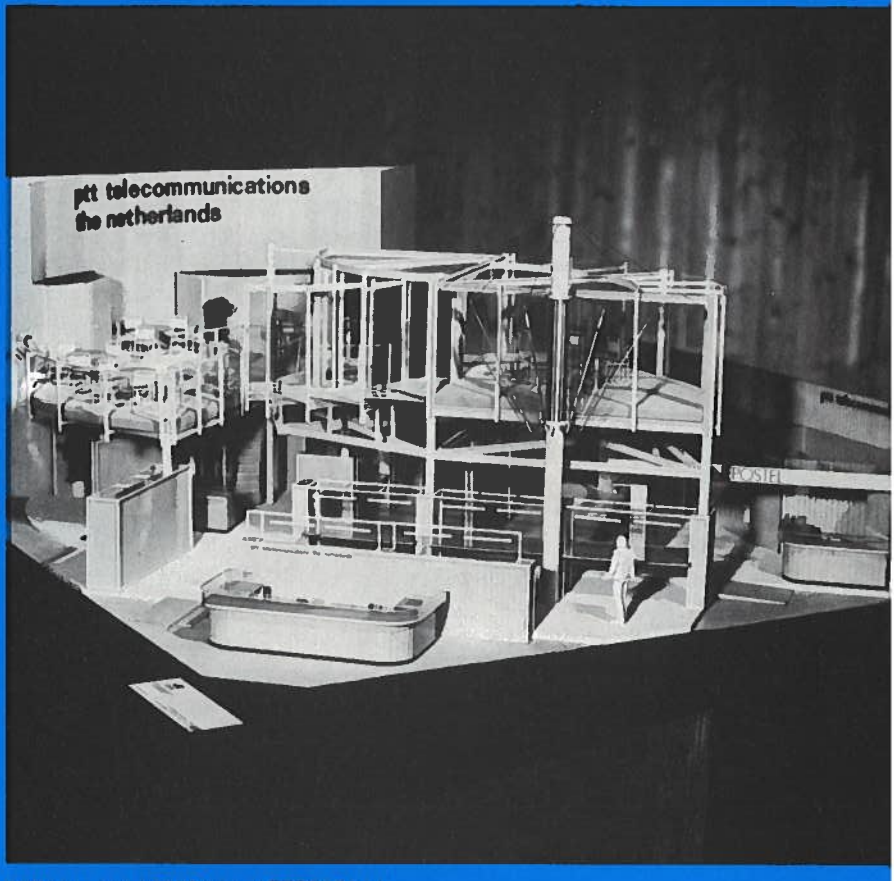
In dit nummer o.a.:
Cryptologie – Wat doe je ermee?
Licht gaat niet altijd met de lichtsnelheid
Telecom '87

Nr. 10, 42e jaargang oktober 1987

technische informatie voor ptt medewerkers



ptt

STUDIEBLAD ptt

technische informatie voor ptt medewerkers

uitgave	AbvaKabo en CFO.
redactie	Hoofdred. Drs. C. Vader, Red. P. J. Boomgaard, ing. B. Kieboom, L. J. Leenders.
redacteur/secr.	R. Scholma, Oude Kerkweg 12, 2355 AV Hoogmade, tel. 01712 - 81 98.
secretariaat	tel. 070 - 43 67 35.
corr.-adres	PTT Centrale Directie, Studieblad PTT, AB 6032, postbus 30 000, 2500 GA 's-Gravenhage.
administratie	AbvaKabo, Bredewater 16, 2715 CA Zoetermeer, postbank 4073, tel. 079 - 53 62 54, voor verzending, administratie e.d.
abonnement	ƒ 18,– per jaar. Voor niet-PTT-ers ƒ 30,– per jaar. Verschijnt maandelijks.
advertenties	Uitgeverij en Drukkerij Smits B.V., Westeinde 135, 2512 GW Den Haag, tel. 070 - 89 53 90.

Inhoudsopgave

Omslagfoto
Waarborg van privacy, toch open en toegankelijk. De presentatie van de Nederlandse PTT tijdens Telecom '87.

Cryptologie – Wat doe je ermee?

Ir. J. van Tilburg

Het toepassen van *cryptologie,* de leer van het geheimschrift, is de laatste jaren zeer sterk toegenomen. Waren vroeger geheimschriften vooral van belang voor militaire toepassingen en diplomatieke diensten, tegenwoordig wordt bijna iedereen al dan niet bewust geconfronteerd met de vele facetten van de cryptologie. Belangrijke oorzaak is de toename van diensten op telecommunicatie- en informatiegebied, waarbij steeds meer informatie, ook van persoonlijke aard, voor derden bereikbaar is. Daarnaast zijn bedrijfsvoeringsprocessen steeds meer afhankelijk van computer- en telecommunicatiesystemen.
Beveiliging van informatie en informatiestromen is daarom een essentieel aspect van de datacommunicatie geworden.

Vercijfering

Een belangrijk middel om een informatieproces te beveiligen is het vercijferen of versluieren van informatie, hetgeen zijn oorsprong vindt in een deelgebied van de cryptologie: de *cryptografie.* De cryptografie houdt zich bezig met het ontwerpen van systemen waarin kennis van de cryptologie wordt gebruikt.
Een tweede deelgebied van de cryptologie, de crypto-analyse, houdt zich bezig met het analyseren van geheimschriften. De *crypto-analyse* is een specialisme. Dankzij goede crypto-analisten zijn we veel te weten gekomen over zwakheden in geheimschriften.
Vooral tijdens de tweede wereldoorlog zijn indrukwekkende prestaties verricht. In het boek Nishi No Kaze, Hare[1]), wordt de rol die de Nederlandse inlichtingendienst in de periode 1932-1942 in Nederlands-Indië heeft gespeeld in de strijd tegen Japan uitvoerig beschreven. Door grote kennis van zaken kon een gedeelte van de Japanse geheime berichtgeving worden ontcijferd, waardoor men de Japanners voortdurend een stap voor was. Het mag duidelijk zijn dat niet goed een van deze deelgebieden kan worden beoefend, zonder voldoende kennis over het andere deelgebied. Belangrijk is hierbij ook de stand van de techniek. Naast de kwaliteit van het *vercijferalgoritme* is ook de manier waarop de vercijfering wordt toegepast, de *identificatiemethode,* het bijbehorend *communicatieprotocol,* het sleutelbeheersysteem en het *onderliggende informatieproces* van belang.

Enkele toepassingen

Cryptologie kan voor verschillende doeleinden worden gebruikt. De banken gebruiken het in betalingssystemen om bijvoorbeeld automatisch geld op te

nemen. Daarnaast wordt vertrouwelijke informatie vaak versluierd in een computersysteem opgeslagen, dit om ongewenste inzage tegen te gaan. Ook de PTT houdt zich actief met cryptologie bezig. Momenteel wordt op het dr. Neher Laboratorium te Leidschendam (DNL) een zogenaamde linkvercijferaar Temporal Input Relation Output (TIRO) ontwikkeld om belangrijke informatie over telefoonverbindingen versluierd te verzenden en op die manier o.a. afluisteren tegen te gaan.
Daarnaast kent de Nederlandse PTT het Toegangs Bewakend Informerend en Alarmerend Systeem (TOBIAS), dat bij DNL volgens de nieuwste cryptografische technieken is ontworpen. Dit systeem wordt o.a. gebruikt om de toegang tot PTT-gebouwen te beheersen. Voorts heeft de Nederlandse PTT een leidende rol in het beveiligen van het mobiele communicatienet.

Beveiligingsfuncties

In het voorgaande zijn enkele toepassingen van de cryptologie genoemd. Het zal de lezer zijn opgevallen dat het doel van beveiliging hierbij verschillend kan zijn. Soms is alleen bescherming tegen ongewenste inzage of afluisteren van belang.
Bij TOBIAS daarentegen speelt de indentiteitsverificatie een belangrijke rol. In het betalingsverkeer is o.a. echtheid van de data belangrijk; wordt een bedrag op de rekening gestort of afgeboekt en hoe groot is het bedrag. Daarom kan in een cryptografisch systeem onderscheid worden gemaakt tussen verschillende beveiligingsdoeleinden, te weten:
- geheimhouding en privacy;
- identificatie;
- data-integriteit.

Geheimhouding en privacy bevorderen dat informatie uitsluitend toegankelijk is voor personen die daartoe gemachtigd (geautoriseerd) zijn. Meestal is dataversluiering in combinatie met identificatie een afdoend middel. Bij *identificatie* spelen bepaalde kenmerken een belangrijke rol. Identificatie kan op verschillende manieren plaatsvinden, bijvoorbeeld door het herkennen van een vingerafdruk (fysieke eigenschap), password (kennis) of een paspoort (bezit). De identificatie is nooit 100% waterdicht. Daarom moet bij de keuze van een indentificatiemethode vooraf een geoorloofde foutkans (de kans op foutieve identificatie) zijn vastgesteld. Naast deze onzekerheid is identificatie slechts een momentopname: het identificatieproces moet daarom doorgaans worden verlengd. In het volgende voorbeeld spelen verschillende identificaties een rol.

Om een voetbalwedstrijd te kunnen bijwonen dient men zich van een toegangsbewijs te voorzien. Bij binnenkomst in het voetbalstadion wordt de controlestrook eraf gescheurd (ongeldig maken). Het indentificatieproces bij een voetbalwedstrijd richt zich dus op betaling voor de wedstrijd. In de nabije toekomst wordt aan een pasjesregeling gedacht. Het beoogde doel hierbij is verbeterde controle op de toegang van toeschouwers. Men kan echter niet voor 100% voorkomen dat met goed nagemaakte toegangsbewijzen, pasjes of door over het hek te klimmen de wedstrijd toch kan worden bijgewoond.
Bij informatie-overdracht wordt vaak de identificatie (van de zender en/of ontvanger) voortgezet door tijdens de indentificatiefase een vercijfersleutel af te spreken waardoor de informatie kan worden vercijferd. *Data-integriteit* moet de echtheid van data waarborgen. Het controle-apparaat moet in staat zijn al dan niet moedwillig aangebrachte modificaties, tussenvoegingen, weglatingen of herhalingen in de data te ontdekken.
Naast deze functies biedt een cryptografisch systeem soms ook de mogelijkheid tot:
- bewijs van herkomst;
- bewijs van ontvangst.

Deze twee functies zijn bijvoorbeeld van belang bij elektronische post ter vervanging van het aangetekend verzenden van informatie. In dergelijke gevallen moet later, eventueel voor een rechtbank, kunnen worden aangetoond dat informatie-uitwisseling heeft plaatsgevonden.

Cryptografisch systeem

In een cryptografisch systeem kan onderscheid worden gemaakt tussen twee belangrijke onderdelen, te weten:
- de vercijfer- en ontcijfermethode;
- de te gebruiken sleutel.

De *vercijfer- en ontcijfermethode* is de algemene omschrijving van de methode *waarop* informatie wordt ver- of ontcijferd. De te gebruiken *sleutel* bepaalt *hoe* de informatie moet worden vercijferd of ontcijferd. De methode is een soort rekenschema dat aangeeft hoe de berekening moet worden uitgevoerd. Bij gebruik van dezelfde methode en invoer zorgt een wisselende sleutel voor een wisselende uitvoer.

