Cdensolvin

51e jaargang • januari/februari 1996 1/2

ptt telecom

Studieblad

Inhoud

PTT Telecom Studieblad is een uitgave van PTT Telecom Opleidingen (OT)

Hoofdredacteur
drs. Y.M. van der Veen
Eind- en tekstredactie
drs. A. Kok
ing. B.M. Franke
Redactieraad
Ing. B.W. Bos
Ing. C.P. Bosman
Prof. dr. J. Bruijning
Ir. L.H.M. Crousen
Dr. P. Licht
Secretariaat
mw. F. Stulp-Huttema
tel. 050-5853732
Correspondentie-adres
PTT Telecom Opleidingen
t.a.v. Studieblad MW 1526
Postbus 13000
9700 EA Groningen
Telefax 050-5853015
Abonnement
f 18,– per jaar. Voor niet-PTT-ers *f* 90,– per jaar.
Verschijnt 11x per jaar (dubbelnummers voorbehouden)
Vormgeving
Studio Dorèl, Groningen
Tekeningen
Sieger Zuidersma
Fotografie
PTT Museum
PTT Telecom
Musée de l'Histoire des PTT d'Alsace, Straatsburg
Universiteitsbibliotheek, Leiden
Vereniging Het Bilderdijk Museum, Amsterdam

ISSN 0165 8913

B Basiskennis

P Projecten

& Onderzoek & Ontwikkeling

A Achtergronden

Themanummer
Geheime berichten

Oorlogen zijn er door beslecht, geheime minnaars gebruiken het om elkaar hun liefde te betuigen, kinderlevens worden er reuze spannend van en ook James Bond lijkt er niet buiten te kunnen. Cryptologie of geheimschrift oefent al eeuwenlang grote aantrekkingskracht uit op jong en oud. Er is in de loop der eeuwen al heel wat energie gestoken in het vercijferen of coderen van berichten en het heeft minstens even zoveel bloed, zweet en tranen gekost al die geheime boodschappen te 'kraken'. Dat laatste lukt in de regel alleen als je in het bezit bent van de juiste sleutel. Voor de anderen is en blijft het abracadabra.

Parallel aan de tentoonstelling *Geheime berichten* die tot en met 15 maart in het PTT Museum te bezichtigen is besteedt het Studieblad in dit dubbelnummer aandacht aan de geschiedenis van het geheimschrift. De Studiebladartikelen en de tentoonstelling bestrijken een lange periode: vanaf zo'n 3000 jaar v. Chr. met het spijkerschrift van de Mesopotamiërs en het hiërogliefenschrift van de Egyptenaren, tot en met de ultramoderne elektronische encryptiemethoden van vandaag de dag. In verschillende opstellingen van het museum kunnen – verscholen achter mysterieuze luiken, gordijnen en deksels – geheimschriften uit de oudheid, middeleeuwen, renaissance, zeventiende, achttiende, negentiende en twintigste eeuw bekeken worden. Daarnaast kan iedereen zelf met geheimschriften experimenteren. Elke opstelling heeft namelijk een bijzonder geheimschrift dat door de bezoekers zelf gemaakt en ontcijferd kan worden. Bijvoorbeeld: een scytale-bericht, middeleeuwse symbolen, planiphèriques, onzichtbare inkten, roosters van Cardano, cryptofoons, computer-encryptie... Ook de Studiebladlezers kunnen hun grijze cellen aan het werk zetten. In het Cryptospel op de bijgevoegde diskette staan verschillende geheime berichten die om ontcijfering schreeuwen.

Cryptospel Bij het Studieblad is een diskette gevoegd waarop 5 crypto-analytische puzzels staan. Kunt u (of uw kinderen!) de geheimschriften oplossen... Het spel is voor elke MS-DOS computer geschikt en kan direct vanaf het A-station worden gespeeld. Stop de diskette dus in uw PC, type *A:\crypto.exe* en u kunt aan de gang.
N.B. let erop dat tijdens het spelen het schijfje NIET beschermd mag zinntegen schrijven!

vijftig jaar

Geheime berichten in WO I: het Zimmermann-telegram

Rob Korving

Oorlogen hebben een grote invloed gehad op de ontwikkeling van geheimschriften en apparatuur om berichten te coderen. Maar ook andersom heeft de ontcijfering van geheime berichten invloed gehad op het verloop van een oorlog. Een voorbeeld van het laatste is de ontcijfering van het zogenaamde Zimmermann-telegram dat de Verenigde Staten rechtstreeks bij de Eerste Wereldoorlog betrok.

In het begin van deze eeuw domineerde Engeland de internationale telegrafie. Vrijwel alle belangrijke zeekabels waren in handen van maatschappijen die of Engels waren of waarvan een belangrijk deel van de aandelen door de Engelsen gecontroleerd werd. De andere landen, Frankrijk, Duitsland en ook Nederland zagen die ontwikkeling met lede ogen aan. Bij internationale conflicten – en Nederland had dat zelf in de Boerenoorlogen aan den lijve ondervonden – werd alle correspondentie over de Engelse kabels gecensureerd en vertraagd. Telegrammen in code, zakelijk of diplomatiek, waren verboden. Zonder overleg kon het telegraafverkeer voor onbepaalde tijd worden gestaakt, bijvoorbeeld bij het begin van een offensief.

De Telconia

Het is daarom ook niet onbegrijpelijk dat de andere mogendheden streefden naar eigen, van Engeland onafhankelijke, telegraafverbindingen. Zo legde Duitsland in 1910 een eigen zeekabel naar de Verenigde Staten. Die kabel liep van Emden via de Azoren naar New York. Van daaruit konden telegrammen over het Amerikaanse net worden verstuurd naar de Westkust. Via de Amerikaanse zeekabels door de Pacific konden vervolgens de Duitse koloniën in de Stille Zuidzee bereikt worden. Dat gold ook voor China waar Duitsland economische belangen had.

Kort na aanvang van de Eerste Wereldoorlog viste het Britse kabelschip *Telconia* de Duitse kabel op en hakte hem door. Vanaf dat ogenblik had Duitsland geen directe verbinding meer met de Verenigde Staten en moesten alle telegrammen naar Amerika en Azië via omwegen verstuurd worden. Een van die omwegen was Zweden, een andere de ambassade van de Verenigde Staten in Berlijn. Maar welke route de

Duitsers ook kozen, elk telegram moest toch ergens over een door Engeland gecontroleerde zeekabel.

De Magdeburg

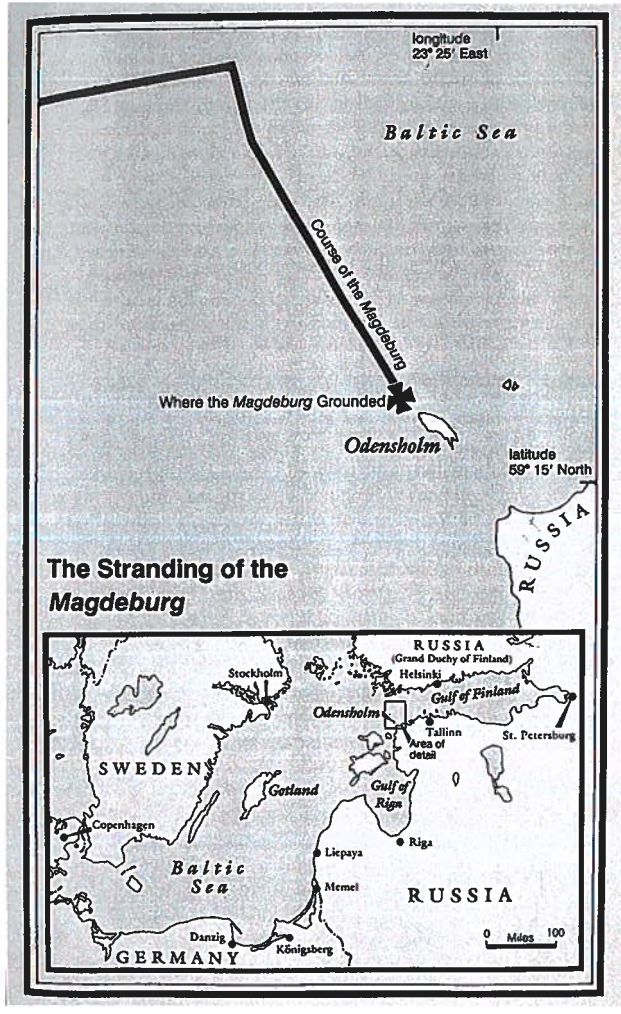
Een aantal dagen na de actie van de Telconia vond er een andere gebeurtenis plaats, die ogenschijnlijk niets met de eerste te maken had. Een Duits oorlogsschip, *de Magdeburg*, strandde in de Baltische Zee. Jaren later schreef Winston Churchill, die in de Eerste Wereldoorlog minister van marine was, hierover in zijn boek *The World Crisis*:

In het begin van september 1914 strandde de Duitse lichte kruiser Magdeburg in de Finse Golf. Een paar uur later visten de Russen het lijk op van een Duitse onderofficier, die de Duitse code- en signaalboeken en de kaarten met een precieze verdeling in kwadranten van de Noordzee en de (bocht van Helgoland?) in zijn armen klemde. Op 6 september kreeg ik bezoek van de Russische marine attaché. Hij had een boodschap uit Petrograd gekregen met het verhaal – van de stranding – en dat de Russische marine in ieder geval in staat was geweest met behulp van de signaal- en codeboeken een deel van het – radio – verkeer van de Duitse marine te ontcijferen. De Russen waren van mening dat Engeland, als de belangrijkste maritieme natie, deze boeken en kaarten zou moeten hebben. Als wij een schip naar Alexandrof zouden sturen, zouden de Russische officieren die de boeken beheerden deze naar Engeland brengen. Wij stuurden onmiddellijk een schip en eind oktober ontvingen Prins Louis van Battenberg (de First Sea Lord) en ik uit de handen van onze loyale bondgenoten deze onschatbare documenten.

Een aantal geschiedschrijvers nam dit aangrijpende verhaal zonder het te controleren over. Er waren er zelfs die het nog een stukje dramatischer maakten, vooral het thema van de dode zeeman met het codeboek tegen zijn borst geklemd was populair.

De kern van Churchill's verhaal klopt, de *Magdeburg* liep door navigatiefouten aan de grond bij het eilandje Odensholm (dat gebeurde overigens niet in september,

▶ Afb. 1
Plaats waar de *Magdeburg* ten onder ging.



maar op 26 augustus 1914). Pogingen om het schip los te trekken faalden en toen er Russische oorlogsschepen naderden gaf de kapitein opdracht in het voor- en achterschip explosieven aan te brengen. De bemanning evacueerde naar een Duitse torpedoboot die in de buurt lag.
Tijdens die evacuatie werd er plotseling alarm geslagen: de lonten van de springladingen waren al aangestoken. In de paniek die toen ontstond gaf de kapitein van de *Magdeburg* opdracht alle codeboeken te vernietigen of in veiligheid te

brengen. Eén boek werd direct overboord gegooid, een tweede werd door een overboord springende marconist meegenomen en het derde codeboek werd vergeten en bleef in de hut van de kapitein achter. De Magdeburg werd door de explosies echter niet vernietigd en de Russen vonden het achtergebleven codeboek in het wrak. Een Russische officier, die zich realiseerde dat er mogelijk ook materiaal in het water was gegooid, liet meteen duikers in het heldere water zoeken. Kort daarop werden de beide andere boeken gevonden. De marconist was het tweede bij zijn sprong in het water verloren!

De Russen boden in oktober van dat jaar het boek uit de kapiteinshut aan de Britse gezant aan, die ervoor zorgde dat het in Rusland werd opgehaald. De kennis van de Duitse codes die de Britse cryptografische afdeling *Room 40* daardoor kreeg, zou de loop van de oorlog gaan beïnvloeden. De andere twee codeboeken hielden de Russen zelf, zo ver ging hun loyaliteit met hun bondgenoot nu ook weer niet.

Een dubbeldekker

Op 16 januari 1916 hielp het toeval de Engelse cryptografische dienst een handje. Omdat de Mexicaanse ambassadeur afwezig was, moest de Duitse minister van Buitenlandse Zaken Arthur Zimmermann zijn diplomatieke contacten via zijn gezant in Mexico-Stad afhandelen. Zimmermann stuurde daarom een gecodeerd telegram aan de Duitse ambassadeur in de Verenigde Staten. Deze zou het daarna doorsturen naar gezant Von Eckardt in Mexico-Stad.
Om er zeker van te zijn dat het telegram ook werkelijk aankwam, werd het via twee verschillende routes gestuurd. De ene liep via het neutrale Zweden, dat de Duitse codetelegrammen als Zweedse verstuurde. Dat was volgens het internationale recht niet toegestaan. Toen *Room 40* in 1915 dit soort telegrammen tussen de Zweedse ontdekte, besloten de Engelsen alle Zweedse telegrammen te vertragen. Toen de Zweden daarover klaagden, kregen zij te horen dat ze dan maar geen Duitse codetelegrammen meer moesten versturen.
De Zweedse regering beloofde beterschap, maar in de praktijk bleven de Duitsers hun telegrammen nog steeds via Stockholm versturen. Wel codeerden zij hun berichten nu

een tweede keer, om op die manier de typisch Duitse cijfergroepen te verbergen. Zo'n tweemaal gecodeerd telegram wordt in de cryptografie een *dubbeldekker* genoemd.

▼ Afb. 2
Spotprent over het Zimmermann-telegram.

