index-profiel. Het laatste geval wordt bereikt door uitwisseling van ionen tussen het kern- en mantelmateriaal tussen A_1 en A_2 . Wordt dit niet vereist, dan moet de afstand A_1, A_2 nul zijn.

De preform-methode

De OVPO-methode

Bij de Outside Vapor Phase Oxidation (neerslag van de buitenzijde van de geoxideerde dampfase) wordt uitgegaan van een ronde staaf Al_2O_3 (aluin) waarop materiaal wordt gedampt. De damp is afkomstig van chemische reacties.



Op deze manier kan dus de bijgemengde concentratie van B_2O_3 of GeO_2 worden geregeld.

Eerst wordt het SiO_2/GeO_2 mengsel opgedampt en wel met een laag voor laag afnemende GeO_2 -concentratie. Op deze wijze wordt een staaf met een verlopend brekingsindexprofiel verkregen. Hierna wordt de SiO_2/B_2O_3 combinatie opgedampt welke als optische mantel dienst doet. De Al_2O_3 -staaf wordt thans verwijderd, waarna het geheel wordt gesinterd. Het is mogelijk van deze staaf een grin-vezel te trekken. Na het trekken van de vezel uit de voorvorm, waarbij het holle middendeel verdwijnt wordt de vezel onmiddellijk gecoat en

wel om dezelfde redenen als genoemd bij het hoofdstuk *fabricage van vezels* (zie blz. 219).

Een nadeel van deze methode is dat het materiaal vrij veel water (hydroxide-groepen) bevat hetgeen een lage demping niet ten goede komt. Deze wateropname vindt vooral plaats tijdens de periode dat de voorvorm poreus is, dus vóór het sinteren. Andere nadelen zijn de breekbaarheid van de poreuze voorvorm, het ontstaan van bubbels en het verdampen van een deel van de GeO_2 , waardoor in het midden van de vezel een onregelmatigheid in het brekingsindexprofiel ontstaat.

De PCVD-methode

De Plasma.Chemical Vapor Deposition (chemische damp-neerslag door vorming van plasma) is een variant op de OVPO-methode.

Het verschil is dat een holle cylinder aan de binnenzijde wordt opgedampt. Er ontstaat dan geen holle ruimte in de voorvorm. De chemische reacties worden hier niet door een vlam maar door een microgolf-resonator (een soort microgolfoven) op gang gebracht. Deze beweegt zich zeer snel langs de voorvorm heen en weer en geeft een momentane neerslag van materiaal. Er ontstaat nu een stevige voorvorm, zodat sinteren niet nodig is. De nadelen van de OVPO-methode zijn hierdoor ondervangen.

(Wordt vervolgd.)



Museumbezoek is minder saai dan vaak wordt beweerd; integendeel!

Wie gewend is regelmatig, individueel, musea te bezoeken zal het laatste beamen. Er zijn zoveel interessante musea in Nederland met zoveel verschillende exposities die de moeite waard zijn, dat het de redactie zinvol lijkt de lezer daar ook eens op te wijzen.

De meeste aandacht zal worden besteed aan technische musea. De selectie, alsmede alle gegevens, zijn verzorgd door ing. L. de Bruijn.

Rijksmuseum van Geologie en Mineralogie

Dit museum ligt in het centrum van de Leidse binnenstad, 5 minuten lopen van het stadhuis.

Het museum is gevestigd in het voormalige Heilige Geest- of Arme Wees- en Kinderhuis, waarvan de oudste gedeelten uit 1607 stammen.

Weer en wind breken de gesteenten, die aan de oppervlakte van de aarde voorkomen, op den duur helemaal af.

Dit afgebroken materiaal wordt door gletsjers, rivieren, zeeën en de wind weggevoerd en op andere plaatsen weer neergelegd.

Hoe dit gebeurt en wat de resultaten zijn, is te zien in de zalen: „*Processen aan de oppervlakte van de aarde*”.

Op de aarde heeft zich in de loop van ongeveer 3,5 miljard jaar leven ontwikkeld.

Dit leven begon in het water dat beschutting bood tegen uitdroging en waarin voedsel in overvloed aanwezig was. Geologisch bekeken is het nog maar kort geleden dat zich uit het leven in het water, leven op het land ontwikkelde.

Ongeveer 400 miljoen jaar geleden groeiden er eerst planten op het land. Later waagden ook dieren zich op het droge.

Overblijfselen van planten en dieren uit het geologisch verleden noemen we fossielen.