Voorbeeld
Een vercijfermethode vervangt iedere letter in de boodschap door een andere. De sleutel geeft aan door welke letter de oorspronkelijke letter moet

worden vervangen en omgekeerd. Het cryptografisch systeem zet de boodschap op deze manier om in een cryptogram of vertaalt het cryptogram tot de boodschap. De methode wordt meestal het *cryptografisch algoritme* genoemd. De te gebruiken sleutel wordt volgens een van te voren afgesproken manier uitgewisseld. De uitwisseling wordt vaak het *sleutelprotocol* genoemd. Sleutels kunnen door een *sleutelbeheercentrum* worden geleverd. Dat sleuteluitwisseling langs veilige kanalen moet plaatsvinden spreekt voor zich.

Een cryptografisch systeem heet *veilig* als het systeem *theoretisch onbreekbaar* is. Dit betekent echter niet dat een theoretisch *breekbaar* systeem ook *praktisch breekbaar* is. Zo kost het bijvoorbeeld enkele eeuwen rekentijd om het systeem van de snelste computer ter wereld te breken. Dergelijke systemen worden veilig genoemd omdat het *praktisch* onmogelijk is binnen een bepaalde tijd het systeem te breken (informatie veroudert snel).
Soms wordt een systeem veilig verklaard op basis van kosten- en batenanalyse. Dit geldt bijvoorbeeld voor vercijferde boodschappen die slechts 1 dag geheim hoeven te blijven. Het cryptogram mag dan best in twee dagen worden gebroken. Dit soort redeneringen zijn echter twijfelachtig en worden daarom verder buiten beschouwing gelaten.
Een theoretisch onbreekbaar systeem is het *one-time padsysteem* waarbij de sleutel eenmalig wordt gebruikt. Voorwaarde is dat de sleutel tenminste even lang moet zijn als de te vercijferen tekst. De sleutel moet ook nog volkomen willekeurig zijn. Het systeem is onhandelbaar voor lange berichten, toepassing hiervan is in veel communicatie-netwerken niet praktisch. In bijna alle in de praktijk toegepaste systemen wordt een relatief korte sleutel (64 bits of meer) gebruikt. Met behulp van deze korte sleutel wordt afhankelijk van de te gebruiken vercijfermethode een zeer lange pseudo-willekeurige sleutel afgeleid of een enorm grote substitutietabel opgesteld.

Vercijfermethode

In de cryptografie kunnen twee belangrijke bouwstenen voor vercijfermethoden worden onderscheiden:
- subsitutie;
- transpositie.

Bij *substitutie* wordt de boodschapletter vervangen (gesubstitueerd) door een andere letter. Daarentegen blijven bij *transpositie* de letters gelijk; de

volgorde van de letters wordt echter veranderd (getransporteerd of gepermuteerd; permutatie, verwisseling; verandering in rangschikking).

Een voorbeeld van substitutie
Het uitgangspunt is een alfabet van 26 letters (A tot en met Z). De gekozen sleutel: AETOLFOHBNCDIZVYJXNWSUGKRP. Bij gebruik van deze sleutel wordt de letter A vervangen door de Letter E, de letter E door een T enzovoort. tot slot wordt de letter P vervangen door een A. Het woord SCHILDERIJ wordt aldus omgezet in UDBZFITPZX.

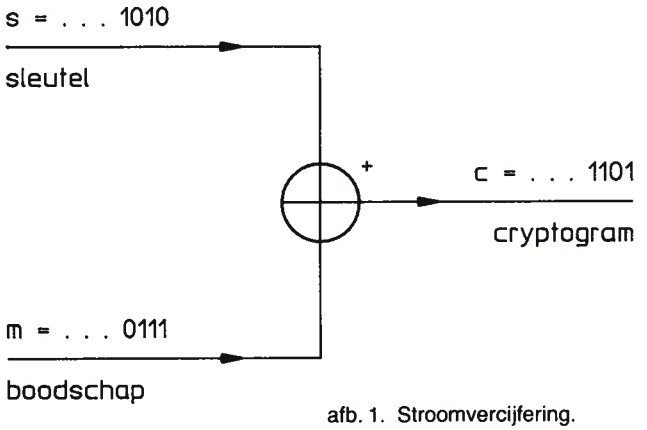
Een voorbeeld van transpositie
Bij transpositie wordt de tekst opgedeeld in blokken, meestal van gelijke woordlengte. De lettervolgorde wordt nu veranderd. Voor de sleutel wordt een bloklengte van 5 letters met de volgende permutatie gekozen: 14523. Bij gebruik van deze sleutel komt de eerste letter uit het boodschapblok op de vierde letter van het cryptogramblok te staan, de vierde letter op de vijfde enzovoort. Het woord SCHILDERIJ wordt op deze manier eerst in twee blokken verdeeld: SCHIL DERIJ. Hierna worden de letters gepermuteerd: HLCSI RJEDI. Het cryptogram is dus HLCSIRJEDI.

Uit de twee voorbeelden blijkt dat substitutie op de symboolwaarde werkt en transpositie op de symboolpositie. In de Nederlandse taal komen de letters E, T, N zeer vaak in een tekst voor, daarentegen worden de letters Q, J sporadisch gebruikt. Evenzo geldt dit voor lettercombinaties. De combinatie EN komt vaak voor, QN echter niet. Door gebruik te maken van deze taalafhankelijke kenmerken (redundantie) blijkt dat tijdens analyse van een cryptogram de oplossing soms kan worden gevonden. De oorzaak is onvolledige versluiering van taalkenmerken door het vercijferalgoritme. Vooral de oudere systemen waren daardoor betrekkelijk eenvoudig te breken. Door herhaaldelijk en afwisselend substituties en transposities toe te passen met gebruik van verschillende sleutels kan een sterk algoritme worden verkregen. Belangrijk bij dit proces is dat de gebruikte sleutel goed gemengd wordt met de invoer. Het nagestreefde doel is de taalkenmerken te laten verdwijnen, zodat de vercijferde tekst op een willekeurige tekst lijkt.
Met deze kennis gewapend lijkt het verstandig om een tekst twee of meermalen te vercijferen met *dezelfde* vercijfermethoden en toepassing van *verschillende* sleutels. Helaas wordt de veiligheid op deze manier niet altijd verhoogd. Dit is eenvoudig te zien in het volgende substitutievoorbeeld.
Als een letter A wordt vervangen door de letter C om vervolgens de C te vervangen door de letter K, dan is dit gelijk aan het eenmaal vervangen

(vercijferen) van de letter A door een K. Een ongelukkige sleutelkeuze kan er zelfs toe leiden dat de originele tekst weer wordt verkregen. Er bestaan systemen die op deze manier soms kunnen worden gebroken. Het is dus oppassen bij herhaald vercijferen van een tekst.
Soms kan het toch gerechtvaarigd zijn (meestal om praktische redenen) om dubbele vercijfering toe te passen. De vercijfermethode moet dan echter wel aan bepaalde eisen voldoen. Helaas is het meestal moeilijk vooraf te bewijzen of een vercijfermethode aan alle voorwaarden voldoet.

Soorten vercijfering

Vercijfering van een tekst kan op twee verschillende manieren worden bewerkstelligd:
- stroomvercijfering;
- blokvercijfering.

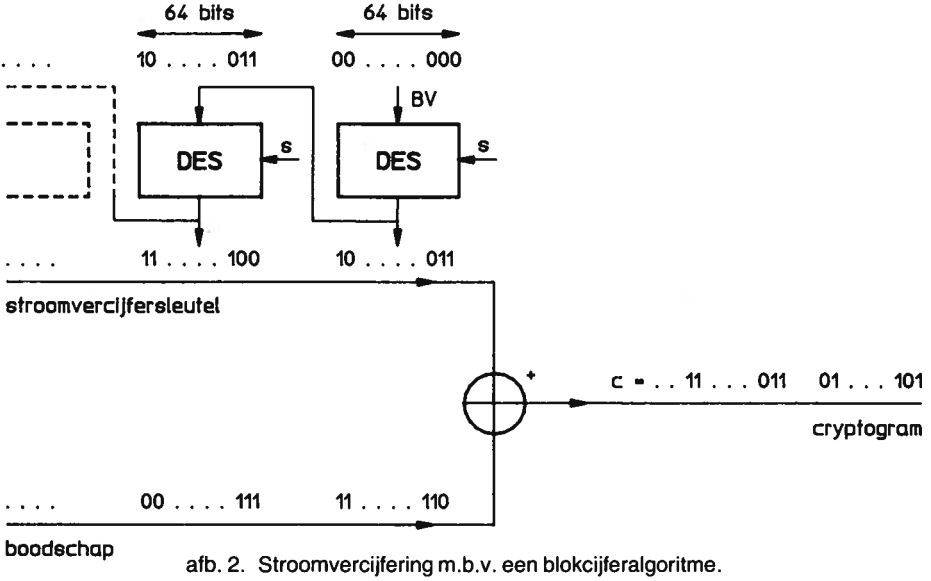


m	s	c
0	0	0
0	1	1
1	0	1
1	1	0

afb. 1. Stroomvercijfering.

Bij *stroomvercijfering* (zie afb. 1) vindt de vercijfering op tekenniveau plaats, dat wil zeggen de te vercijferen boodschap wordt als een stroom tekens beschouwd die elk afzonderlijk zijn vercijferd. In het vervolg is ervan uitgegaan dat de boodschap in binaire vorm (eenen en nullen) wordt aangeboden. De tekenstroom wordt dan een bitstroom genoemd. De inkomende bitstroom wordt bijvoorbeeld met behulp van een binaire optelling gecombineerd met een stroom sleutelbits tot de uitgaande vercijferde bitstroom. Het is nu de kunst om vanuit een kleine willekeurig gekozen sleutel een zeer lange pseudo-willekeurige sleutelrij af te leiden.

Blokvercijfering betekent dat de boodschap in een aantal groepen (blokken) met vaste lengte wordt verdeeld. Ieder blok is als geheel vercijferd. Een voorbeeld van een blokvercijferalgoritme is Data Encryption Standaard[2]) (DES) dat in IC-vorm te koop is. DES is een algoritme dat een blok van 64 bits (klare tekst) omzet met behulp van een 56 bits sleutel in een ander blok (cryptogram) van 64 bits (zie afb. 2). Om een indruk van de vercijfersnelheid te krijgen: een commercieel verkrijgbare CMOS-versie van de DES kan ruim 15 Mbits per seconde vercijferen.



afb. 2. Stroomvercijfering m.b.v. een blokcijferalgoritme.

Het blijkt dat met blokvercijferalgoritmes op verschillende manieren stroomvercijferaars gemaakt kunnen worden. Ter illustratie zal een van de mogelijke methoden worden besproken.
Stel dat het blokvercijferalgoritme DES wordt gekozen. De gekozen sleutel S bestaat uit 56 bits en heeft een beginwaarde (BW) van 64 bits.
De BW kan eventueel een vaste zijn, bijvoorbeeld allemaal nullen. Na de eerste vercijferslag zijn 64 vercijferde bits beschikbaar. De vercijferde bits zijn de eerste 64 bits van de stroomvercijfersleutel. Deze 64 bits worden ook naar de ingang van het DES teruggevoerd. Vervolgens vindt weer een vercijferslag plaats met dezelfde DES-sleutel S waardoor 64 andere vercijferde bits worden verkregen. Deze vercijferde bits zijn de volgende 64 bits van de stroomvercijfersleutel. Ook deze 64 bits worden weer naar de ingang van het DES gebracht enzovoort.