De Amerikaanse ambassade

De tweede route van de Duitsers liep via de Amerikaanse ambassade in Berlijn. De Verenigde Staten waren begin 1916 nog niet in oorlog met Duitsland. De vredesgezinde president Wilson had de Amerikaanse ambassadeur persoonlijk toestemming voor deze praktijk gegeven. Ook hier pasten de Duitsers de dubbeldekker toe. Jammer genoeg verborg de tweede codering de typische cijfergroepen niet helemaal. Room 40 kraakte de bovenste code, die ze *13040* noemden en zagen dat de tekst oorspronkelijk gecodeerd was in *0075*, een code die dankzij de het codeboek van de *Magdeburg* gedeeltelijk bekend was. Er stond:

Zeer geheim, bestemd voor uwe excellenties persoonlijke informatie en bestemd om verstuurd te worden aan de Keizerlijke minister in (?) met telegram No (?) via een veilige route.

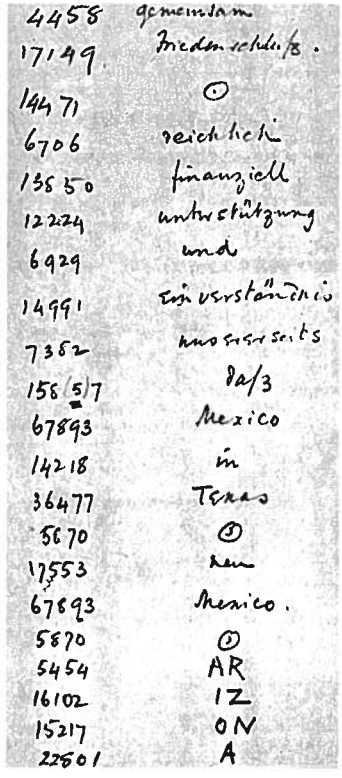
Wij zijn van plan om op 1 februari te beginnen met de onbeperkte duikbootoorlog. Daarbij zullen we proberen de Verenigde Staten neutraal te houden (?). Als dat niet lukt, stellen we (?) een bondgenootschap voor op de volgende grondslag:

(?) oorlogvoeren
(?) vrede sluiten
(?)

Uwe excellentie kan op dit ogenblik de president van (?) in het geheim informeren dat (?) oorlog met de Verenigde Staten en tegelijkertijd dat we onderhandelen met Japan. (?) dat (?) onze onderzeeboten (?) Engeland tot vrede zullen dwingen in een paar maanden. Bevestig de ontvangst.

Zimmermann

De tekst werd onmiddellijk herkend als van groot belang, maar de open stukken lieten nog ruimte voor meerdere interpretaties. Terwijl Room 40 zich het hoofd brak over de onbekende woorden, stuurde Bernstorff het telegram op 19 januari via Western Union naar de Duitse gezant in Mexico. In plaats van code *0075* – die Von Eckardt blijkbaar nog niet had – codeerde de Duitse ambassade het in de door de Engelsen gekraakte code *13040*.

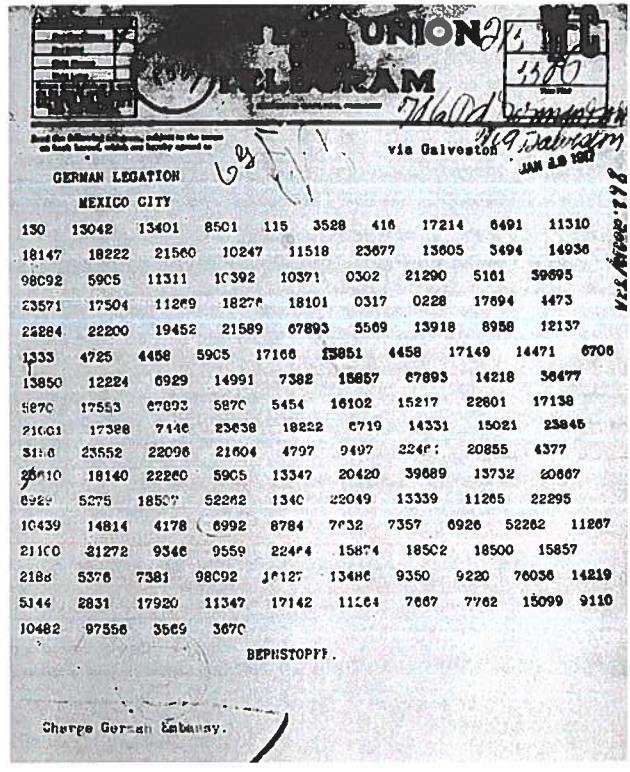


▲ Afb. 3
Gedeeltelijke ontcijfering van het Zimmermann-telegram.

Dilemma

De Engelse geheime dienst zag direct de enorme impact van het Duitse telegram in. Toch bleef er ruimte voor twijfel. Als de interpretatie op basis van de gedeeltelijke decodering inderdaad juist was, bood Duitsland in het telegram Mexico een bondgenootschap aan. Dat zou de Verenigde Staten bij de oorlog in Europa kunnen betrekken. Aan de andere kant konden juist die ontbrekende stukken tekst de inhoud van

het telegram totaal veranderen. Een tweede complicatie was dat als de Engelsen de informatie direct aan de Amerikanen doorgaven, de Duitsers zouden weten dat *0075* gekraakt was. En tegenover de Verenigde Staten zouden de Engelsen dan toegeven dat ze het telegraafverkeer van het neutrale Zweden onderschepten!


UNION

via Galveston

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98C92 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
9870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7146 23638 18222 6719 14331 15021 23845
31[illegible] 23552 22096 21604 4797 9497 224[illegible] 20855 4377
[illegible]10 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7032 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
218[illegible] 5376 7381 98C92 [illegible]127 134H6 9350 9220 76036 14219
5144 2831 17920 11347 17142 11164 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTORFF.

Charge German Embassy.

► Afb. 4
Het Zimmermann-telegram zoals ambassadeur Bernstorff het in code *0075* doorstuurde naar zijn gezant in Mexico.

De oplossing voor dit dilemma kwam van het hoofd van Room 40, W.R. Hall. Die realiseerde zich plotseling dat het telegram in Washington opnieuw verzonden was. Misschien wel in een andere code?
Via de Britse geheime dienst kreeg hij de beschikking over een kopie van het telegram. Het resultaat overtrof zijn stoutste verwachtingen: het telegram was ditmaal omgezet in code *13040*. De tekst luidde:

Zeer geheim, bestemd voor uwe excellenties persoonlijke informatie en bestemd om verstuurd te worden aan de Keizerlijke minister in Mexico met telegram No (158) via een veilige route.

Wij zijn van plan om op 1 februari te beginnen met de onbeperkte duikboot-oorlog. Ondanks dat zullen we ons best doen om de Verenigde Staten neutraal te houden. Als ons dat niet lukt, stellen we Mexico een bondgenootschap voor op de volgende grondslag:

samen oorlogvoeren, samen vrede sluiten, ruime financiële ondersteuning en een bevestiging van onze kant dat Mexico de verloren delen van Texas, New Mexico en Arizona mag heroveren. Ik laat de details van deze overeenkomst aan u (de minister in Mexico) over.

U kunt de president in het geheim informeren over het bovenstaande zodra de oorlog met de Verenigde Staten een feit is en hem tegelijkertijd de suggestie doen om, op zijn eigen initiatief, bij Japan aan te dringen op steun en tegelijkertijd te bemiddelen tussen ons en Japan.

Breng s.v.p. de president onder ogen dat de genadeloze toepassing van onze onderzeeboten de mogelijkheid schept om Engeland binnen een paar maanden tot vrede te dwingen.

Bevestig de ontvangst.

Zimmermann

De lont in het kruitvat

De kans die het *Zimmermann-telegram* bood om de Verenigde Staten bij de oorlog in Europa te betrekken was voor Engeland te mooi om te laten schieten. Op 24 februari stuurde Hall het gedecodeerde telegram naar Washington. Drie dagen later, toen president Wilson geconfronteerd werd met de inhoud ervan, barstte de bom. Woedend over de onbetrouwbaarheid van de Duitsers gaf hij de opdracht de hele affaire publiek te maken. Het Duitse aanbod om een

deel van hun land aan Mexico te geven deed het Amerikaanse volk op zijn achterste benen staan.

Maar er waren ook sceptici, die stelden dat de hele affaire alleen bedoeld was om de Verenigde Staten bij de oorlog te betrekken en dus doorgestoken kaart was. De Amerikanen waren wel op de hoogte van de dubbeldekker, maar konden deze niet decoderen. En de Britten waren niet bereid om *13040* en nog minder om *0075* af te staan. Nadat Wilson persoonlijk had bemiddeld bij de Western Union om een kopie van het betreffende telegram te krijgen, stuurde het Amerikaanse ministerie van Buitenlandse Zaken de kopie aan Room 40. Die decodeerde het en stuurde vervolgens het resultaat nog dezelfde dag terug.

Alle betrokkenen, de Mexicaanse regering, Ambassadeur Bernstorff en Von Eckardt en de Japanners ontkenden bij hoog en laag iets van de zaak af te weten. Daarom is het nog verbazingwekkender dat Arthur Zimmermann een paar dagen later tot ieders verbazing in het openbaar toegaf dat de inhoud van het telegram inderdaad juist was. Op 2 april 1916 vroeg Wilson het Amerikaanse Congres om de oorlog met Duitsland toe te staan. Hij gebruikte het Zimmermann-telegram als een van de belangrijkste argumenten. De rest is bekend: de komst van de Amerikaanse troepen naar Europa deed in 1918 de balans aan het Westelijk Front doorslaan in het voordeel van de geallieerden.

Drs. R.A. Korving studeerde Geschiedenis aan de Rijksuniversiteit te Leiden. Sinds 1 juli 1989 is hij werkzaam bij het PTT Museum als conservator Telecommunicatie.

Geheimschrift door de eeuwen heen: op zoek naar de sleutel

Loes Baas
Jacques Caspers
Ben Koevoets
Anneke Kok

Zolang mensen met elkaar communiceren gebruiken ze al methoden om geheime berichten in een speciale code om te zetten. Geheimtaal en geheimschrift zijn van oudsher vooral populair bij kinderen, geliefden, geheime genootschappen, diplomaten en in onze tijd ook bij maffia en andere criminele organisaties én bij leger en politie die de laatsten juist bestrijden. Maar ook u en ik komen dagelijks, vaak zonder dat we het weten, in aanraking met geheimschrift of cryptologie. Bij de flappentapper en andere pincode-apparaten bijvoorbeeld worden persoonlijke gegevens versleuteld. Parallel aan een tentoonstelling die momenteel in het PTT Museum te zien is behandelt het Studieblad de historie van berichten die alleen begrepen kunnen worden wanneer je over de juiste sleutel beschikt.

Jongensboeken zijn erover volgeschreven, in James Bond-films speelt het een prominente rol, 'hackers' hebben er hun levenswerk van gemaakt en vele honderden wetenschappers en andere slimme breinen houden zich er dagelijks mee bezig: het bedenken of juist 'kraken' van geheime gecodeerde berichten. Bij encryptie of geheimschrift wordt vaak volgens een wiskundige formule, een algoritme, een bericht 'vercijferd'. Meestal gaat dat in de vorm van letter- of cij-

◀ Afb. 1
Criminelen, detectives en politie proberen elkaar via geheimschrift te slim af te zijn.

fercombinaties en/of verkortingen van meerdere woorden die tezamen zinnen vormen. Alleen ingewijden die in het bezit zijn van de zogenaamde sleutel, kunnen het bericht omzetten in de oorspronkelijke vorm. Voor wie niet over de juiste sleutel beschikt is het bericht abracadabra.

Mene, mene tekel ufarsin (Daniël 5: 25)

Al in de Bijbel wordt gewag gemaakt van geheimschrift. Het boek Daniël in het Oude Testament beschrijft hoe Koning Belsassar een groot feestmaal aanrichtte ter ere van de goden van goud, zilver, brons, ijzer, hout en steen. Opeens verschijnt er uit het niets een grote mensenhand die de geheimzinnige boodschap *mene, mene tekel ufarsin* op de muur van het paleis schrijft. De geschrokken koning richt zich tot de wijzen van Babel en zegt: 'Wie dit schrift kan lezen en er mij de verklaring van geeft, zal met purper bekleed, de gouden keten dragen om zijn hals en als derde heersen in het koninkrijk.' Het blijkt uiteindelijk de wijze balling Daniël te zijn die er als enige in slaagt de boodschap te ontcijferen. Hij vertaalt het bericht voor de koning als volgt: 'Geteld heeft God uw regeringsjaren en er een eind aan gemaakt; gewogen bent u op de weegschaal en te licht bevonden; verdeeld is uw koninkrijk en aan de Meden en Perzen gegeven' (Daniël 5: 26-28). Nog dezelfde nacht wordt Belsassar, de koning der Chaldeeën, gedood.

De klassieke oudheid

Een nog ouder voorbeeld dan dit bijbelse verhaal en wèl met materiële getuigenissen, stamt uit het oude Mesopotamië. Daar hadden veehandelaren behoefte aan controle op de levering van het aantal stuks vee. In een kleitablet met riet legden ze middels inscripties, het welbekende spijkerschrift, de aantallen en de soort beesten vast. Opgerold en verzegeld werd dit geheel vervolgens aan de 'transporteurs', de lange-afstand-herders, meegegeven. De ontvanger kon op deze manier controleren of de geleverde aantallen klopten. Alleen de verzender en de ontvanger hadden kennis van de inhoud van het bericht. Aan deze eenvoudige vorm van encryptie ligt het ontstaan van het schrift ten grondslag, dat in vorm, betekenis en taal zou uitwaaieren over de wereld.