De oppervlakte van Nederland bestaat bijna overal uit materiaal dat ons land in de laatste 2,5 miljoen jaar heeft bedekt. Die periode is gekenmerkt door een afwisseling van warmere en koudere tijden (ijstijden). In een warm tijdperk, 1,5 miljoen jaar geleden, werd bij Tegelen (Limburg) klei afgezet, waarin veel fossielen zijn gevonden, o.a. van het Tegels hert.

Naast een algemene rondleiding door het museum bestaat de mogelijkheid speciale aandacht te besteden aan een bepaald onderwerp, zoals:

- het ontstaan van gesteenten;
- vulkanen;
- ontwikkeling van het leven op aarde;
- dinosauriërs en andere grote dieren van vroeger;
- geologische tijdschaal;
- ouderdomsbepaling;
- kostbare stenen;
- de mens en zijn ontwikkeling;
- afbraak en opbouw van gebergten;
- geologie van Nederland.

In het museum is voorts van **1 juli** tot en met **21 augustus 1983** de speciale tentoonstelling **De mens als jager** te zien.

Deze tentoonstelling, die is samengesteld door het Museum voor het Onderwijs te Den Haag en aangevuld met materiaal van het Rijksmuseum van Geologie en Mineralogie, geeft een overzicht van de levenswijze van de prehistorische mens, die de jacht gebruikte om aan voedsel te komen.

De mens als jager laat zien, wat belangrijk was in het bestaan van de prehistorische mens.

Skeletten van **prehistorische dieren** zijn opgesteld in een deel van de permanente tentoonstelling van het museum.

Het Rijksmuseum van Geologie en Mineralogie, Hooglandse Kerkgracht 17, 2312 HS Leiden, tel. 071-124741 is geopend op maandag t/m vrijdag van 10-17 uur; op zondag van 14 tot 17 uur.

Op feestdagen gesloten. *Toegang gratis.*

Andere musea in Leiden zijn:

- Academisch Historisch Museum, Rapenburg 73, di., wo. en do.: 13-17 uur.
Toegang gratis;
- Hortus Botanicus der Rijksuniversiteit, Rapenburg 73, Universiteitsplein, tuin: ma. t/m va. 9-17 uur, zo. 10-17 uur;
- Stedelijk Molenmuseum „De Valk” 2de Binnenvestgracht 1, di. t/m za.: 10-17 uur; zon- en feestdagen 13-17 uur, volwassenen *f* 1,50, kinderen 6-16 jaar *f* 0,75; boven 65 jaar *f* 0,40;
- Koninklijk Nederlands Leger- en Wapenmuseum „Generaal Hofer”, Pesthuislaan 7, ma. t/m vr. 9.30-17 uur; zo. 13-17 uur, *f* 2,50; t/m 16 jaar en boven 65 jaar *f* 1,—;
- Pilgrim Fathers Documentatie Centrum, Biosotkade 2a, ma. t/m vr. 9-12 en 14-16,30 uur, *toegang gratis;*

- Rijksmuseum' van Oudheden, Rapenburg 28, ma. t/m za. 10-17 uur, zon- en feestdagen 13-17 uur, *f* 3,50; tot 18 jaar en boven 65 jaar *f* 2,—;
 - Museum „Boerhaave”, Steenstraat 1a, 1/10-1/6: ma. t/m za. 10-16 uur, zo. 13-16 uur, 1/6-1/10: ma. t/m za. 10-17 uur, zo. 13-17 uur, *f* 3,50; tot 18 jaar en boven 65 jaar *f* 2,—;
 - Rijksmuseum voor Volkenkunde, Steenstraat 1, ma. t/m za. 10-17 uur, zon- en feestdagen 13-17 uur, *f* 3,50, tot 18 jaar en boven 65 jaar *f* 2,—;
 - Stedelijk Museum „De Lakenhal”, Oude Singel 28-32, d. t/m za. 10-17 uur; zon-en feestdagen 13-17 uur, *f* 1,75, 6-16 jaar *f* 0,90;
 - Prentenkabinet der Rijksuniversiteit, Rapenburg 65, di. t/m vr. 14-17 uur;
 - Stichting Openbare Bibliotheek Leiden, Nieuwstraat 4.
-

SPELDBANDEN

Voor het overzichtelijk opbergen van uw Studiebladen kunt u het beste gebruikmaken van de bekende groene speldbanden, waarin één volledige jaargang past.

Deze speldbanden worden geleverd met de jaargangaanduiding 1977 t/m 1984.

De prijs bedraagt *f* 7,50 per band.

Bestelling: door storting op giro 4073, t.n.v. Studieblad PTT, Brede- water 16, Zoetermeer, onder vermelding van de gewenste jaargang- aanduiding.