De zo verkregen stroomvercijfersleutel wordt, net als die in afb. 1, opgeteld bij de te vercijferen boodschap. Zolang gewaarborgd blijft dat de uitvoer zich niet snel zal herhalen, wat bij het DES het geval is, kan een zeer lange pseudo-willekeurige sleutelrij worden verkregen uit slechts 56 DES-sleutel bits.

Symmetrisch of asymmetrische systemen

De tot nu toe beschreven vercijfermethoden kenmerken zich door het gebruik van dezelfde sleutel voor vercijfering en ontcijfering van de boodschap. Dit was aanleiding om systemen volgens deze methode aan te duiden als *symmetrische systemen* (aan beide kanten dezelfde sleutel). Ter illustratie noem:
- de boodschap B;
- het cryptogram C;
- de sleutel S.

De vercijferprocedure V staat dan genoteerd als C = V (B, S) en de ontcijferprocedure 0 als B = 0 (C, S).
Een belangrijk kenmerk en kwaliteitsvoorwaarde van een symmetrische systeem bepaalt dat het aboluut noodzakelijk is om de gebruikte sleutel S geheim te houden. De sleutel moet dus van te voren op een veilige manier worden uitgewisseld. Symmetrische sleutelsystemen staan bekend als privé-sleutelsystemen.
Naast de symmetrische systemen bestaan er sinds 1976 in de openbare literatuur dankzij Whitfield Diffie en Martin Hellman[3]) *asymmetrische systemen.* Dit zijn systemen waarbij de sleutels aan de vercijfer- en ontcijferkant verschillend zijn. Door de asymmetrie in het sleutelgebruik is het niet meer nodig om volledige geheimhouding van de beide sleutels te handhaven. Asymmetrische systemen worden wel openbare sleutelsystemen genoemd, dit in tegenstelling tot de symmetrische systemen die ook privé-sleutelsystemen worden genoemd.
Voor een openbaar systeem geldt nu: C = V (B, S1) en B = (C, S2). Openbaar maken van sleutel S1 betekent dat iedereen een bericht kan vercijferen en toezenden aan degene die de *geheime* sleutel S2 bezit. Een eigenaardigheid van het asymmetrische systeem ontstaat als, in plaats van sleutel S1, sleutel S2 wordt bekend gemaakt. De zender kan zijn bericht met de geheime sleutel S1 vercijferen. Iedereen die het bericht kan ontvangen is in principe in staat het te ontcijferen. De privacy en geheimhouding zijn niet gewaarborgd. De ontvanger is echter verzekerd van de herkomst, want alleen de bezitter van sleutel S1 kan het bericht hebben vercijferd. Een

toepassing hiervan is de zogenaamde alternatieve of digitale handtekening. Een contract of order kan op deze manier worden ondertekend of bevestigd. In het tot nu toe beschreven asymmetrische systeem geldt dat
B = 0 ({V (B, S1)}, S2). Als ook nog de sleutels S1 en S2 onderling verwisseld mogen worden geldt: B = 0 ({V (B, S2)}, S1). Sleutel S2 kan dan ook voor vercijferen van een boodschap worden gebruikt. Ontcijferen vindt in dat geval plaats met sleutel S1 waarbij geldt: C = V (B, S2) met B = 0 (C, S1), maar niet dat V (B, S2) = V (B, S1). Met dit systeem is het mogelijk naast zetten van een handtekening ook nog een boodschap te adresseren. Om de waarde van dit systeem noodzaakt tot uitbreiding van de sleutelnotatie. Stel dat persoon A een bericht B naar persoon Z wil sturen. A bezit de sleutels SA1 en SA2. Z bezit de sleutels SZ1 en SZ2. Zowel A als Z maken de eerste sleutel SA1 respectievelijk SZ1 publiekelijk bekend. Als A een door hem ondertekende boodschap V (B, SA2) naar Z wil sturen, versluiert hij dit bericht met de publieke sleutel SZ1 van Z. Persoon A is er nu van verzekerd dat alleen Z het bericht V ({V (B, SA2)}, SZ1) kan ontcijferen, omdat *alleen* Z de geheime sleutel SZ2 kent. Persoon Z zoekt de publieke sleutel van A op en ontcijfert V (B, SA2). Persoon Z is nu in staat om de boodschap B te lezen waarbij tevens het bewijs is geleverd dat persoon A het bericht verzond. Zolang A en Z de inhoud van het bericht B niet aan derden prijsgeven, kent niemand de inhoud van de boodschap (privacy). Op zijn beurt kan Z een bewijs van ontvangst naar A sturen.
Door nog een eigenschap op te leggen is het mogelijk een geheel nieuw elektronisch betalingssysteem te definiëren. In dit systeem is het onder meer ondoenlijk om later te achterhalen wie het ontvangen geld heeft uitgegeven; het is echter wel mogelijk te bewijzen dat het geld werd overgemaakt. Ook kan met dit systeem een elegante manier van elektronisch stemmen tijdens verkiezingen worden verkregen. Beschrijving hiervan voert in dit artikel helaas te ver. In ieder geval is het duidelijk hoe ingenieus en belangrijk asymmetrische algoritmen zijn.

Een asymmetrisch algoritme dat alle hiervoor genoemde eigenschappen bezit is gebaseerd op het zogenaamde RSA algoritme[4]), genoemd naar de ontwerpers ervan: Ronald Rivest, Adi Shamir en Leonard Adleman.

Sleutelbeheer

Sleutelbeheer is een van de meest verwaarloosde onderwerpen in veel artikelen over cryptologie. Ten onrechte, maar wel begrijpelijk. Het onderwerp zal ook hier onvolledig beschreven worden omdat beschrijven van het

sleutelbeheer om diepgaande kennis van uiteenlopende methoden vraagt. Sleutelbeheer is tevens sterk afhankelijk van de toepassing, in dit geval de omgeving waarin het gebruikt wordt (elektronische post, toegangscontrole, satellietverkeer). Sleutelbeheer speelt een zeer belangrijke rol bij het vaststellen van de te gebruiken sleutel. Hierbij moeten ook de geheimhouding en onschendbaarheid van de sleutel worden gewaarborgd. Zoals opgemerkt is bij symmetrische systemen de geheimhouding van de gebruikte sleutel van essentieel belang voor de geheimhouding van de boodschap. Indien een vercijferde boodschap na ontvangst direct wordt ontcijferd, kan de gebruikte sleutel hierna worden vernietigd. In de situatie dat een boodschap gedurende langere tijd vercijferd wordt opgeslagen, is het van essentieel belang dat ook de gebruikte sleutel veilig wordt bewaard. Dit leidt al snel tot organisatorische problemen.
Het klinkt tegenstrijdig, maar in de cryptologie wordt er altijd van uitgegaan dat het cryptografisch algoritme bekend is. Geheimhouden van nieuwe algoritmen verhoogt de veiligheid slechts gedurende een korte periode. Dit is niet uitsluitend aan lekken in de organisatie te wijten, maar ook aan de vindingrijkheid van de crypto-analist. De crypto-analisten vinden vaak andere wegen om geheimschriften te breken. Het Japanse cryptografisch systeem Purple werd bijvoorbeeld gebroken zonder kennis van het systeem. David Kahn[5]) beschrijft op voortreffelijke wijze de rol van de crypto-analyse in de geschiedschrijving, maar vanuit een Amerikaanse optiek! De crypto-analyse wordt in het algemeen bemoeilijkt naarmate minder vercijferde tekst beschikbaar is. Hieruit mag worden geconcludeerd dat bij gebruik van slechts één enkele sleutel, de cryptonalist in de kaart wordt gespeeld. Het wisselen van de sleutel is dus aan te bevelen. Sleutelprotocollen zorgen hiervoor en houden bij welke sleutel wordt gebruikt, en wanneer deze moet worden vervangen. Vervanging van sleutels is afhankelijk van verschillende omstandigheden:
- tijd;
- hoeveelheid vercijferde data;
- ontvanger;
- boodschapklasse.

Toelichting
Onder *tijd* wordt de vercijfertijd verstaan waarbij liefst na een willekeurig aantal seconden de sleutel wordt vervangen. Dit geldt ook na verzending van een *willekeurige hoeveelheid* vercijferde data. Het spreekt vanzelf dat na verwisseling van *ontvangers* ook de sleutels moeten worden vervangen. Daarnaast geeft de *boodschapklasse* aan hoe belangrijk de te vercijferen

informatie is, dit heeft direct invloed op de eerdergenoemde parameters: tijd en hoeveelheid. De boodschapklasse heeft echter ook invloed op cryptografische algoritmen. Zo zal de Amerikaanse National Security Agency (NSA) niet langer op DES gebaseerde cryptografische produkten voor regeringsgebruik aanbevelen[6]), hetgeen betekent dat voor hoog-geclassificeerde boodschappen DES niet meer zal worden gebruikt. Een van de eenvoudigste methoden om sleutels te verwisselen op een lijnverbinding, is definiëring van de sleutelhiërarchie. Bijvoorbeeld een lijnsleutel (LS) installeert steeds een nieuwe sessiesleutel (SS). De SS wordt vervolgens gebruikt voor de dataversluiering en de LS alleen voor het installeren van een nieuwe SS. Omdat de SS een willekeurig getal is, kan de crypto-analist deze niet breken met taalkenmerken, een aanzienlijke verhoging van systeembeveiliging. Het is hier belangrijk op te merken dat de LS niet op dezelfde manier gebroken mag worden als de SS, omdat anders een zogenaamd *domino-effect* ontstaat. Bij het domino-effect geldt: als SS kan worden gebroken, kan ook LS worden gebroken. De sleutel LS moet zich dus op een hoger beveiligingsniveau bevinden dan de SS. Dit is bijvoorbeeld te realiseren door de LS langer te maken dan de SS, of door een sterkere vercijfermethode voor het overbrengen van SS dan voor het versluieren van de data. De vraag blijft: ,,Wat is sterker, en na hoeveel tijd moet de sleutel worden vervangen?''. Naast het leveren van een nieuwe sleutel, is het ook van belang te weten of de te gebruiken sleutel echt is. Er moet een soort waarmerk van herkomst zijn. Dit waarmerk kan bijvoorbeeld met een asymmetrisch algoritme worden verkregen, maar ook hier ontstaat een vraag: ,,Is de te gebruiken (publieke) sleutel niet vals?''. Het is duidelijk dat er steeds personen of instanties moeten worden vertrouwd. Het probleem is alleen op te lossen in wederzijds vertrouwen. Alleen dan kunnen verbindingen worden gemaakt (eventueel via verschillende instanties).