Niet alle schrift is bedoeld als geheimschrift, maar sommige vormen van schrift zijn voor buitenstaanders lang geheim gebleven. Net zomin als het spijkerschrift van de Mesopotamiërs was het hiërogliefenschrift van de Egyptenaren een vorm van geheimschrift in de strikte betekenis van het woord. Echt geheimschrift is immers alleen bekend bij een zeer kleine groep ingewijden en het hiërogliefenschrift was het schrift dat geletterde Egyptenaren gebruikten. Voor buitenstaanders bleven de hiërogliefen echter eeuwenlang een raadsel. Pas met de vondst van de steen van Rosetta in 1799 en de ontcijfering ervan in 1822 kwam er een eind aan alle geheimzinnigheid rondom het hiërogliefenschrift. De steen van Rosetta zorgde ervoor dat na vele eeuwen de Oud-Egyptische cultuur tot een open boek werd.
Ook de oude Grieken en Romeinen gebruikten geheimschrift. Op vaak zeer geraffineerde wijze werden berichten 'verstopt', meestal uit strategisch oogpunt. Een mooi voorbeeld daarvan is de zogenaamde 'scytale', een uitvinding uit het oude Griekenland. Het principe van de scytale is simpel. Een lange reep papier werd om een stok gewikkeld en de boodschap werd er in de lengterichting op geschreven. Afgewikkeld was het bericht onbegrijpelijk. Pas wanneer de ontvanger de strook om een stok van gelijke dikte wikkelde werd de boodschap weer leesbaar.
Ook Julius Caesar zag de mogelijkheden van geheimschrift in en gebruikte een, weliswaar vrij eenvoudige, vorm van encryptie om zijn strijdplannen te communiceren zonder dat zijn vijanden ze konden lezen. De Romeinse keizer vercijferde zijn boodschappen door elke letter te vervangen door een andere die drie plaatsen verderop stond in het alfabet, de zogenaamde mono-alfabetische substitutie. Zo veranderde zijn naam *Julius Caesar* in *Mxolxv Fdhvdu.*

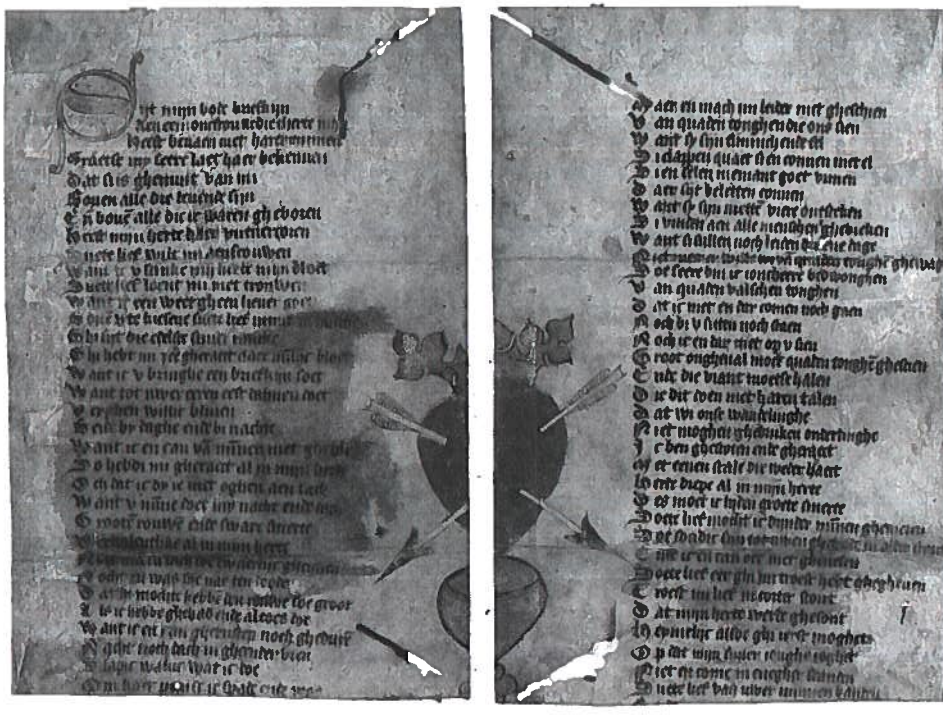
Middeleeuwen en Renaissance

In de Middeleeuwen lijkt geheimschrift in de westerse wereld moeilijk te vinden. Na het ineenstorten van het Romeinse Rijk beleefden kunsten en wetenschappen in Europa een terugslag. Toch was er in deze periode sprake van een soort geheimschrift, de zogenaamde Tyroonse noten. Het bestond uit afkortingen die alleen door kenners geschreven en gelezen konden worden. De basis voor het Tyroonse notenschrift werd al in de Romeinse tijd gelegd

door Marcus Tullius Tiro, een bevrijde slaaf die later secretaris van de grote redenaar Marcus Tullius Cicero zou worden. In de Middeleeuwen groeide het aantal afkortingen uit tot meer dan 12000. Veelgebruikte zinnen werden vaak ingekort tot één teken en waren zo voor niet-ingewijden onleesbaar.

Iets dergelijks vinden we ook terug in de Middeleeuwse 'scriptoria' waar monniken, staande aan lange rijen lessenaars, collectief en letterlijk gedicteerd en gedirigeerd teksten op perkament schreven en zo vermenigvuldigden. Een enorm arbeidsintensief karwei, waar menigeen zich vandaag de dag nauwelijks nog iets bij voor kan stellen. Geen wonder dat de geestelijken behoefte hadden aan een efficiëntere schrijfwijze. Zo ontstond de zogenaamde *abbreviatuur*, de afkorting van woorden en soms zinsdelen. De afkortingen waren alleen voor ingewijden te lezen. Het bespaarde niet alleen tijd maar het verhoogde ook de status van de gebruikers. Leken werden op deze manier buitengesloten, zo die al (Latijn) konden lezen.

▼ Foto 1
Minnebrief op rijm, circa 1400. Het met pijlen doorboorde rode hart moet de inhoud van het gedicht symboliseren.



Afgeschermd van de buitenwereld bloeide ook de kunst in de Middeleeuwse kloosters. Manuscripten werden verluchtigd met uiterst verfijnde miniaturen en symbolen. Deze symbolen en de interpretatie ervan kunnen ook worden beschouwd als een vorm van geheimschrift.

De ontwikkeling van geheimschrift kreeg in de periode na de Middeleeuwen een enorme stimulans. Een belangrijke oorzaak was te vinden in de opkomst van nieuwe staten in Europa en de toename van diplomatieke betrekkingen tussen de Europese monarchieën. Tal van wetenschappers bestudeerden de cryptografie en verhieven deze tot dan toe vrij duistere bezigheid tot een specialistische studie. Figuren als Alberti, Trithemius, Porta, Cardano en Viginere legden daarmee de basis voor de ontwikkeling van geheimschrift tot een moderne wetenschap.

Cabinets Noirs

De Zwarte Kamer of het Cabinet Noir was een verschijnsel dat al in de vijftiende eeuw onder Lodewijk XI bestond. Het ging om een vorm van interceptie, aanvankelijk bedoeld om door te dringen tot de geheimenissen van het intieme leven ('amore') van de onderdanen. Deze vorm van georganiseerde onbescheidenheid was aanvankelijk bedoeld voor de verstrooiïng van Zijne Majesteit. 'Le roi s' amuse', iets wat met name gold voor Lodewijk XIV. In latere tijden fungeerde het Cabinet Noir vooral als een soort inlichtingendienst die greep moest houden op het diplomatieke postverkeer. Onder leiding van een post-intendant werkte een aantal beambten aan deze vorm van spionage. Brieven werden door omgekochte boden bezorgd op het Zwarte Kabinet, geopend, gelezen en – indien staatsgevaarlijk of anderszins belangrijk – snel overgeschreven en zonodig zelfs vertaald. Vervolgens werden ze met kunstgrepen en vervalste lakstempels weer toegevouwen en met de minst mogelijke vertraging alsnog bij de geadresseerde bezorgd. Geen wonder dat men deze praktijken probeerde te omzeilen door uitsluitend van eigen koeriers gebruik te maken (wat voor kleine mogendheden uiteraard erg duur was) of, wat vaak voorkwam, te ontduiken door brieven in gecodeerde taal te verzenden. Dit laatste leverde heel wat creatieve en ingenieuze staaltjes van geheimschrift op. De Zwarte Kamers bereikten

hun grootste bloei onder het regime van Lodewijk XV en zij bleven tot de revoluties van 1848 in gebruik, ook de Zwarte Kamer in Den Haag.

Geheimschrift en kunst

Geheimschrift kan ook tot zeer artistieke en esthetische vormen leiden. Een fraai voorbeeld daarvan is te vinden in de correspondentie van dichter/advocaat Willem Bilderdijk (1756-1831). Deze was aan het eind van de 18e eeuw door de Franse bezetter verbannen en schreef vanuit zijn exil in Engeland fraaie brieven aan zijn Amsterdamse schoonzuster, in spiegelschrift en in getekende rebusvorm. Reeds als vijftienjarige gaf de jonge Willem Bilderdijk in rebusvorm getekende chronostichons (datum/tijdvermeldingen) blijk van een dermate hoge vorm van eruditie en kennis van de klassieken, dat alleen al op grond van die eruditie het aantal personen dat deze berichten zou kunnen decoderen, uitermate klein geacht moet worden.

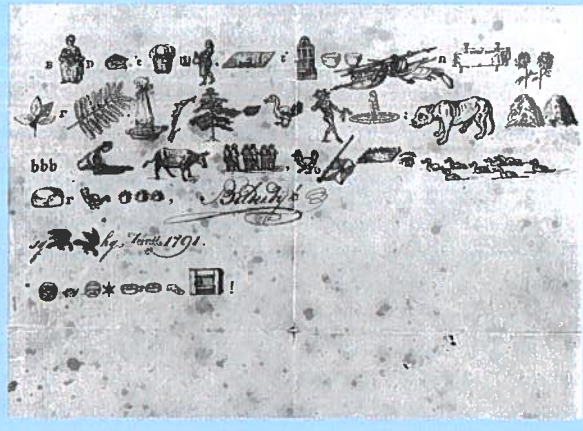


Foto 2 Rebusbrief Bilderdijk

Transscriptie: *Beminde meid, 't was ons waard uw thuiskomst buiten desasters te ervaren. Wij vinden ons gans niet wel, doch hopen beter in't vervolg en zijn uw hoogachtende broeder en zuster. 's-Gravenhage, half juni 1791. Duid ons duister schrijven ten beste.*

Telegrafie

De expansiedrift van Napoleon legde niet alleen via de steen van Rosetta het tot dan toe geheim gebleven taalgebied van de Egyptische hiërogliefen open, het creëerde ook een geheimtaal door de lucht: optische telegrafie zoals die werd geïntroduceerd door de gebroeders Chappe. De optische telegraaf was een op een hooggelegen punt (zoals kerktorens) geïnstalleerde seinpaal die gecodeerde berichten overseinde naar een soortgelijke seinpaal kilometers verderop. Iedere stand van de 'seinarmen' stond voor een letter, woord of soms zelfs voor een hele zin. De sleutel tot ontcijfering was vastgelegd in een codeboek dat in handen was van de formele opsteller en de ontvanger van het bericht. De bedienaars van deze seinpalen kenden de betekenis van wat ze seinden dus niet. Een bericht kon in een kwartier worden overgeseind van Parijs naar Rijssel (Lille), een

◀ Foto 3
De Wheatstone cryptograaf (1867).

afstand van maar liefst 220 kilometer. Ter vergelijking: een koerier te paard deed er minstens twintig uur over. Ook in ons land was de optische telegraaf een tijdlang een populair telecommunicatiemiddel. Maar met het vertrek van de Fransen uit ons land werden ze – evenals zovele andere Franse souvenirs – zo snel mogelijk afgebroken.

Na de komst van de elektrische telegraaf in Nederland (1852), werd een deel van de telegrammen in code verstuurd. Zakelijke telegrammen werden om twee redenen in code omgezet. Ten eerste was een gecodeerd telegram vaak korter en dus goedkoper dan een 'gewoon' telegram. Ten tweede probeerde men zo de informatie geheim te houden voor de concurrentie.
Om zakelijke telegrammen te coderen verschenen er speciale codeboeken zoals de *ABC Universal Commercial Electronic Telegraphic Code* waarvan vele edities tot halverwege deze eeuw in gebruik waren. Deze boeken werden voornamelijk gebruikt door banken, handelaren en reders. Ze stegen sterk in populariteit toen het in 1866 mogelijk werd om via de eerste transatlantische zeekabel telegrammen naar de Verenigde Staten te versturen.
Er kwam ook een Nederlandse codeboek, de *Mercuurcode*. Voor kleine bedrijven die handel dreven met Nederlandsch Indië waren de commerciële codeboeken vaak te duur. Voor hen kwam in 1925 de *Javacode* op de markt. Deze cijfercode kostte acht gulden, nog steeds een flinke som geld in die tijd. Maar vergeleken met de Mercuurcode van tachtig gulden was het een koopje.

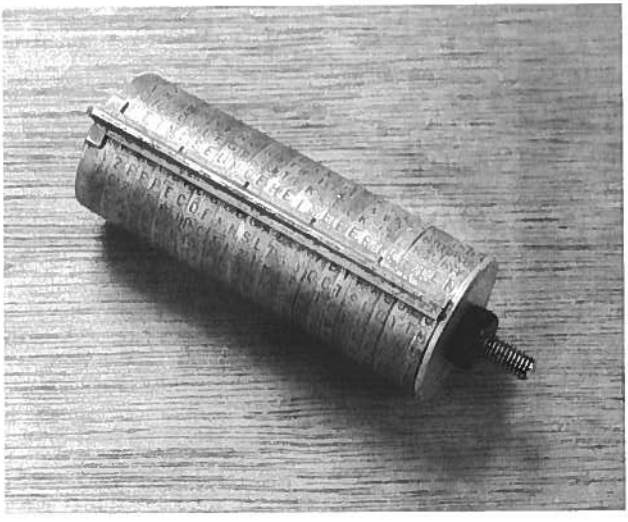
Oorlog en vrede

Het uitbreken van de Eerste Wereldoorlog leidde tot een grote opleving in het gebruik van geheimschrift. De ontcijfering van een gecodeerd Duits telegram zorgde er zelfs voor dat Amerika rechtstreeks bij de oorlog betrokken werd. In dat telegram van 19 januari 1917 beloofde de Duitse minister van Buitenlandse Zaken, Arthur Zimmermann, dat Mexico een deel van de Verenigde Staten mocht heroveren in ruil voor een bondgenootschap met Duitsland. De Britse geheime dienst onderschepte het telegram, decodeerde het en stuurde het naar de Amerikaanse President Wilson. Die besloot het terstond te publiceren, wat voor een enorme

opschudding onder het Amerikaanse volk zorgde. Samen met het invoeren van de onbeperkte duikbootoorlog door de Duitsers, zorgde het Zimmermann-telegram ervoor dat de – tot dan toe neutrale – Verenigde Staten de oorlog aan Duitsland verklaarden[1].

In navolging van de Zwarte Kamers in Europa kreeg ook de Amerikaanse Intelligence-dienst *MI-8* de bijnaam *The Black Chamber*. Onder leiding van Herbert O. Yardley kraakte *MI-8* begin jaren twintig de diplomatieke codes van verschillende landen, waaronder die van Japan. De Amerikaanse minister van Buitenlandse Zaken Hughes, gebruikte deze kennis tijdens de Washington Naval Conference in 1920-1921. Omdat hij daags tevoren op de hoogte was van de argumenten van de Japanners, kon Hughes hen in de onderhandelingen steeds te slim af zijn. In 1929 werd *MI-8* opgeheven en een teleurgestelde Yardley onthulde in zijn boek *The American Black Chamber* hoe zijn geheime organisatie te werk ging. Dit uiteraard tot groot verdriet van het Amerikaanse leger, dat doorging met het kraken van diplomatieke codes, en tot grote vreugde van de Japanners die na publikatie van Yardley's boek terstond hun codes veranderden. Yardley's taak werd overgenomen door de roemruchte US Army-medewerker William F. Friedman. Friedman stelde een briljant team van crypto-analisten samen dat de Japanse

[1] Elders in dit nummer van het Studieblad is een speciaal artikel gewijd aan het Zimmermann-telegram.

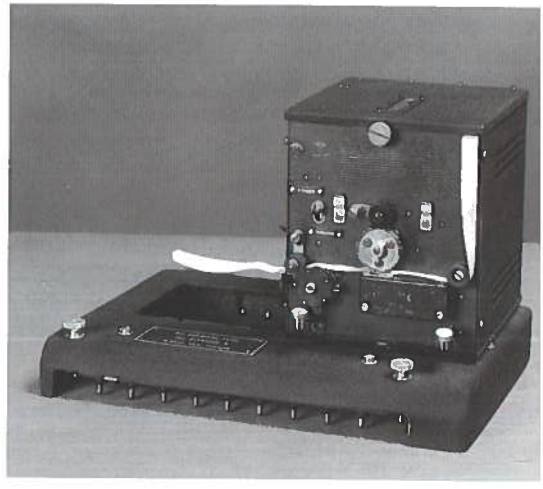


◀ Foto 4
M-94 coderol. Gebruikt door het Amerikaanse leger tussen 1922 en 1943.

diplomatieke codeersystemen – inmiddels geautomatiseerd – ontcijferde. Niet voor niets wordt Friedman wereldwijd gezien als de bekendste crypto-analist van deze eeuw.

Niet alleen in oorlogstijd, maar ook in vredestijd bestond de behoefte het afluisteren van berichten uit de ether tegen te gaan. Overheden wilden geheimhouding, particulieren privacy. Ook in ons land. Op 7 januari 1929 werd de radiotelefonieverbinding met Nederlands-Indië geopend. Voor de bezitters van een gevoelige radio-ontvanger was het mogelijk om op de kortegolf mee te luisteren met de gesprekken. Voor particulieren, die af en toe intieme familie-aangelegenheden te bespreken hadden, een minder prettige gedachte. Maar ook voor zakenmensen, die hun handelstransacties liever niet aan de grote klok hingen was het een bezwaar. Het Radiolaboratorium van PTT ontwikkelde daarom een methode waarmee de gesprekken onverstaanbaar konden worden gemaakt voor de meeluisterende radiobezitters. Met ingang van 19 oktober 1931 werden de gesprekken afgewikkeld via een zogenaamde geheimtelefonie-installatie. Het gesproken woord werd daarbij als het ware 'omgekeerd'. De hoge tonen werden omgezet in lage tonen en andersom. Aan de ontvangende kant werd de omkering weer ongedaan gemaakt. Dit principe van bandomkering of bandverschuiving is tot in de jaren zeventig toegepast.

▼ Foto 5 + 6
Links de Enigma codeermachine, zoals die door het Duitse leger gebruikt werd in WO II.
Rechts een Enigma printer.



Vlak na de Eerste Wereldoorlog, op 7 oktober 1919, diende de Delftenaar Hugo Alexander Koch een patent in voor een 'geheimschrijfmachine'. De ironie wil dat dit patent de basis zou vormen van de legendarische Enigma, de codeermachine die gedurende de Tweede Wereldoorlog gebruikt werd door de Duitse strijdkrachten. De Kriegsmarine gebruikte de Enigma voor de communicatie met de U-boten die de geallieerde konvooien op zee belaagden. Project Ultra, het ontcijferen van de Enigma-codes, kostte de geallieerden de nodige hoofdbrekens. Gedurende zes jaar werkten meer dan duizend mannen en vrouwen aan het ontcijferen ervan. Project Ultra werd bestuurd vanuit een Victoriaanse villa in Bletchley Park, even buiten Londen. Vierentwintig uur per dag werd het Duitse radioverkeer afgeluisterd. Dag en nacht werd geprobeerd om die boodschappen te ontcijferen. Dat lukte bij vlagen[2].

[2] Zie voor meer informatie het artikel *Geheime berichten in WO II: project ULTRA en de Enigma* elders in dit nummer van het Studieblad.

▼Afb. 2
Met een in citroen gedoopte pen kun je onzichtbaar schrijven. Door het papier te verwarmen boven kaarslicht (of onder een strijkijzer) wordt de boodschap leesbaar.

De Duitse Enigma was overigens niet de enige codeermachine die ontwikkeld werd tussen en tijdens de twee wereldoorlogen. De Zweedse overheid koos in 1925 bijvoorbeeld

voor de B21 van de kleine firma A.B. Cryptograph. De drijvende kracht in die firma was Boris Hagelin. Het principe van de B21 kwam in grote lijnen overeen met dat van de Enigma. De latere modellen van Hagelin gaven direct een gedrukte cijfertekst, wat het coderen natuurlijk aanzienlijk vergemakkelijkte. Na de Tweede Wereldoorlog verplaatste Hagelin zijn bedrijf naar Zug in Zwitserland, waar Crypto AG nog steeds zeer geavanceerde codeermachines maakt.

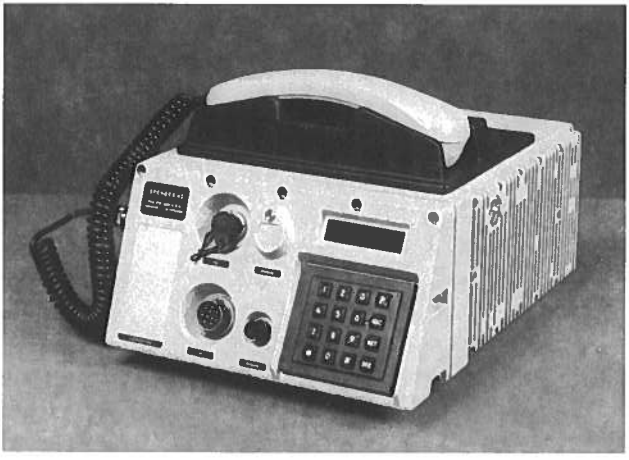
Ook het Amerikaanse leger zette in WO II geavanceerde decoderingstechnieken in om vijandelijke berichten te onderscheppen. Door met de zogeheten SIGINT-techniek de Japanse militaire code te kraken was men van tevoren op de hoogte van Japanse plannen om Midway Island te confisqueren. Uiteindelijk leidde dit tot de ondergang van Japan's machtige zeevloot en volgens de Amerikaanse overheid heeft het gebruik van SIGINT de oorlog met minimaal een jaar bekort. SIGINT speelt ook vandaag de dag nog een belangrijke rol in de handhaving van Amerika als supermacht. Maar de Amerikanen gebruikten ook meer natuurlijke en aanzienlijk goedkopere 'geheimtalen'. Zowel tijdens de Eerste als de Tweede Wereldoorlog werden er indianen ingezet voor communicatie via radiotelefonie. Hun taal was slechts door een handjevol Europeanen te begrijpen en wanneer het nog een keer gecodeerd was door (vrijwel) niemand. Dat dit principe veelvuldig werd toegepast blijkt uit het feit dat het Amerikaanse leger in 1944 Choctaw-, Commanche-, Kiowa-, Wiinebago-, Seminole-, Navajo-, Hopi- en Cherokee-indianen in dienst had.

Spraakversluiering

In de jaren vijftig nam het particuliere gebruik van radiotelefonie sterk toe (de mobilofoon). De vraag naar spraakversluiering, het onherkenbaar maken van de spraak voor meeluisteraars, steeg eveneens. Aanvankelijk bracht de zogenaamde scramble-apparatuur uitkomst. Het signaal wordt hierdoor zodanig vervormd dat er alleen een piepend geluid overblijft, dat aan de ontvangstzijde weer gedecodeerd moet worden. Maar ook voor de scannerluisteraar was deze scramble-apparatuur na enkele jaren voorhanden. Zodra het mogelijk werd geluid te digitaliseren, kon spraak met behulp van geavanceerde computers worden gecodeerd.

Een – sprekend – voorbeeld hiervan is GSM, het digitale mobiele telefoonnet van PTT Telecom dat, in tegenstelling tot de analoge autotelefoonnetten (ATF), niet afgeluisterd kan worden[3].

[3] In het laatste artikel in dit themanummer van het Studieblad wordt nader ingegaan op de gebruikte encryptiemethoden bij GSM.



◀ Foto 7
De Spendex 40, een militaire cryptofoon die vanaf 1980 wordt gebruikt.

Over computers, pincodes en buzzers

Tot de jaren zestig was cryptografie het exclusieve domein van de overheid. Voor de gewone burgers bleef het lange tijd iets James Bond-achtigs houden. Maar nu er in onze samenleving steeds meer computers komen, die ook nog met elkaar moeten communiceren, verandert dat. Moderne computers zijn in staat om duizenden instructies per seconde te verwerken. Daardoor kunnen er codeersystemen worden ontwikkeld die zo gecompliceerd zijn dat ze nooit handmatig of met mechanische apparaten gemaakt zouden kunnen worden. Een bekend algoritme is DES (Data Encryption Standard), dat in 1976 door IBM en het Amerikaanse National Institute of Standards and Technology voor de Amerikaanse overheid is ontwikkeld. Maar, ondanks het enorm grote aantal theoretische mogelijkheden, gaan er nu alweer geruchten dat ook DES niet 'echt' veilig zou zijn. Supercomputers kunnen het algoritme mogelijk 'kraken' en bovendien zou DES in opdracht van de Amerikaanse overheid een 'achterdeur' bevatten, waardoor berichten in 'noodgevallen' door Justitie of geheime diensten gedecodeerd kunnen worden. Toch is DES op dit

moment nog de meest gebruikte encryptietechnologie. Vooral in de bankwereld wordt DES veel toegepast. Zo vormt bijvoorbeeld de combinatie van onze pin-code (Persoonlijk Identificatie Nummer) en de gecodeerde informatie die op ons betaalpasje of creditcard aanwezig is, een sleutel voor DES.

▲ Afb. 3

Ook de militaire wereld staat vandaag de dag nog bol van de geheimtaal. De elektronische oorlogsvoering tijdens de Golfoorlog bestond in feite uit enorm druk gecodeerd dataverkeer in de ether, een schijnbaar Babylonische spraakverwarring. De in Operatie Desert Storm gebruikte Awacs-vliegtuigen bijvoorbeeld – met zo'n eivormige antenne bovenop de romp – zijn in feite vliegende interceptie- en decodeer-machines.

Maar ook dichter bij huis is geheimtaal niet meer te omzeilen. In de vorm van de Buzzer, het flitsende semafoontje van PTT Telecom, is het zelfs ontzettend trendy. De gebruiker

van de Buzzer betaalt – in tegenstelling tot de semafoon – alleen de aankoopprijs, dus geen abonnementskosten. De gebruikers, die zich vooral in de leefstijdscategorie 12-25 jaar bevinden, kunnen te allen tijde door vrienden of ouders worden opgepiept of 'opgevibreerd'. De boodschap kan een telefoonnummer zijn dat moet worden teruggebeld, maar veel leuker en spannender is natuurlijk het gebruik van een gecodeerd bericht. Er zijn zelfs boekjes met veelgebruikte buzzingcodes op de markt, maar doorgewinterde buzzergebruikers verzinnen liever hun eigen geheime codes.
De bovennatuurlijke krachten zoals die een rol speelden in het Babylonische Rijk, hebben gaandeweg plaatsgemaakt voor de wonderen van de moderne techniek.

Drs. L.A. Baas studeerde Geschiedenis aan de Rijksuniversiteit Leiden. Van 1992 tot 1995 was zij in dienst bij het PTT Museum te Den Haag. Sinds 1995 is mevrouw Baas werkzaam als freelance historisch onderzoekster en publiciste.

J. Caspers werkte van 1963 t/m 1989 bij het Telecomdistrict Den Haag in het onderhoud van telefooncentrales, telegraafoverdraagstation en de Centrale Besturing Semafonie. Sinds 1 december 1989 is de heer Caspers in dienst bij de afdeling Telecommunicatie van het PTT Museum waar hij zich onder meer bezighoudt met onderzoek voor tentoonstellingen.