One-way functies

Zonder de beschreven beveiligingsmethoden was het bestaan van zogenaamde *one-way functies* niet mogelijk. Daarom is het nu tijd om aandacht te besteden aan een van de waarschijnlijk belangrijkste functies in de cryptografie.
In het algemeen is een functie (f) een soort voorschrift of computerprogramma dat voor een toegestane invoer x een resultaat of uitvoer y berekent. Afhankelijk van de karakteristieke eigenschap van f kunnen resultaten en uitvoer worden onderverdeeld in groepen. De functie f wordt een one-way functie genoemd als de uitkomst y (vaak als f (x) genoteerd) echter

is gegeven, moet het onmogelijk of ondoenlijk zijn om de invoer of startwaarde x te bepalen. Een meervoudige one-way functie is de zogenaamde pariteitsfunctie. Voor een getal geldt dat het even pariteit bezit als de som van de cijfers even is. Voor een binair getal komt dit overeen met het tellen van het aantal enen. De pariteit y = 1 als het aantal enen oneven is en y = 0 als het oneven is. Bijvoorbeeld als x = 10111, dan is de pariteit y = f (x) = f (10111) = 0, daarentegen is f (10011) = 1. Het is duidelijk dat het *onmogelijk* is om vanuit y weer x te bepalen.
Een andere one-way functie is het in factoren ontbinden van een groot getal. Het is eenvoudig om vanuit bijvoorbeeld twee gegeven priemgetallen (getallen die alleen door 1 of zichzelf deelbaar zijn) het produkt te bepalen: 47 × 61 = 2867. Het is moeilijker om vanuit het getal 2867 de twee priemgetallen te bepalen. Als de getallen groter worden kunnen we hiervoor de hulp van een computer inroepen. Als de getallen erg groot zijn, bijvoorbeeld 100 cijfers, is het zelfs met behulp van de snelste computer ter wereld *ondoenlijk* om de twee priemgetallen te bepalen (het kost ettelijke eeuwen computertijd). Een one-way functie wordt in computersystemen gebruikt om de passwords op te slaan. Tijdens het intikken van een password wordt de waarde y = f (password) berekend. Het resultaat y wordt vergeleken met de onder naam opgeslagen waarde van y. De waarde y mag dus bekend zijn, omdat het onmogelijk of ondoenlijk is vanuit y het originele password te bepalen. Dit sluit echter niet uit dat er een ander password bestaat dat dezelfde waarde y oplevert. Bij sommige one-way functies is het een eis dat dit niet mag voorkomen.
Een andere toepassing komt overeen met het toevoegen van de waarde y aan een bericht. Van de pariteitsfunctie is bekend dat iedere boodschap x met daaraan toegevoegd de pariteit y, een even aantal enen moet bevatten. Bijvoorbeeld als x = 101, dan is y = 0. Is dit niet het geval, dan is duidelijk dat het bericht verminkt is. Door het toepassen van speciale one-way functies is het mogelijk de onschendbaarheid (de echtheid van het bericht) met te verwaarlozen onzekerheid vast te stellen. Dit is o.a. van belang bij het opslaan of overdragen van belangrijke gegevens in een computersysteem.

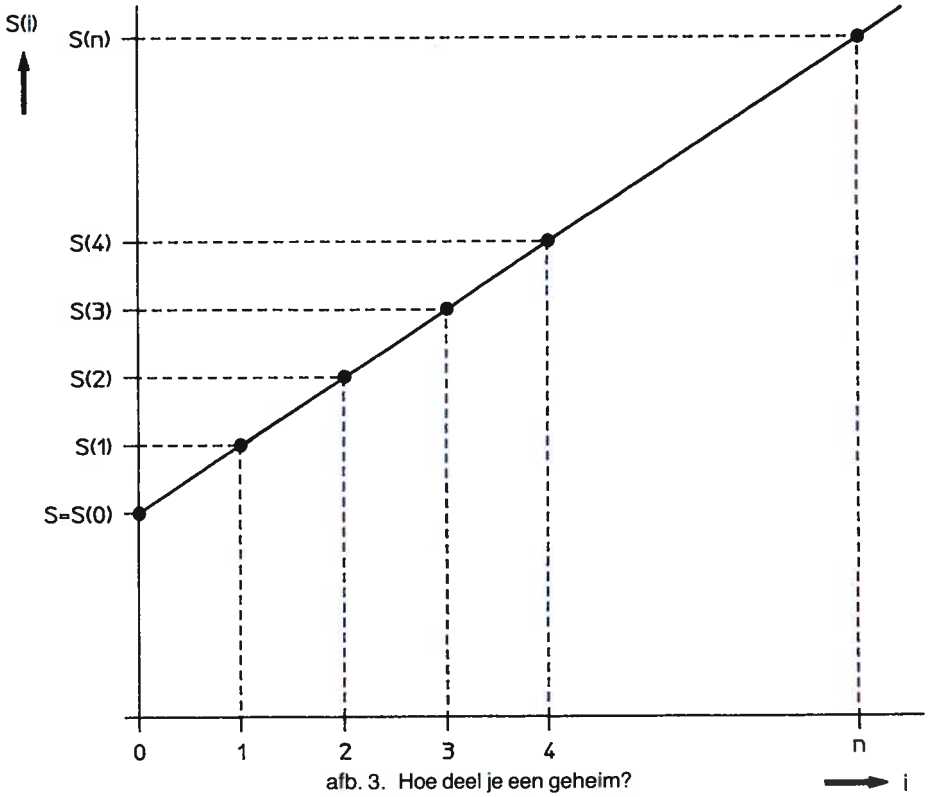
Sleutelonafhankelijke one-way functie
In de situatie dat iedere gebruiker een unieke one-way functie moet bezitten, moet op eenvoudige manier kunnen worden bepaald welke gebruiker welke functie bezit. Om de juiste functie voor individuele gebruikers te selecteren wordt gebruik gemaakt van een gebruikerssleutel. De gebruikerssleutel geeft aan welke functie een gebruiker bezit. Dit probleem kan worden

opgelost met een speciale one-way functie. Iedere gebruiker krijgt in dit geval een unieke sleutel toegewezen en houdt de sleutel geheim. Stel dat de geheime sleutel S opgedeeld kan worden in twee deelsleutels S1 en S2, dan kan worden volstaan met een enkele one-way functie en wel als volgt: $y = f(x + S1) + S2$ (merk op dat de functie f publiek bekend mag zijn). Meer algemeen staat hier $(g(x, S) = f(x + S1) + S2$. Daarom wordt g een *sleutelafhankelijke one-way functie* genoemd.
Bij mobiele communicatie kan van een sleutelafhankelijke one-way functie gebruik worden gemaakt om de identiteit van de abonnee vast te stellen.[7]) Iedere abonnee krijgt een eigen geheime sleutel toegewezen. De abonnee moet bij het begin van een gesprek bewijzen dat de geheime sleutel in zijn bezit is. De centrale stuurt hiervoor een willekeurig getal naar de abonnee. De abonnee bepaalt vervolgens $y = g$ (getal, sleutel) en stuurt het resultaat y terug. De centrale verifieeert het ontvangen resultaat met het in de centrale berekende resultaat. Afhankelijk van het vergelijkings-resultaat wordt de verbinding verbroken of opgebouwd. Een belangrijke voorwaarde is wel dat meeluisteraars niet in staat mogen zijn uit de opgevangen x en y en het bekend zijn van de functie g de geheime sleutel van de abonnee te bepalen. Bij het vaststellen of de functie g voldoet, komt de crypto-analyse weer in actie. Een 2e eis is dat het voor de illegale gebruiker niet lonend mag zijn om de waarde y te gokken. Met andere woorden de kans op succes bij gokken moet verwaarloosbaar zijn (na gemiddeld een miljoen maal gokken mag de meeluisteraar één keer succes hebben. Roulette spelen is in vergelijking hiermee meer winstgevend: kans 1/35. Een derde eis is dat het niet uitvoerbaar moet zijn om een lijst op te stellen met corresponderende x en y paren.

Naast de voorgaande functies bestaan er ook een aantal one-way functies, waarbij het met wat extra informatie wel mogelijk is om vanuit het resultaat y de waarde van x te bepalen. Zonder de extra informatie blijft het echter onmogelijk om achter de waarde van x te komen. Dit soort functies worden *one-way trapdoor functies* genoemd. Er is als het ware een achterdeur om de juiste waarde van x te leren kennen. Een bijzondere one-way trapdoor functie is een functie waarbij voor iedere toegestane invoer x, het resultaat y berekend kan worden en omgekeerd (dat wil zeggen als $g(a, S) = g(b, S)$, dan is $a = b$). Dit soort functies kwam aan de orde bij de asymmetrische systemen. Het is dan ook precies wat met een publiek sleutelsysteem wordt bedoeld. Door achterhouden van informatie (geheimhouding) is het voor buitenstaanders onuitvoerbaar om achter de inhoud van berichten te komen.

Hoe deel je een geheim?

Geheimhouding is van essentieel (levens)belang. In een aantal gevallen mag de veiligheid van het systeem niet afhangen van slechts één gebruiker. Een kluis mag bijvoorbeeld alleen worden geopend in aanwezigheid van tenminste twee personen. Ter illustratie het volgende voorbeeld.
Een rechte lijn wordt uniek vastgelegd door twee punten. Dat wil zeggen als twee punten van een rechte lijn bekend zijn, dan kan de lijn worden getekend. In afb. 3 is de grafiek van een lijn getekend. De gebruikers zijn genummerd met 1, 2, 3, 4, . . ., n. De deelsleutels S(i) corresponderen met de persoon i, dus persoon 1 bezit deelsleutel S(1) en persoon 2 bezit deelsleutel S(2). Door nu S(0) gelijk te stellen aan de te gebruiken sleutel S, is het altijd mogelijk om bij aanwezigheid van minimaal twee personen de lijn te tekenen en het snijpunt van de lijn met de y-as S(0) = S te bepalen. In de praktijk komt het er op neer dat een computer uit de ingevoerde gegevens de sleutel S bepaalt. Het bepalen van de S is onmogelijk als er slechts 1 persoon aanwezig is.



afb. 3. Hoe deel je een geheim?

Tot slot

Dit artikel trachtte de cryptologie uit de geheimsfeer te halen. Cryptologie is waarschijnlijk het op één na oudste beroep ter wereld en kent daarom een rijke, soms exotisch verleden. Het breken van oude vercijfersystemen valt vaak tegen, daarvoor moet grote kennis van zaken in de strijd worden geworpen in de vorm van crypto-analyse. Tevens wil ik een misvatting rechtzetten: *computerkrakers zijn geen cryptonalisten*! Het analyseren van een geheimschrift is iets geheel anders dan het inbreken in een computersysteem. De toegeschreven vindingrijkheid aan computerkrakers is vaak niets anders dan laksheid of medeplichtigheid van gebruikers of de opzet van computer-(operating)systemen.
Systeembeheerders worden hierdoor met de rug tegen de muur geplaatst. Verder worden door kostenfactoren, tijdgebrek en het toetsen van enig gebruikersgemak compromissen gesloten. In goed beveiligde systemen is het vrijwel onmogelijk op de informatie in te breken. Cryptologie is een niet te onderschatten hulpmiddel bij systeembeveiliging. Helaas is systeembeveiliging vaak sluitpost op de rekening tijdens het definiëren van nieuwe systemen. Wie is de schuldige? De fabrikant, de systeembeheerder of de klant?
Naast het beveilgen van systemen biedt cryptologie ook mogelijkheden voor alternatieve handtekeningen en bewijsvormen. Met behulp van de cryptologie kan worden vastgelegd of informatie al dan niet moedwillig veranderd, verwijderd of tussengevoegd is. Identificatietechnieken zoals toegangscontrole en registratie kunnen effectief worden gerealiseerd.
Daarnaast vindt cryptologie toepassing in elektronische betalingssystemen, elektronisch stemmen en elektronische post. Echter voordat er drastische wijzigingen komen in bijvoorbeeld het hedendaagse betalingscircuit, zal het gebruik van cryptologie toch eerst gemeengoed moeten worden om het vertrouwen van de gebruikers te wekken. Opdat dan de vraag: ,,Cryptologie, wat doe je ermee?'' tot het verleden behoort.