Drs. B. Koevoets studeerde Kunstgeschiedenis en Onderwijskunde aan de Rijksuniversiteit Utrecht. Hij was onder meer werkzaam in het middelbaar onderwijs en aan de Rijksuniversiteit te Leiden. Sinds 1989 is de heer Koevoets directeur van het PTT Museum. Daarnaast is hij lid van dè onderwijsraad en vervult hij diverse functies in de (inter)nationale museumwereld.

vijftig jaar

Geheime berichten in WO I: le télégramme de la victoire

Rob Korving

Wie nu in de bossen bij het Noord-Franse stadje Compiègne ronddwaalt, loopt nog steeds kans op munitie uit de Eerste Wereldoorlog te stuiten. Wekelijks haalt de Franse explosievendienst hier de resten op van de langdurige en zeer bloedige loopgravenoorlog. WO I was niet alleen de eerste oorlog waarin een groot deel van Europa werd meegesleurd, het was ook de eerste maal in de geschiedenis dat telecommunicatie een belangrijke rol in de strijd speelde.

Ruim voor de Eerste Wereldoorlog was het Franse leger al bezig het Duitse radio-telegrafieverkeer af te luisteren. Toen de oorlog uitbrak hadden de Fransen dan ook al behoorlijk wat ervaring met het afluisteren en decoderen van radio-telegrammen. De crypto-analytische afdeling registreerde zoveel mogelijk informatie. Niet alleen de inhoud van het bericht, maar ook de gebruikte frequenties, de tijd van uitzending en de vermoedelijke lokatie van de zender werden vastgelegd. Op deze manier bouwde de Franse crypto-analytische dienst een formidabele kennis op van de Duitse militaire codes en van hun militaire terminologie. Alleen de radio-telegrammen zelf waren al goed voor een slordige honderd miljoen woorden.

Zolang de Duitsers hun landsgrenzen nog niet waren overgetrokken, legde al die kennis overigens weinig gewicht in de schaal. Het Duitse leger gebruikte voor zijn communicatie vooral een uitgebreid net van – lastig af te luisteren – vaste telegraaf- en telefoonverbindingen. De nog betrekkelijk nieuwe radio-telegrafie werd maar zelden ingezet. Dat veranderde toen de aanleg van telegraaf- en telefoonverbindingen ver achterbleef bij de snelle Duitse opmars. Radio-telegrafie werd hèt communicatiemiddel bij uitstek en het aantal berichten dat de Fransen konden onderscheppen nam in hoog tempo toe. Daarna liep het Duitse offensief vast en raakten beide partijen hopeloos verstrikt in een bloedige loopgravenoorlog. De Duitsers schakelden geleidelijk weer over op vaste verbindingen. Maar al snel bleek dat deze verbindingen uiterst kwetsbaar waren voor de voortdurende artillerie-beschietingen. Radio-telegrafie kende dit bezwaar niet en het belang van deze vorm van de communicatie werd in de loop van de oorlog dan ook steeds groter.

Een race tegen de tijd, de ÜBCHI-codering

De Duitsers gebruikten in de loop van WO I diverse codes, waarvan de sleutels snel wisselden. Meestal eens per acht à negen dagen, tijdens offensieven zelfs elke dag. Gedurende de hele oorlog bleef het ontcijferen voor de Fransen een race tegen de tijd. Soms hielp het lot een handje, bijvoorbeeld wanneer een Duitse telegrafist een stukje oefentekst seinde, een stukje niet-gecodeerde tekst in een gecodeerd bericht meestuurde, of een codesleutel gebruikte die erg voor de hand lag.

Na verloop van tijd stapten de Duitsers af van de omvangrijke en lastig te wisselen codeboeken, en voerden een coderingsmethode in die de Fransen ÜBCHI noemden. Het ging om een zogenaamde *dubbele transpositie*. Een dergelijke code werkt met een willekeurig aantal woorden dat als sleutel wordt gebruikt, zoals in het volgende voorbeeld duidelijk wordt. Die sleutel is hier *Die Wacht am Rhein*. Eerst wordt aan de letters van de sleutel een waarde toegekend. Daar zijn verschillende technieken voor, bijvoorbeeld zoals hier

▼ Foto 1
Strijd in de loopgraven, WO 1.

de volgorde van de letters in het alfabet. Letters die meerdere keren voorkomen in de sleuteltekst, krijgen een opeenvolgende waarde. Zo krijgt de eerste *A* in de sleutel de waarde *1* en de tweede *A* de waarde *2*. De volgende letter is de *C*, die de waarde *3* krijgt, de vierde de *D* waaraan *4* wordt toegekend. Het geheel ziet er als volgt uit:

D I E W A C H T A M R H E I N

4 9 5 15 1 3 7 14 2 11 13 8 6 10 12
(stap 1)

Onder deze getallen wordt het bericht in een tabel geschreven. De tekst *Tiende divisie X Val overdag Montigny sector aan X Vooraf gasaanval* ziet er dan zo uit:

4 9 5 15 1 3 7 14 2 11 13 8 6 10 12

T I E N D E D I V I S I E X V
A L O V E R D A G M O N T I G
Y S E C T O R A A N X V O O R
A F G A S A A N V A L

Uit deze tabel worden, in de volgorde van de waarde van de letters, een aantal groepen van vier letters gemaakt. De eerste groep, onder de 1, bevat de letters DETS. De tweede groep de letters VGAV enzovoort. Dat geeft het volgende resultaat:

DETS VGAV EROA TAYA EOEG ETO DDRA INV ILSF XIO IMNA VGR SOXL IAAN NVCA (stap 2)

De meesten van u zullen zich hier misschien al geen raad meer mee weten, maar met wat wiskundige technieken lost een cryptoloog een enkele transpositie snel op. In de volgende stap wordt de transpositie herhaald. De lettergroepen worden opnieuw in een tabel geschreven. Bovendien worden er net zoveel loze letters aan toegevoegd als er woorden in de codesleutel waren. In ons geval zijn dat er vier, de loze letters zijn WXYZ.

4 9 5 15 1 3 7 14 2 11 13 8 6 10 12

D E T S V G A V E R O A T A Y
A E O E G E T O D D R A I N V
I L S F X I O I M N A V G R S
O X L I A A N N V C A *W X Y Z*
(stap 3)

Opnieuw worden er verticale groepen van vier letters genomen. Dat geeft het volgende resultaat:

VGXA EDMV GEIA DAIO TOSL TIGX ATON AAVW EELX ANRY RDNC YVSZ ORAA VOIN SEFI (stap 4)

Ten slotte worden deze lettergroepen verdeeld in standaardgroepen van vijf letters en in Morse verzonden:

VGXAE DMVGE IADAI OTOSL TIGXA TONAA VWEEL XANRY RDNCY VSZOR AAVOI NSEFI (stap 5)

Het ontcijferen verliep in de omgekeerde volgorde. De dubbele transpositie is lastig te breken. Bovendien moesten de Franse crypto-analisten eerst proberen uit te vinden hoeveel regels en kolommen de gebruikte tabel had voordat ze konden proberen om met een scala aan wiskundige technieken de tekst te ontcijferen. De ontcijfering van een dubbele transpositie werd overigens wel iets eenvoudiger wanneer er berichten beschikbaar waren met exact dezelfde lengte, die bovendien gecodeerd waren met dezelfde sleutel. En bij druk radioverkeer kwam dit nogal eens voor.

Ondanks de problemen lukte het de Franse crypto-analisten om ÜBCHI regelmatig te breken. Op een gegeven ogenblik was hun succes zelfs zo groot dat het hele front met spanning naar de nieuwe ontcijferde berichten uitkeek. De Duitsers hadden blijkbaar niets in de gaten en vertrouwden blindelings op hun systeem. Dat veranderde toen de Duitse keizer, Wilhem II, het front in Thielt (België) bezocht. Doordat het bericht van zijn komst ontcijferd was, werd hij bij Thielt door de Fransen beschoten. Dat verhaal was te mooi om geheim te houden en een dag later werd er dan ook met veel tamtam verslag van gedaan in *Le Matin*. Dat konden zelfs de Duitsers niet meer over het hoofd zien en

de volgende dag werden alle codes veranderd. De Fransen ontcijferden de nieuwe Duitse codes meestal nog makkelijker dan ÜBCHI. Maar in 1918 kwam daar verandering in.

ADFGX

Afgezien van de in maart gesloten vrede van Brest-Litovsk, waardoor de oorlog met Rusland werd beëindigd, begon 1918 als een slecht jaar voor de Duitsers. De invloed van Amerikaanse troepen aan het Westelijke Front werd steeds duidelijker merkbaar, de U-boten hadden Engeland nog lang niet op de knieën gedwongen en het moreel van de Duitse troepen aan het Westelijk Front was beneden peil. De oplossing was – althans volgens de Duitse generale staf – een nieuw offensief.
In maart 1918 kwamen de Duitsers wederom met een gewijzigde code. Terwijl alle inlichtingen wezen op een nieuw Duits offensief, waren de geallieerden verstoken van informatie uit radio-telegrammen. Bij de eerste berichten in de nieuwe code kregen de Franse crypto-analisten een

▶ Afb. 1
Voorbeeld van een ADFGX-transpositie.

THE ADFGX CIPHER — TRANSPOSITION KEY

8	9	14	7	19	13	16	1	15	6	3	10	17	2	20	5	11	18	4	12
F	X	D	D	A	G	G	F	X	A	D	G	G	X	D	D	A	G	X	A
G	X	A	G	X	A	F	A	G	X	G	X	X	A	A	A	D	F	G	A
G	X	D	D	F	A	A	D	A	D	X	A	D	X	X	D	G	G	G	G
X	A	F	X	X	A	X	X	G	F	F	A	F	F	A	X	F	A	G	G
G	X	X	D	X	A	F	F												

Message : Forced to retreat ten km to Abbeville few casualties

THE ADFGX CIPHER — COMPLETED TRANSPOSITION

FADXF XAXFD GXFXG GGDAD XAXDF DGDXD

FGGXG XXXAX GXAAA DGFAA GGGAA AADAD

FXXGA GGFAX FGXDF GFGAA XFXXD AXA

onbehagelijk gevoel. ADFGX, zoals de code werd genoemd omdat dit de enige letters waren die in de berichten voorkwamen, was iets totaal nieuws.

De belangrijkste Franse crypto-analist uit de Eerste Wereldoorlog, luitenant George Painvin, kwam er wel snel achter dat de basis van ADFGX een bekende methode van versleutelen, *het schaakbord*, was. Maar daar bleef het bij, ondanks al zijn pogingen lukte het hem niet om uit ADFGX begrijpelijke teksten te krijgen. Waarschijnlijk was de Duitse code een combinatie van twee systemen en werd de code uit het schaakbord nog een keer gecodeerd met een transpositie. De meeste wiskundige technieken zijn in zo'n geval onbruikbaar.

De tekst: *Tiende divisie...* ziet er gecodeerd met een schaakbord en opgedeeld in groepen van vijf letters als volgt uit:

GXFGA XAFXF AXXFF GFVFG DGFGAX

	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	l	0	j	d
G	5	s	i	y	h	u
V	p	1	v	b	6	r
X	e	q	7	t	2	g

Eind maart 1918 begonnen de Duitsers inderdaad met hun lente-offensief en braken dwars door het geallieerde front bij de Somme. Toen de strijd luwde stonden ze nog maar een goede 90 kilometer van Parijs, dat onder Duits vuur kwam te liggen. De enorme hoeveelheid radioverkeer tijdens het offensief verminderde en Painvin kreeg de tijd om de opgevangen berichten te analyseren. Hij slaagde erin om een deel te ontcijferen. Met behulp van die kennis probeerde hij de recente berichten aan te pakken. Daarbij hielp het toeval hem een handje. De Fransen onderschepten twee even lange telegrammen, die grotendeels dezelfde tekst bevatten. Het decoderen lukte en Painvin kreeg de sleutel eind mei in handen.

▶ Foto 2
George Painvin, de belangrijkste Franse crypto-analist in WO 1.

Chi 126, het télégramme de la victoire

Op het geallieerde hoofdkwartier was inmiddels duidelijk dat generaal Ludendorff het niet bij dit offensief zou laten. De vraag was, waar kwam de nieuwe aanval? Op 3 juni werd een cryptogram opgevangen dat als code Chi(ffre) 126 had en blijkbaar van het Duitse hoofdkwartier afkomstig was. De tekst luidde als volgt:

FGAXA XAXFF FAFFA AVDFA GAXFX FAAAG DXGGX AGXFD XGAGX
GAXGX AGXVF VXXAG XFDAX GDAAF DGGAF FXGGX XDFAX GXAXV
AGXGG DAFGD GXVAX XFXGV FFGGA XDGAX ADVGG A

Painvin paste op dit telegram zijn sleutel toe en er verscheen inderdaad een begrijpelijk bericht:

Munitionierung besleunigen Punkt Soweit nicut (nicht) eingesehen auch bei Tag (De aanvoer van munitie bespoedigen. Punt. Als het niet ontdekt kan worden ook overdag)

Het bericht was bestemd voor het front tussen Montdidier en Compiègne. Terecht vermoedden de geallieerden dat de volgende aanval gericht zou zijn op dit deel van het front. Het opperbevel gaf opdracht om de voorste linies grotendeels te ontruimen en wachtte gespannen af. Op 9 juni kwam de aanval inderdaad, vooraf gegaan door een gigantisch bombardement met vrijwel alle materieel die de Duitsers in die regio voorhanden hadden. Even leek hun opmars nog succes te hebben, maar twee dagen later brachten de Franse divisies generaal Ludendorff tot staan.
Na die datum slaagden de Duitsers er niet meer in een nieuw groot offensief tot stand te brengen. In Duitsland kwam de keizer ook politiek onder druk te staan. Op 11 november 1918 was de oorlog voorbij. In het bos van Compiègne werd een wapenstilstand gesloten. George Painvin overleefde de oorlog al was hij, zittend achter zijn bureau, in die tijd ruim 15 kilo gewicht kwijtgeraakt!