Literatuuropgave

1) Haslach, R. D., Nishi No Kaze, Hare, Van Kampen & Zn./Uniboek B.V., 1985.
2) FIPS Publication 46, Data Encryption Standard, National Bureau of Standards, U.S. Dept. of Commerce, Washington DC, 1980.
3) Diffie, W. en M. E. Hellman, New Directions in Cryptography, IEEE Trans. Inf. Theory, Vol. IT-22, No. 6, blz. 644-654, 1976.
4) Rivest, R. L., A. Shamir en L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Commun. ACM, Vol. 21, nr. 2, blz. 120-126, 1978.
5) Kahn, D., The Codebreakers, the story of secret writing, Macmillan Comapany, New York, 1967.
6) Dienstreisverslag 1422 DNL/86.
7) Memorandum 1490 DNL/87.

Licht gaat niet altijd met lichtsnelheid

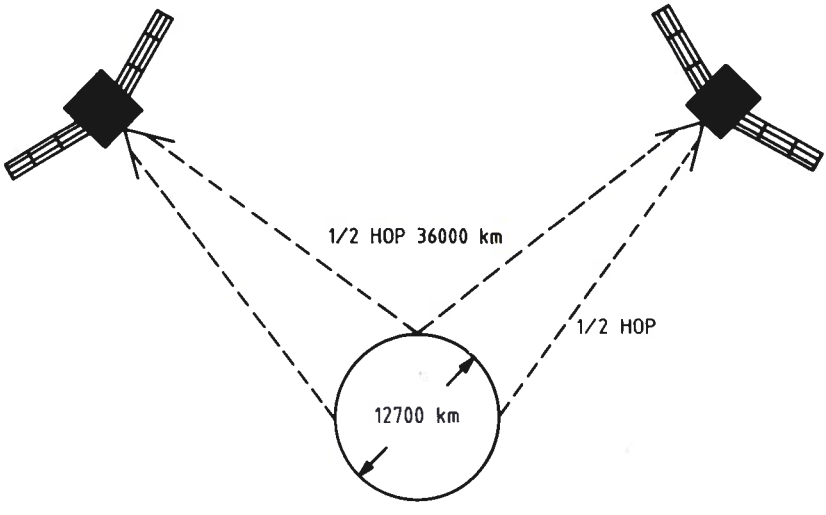
drs. C. Vader

Licht is net als micro- en radiogolven een vorm van elektromagnetisch energietransport. In een optisch ijl medium, dat is in de lucht en in de ruimte, reist de energie met de lichtsnelheid, waarvan velen weten dat deze 300 000km/s is, ruim een miljard km per uur.

Niet algemeen bekend is dat het licht in optisch dichte media, zoals water of glas, met een heel wat lagere snelheid reist dan in de lucht of in de ruimte. In glas is de snelheid van het licht ongeveer $^2/_3$ x de lichtsnelheid, in water ongeveer $^3/_4$. De conclusie hieruit is dat optische transmissie door glasvezelkabel niet met de lichtsnelheid gaat, maar met de snelheid van het licht in glas, dus 200 000 km per s! Satellietverkeer met zijn lange vertragingstijden (ongeveer 1 s) gaat wel met lichtsnelheid; de vertraging is het gevolg van de lange afstanden, 72 000 km tot 80 000 km per hop en een veelvoud daarvan bij meer dan één hop (zie afb. 1).

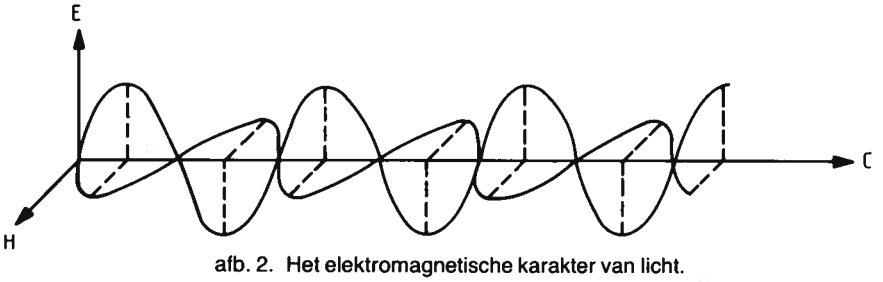
Breking van het licht (zie afb. 2)

De lichtgolf is een wisselveld met een frequentie van gemiddeld 5 x 10^{14} Hz, bestaande uit een elektrische (E)-component en een magnetische (H)-com-



afb. 1. Transmissie met 2 hops om de andere kant van de wereld te bereiken.

ponent. De componenten staan onderling loodrecht op elkaar en beide staan loodrecht op de voortplantingsrichting (zie afb. 2).
Bij radiofrequenties kan de magnetische component belangrijk zijn, denk aan de Ferriet-antenne. Bij hogere frequenties is er vooral interactie met de elektrische component. De elektronen die de lichtgolf op zijn weg ontmoet, deinen mee in het ritme van de frequentie. Zijn deze elektronen plaatsgebonden, zoals in isolerend materiaal, dan is de invloed hiervan een verlaging van de voortplantingssnelheid. Vaak zijn isolerende stoffen lichtdoorlatend. Zijn de elektronen daarentegen vrij en beweeglijk, zoals in metaal, dan wordt hierdoor het binnendringen van elk elektrisch veld verhinderd en dus ook het binnendringen van licht. Metalen laten dan ook geen licht door. Ook het inblikken van voedingsapparaten om geen radiostoring te geven, berust op hetzelfde principe.
De verlaging van de voorplantingsnelheid van licht bij het binnentreden in een isolerende stof komt tot uiting in het verschijnsel lichtbreking, de verandering van de voortplantingsrichting bij overgang van het ene medium naar het andere (zie afb. 3).



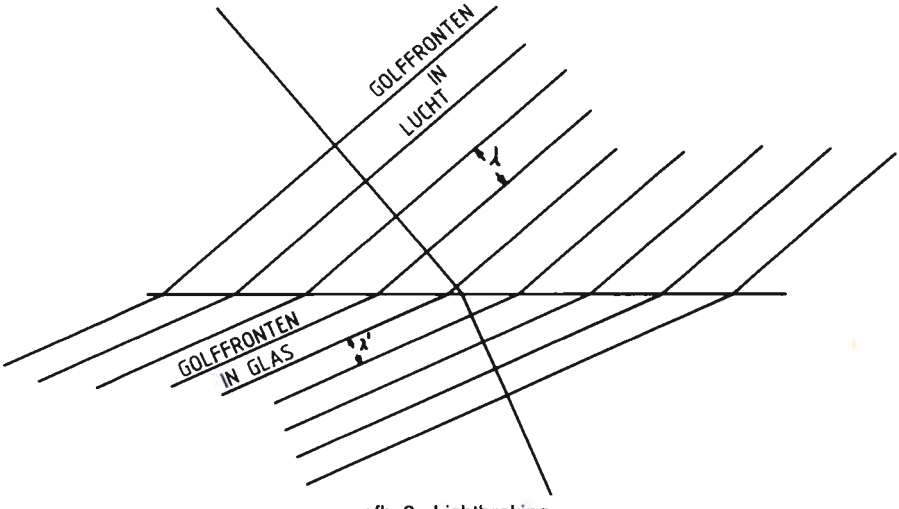
afb. 2. Het elektromagnetische karakter van licht.

Door de lagere voortplantingssnelheid in het optisch dichte medium (water of glas wordt de golflengte kleiner dan in lucht, want de frequentie blijft onveranderd (zie afb. 3).

De golflengte is $\lambda = \frac{c}{f} = \frac{\text{voortplantingssnelheid}}{\text{frequentie.}}$

Aan het grensvlak verspringen de golffronten niet en op afb. 3 is te zien dat hierdoor de stand van de golffronten verandert en daarmee ook de voortplantingsrichting. Is c de lichtsnelheid en c' die in glas, dan is de brekingsindex $n = \frac{c}{c'} = \frac{\lambda}{\lambda'}$.

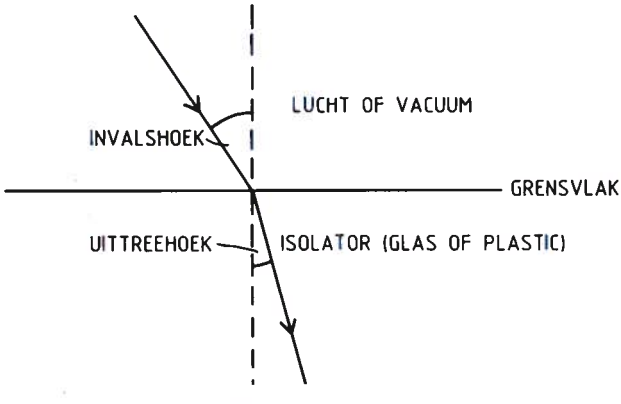
De brekingsindex is een materiaalconstante, die tevens frequentie-afhankelijk is. In het ultra-violet (UV)-gebied verdwijnt bij de meeste stoffen het lichtbrekend vermogen en maakt plaats voor absorptie (demping). Bij glas is



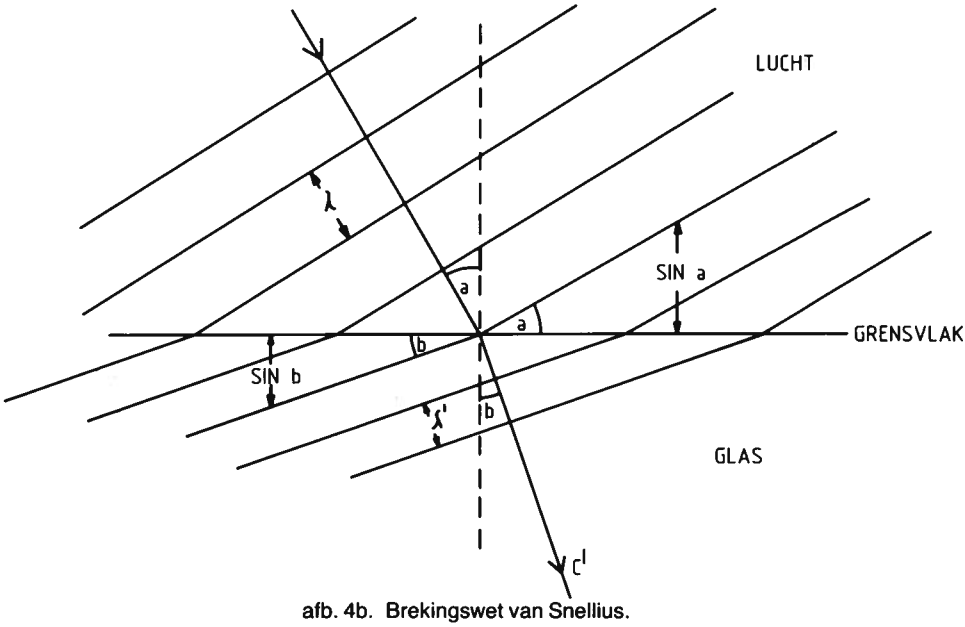
afb. 3. Lichtbreking.

n ongeveer 1,5 met kleine variaties, afhankelijk van de glassoort. Is a de intreehoek (zie afb. 4a + b) en b de uittreehoek, dan is de brekingsindex $N = \frac{\sin a}{\sin b}$.

Dit is de Brekingswet van Snellius (Leidse wiskundige 1591-1626). Deze formule is ook te schrijven als sin a = n. sin b. Dit gaat goed totdat n. sin b = 1; als sin b groter wordt dan $\frac{1}{n}$, dan wordt de straal niet meer doorgelaten, doch gereflecteerd aan het grensvlak. Toch is er geen scherpe grens tussen doorlaat en reflectie, want hoe groter hoek b wordt, hoe groter



afb. 4a.

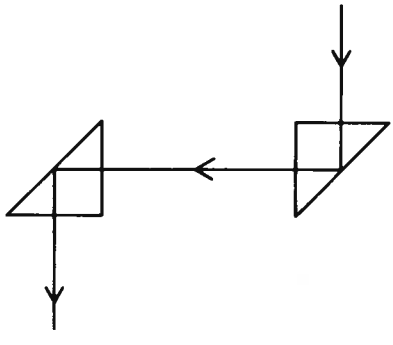


afb. 4b. Brekingswet van Snellius.

deel van het licht gereflecteerd wordt en hoe minder doorgelaten, totdat vanaf sin b = $\frac{1}{n}$ niets meer wordt doorgelaten en alles gereflecteerd.

Hoek b met sin b = $\frac{1}{n}$ heet de grenshoek of glanshoek.

Hoe loodrechter het licht het glas treft, hoe beter het wordt doorgelaten; denk bijvoorbeeld aan de gebogen autoruiten en de bolle voorruit die 25 jaar geleden bij autobussen in de mode was. Van de reflectie bij grote invalshoeken wordt nuttig gebruik gemaakt bij prisma-optiek, zoals die voorkomt bij kijkers, fotocamera's en periscopen (zie afb. 5).



afb. 5. Prisma-optiek.

Telecom '87

R. Scholma

De Internationale presentatie van PTT

Van 20 t/m 27 oktober 1987 vindt in Genève (Zwitserland) een internationale presentatie op (tele-)communicatiegebied, plaats in Genève (Zwitserland).
Telecom '87 is een internationale vakbeurs waar eens per 4 jaar grondig inzicht kan worden verkregen in de ontwikkelingen op telecommunicatiegebied. De Nederlandse PTT neemt hier voor de eerste keer aan deel.

Het doel van iedere deelnemende organisatie is internationale presentatie en het leggen van contacten. Goed beschouwd houdt dit nauw verband met de kwaliteit die organisaties willen uitdragen. Presentatie en functionaliteit (vorm en inhoud) moeten met elkaar in overeenstemming zijn, zeker in een tijd waar klanten functionaliteit van organisaties willen ervaren.
Deelnemen aan iedere beurs is een uitdaging die niet vrij is van risico's. Werknemers van de verschillende organisaties moeten immers tot lang na de presentatie waarmaken wat tijdens de beurs werd uitgedragen!

Toegankelijkheid, rust en vertrouwen

De snelgroeiende communicatiebehoeften van de samenleving confronteren organisaties intern met problemen die om korte-termijnoplossingen vragen. Enkele voorbeelden:
- opleidingen blijven achter op de technologische ontwikkelingen, ook in landen als de Verenigde Saten van Amerika en Japan waarvan toch wordt gezegd dat zij de internationale voorlopers zijn;
- reorganisaties, o.a. noodzakelijk voor effectieve marktbenadering, doen een dringend beroep op creativiteit, vindingrijkheid en flexibiliteit van de werknemers. Vertrouwde cultuurelementen moeten worden doorbroken, hetgeen om groot aanpassingsvermogen vraagt.

Technologische ontwikkelingen dwingen PTT-organisaties ertoe zich extern te profileren als snelle en betrouwbare informatie-transporteurs. Nadat het besluit, deel te nemen aan Telecom door de hoofddirecteur Commerciële Zaken Telecommunicatie was genomen, startte een stuurgroep onder leiding van ing. G. J. van Velzen (plv. hdr CZ). Een beursprogramma werd ontwikkeld en een eisenlijst voor de stand werd opgesteld. Het resultaat van deze uitbestede arbeid is een zeer toegankelijke stand (zie

omslagfoto). De gekozen kleurencombinatie doet de PTT-stand overkomen als een *Eiland van rust temidden van de woeste golven* (vrij naar het Saevis Tranquilis in Undis, de wapenspreuk van Willem van Oranje).
Het geraffineerde lijnenspel van de totale constructie getuigt van snelheid en suggereert op hetzelfde moment vertrouwen (openheid en privacy). Zo ontstond vanuit een gedachte de vorm die onze organisatie internationaal wil uitdragen.

Telecommunicatie: maatwerk met haken en ogen

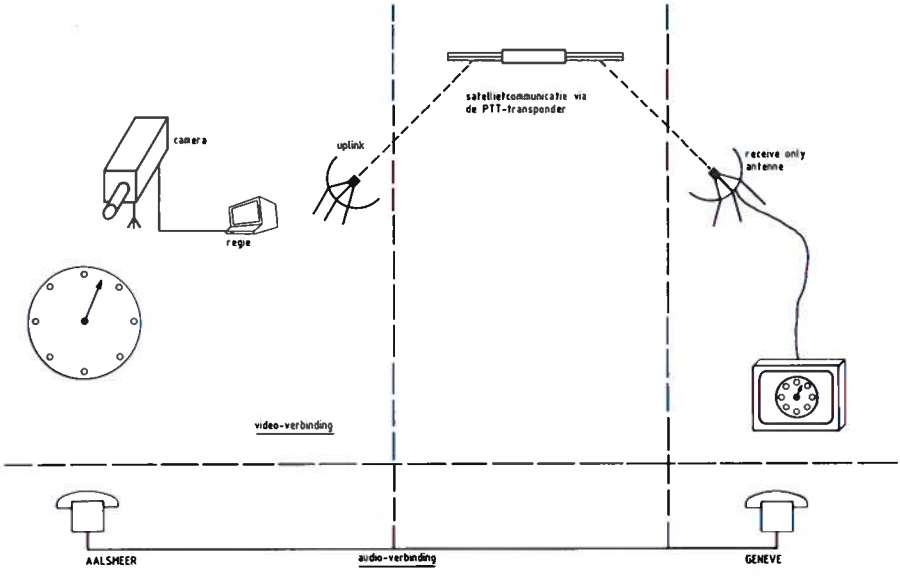
Telecommunicatiebehoeften van klanten beslaan in algemene zin alle mogelijkheden die de techniek voor informatie-overdracht kan bieden:
- spraak;
- tekst;
- beeld;
- data.

Omdat iedere gebruiker zijn eigen specifieke wensen heeft, is het niet verwonderlijk dat de vraag naar op *maat gesneden* netwerken toeneemt.
Keuze tussen een maatkostuum of een confectiepak is afhankelijk van de eisen die afzonderlijke bedrijven aan hun communicatiebehoeften stellen. De eisen die multi-nationals stellen aan de mogelijkheden en kwaliteiten van communicatie-apparatuur zijn bijvoorbeeld niet vergelijkbaar met die van kleinschaliger bedrijven.
Van PTT wordt echter beantwoording van de eisen door beide groepen verwacht.

Communicatie is primair
PTT-Telecommunicatie speelt een onmisbare rol in de wereld van informatie-overdracht. Internationaal beweegt handelsinformatie zich voor het grootste deel over telecommunicatie-infrastructuren. In vergelijking met het fysieke transport per vliegtuig of vrachtwagen, is informatietransport voor velen een abstract gebeuren. Kwaliteitseisen van klanten zijn overwegend gericht op transportsnelheid, betrouwbaarheid, privacy, gebruikersvriendelijkheid van de apparatuur en de service.
Aan PTT-Telecommunicatie om de gevraagde mogelijkheden technisch te realiseren. Voor klanten is communicatie primair, niet de techniek!

Het imago van Nederland
Bloemen bepalen overal ter wereld het gezicht van Nederland, dat bekend

staat als het grootste bloemen-exporterende land. De bloemenhandel geeft forse injecties aan de Nederlandse economie. Wist u bijvoorbeeld dat Arabische landen voor vele tienduizenden guldens per maand aan *frische Schnittblumen aus Holland* importeren?
Treedt tijdens het transport stagnatie op waardoor bloemen verwelkt hun plaats van bestemming bereiken, dan verliest Nederland een zorgvuldig opgebouwd imago. De invloed daarvan is direct, en in negatieve zin, op de economische thuismarkt voelbaar.
Bij het transport van aan bederf onderhevige produkten is goede coördinatie van groot belang. Recent was tijdens de televisie-uitzending over het 100-jarig bestaan van de coöperatieve groenten- en fruitveiling de, voor buitenstaanders onbegrijpelijk, nerveuze communicatiesfeer waarneembaar.
In- en verkoop, evenals de regeling voor het transport, vinden per telefoon vanuit de veilingboxen plaats. De veiling moet nu nog worden bezocht om te kunnen handelen. Nu nog, want het kan ook anders.



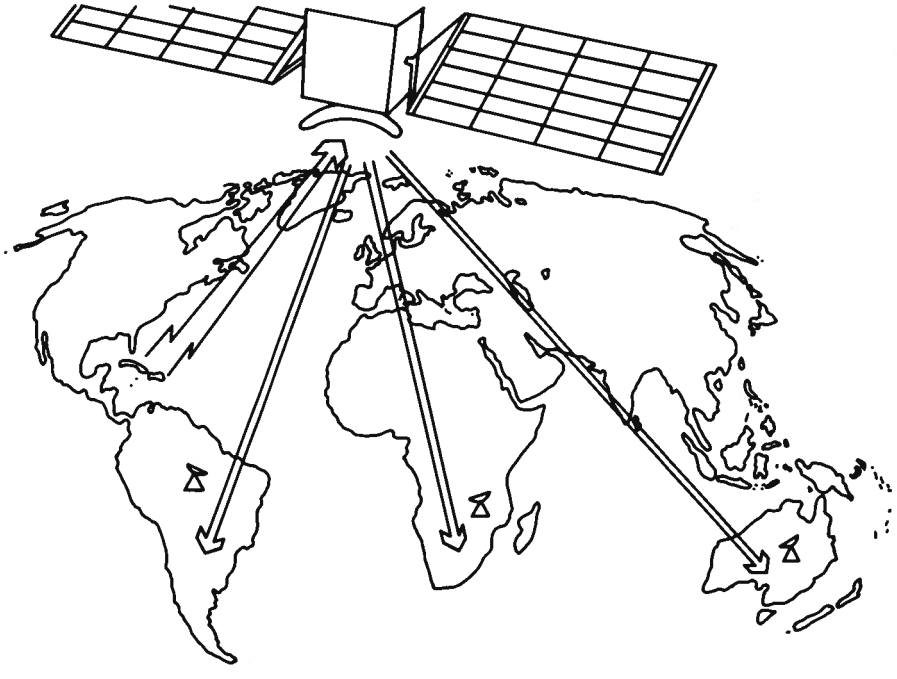
afb. 1. Het Tele-Event-experiment tussen Aalsmeer en Canada.

Tele-Events

Tijdens Telecom '87 vinden 4 Tele-Events per dag vanaf de Aalsmeerse bloemenveiling plaats. Op de lokatie Aalsmeer houdt een camera de afslagklok gevangen. In Genève zien deelnemers aan dit Tele-Event-experiment de klok op een beeldscherm. Hoe de verbinding tot stand komt, toont afb. 1.