Drs. R.A. Korving studeerde Geschiedenis aan de Rijksuniversiteit te Leiden. Sinds 1 juli 1989 is hij werkzaam bij het PTT Museum als conservator Telecommunicatie.

vijftig jaar

Geheime berichten in WO II: project ULTRA en de Enigma

Rob Korving

Over het supergeheime Engelse project ULTRA – opsporen en uitschakelen van Duitse U-boten – is na de Tweede Wereldoorlog buitengewoon veel gespeculeerd. Zo geheim was ULTRA dat het jaren duurde voordat de betrokkenen het waagden erover te praten en het duurde nog langer voordat er materiaal over vrijkwam. Het Studieblad nam een duik in de archieven.

In de Eerste Wereldoorlog had de Duitse *Kriegsmarine* onderzeeboten ingezet om Engeland op de knieën te krijgen. Dat was mislukt. De gebruikte tactiek was simpel, iedere U-boot opereerde zelfstandig en moest zoveel mogelijk geallieerde schepen tot zinken brengen. De U-boten hadden een radio aan boord, maar om ontdekking te voorkomen, werd absolute radiostilte zoveel mogelijk gehandhaafd.

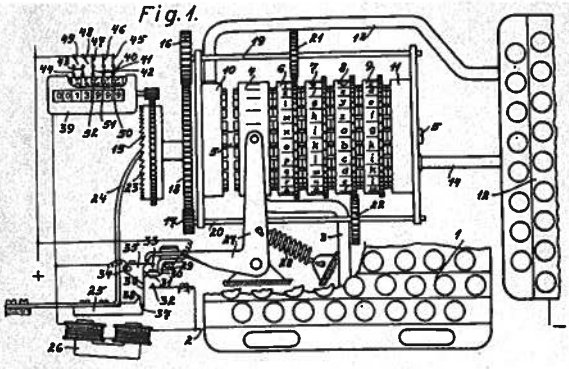
In de Tweede Wereldoorlog werd de solitaire actie van U-boten verlaten. Radio-telegrafie ging een veel belangrijker rol spelen dan in WO I. De U-boten opereerden nu, net als wolven, groepsgewijs in zogenaamde *roedels*. Als een onderzeeboot een konvooi opspoorde, werd de positie – in code – meteen doorgeseind aan het U-boot hoofdkwartier dat eerst in Parijs en later in Kiel was gevestigd. Vervolgens bleef de kapitein het konvooi volgen zonder het aan te vallen. Het hoofdkwartier dirigeerde zo snel mogelijk een aantal andere U-boten naar de opgegeven plek. Zodra er voldoende waren – het aantal liep meestal uiteen van tien tot zestien – werd het konvooi aangevallen. Het aantal tot zinken gebrachte geallieerde schepen liep hierdoor dramatisch op.

ULTRA

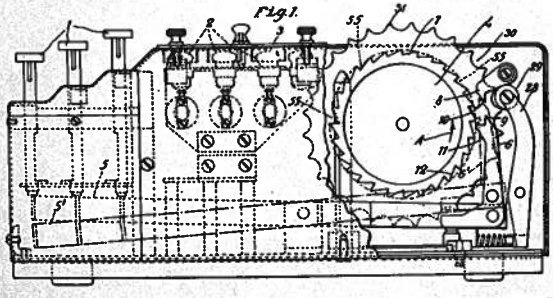
Project ULTRA startte eigenlijk pas nadat de Duitsers en de Russen in september 1939 Polen binnenvielen. Een aantal medewerkers van de Poolse geheime dienst, die flinke ervaring had met het ontcijferen van de Duitse codes, vluchtte via Frankrijk naar Engeland. Tussen de Franse en de Poolse geheime diensten bestond al sinds 1931 een goede samenwerking. Beide diensten deden verwoede pogingen om de Duitse gecodeerde radioberichten te ontcijferen. Tot 1926 gaf dat geen onoverkomelijke problemen. Maar vanaf die tijd werd een steeds groter deel van de radio-telegrammen onleesbaar. Uit het type code was duidelijk dat de Duitsers

inmiddels gebruik maakten van een of andere codeermachine. In 1931 kwam het antwoord op dit raadsel. De Franse geheime dienst werd benaderd door een Duitser die geheime informatie te koop aanbood. Deze spion, die van de Fransen de codenaam REX kreeg, werkte in Duitsland bij een afdeling die telegrammen voor de Wehrmacht codeerde en decodeerde. Uit de informatie die REX gaf bleek dat de Duitsers inderdaad gebruik maakten van een geavanceerde elektro-mechanische codeermachine, de *Enigma*.

De Enigma werd door een kleine Berlijnse firma, *Gewerschaft Securitas* gemaakt. De eigenaar, Arthur Scherbius, had in 1919 een Nederlands patent aangekocht dat het



A drawing from Arthur Scherbius's U.S. initial patent for the Enigma. Figure 1 shows the typewriter keyboard (1), the input plate (4), the rotors (6, 7, 8, 9), and the output (12), here a perforator for a teletypewriter paper tape. There is no reversing rotor; the current goes through the rotor sequence only once.



A side elevation of an Enigma machine, from Willi Korn's patent for adding notches to each rotor's alphabet ring to vary the advancing of the adjacent rotors.

◀ Afb. 1
Patent op de Enigma, zoals aangekocht door Arthur Scherbius.

principe beschreef van een codeermachine met een aantal draaiende codeschijven (rotoren).
Scherbius slaagde erin om het Nederlandse patent om te zetten in een werkend en verkoopbaar apparaat. Hij bood het aan de Duitse overheid en een aantal grote bedrijven aan. Die testten de Enigma, vonden het een uitstekend apparaat, maar bestelden er slechts een paar van. Eind jaren '20, tijdens de opkomst van het Hitler-regime en de daarmee verbonden snelle opbouw van de Duitse strijdkrachten, veranderde dat. Tijdens de Tweede Wereldoorlog was de Enigma uitgegroeid tot de standaard-codeermachine van de Duitsers. De Kriegsmarine, de Wehrmacht en de Duitse geheime diensten kochten er enkele honderden.

De Enigma

De Enigma werd in een aantal varianten op de markt gebracht. Er waren uitvoeringen voor commercieel en voor militair gebruik. Het was een zeer robuust apparaat. In de eenvoudigste uitvoering, die ook door de Nederlandse PTT gebruikt is om overheidstelegrammen met Indië te coderen, bestond de Enigma uit een stuk of zes onderdelen. Er was een toetsenbord, één vaste rotor (de reflector) en drie draaiende rotoren, een batterij en een paneel met letters waaronder lampjes waren gemonteerd.
Een Enigma met 'commerciële' rotoren kon niet gebruikt worden om een militair bericht te ontcijferen of omgekeerd. Bovendien gebruikten de Duitse legeronderdelen voor hun communicatie verschillende typen rotoren. Een U-boot had een set van vijf verschillende rotoren aan boord, waarvan er steeds drie werden gebruikt.
De draaibare rotoren, die in willekeurige volgorde in de Enigma geplaatst konden worden, hadden aan beide kanten elektrische contacten. Tussen die contacten zat bedrading, die per type rotor verschilde. Bovendien had iedere rotor een letterring die ook nog veranderd kon worden. De ring kon in een groot aantal standen worden vastgezet.

Om een bericht te coderen werden eerst de letterringen van de rotoren in een bepaalde stand gezet (stap 1).

Daarna werden de rotoren in een bepaalde volgorde in de Enigma gezet (stap 2). Vervolgens draaide de bediener van het apparaat ze in de beginstand (stap 3). De Enigma was nu klaar voor gebruik. Een bericht coderen gebeurde door het letter voor letter in te typen (stap 4). Bij iedere aanslag lichtte een lampje op, waardoor de gecodeerde letter zichtbaar werd. In de praktijk werd het coderen en decoderen vaak door twee telegrafisten gedaan; de een typte de boodschap in, terwijl de ander de gecodeerde of gedecodeerde letters opschreef.

De Enigma had niet de mogelijkheid om een gecodeerd bericht direct in schrift om te zetten. Het coderen en decoderen was daardoor een tijdrovende bezigheid. Wel handig was dat dezelfde basisinstelling gebruikt kon worden om een bericht te coderen èn te decoderen. Door de toepassing van drie rotoren (later werden het er vier), die ieder in een groot aantal posities konden worden gezet, was het aantal mogelijke codes zeer groot. Toch had de Enigma ook zijn zwakke kanten. Een gecodeerde letter kon nooit dezelfde zijn als de letter in de originele tekst. De cryptologen van project Ultra maakten dankbaar van deze eigenschaft gebruik. Verder moest de beginpositie van de rotoren aan het begin van een telegram worden verzonden. Dat gebeurde in een code die beduidend minder veilig was.

Dat de Duitsers de Enigma gebruikten, hadden ook de Polen inmiddels ontdekt. Via een stroman slaagden zij erin om een commercieel apparaat te kopen. Maar hun onderzoek zat verder muurvast. Dat veranderde toen de Fransen informatie doorspeelden die ze REX hadden ontfutseld. Het ging om een beschrijving van de werking van de Enigma, een handleiding voor het coderen en het belangrijkste van alles: de volgorde waarin de rotoren de komende periode zouden worden geplaatst.

▲ Foto 1
De Enigma die werd gebruikt door de Kriegsmarine.

Rewjeski en de bomba

Onder leiding van hun begaafdste cryptoloog, Marian Rewjeski, slaagden de Polen erin de interne bedrading van een paar rotoren te reconstrueren. Ze maakten tabellen en

lieten bij een kleine Poolse firma een apparaat bouwen waarmee snel getest kon worden of een bepaalde instelling van de Enigma inderdaad leesbare tekst opleverde. Dit apparaat noemden zij een *bomba* (Pools voor *bom*). Met deze bomba slaagden zij erin een deel van de Duitse gecodeerde berichten te ontcijferen.

De Polen hielden hun succes in eerste instantie zelfs voor hun geallieerde bondgenoten verborgen. Maar kort na de Duitse inval in Polen werd alle informatie over het Poolse Enigma-project samen met een tweetal bomba's toch doorgespeeld aan de geallieerden. De Fransen waren in de tussentijd overigens geen stap verder gekomen en de Engelse cryptologische afdeling stelde weinig voor. De Poolse kennis en vooral de bomba's kwamen dan ook als een geschenk uit de hemel.

Bletchley Park

Kort na de Britse oorlogsverklaring werd de Britse cryptologische dienst overgebracht naar een grote villa in Bletchley Park, een goede 75 kilometer buiten Londen. De kans op Duitse bombardementen was daar een stuk geringer dan in de stad zelf. Via een slimme recrutering werd de afdeling uitgebreid, van een paar medewerkers tot bijna honderd man. Project ULTRA was een feit. De bewoners van Bletchley Park vormden een bont gezelschap. Er waren geniale wiskundigen onder, zoals Alan Turing en Gordon Welchman, maar ook historici, een docent oude talen en zelfs een paar archeologen. Een aantal van hen was gerecruteerd met behulp van een prijsvraag in de Britse kranten. Wie het beste een aantal ingewikkelde cryptogrammen kon oplossen, kreeg een prijs en werd direct gevraagd zijn of haar medewerking te verlenen aan ULTRA.

In de villa werd dag en nacht gewerkt. De medewerkers logeerden in hotels en pensions in de directe omgeving. Omdat het huis al snel veel te klein was, werden er een aantal houten noodgebouwtjes op het terrein neergezet, de zogenaamde hutten. Vooral bekend werden *hut 4* (Wehrmacht), *hut 8* (Kriegsmarine) en *hut 11* (hier stonden de tot *bombes* omgedoopte opvolgers van de Poolse bomba's).
De Engelse aanpak voor het ontcijferen van de Enigma-

◀ Foto 2
Bletchley Park.

code verschilde aanzienlijk van die van de Polen. De laatsten gebruikten de 'brute force' aanval; ze testten alle mogelijke standen van de rotoren uit met hun bomba's totdat er een leesbare tekst ontstond. Door het grote aantal mogelijkheden was dat een behoorlijk tijdrovend en arbeidsintensief proces. De Engelsen werkten met stukken tekst waarvan ze vermoedden dat die in een bericht voorkwamen. Zo'n stuk tekst noemden zij een *crib*, een wieg. Een voorbeeld van zo'n crib was de vaste Duitse frase 'nichts zu melden'.
Turing en Welchman zagen al snel in dat het reciproque karakter van de Enigma – als een A gecodeerd een Z opleverde dan leverde een Z bij dezelfde instelling ook weer een A op – een zwakke plek van de machine was. Een tweede aanknopingspunt was het Duitse gebruik van vaste uitdrukkingen. Zo werden weerberichten en plaatsbepalingen doorgegeven met behulp van lijsten met afkortingen.

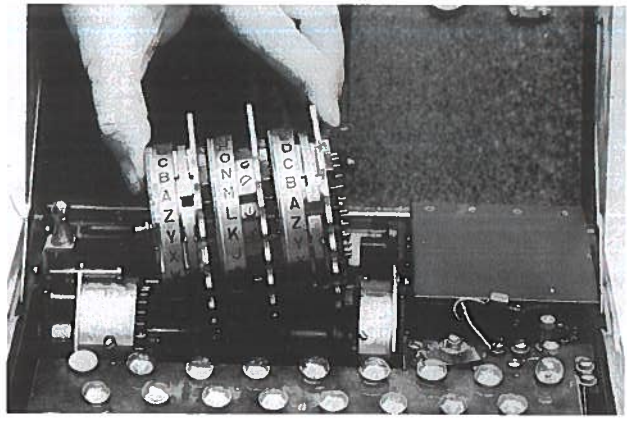
De U-33 en de Krebs

Ondanks alle inspanningen lukte het de Engelsen de eerste tijd niet om een substantieel deel van de Duitse berichten op tijd te ontcijferen. Tot op 12 februari 1940 de Britse mijnenveger *Gleaner* in de buurt van Schotland bij toeval de Duitse onderzeeër *U-33* ontdekte. De *Gleaner* gooide een serie dieptebommen, die de onderzeeboot zo beschadigden dat hij naar de oppervlakte moest komen. Voor zij evacueerde blies de bemanning het schip op. De *Gleaner* pikte daarna de Duitse zeelui op. Toen hun kleren gedroogd wer-

den, bleek in een van de leren broeken een vreemde set ronde schijven te zitten. De matroos die de opdracht had gekregen om de rotoren van de Enigma overboord te gooien, was dat in alle paniek vergeten!