Bij een Tele-Event is naast beeldoverdracht een telefoonverbinding onontbeerlijk. In Genève wordt het verloop van de afslag op het beeldscherm gevolgd en kan de klok vanuit Genève ook worden stilgezet. Per telefax kan dan worden doorgegeven waar de gekochte goederen moeten worden afgeleverd.
Als de deelnemers straks, op Telecom '87, de afslagklok stilzetten op een voor hun gunstige afslagprijs voor een bos bloemen, worden deze direct na de veiling op verschillende plaatsen van bestemming bezorgd. KLM en PTT-Post verzorgen het transport. De staat van versheid zal vertelt of er een kink in de transportweg is ontstaan.
„Zeg het met bloemen''; wie had ooit gedacht dat dit ook iets over de kwaliteit van PTT-Telecommunicatie zou zeggen?

De andere Tele-Events betreffen interactieve beeldverbindingen die betrekking hebben op het Rotterdamse Havenbedrijf, KLM, Schiphol, Teleport Amsterdam en de rol die PTT-Telecommunicatie daarbij speelt. Deze beursonderdelen staan in het teken van *Nederland, Transport en Distributieland.*



afb. 2. De mogelijkheden van Tele-Events zijn in principe onbeperkt.

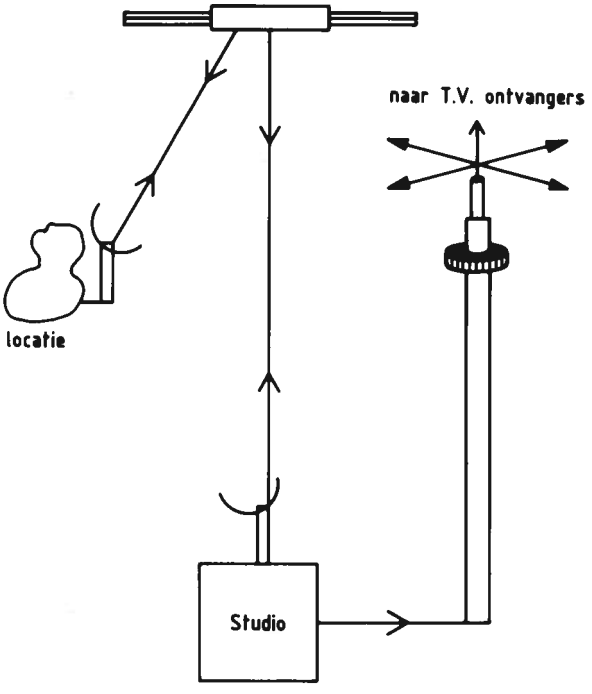
Tijdens de Tele-Events vanuit Aalsmeer is er sprake van 1 ontvanger; de beurs in Genève. Voor alle duidelijkheid moet worden vermeld dat in principe geen beperkingen voor het aantal ontvangers bestaat. Afb. 2 geeft de mogelijkheden weer.
Het vraagt weinig voorstellingsvermogen om te bedenken dat op nationaal niveau ons eigen NETWERK op deze manier live kan worden uitgezonden. Is dat geen aardig idee voor de nieuwjaarstoespraak van de directeur-generaal? Toepassing van Tele-Events in de eigen organisatie kan ook nuttig zijn voor trainingen en opleidingsprogramma's.
Toekomstgedachten? In ieder geval zijn ze technisch reeds nu te realiseren. De markt is in beweging. Internationaal dwingt dit tot reactie op de nationale markt: het is goed te weten dat PTT met Tele-Events voorloper op de markt is geworden.

Telegration

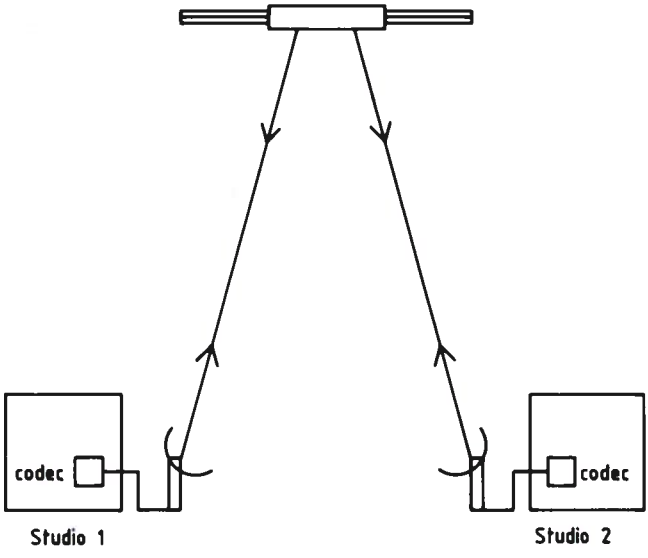
De ontwikkeling van Telegration (integratie van communicatiemogelijkheden en -middelen) stelt niet alleen eisen aan techniek. Politieke, juridische en economische belangen spelen een grote rol bij opzet en beheer van telecommunicatie-netwerken. Voor klanten is naast technische mogelijkheden en kwaliteit de tariefstelling van groot belang; investering moet in verantwoorde verhouding tot opbrengst staan. Voor de internationale PTT's levert dit een aantal problemen op. Als dienstverlenende organisaties moeten zij voorkomen dat telecommunicatie een elite-aangelegenheid wordt. Aan de andere kant blijft de vraag of het redelijk is om grootgebruikers hetzelfde tarief te berekenen als particuliere gebruikers.
Tijdens Telecom '87 wordt slechts een deel van alle mogelijkheden getoond. Het zijn de experimenten met Tele-Events. Om een helder beeld van de ontwikkelingen te krijgen wordt hierna het verschil tussen Video-Conferencing omroep en Tele-Events beschreven.

Video-Conferencing (VC)
Video-Conferencing is een vergadermethode waarbij besparing een belangrijke rol speelt (zie afb. 3a). Video-Conferencing vanuit openbare VC-ruimten kost *f* 2 000,— per uur binnen Europa en *f* 3 500,— per uur voor vergaderingen met de Verenigde Staten en Canada. Directe besparingen voor gebruikers zijn reis- en verblijfkosten, terwijl indirect tijd wordt bespaard; gelet op de huidige kosten van arbeidsuren is dit een niet geringe besparing. De huurprijzen voor VC zijn voor bedrijven en particulieren een verantwoorde investering. Het verantwoord rendement zou echter nooit zijn bereikt zonder signaalcompressie-techniek.

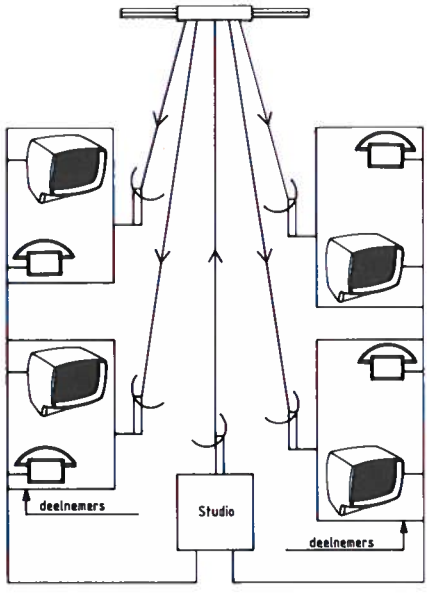
Video-Conferencing is tot op zekere hoogte te vergelijken met live TV-uitzendingen (zie afb. 3b). Tot op zekere hoogte, want TV-kijkers (deelnemers) kunnen niet actief aan de uitzending deelnemen. Een ander verschil tussen VC en TV is de beelddynamiek. Om bij VC dezelfde beelddynamiek te realiseren als bij TV is een digitaal signaaltransport van 140 Mbit/s vereist. De kosten van een dergelijk signaaltransport vragen van gebruikers een te grote investering. Het Dr. Neherlaboratorium (DNL) ontwikkelde in samenwerking met andere PTT's daarom een bijzondere codec. Met deze codec wordt het signaal gecomprimeerd tot 2 Mbit/s.
Signaalcompressie leidde tot tariefbeheersing van zowel Video-Conferencing als Tele-Events. Zo blijkt dat communicatie voor klanten weliswaar primair is, maar dat verantwoorde communicatie onmogelijk is als de technische deskundigheid bij de netwerkbeheerder ontbreekt. (Zie voor de verschillen tussen omroep, Tele-Events en Video-Conferencing de afbeeldingen 3a, b en c.)



afb. 3a. **Omroep:** geen interactie tussen deelnemer(kijkers) en studio.



afb. 3b. **Video Conferencing:** interactief beeld en geluid.



afb. 3c. **Tele-Event:** interactief video spraak- en tekstoverdracht m.b.v. telefoon of telefax.

Tot slot

Telecom wordt eenmaal per 4 jaar door de *International Telecommunications Union* (ITU) georganiseerd. Het doel van de ITU is om alle leden te informeren over de laatste ontwikkelingen op het gebied van Telecommunicatie. Dit gebied beslaat niet alleen de techniek, maar ook de rol die telecommunicatie speelt op sociale en economische terreinen. Naast de tentoonstelling is er een forum waar informatie-uitwisseling in vijf parallelsessies plaatsvindt. Aan de 2e sessie levert de hoofddirecteur Telecommunicatie, de heer drs. A. Dek zijn bijdrage met het onderwerp: – Integration of interconnection of Networks and Services: Boundaries between Basic Regulated and Deregulated and/or enhanced Services – (Integratie van interconnectie in het werken en diensten: afbakening tussen gereguleerde basisdiensten en/of hoogwaardige diensten).
Hoe kunnen deelnemende landen beter de ontwikkelingen laten zien dan in filmbeelden? Nederland stuurt een film in voor Golden Antenne '87, een filmfestival waarbij de beste inzending wordt bekroond met de Antenne d'Or (de gouden antenne). Een boekenmarkt maakt Telecom '87 compleet. De Nederlandse inzending is een gezamenlijke uitgave van Nepostel en DNL: Transmissie-aspecten van digitale communicatie-systemen, gescheven door ir. H. Ekkelkamp. Op de boekenmarkt ligt uiteraard de Engelstalige uitgave. Als bijzonderheid is te vermelden dat het boek ook in het Bahassa-Indonesia is verschenen.

De Nederlandse PTT zal zich temidden van 39 deelnemende landen[1]) en een groot aantal bedrijven presenteren onder het Telecom thema Communications Age: Networks and Services for a World of Nations. Deelname van onze organisatie is meer dan een compliment aan de werknemers, het is een uitgesproken vertrouwen dat zij waar zullen maken wat op Telecom '87 wordt uitgedragen.

Noot
1) Australië, België, Brazilië, Bulgarije, Canada, China, Denemarken, de Bondsrepubliek Duitsland en de DDR, Finland, Frankrijk, Groot-Brittannië, Hongarije, IJsland, India, Indonesië, Ierland, Iran, Israël, Italië, Japan, Joegoslavië, Korea, Luxemburg, Maleisië, Nederland, Nieuw-Zeeland, Noorwegen, Oostenrijk, de Philippijnen, Portugal, Saoedi-Arabië, Singapore, Spanje, Tsjechoslowakije, de USSR, De Verenigde Staten, Zweden en Zwitserland.