Door deze buitenkans kreeg ULTRA de interne bedrading van drie rotoren te pakken. Toch lukte het nog steeds maar mondjesmaat om berichten te ontcijferen. Tot in 1941 het toeval weer een handje hielp. Tijdens een Engelse aanval op een walvisstation op een van de Lofoten, een groep eilanden bij Noorwegen, werd een bewapende Duitse trawler veroverd. De Enigma die de *Krebs* aan boord had was weliswaar overboord gegooid, maar in de stuurhut lagen de instellingen voor de lopende maand nog. Bovendien vonden de Engelsen in de hut van de kapitein twee extra rotoren.

▶ Foto 3
Enigma-rotoren.



De Wetterkurzschlüssel

Met al die informatie lukte het een tijdlang het grootste deel van de onderschepte berichten te decoderen. Maar toen de instellingen van de Enigma weer wijzigden, besloten de Britten het lot een handje te helpen. Omdat de depressies die in de buurt van IJsland ontstonden het weer in Europa beïnvloeden, opereerden in dat gebied als trawler vermomde Duitse weerschepen. Die hadden ook een Enigma aan boord.
Het doel van de Britse actie was de Duitse trawler *München*. De Engelsen naderden het zwak bewapende schip heimelijk

en na een kort vuurgevecht werd het veroverd. Ze vonden geen spoor van een Enigma, maar wel de zogenaamde *Wetterkurzschlüssel*, het codeboek waarmee de Duitse weerberichten werden gedecodeerd. Omdat dit soort weerberichten ook door U-boten werd verzonden, leverde het boek de Engelsen op termijn een schat aan cribs op.

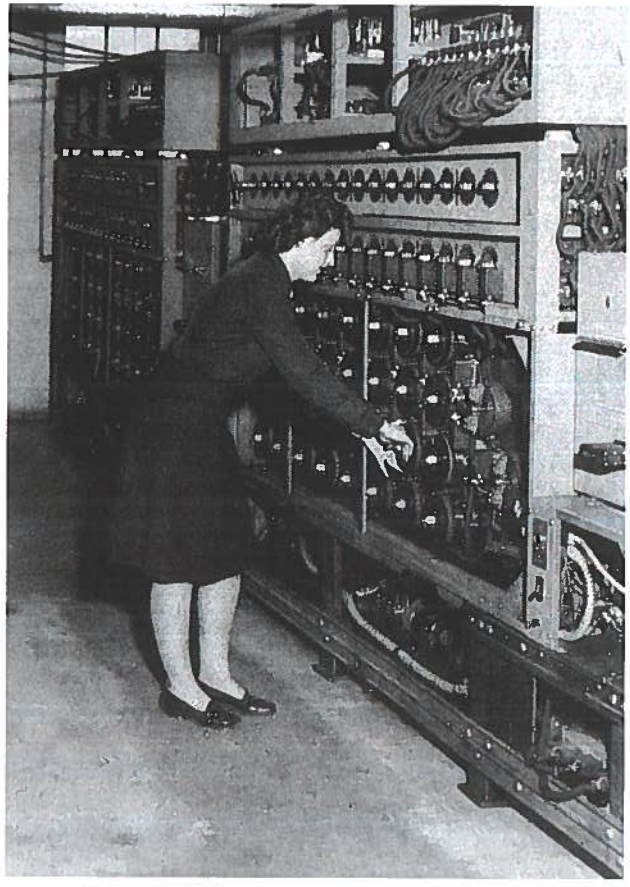
Een vierde rotor

In 1942 stopte de stroom van gedecodeerde berichten uit Bletchley Park plotseling. De Kriegsmarine was argwanend geworden en had een Enigma met vier, in plaats van drie rotoren in dienst genomen. De bombes waren daarvoor niet geschikt en op dit kritische moment in de oorlog konden de geallieerden een tijdlang niet achterhalen waar de U-boten zich bevonden. Het aantal schepen dat getorpedeerd werd nam snel toe en binnen ULTRA werd wanhopig gezocht naar een oplossing. Zonder veel succes overigens. In heel 1942 werden uiteindelijk maar een paar berichten van en aan Duitse U-boten gedecodeerd. Het toeval kwam de Britten echter ook dit keer weer te hulp. In september 1942 werd de Duitse onderzeeër U-559 in de Middellandse Zee aangevallen en naar de oppervlakte gedirigeerd. Britse zeelui slaagden er in om de instellingen van de Enigma voor de lopende periode uit het schip te halen.
De uiteindelijke doorbraak kwam met de komst van massale Amerikaanse hulp. Er kwamen experts van IBM over om de werking van de bombes te bestuderen. Het aantal nam ook snel toe, waardoor het mogelijk werd om meer cribs uit te testen. Het personeelsbestand van Bletchley Park breidde zich fors uit. Op het hoogtepunt werkten er naast de cryptologen nog eens zo'n 2000 WREN's (vrouwelijk marinepersoneel). Zij bedienden vooral de nieuwe bombes. De Duitse geheime berichten werden vaak dezelfde dag nog gekraakt en de rest van de oorlog hoefden de geallieerden niet meer te vertrouwen op het onberekenbare toeval.

Dönitz

De informatie die de geallieerden van de staf in Bletchley Park kreeg, heeft ongetwijfeld invloed gehad op het verloop van de oorlog. Na 1943 daalde het aantal door U-boten tot zinken gebrachte schepen aanzienlijk. Voor een deel kwam

▶ Foto 4
Bediening van een bombe.



dat door het ontcijferen van de met de Enigma gecodeerde berichten. Doordat de positie van de roedels U-boten bekend was, konden konvooien langs deze gebieden worden gedirigeerd. Toch is het onjuist alle successen aan ULTRA toe te schrijven. Ook een verbetering van het konvooisysteem, de beschikking over meer en snellere torpedobootjagers en de komst van vliegtuigen met radar en een grote actieradius beïnvloeden de strijd tegen de Duitse onderzeeboten.

Hadden de Duitsers dan al die tijd niets door? Er zijn in de loop van de oorlog genoeg aanwijzingen geweest dat de Enigma niet veilig meer was. Toch bleven de Duitse experts

onvoorwaardelijk in het apparaat geloven en werd het niet vervangen. Theoretisch hadden zij gelijk, zonder cribs waren de Enigma-telegrammen met de apparatuur van die tijd onbreekbaar. Zelfs nu nog is een 'brute force' benadering met snelle computers een tijdrovende zaak. Los daarvan zou de ontwikkeling van een nieuwe codeermachine en van de vervanging van alle in gebruik zijnde Enigma's een zeer omvangrijke operatie geweest zijn.
Het lijkt erop dat de voor de U-boten verantwoordelijke admiraal, Dönitz, de laatste twee jaar van de oorlog een aantal maal getwijfeld heeft aan de betrouwbaarheid van de Enigma. Toch waren er steeds ook andere redenen waarom de geallieerden zijn U-boten konden opsporen. Tot de laatste dag heeft de Kriegsmarine de Enigma gebruikt. De Wehrmacht daarentegen vertrouwde tegen het eind van de oorlog steeds meer op de *Geheimschreiber* van Siemens, die direct aan het telexnet kon worden gekoppeld. Maar de geallieerden slaagden er ook in om ook deze codes met behulp van de Colossus, een van de eerste elektronische computers, te kraken.

Drs. R.A. Korving studeerde Geschiedenis aan de Rijksuniversiteit te Leiden. Sinds 1 juli 1989 is hij werkzaam bij het PTT Museum als conservator Telecommunicatie.

Cryptologie
Deel 1: Beveiliging van informatie- en communicatiesystemen

Gert Roelofsen
Johan (Hans) van Tilburg*

Mensen versturen hun vertrouwelijke berichten al eeuwenlang op zo'n manier dat de inhoud ervan voor derden niet-leesbaar is. Een van oudsher bekende vorm is het schrijven van brieven in geheimtaal. De oude Grieken en Romeinen hielden zich hier al mee bezig. Tegenwoordig wordt het versluieren van informatie op veel meer terreinen toegepast. De sterke opkomst van nieuwe communicatie- en informatietechnologie is daar de oorzaak van. Voor cryptografen, mensen die gespecialiseerd zijn in de ontwikkeling van vercijfermethodes, zijn het dan ook gouden tijden. Zij zijn het die met hun kennis en vindingrijkheid de grondslag leggen voor onder andere computer- en gebouwbeveiliging, een veilig verloop van het betalingsverkeer, niet-afluisterbare mobiele communicatienetwerken en vertrouwelijke elektronische postsystemen. Kortom, zij leveren het gereedschap dat voor de geheimhouding en integriteit van het berichtenverkeer zorgt. Zaken waaraan in het informatietijdperk zo dringend behoefte bestaat.

* Dit artikel is voor PTT Telecom Studieblad bewerkt en van aantekeningen voorzien door Ysbrand van der Veen.

De cryptologie, de leer van het geheimschrijven, bestaat uit twee nauw verwante activiteiten:
- de cryptografie oftewel het ontwerpen van geheimschriften,
- de crypto-analyse, dat wil zeggen het analyseren van geheimschriften.

Het klassieke doel van de cryptografie is de geheimhouding van een boodschap te waarborgen, waardoor vreemde ogen geen kennis van de inhoud kunnen nemen. Dit valt onder andere te bereiken door de 'klare' tekst van een boodschap met behulp van een *cryptografisch algoritme* en een *geheime sleutel* te vercijferen. Alleen wie de geheime sleutel bezit zal de vercijferde tekst vervolgens weer kunnen ontcijferen; dat is althans de bedoeling van de cryptograaf. De werkelijkheid ziet er soms anders uit, omdat crypto-analisten zullen proberen het gebruikte algoritme te 'breken' of 'kraken' en op die manier achter de geheime sleutel te komen[1].

[1] N.B. Het analyseren van geheimschriften is iets totaal anders dan het inbreken op computersystemen. De aan computerkrakers toegeschreven vindingrijkheid bestaat vaak alleen maar uit het gebruik maken van de laksheid of medeplichtigheid van gebruikers en uit het onvoldoende beveiligd zijn van computersystemen. In goed beveiligde systemen is het vrijwel onmogelijk op de informatie in te breken.

De bekendste bouwstenen van een cryptografisch algoritme zijn de *substitutie*, het volgens een vast patroon vervangen van letters/symbolen in de 'klare' tekst, en de *transpositie* (of permutatie), het veranderen van de volgorde in het oorspronkelijke bericht. Een variant van de substitutietechniek is het codeboek waarbij woorden en begrippen door codes vervangen worden. Een andere variant is de poly-alfabetische substitutie waarbij voor de vervanging van symbolen steeds wisselende patronen worden gebruikt. In het vervolg van het artikel komen we hierop terug.

In onze moderne tijd wordt de cryptografie niet alleen toegepast om berichten te vercijferen maar ook om de echtheid ervan te waarborgen. Voorbeelden hiervan zijn:
- identificatie van een persoon; is iemand inderdaad wie hij/zij beweert te zijn,
- vaststelling van de integriteit van een bericht; heeft het bericht tijdens de verzending geen veranderingen ondergaan.

In samenhang met dit moderne gebruik van de cryptografie is het begrip *cryptografisch protocol* de afgelopen jaren steeds belangrijker geworden. We doelen dan op een samenstel van elkaar opvolgende acties, zoals een berichtenuitwisseling die tot doel heeft een bepaalde beveiligingsfunctie te realiseren. Doorgaans wordt daarbij gebruik gemaakt van één of meerdere cryptografische algoritmen.

Het valt buiten het kader van dit artikel om een uitgebreide beschrijving van de geschiedenis van de cryptologie te geven. Wij verwijzen u daarvoor naar de voorgaande artikelen in dit themanummer van het Studieblad. Voor een goed overzicht is het echter wel handig hier even snel door de rijke en boeiende geschiedenis van de crytografie heen te bladeren. Vanuit de historische ontwikkeling zijn de huidige toepassingen van het geheimschrijven namelijk gemakkelijker te plaatsen en begrijpen. De kern van dit artikel bestaat vervolgens uit een overzicht van moderne cryptografische technieken en toepassingen. De huidige ontwikkelingen in de telecommunicatiesector – draadloos en draadgebonden – zijn zonder deze technieken en toepassingen eenvoudigweg ondenkbaar.

Enkele bladzijden uit de geschiedenis van de cryptologie

Over de geschiedenis van de cryptologie is veel geschreven. Een klassiek boek is 'The codebreakers' van David Kahn. In het Nederlands zijn er helaas maar weinig boeken over dit onderwerp verschenen. Een toegankelijk en populair Nederlandstalig overzicht van de cryptologie zult u in de boekhandel vergeefs zoeken[2]. Deze speciale uitgave van het Studieblad voorziet dan ook in een leemte.

[2] Een goed Engels overzicht geeft: D. Kahn, *The codebreakers*, New York, 1967. Het boek van D. Tyler Moore en M. Waller, *Cloak and Cipher* (1962) is in een Nederlandse vertaling verschenen maar helaas niet meer verkrijgbaar: *Geheimschriften en codes*, Prisma 1328, Utrecht / Antwerpen 1968. Wie toch naast dit nummer van het Studieblad op zoek wil naar een Nederlandstalig overzicht van de cryptologie zal terug moeten vallen op collegedictaten die op universiteiten worden gebruikt.