Nederland Distributieland

Commerciële dienstensector

De economische ontwikkeling is wat betreft de commerciële dienstensector in 1986 gunstig verlopen. De produktie steeg met 3,5% en zal naar verwachting in 1987 nog eens met ca. 3% stijgen. In 1986 is de werkgelegenheid in de commerciële dienstensector fors toegenomen met 41 000 arbeidsjaren en zal in 1987 met naar schatting 22 000 arbeidsjaren toenemen. Daarmee levert de commerciële dienstensector een belangrijke bijdrage aan de groei in de werkgelegenheid.
Ook op langere termijn zal de dienstensector een belangrijke bijdrage aan de werkgelegenheid en toegevoegde waarde moeten (blijven) geven. De beleidsinspanningen in 1988 zullen met name op die terreinen gericht zijn die in verband met hun stuwende karakter van belang zijn voor de totale economische bedrijvigheid. Hierbij valt te denken aan telecommunicatiediensten en distributie.

Informatiebeleid en nieuwe diensten

Bij de voorbereiding van de verzelfstandiging van de PTT is naast de ministers van Verkeer en Waterstaat en van Financiën ook de minister van EZ betrokken. Uitgangspunt voor EZ is dat enerzijds de PTT in staat moet worden gesteld adequaat met de problemen van de invoering van moderne telecommunicatie-infrastructuur om te gaan en anderzijds het bedrijfsleven optimale kansen moet krijgen met name op de markt van randapparatuur en tele-informatiediensten.
Eind 1986 werd het rapport van de Commissie Zegveld afgerond. Hierin wordt geconcludeerd dat integratie van lokale kabelnetwerken en de PTT-infrastructuur op de langere termijn onvermijdelijk is. De integratie dient naar de mening van de Commissie betrekking te hebben op zowel het beheer als de techniek. De eigendomsoverdracht van de lokale kabelnetwerken aan de concessiehouder zal de integratie moeten completeren. Een tweede aanbeveling betreft de organisatie van de integratie. Deze dient op lokaal niveau en zo mogelijk binnen op te richten Lokale Exploitatie Samenwerkingseenheden (LES) gestalte te krijgen. De keuzevrijheid van en de gebruiksmogelijkheden voor de consument dienen hierbij geoptimaliseerd te worden.
In juli 1987 kwamen de resultaten beschikbaar van de evaluatie van de Subsidieregeling Computerdienstverlening 1983. Deze regeling werd per

1 januari 1987 beëindigd. Ruim 90% van de ƒ 43 mln. subsidiegelden kwam ten goede aan produktontwikkeling binnen de computer service-industrie. Het bevorderen van de export van Nederlandse software was een van de doelstellingen van deze regeling. Gebleken is dat 40% van de omzet van de gesubsidieerde produkten in het buitenland werd gerealiseerd. Daarnaast zijn met de regeling 400 arbeidsplaatsen gecreëerd. Mede onder invloed van de regeling is de aandacht voor het speur- en ontwikkelingswerk en produktontwikkeling in de software-industrie de laatste jaren toegenomen. De regeling heeft een belangrijke signaalfunctie vervuld voor de bedrijfstak. Tenslotte zal in het kader van de Technologie Stimulering 1987 ondersteuning worden gegeven aan haalbaarheidsstudies en demonstratieprojecten in de software branche.
Het door EZ ondersteunde herstructureringsproject voor de bioscoopbranche zal uiterlijk medio 1988 worden afgerond. Door meer zorg te besteden aan de relatie met de bioscoopbezoeker, door een betere technische presentatie en door een betere communicatie binnen de branche wordt een meer rendabele exploitatie van het bioscoopbedrijf bereikt.

Distributie

Ons land heeft in de loop der tijd een sterke internationale positie op distributiegebied weten te bereiken. Binnen de totale commerciële dienstensector neemt de distributiesector ca 50% voor zijn rekening wat betreft het aantal ondernemingen, de werkgelegenheid en de vorming van de toegevoegde waarde. Met betrekking tot de export is dit aandeel zelfs ca 85%. Deze positie is echter niet onbedreigd. Steeds duidelijker immers tekenen zich op mondiale schaal structurele veranderingsprocessen af op sociaal-economisch en technologisch terrein die van invloed zullen zijn op onder meer distributieprocessen en als gevolg waarvan (nieuwe) eisen zullen worden gesteld ten aanzien van het vervullen van de internationale distributiefunctie.
Een versterking van de internationale distributiefunctie van ons land is uiteraard van eminent belang voor de Nederlandse distributiesector en de daaraan gerelateerde bedrijvigheid. Daar distributie een onderdeel uitmaakt van de totale economische bedrijvigheid is een versterking en verdere uitbouw van de distributiefunctie een van de elementen die zal leiden tot een verbetering van de concurrentiepositie van het Nederlandse bedrijfsleven.
Teneinde de Nederlandse positie als internationaal distributiecentrum voor de toekomst zeker te stellen is een actieve opstelling van de overheid en het

bedrijfsleven gezamenlijk noodzakelijk om bestaande knelpunten op te lossen en dreigende knelpunten te voorkomen. Deze knelpunten betreffen een breed scala van onderwerpen op het gebied van infrastructuur, informatica, promotie en logistiek.
In overleg met andere betrokken ministeries en het bedrijfsleven zal worden nagegaan welke initiatieven genomen kunnen worden om tot een versterking van de distributiefunctie te komen. Belangrijke activiteiten die reeds op gang zijn gekomen zijn:

- de start van de opbouw van een geavanceerd communicatienetwerk in de Rotterdamse haven (INTIS) die mede door een financiële bijdrage van EZ van *f* 5,8 mln mogelijk werd gemaakt;
- de vorming van een nationaal collectief „Nederland Distributieland", gericht op de promotie van ons land als distributieknooppunt en de acquisitie van mondiale goederenstromen. EZ en V&W hebben hiertoe gezamenlijk *f* 10 mln toegezegd.

Hoofd Bedrijfschap Ambachten
15 sept. 1987.

Persberichten

Philips

De Franse PTT heeft bij Philips Frankrijk een order geplaatst voor 900 000 Minitel-terminals, te leveren in de loop van dit jaar en in 1988. Het gebruik van dergelijke videotex-terminals, onder meer voor het via de telefoon raadplegen van databanken, is binnen enkele jaren in Frankrijk zeer snel gegroeid. Sinds 1983 produceerde Philips meer dan 600 000 Minitel-terminals; eind vorig jaar waren er in totaal twee miljoen in gebruik. In 1986 resulteerde dat ook in een zeer intensief gebruik: maandelijks werd 23 miljoen maal contact gelegd met de meer dan 4000 databanken. De doelstelling van de Franse PTT: tien miljoen geïnstalleerde terminals binnen tien jaar lijkt dan ook te worden gerealiseerd.
De Minitel-terminal, met een reeks uitbreidingsmogelijkheden, is veelzijdig toepasbaar. Klassiek zijn intussen functies als elektronisch telefoonboek, inzage in het banksaldo, weerberichten, verkeersinformatie, het maken van reserveringen, e.d. Nieuwe functies zijn het begeleiden van fabricageprocessen en kwaliteitscontrole. Ook wordt Minitel gebruikt voor berichtenverkeer. Buiten Frankrijk zijn zo'n 50 000 Minitels in gebruik in 12 landen. Een

van de eerste gebruikers in de bankwereld was de Spaanse Banco de Santander, met 15 000 terminals in bankkantoren en bij grote cliënten. De Belgische federatie voor vrachtvervoer stelt haar leden in staat via Minitels zich te informeren over vraag en aanbod en over vervoerscondities in andere landen. Op grond van toenemende belangstelling en diversiteit in gebruik wordt de Philips-reeks Minitel-terminals verder uitgebreid met nieuwe typen, onder meer met chipkaart-toegangsbeveiliging en met zelfstandige computercapaciteit.

PTT

Texbox 111 verzendt en ontvangt documenten voor PC via Teletex

Om personal Computers (IBM of IBM-compatible) via Teletex met elkaar te laten communiceren, heeft PTT Telecommunicatie de PTT Texbox 111 geïntroduceerd. Het is een store-and-forward communicatie-eenheid tussen PC en Datanet 1 die wordt aangestuurd door een gebruikerssoftware op de PC met verzend- en ontvangcommando's. Dit menu zet geproduceerde of opgeslagen brieven, rapporten en documenten van de PC over naar de Texbox 111, die vervolgens zelfstandig de verzending ervan regelt, ook als de PC is uitgeschakeld. Ook de ontvangst van berichten is een zaak van de Texbox 111: deze houdt de berichten vast totdat ze naar de PC overgehaald worden voor verdere afhandeling.
De PTT Texbox 111 heeft verder een aantal extra faciliteiten waaronder verkort kiezen, meervoudig adresseren, automatische nummerherhaling en uitgesteld verzenden. Verder houdt de Texbox een logboek bij van alle ingekomen en verzonden post. Is de PTT Texbox 111 in eerste instantie ontwikkeld voor bepaalde combinaties van computers, printers en tekstverwerkingsapparatuur, in de toekomst zal het toestel voor steeds meer configuraties geschikt worden gemaakt.
Teletex is een wereldwijd gestandaardiseerde communicatievorm voor kantoorapparatuur. De ruime opmaakmogelijkheden op basis van A4-formaat en de uitgebreide karakterset van 309 tekens garanderen een kopiegetrouwe documentenoverdracht van hoge kwaliteit. Via Teletex worden documenten verzonden met een snelheid van 6 pagina's per minuut. In Nederland maakt de Teletex-dienst gebruik van Datanet 1. Internationale koppeling van datanetwerken maakt wereldwijde communicatie mogelijk. Door koppeling van het *telex*net aan het datanet zijn ook teletex- en telexabonnees in staat met elkaar te communiceren, nationaal en internationaal.

Voor meer inlichtingen over de PTT Texbox 111 kunt u – gratis – bellen 06-0403.

Het weten waard

De ontwikkeling van het krulsnoer, puur liefdewerk

Telefoongebruikers danken aan Eddy Love een stukje comfort dat vandaag de dag als vanzelfsprekend wordt beschouwd, het krulsnoer aan hun telefoonhoorn.
In het begin van de jaren '40 bestonden die krulsnoeren nog niet en het ergerde Eddy Love, verkoper bij Koiled Kords Inc., dat de toen gangbare telefoonsnoeren regelmatig ontward moesten worden. Weet u nog hoe dat ging? Toestel boven het hoofd houden, hoorn langs het lichaam laten hangen en dan maar wachten tot de hoorn was uitgedraaid, een handeling die een aantal keren per dag kon worden herhaald. Eddy ontwikkelde, hoewel hij geen technische achtergrond had, zelf modellen van intrekbare snoeren. Zijn produktieproces verliep als volgt: bij verhoogde temperatuur werden de eerste grove snoermodellen tot een spiraal gerold, de aldus ontstane spiralen werden vervolgens in tegenrichting opgerold en verkregen zo hun verend effect. Eddy Love had weliswaar geen technische achtergrond, maar was wel een superverkoper bij de firma waar hij werkte. Hij slaagde er dan ook in zijn modellen aan verschillende firma's aan te bieden voor onderzoek en verbetering. Het kostte een flink aantal teleurstellende mislukkingen voordat een acceptabel Koiled Kord werd verkregen. Naar wordt aangenomen bracht Kellogg Company het Koiled Kord als eerste op de markt.
Zo bleek het oorspronkelijke idee van Eddy Love een goed idee, gelet op het universele hedendaagse gebruik. Zeker is dat niemand meer terugverlangt naar het oude rechte hoorn-snoer met zijn talrijke knopen en Franse slagen.

Overgenomen uit: Telephony, 11 augustus 1986