Voor wie meer wil weten over cryptologie

In het recente verleden zijn heel wat boeken over cryptologie verschenen. Een praktisch en uitgebreid overzicht van cryptografische technieken wordt gegeven in: Bruce Schneider, *Applied Cryptography*, New York, 1996 (Second Edition).
Hoewel op historische deelonderwerpen nog regelmatig boeken verschijnen geeft het eerdergenoemde boek *The codebreakers* van David Kahn (zie noot 2) nog steeds het beste overzicht van de geschiedenis van de cryptologie tot ongeveer 1950.

De belangrijke rol van de crypto-analyse in Nederlands-Indië wordt beschreven in: R.D. Haslach. *Nishi No Kaze Hare, Nederlands-Indische inlichtingendienst contra agressor Japan*. Dankzij goede crypto-analisten is men daar veel te weten gekomen over zwakheden in bepaalde geheimschriften. Vooral tijdens de Tweede Wereldoorlog zijn indrukwekkende prestaties verricht. Door grote kennis van zaken kon een gedeelte van de Japanse geheime berichtgeving ontcijferd worden. De Nederlands-Indische inlichtingendienst bleek geregeld een stap op de Japanners vooruit. Eens te meer wordt daarmee duidelijk dat de cryptografie niet goed beoefenend kan worden zonder voldoende kennis van de crypto-analyse.
Naast bovengenoemde boeken is er een Engelstalig tijdschrift dat zich voornamelijk richt op de geschiedenis van de cryptologie. Dit tijdschrift *Cryptologia: a cryptology journal* wordt gepubliceerd door de US Military Academy West Point en verschijnt eens per kwar-

taal. Ook geïnteresseerden in moderne cryptografische technieken kunnen in het actuele tijdschriftenaanbod hun hart ophalen. Zo verschijnt sinds 1988 het kwartaalblad *Journal of Cryptology*, een uitgave van de International Association for Cryptologic Research (IACR). Over cryptografische onderwerpen verschijnen ook regelmatig artikelen in *IEEE Transactions on Information Theory* en in *Design, Codes and Cryptography*. Een meer algemeen en populair tijdschrift dat aandacht besteed aan cryptografie is *Computers and Security*.
Behalve het uitgeven van een tijdschrift verzorgt de internationale beroepsgroep van cryptologen (IACR) ook diverse congressen. In de Verenigde Staten (Crypto) en Europa (Eurocrypt) is sprake van een jaarlijks terugkerend evenement. In Australië en Azië belegt de International Association for Cryptologic Research eens in de paar jaar congressen.

De IACR heeft een eigen pagina op het World Wide Web (WWW) van Internet: *http://www.swcp.com/~iacr/*. Een goed uitgangspunt voor het zoeken naar verdere informatie over cryptologie op het World Wide Web is daarnaast de pagina van de Belgische Koninklijke Militaire Academie: *http://te1.rma.ac.be/crypto.html*. Er bestaan ook diverse nieuwsgroepen op Internet over cryptologie en daaraan gerelateerde onderwerpen. De bekendste hiervan is *sci.crypt* waarin gediscussieerd wordt over actuele, aan cryptologische technieken gerelateerde onderwerpen. Ook is er een uitgebreide rubriek te vinden met antwoorden op veel gestelde vragen over cryptologie (FAQ, Frequently Asked Questions) die regelmatig wordt aangepast. Andere aan cryptologie gerelateerde nieuwsgroepen zijn:

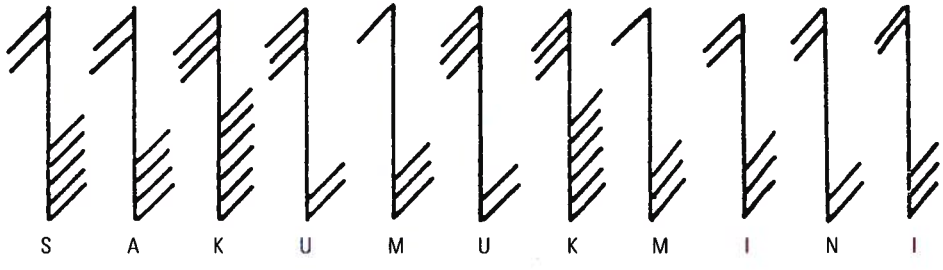
alt.privacy	aan privacy gerelateerde onderwerpen
alt.security	algemeen beveiliging (diverse sub-groepen)
comp.risks	informatie over cryptologie, afluisteren, inbraak e.d.
comp.security.announce	onder andere beschrijving van beveiligingslekken
talk.politics.crypto	politieke aspecten van cryptologie.

Voor enthousiaste surfers willen we ten slotte nog de volgende WEB-sites noemen:
http://www.yahoo.com/Computers_and_Internet/Security_and_Encryption/,
http://www.quadralay.com/www/Crypt/General/General.html, http://www.eff.org/pub/Crypto/,
http://theory.lcs.mit.edu/~rivest/crypto-security.html,
http://daedalus.dra.hmg.gb/lowton/curr_hot.html,
http://www.cs.cmu.edu/afs/cs.cmu.edu/user/bsy/www/sec.html, http://www.digicash.com/,
http://www.awpi.com/IntelWeb/US/S-GB/index.html,
http://www.netscape.com/info/security-doc.html,
http://www.rsa.com/, http://www.intermarket.com/ecl/,
http://www.phantom.com/~skapp/links.html,
http://www.cl.cam.ac.uk/users/rja14/
Onder FTP is bereikbaar:
ftp://ftp.research.att.com/dist/internet_security/

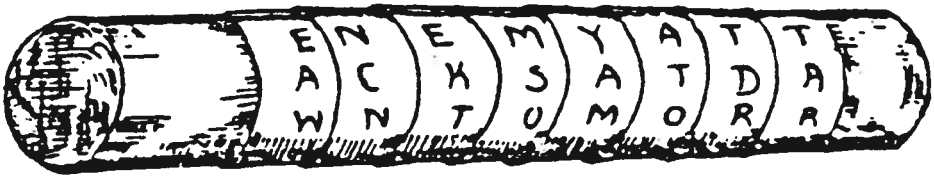
Hoe de voornaamste klassieke vercijfertechnieken precies werken komt in de volgende paragraaf uitgebreid aan bod. Eerst willen we u in vogelvlucht meenemen door de ontwikkeling die de cryptografie in haar vierduizendjarig bestaan heeft doorgemaakt.

± *2000-1000 v. C.* In Egypte wordt de levensgeschiedenis van doden in hiërogliefen op de muren van hun graftombes geschreven. Hoewel oorspronkelijk niet bedoeld als geheimschrift worden deze hiërogliefen in de loop van de tijd steeds complexer. De priesters houden ze buiten het bereik van de massa. Hiërogliefen zijn daarmee de vroegst bekende vorm van geheimschrift. Voor latere generaties lezers hebben ze de vorm van raadsels die gemaakt lijken om hun interesse te

▼ Afb. 1
Geheime runen op de Zweedse steen van Rök.



wekken. Een vergelijkbare ontwikkeling ondergaat het runenschrift. Op het moment dat deze schriftvorm algemeen bekend raakt, zien we zogenaamde geheime runen ontstaan. Een voorbeeld daarvan is nog steeds te vinden op de Zweedse steen van Rök, nabij Linköping (afb.1).



Ongeveer 1000-0 v. C. De Grieken en Romeinen maken veelvuldig gebruik van cryptografische technieken. De Grieken vinden het eerste cryptografisch 'apparaat' uit: de scytale. Om deze staf met een bepaalde dikte wordt een langwerpig stuk perkament gewikkeld. De parallelle stroken perkament worden vervolgens in lengterichting beschreven, waarna het bericht van de staf wordt afgehaald en verzonden. De ontvanger maakt de tekst ten slotte weer leesbaar door deze om een staf van gelijke dikte te wikkelen.

Bij de Romeinen gebruikt Julius Caesar een naar hem genoemde vorm van geheimschrift, die verderop in dit artikel nader wordt toegelicht.

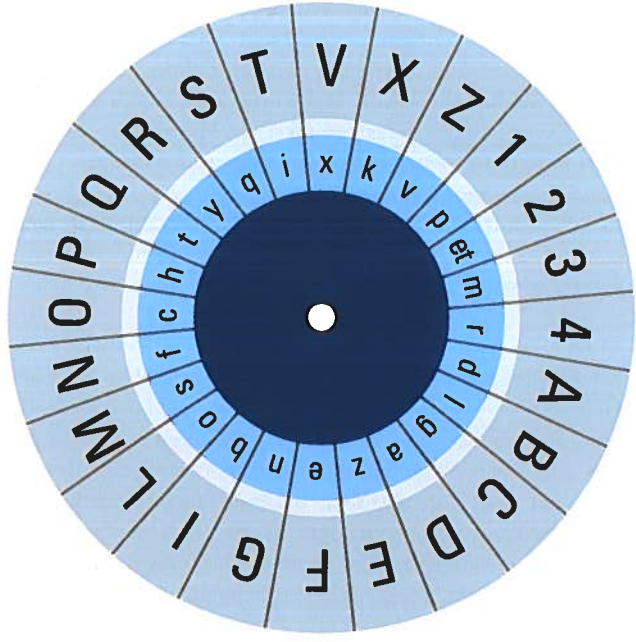
5e-14e eeuw. De cryptologie ontwikkelt zich in Arabië als een volwaardige wetenschap. Het Arabische woord 'sfir' en het Hebreeuwse woord 'safhar' (figuur, vorm) liggen aan de basis van woorden als 'cipher' en 'vercijferen'. In de 'Subh al-a 'sha', een 14-delige Arabische encyclopedie die een overzicht geeft van alle toen bekende takken van kennis, heeft de cryptologie een eigen sectie. Daarin zijn onder meer een zevental vercijfersystemen beschreven en komen we voor het eerst het gebruik van bepaalde taaleigenschappen (bijv. de frequentie waarin bepaalde lettercombinaties voorkomen) tegen als middel voor crypto-analyse.
In de westerse wereld is dit een donkere periode voor de cryptologie zonder relevante ontwikkelingen.

15e-16e eeuw. In Europa wordt de draad uit de Romeinse tijd weer opgepakt en komt de cryptologie opnieuw in de

▲ Afb. 2
De Scytale. Het volledige verhaal is als volgt. Lysander was een legeraanvoerder van de Spartanen in de oorlog tegen Athene (405 v. C). De Perzen zeiden hem te steunen maar daar was Lysander niet zeker van. Op een dag kwam een slaaf bij Lysander die een riem droeg met een reeks letters die ogenschijnlijk geen betekenis hadden. Toen de riem om een staaf van de juiste dikte gewikkeld werd, werd een boodschap leesbaar van een informant die Lysander voor een Perzisch komplot tegen hem waarschuwde. Lysander kon daardoor tijdig actie tegen de Perzen ondernemen.

belangstelling te staan. De wedergeboorte (renaissance) van de oudheid die we in de beoefening van de beeldende kunst, architectuur, wetenschap en literatuur zien, ontmoeten we dus ook in cryptologie. De Italiaan Leon Battista Alberti, een universalist, mag als vader van de westerse cryptologie worden beschouwd. Hij is de auteur van het oudste westerse manuscript over crypto-analyse (1466). De door hem ontworpen systemen vormen de basis voor poly-alfabetische substituties en codes. Ook ontwerpt hij een vercijfer-apparaat (de 'Alberti disk') bestaande uit twee concentrische, ten opzichte van elkaar draaibare cirkels. De ene schijf bevat het 'klare' alfabet. De andere een crypto-alfabet waarmee 'klare' tekst wordt vercijferd. De relatieve positie van de cirkels verandert volgens een door zender en ontvanger afgesproken patroon.

▶ Afb. 3
De chifreerschijf van Leon Battista Alberti



De ideeën voor poly-alfabetische vercijfering worden aan het einde van deze periode door verschillende mensen verder uitgewerkt en beschreven. Onder hen vinden we de Benedictijner monnik, alchemist en occultist Johannes Trithemius en de Fransman Blaise de Vigènere.

17e-18e eeuw. Antoine de Rossignol wordt Frankrijks eerste full-time cryptoloog. We zien de opkomst in Europa van zogenaamde 'Black Chambers'. Dit zijn efficiënte, goed georganiseerde instellingen waar dagelijks diplomatieke post wordt geopend en indien nodig teksten worden gekraakt. Vanuit de Black Chambers ontstaan in diverse landen de veiligheidsorganisaties die we nog steeds kennen.

19e-begin 20e eeuw. De Nederlander A. Kerckhoffs formuleert als eerste de stelling dat de veiligheid van cryptografische algoritmen slechts mag afhangen van de geheimhouding van de gebruikte (geheime) sleutel. De beoefening van de cryptografie krijgt in deze periode een steeds professioneler karakter. Handbediende, mechanische apparaten gaan het tijdrovende schrijfwerk overnemen. Tot na de Tweede Wereldoorlog wordt deze apparatuur op grote schaal gebruikt.
Ook in niet-professionele kring ontstaat belangstelling voor de cryptologie. Schrijvers als Edgar Allen Poe ('Gold Bug') en Arthur Conan Doyle (Sherlock Holmes: 'Adventure of the Dancing Men') verwerken 'cryptogrammen' in hun boeken en laten zien hoe ze kunnen worden opgelost. In Engelse kranten plaatsen particulieren vercijferde boodschappen in zogenaamde 'agony columns'. De meeste vallen zonder veel moeite te kraken; enkele zijn echter ook met de huidige analyse-mogelijkheden (nog) onoplosbaar.

1900-1950. Het gebruik van machines blijft toenemen en ook elektrisch aangedreven apparaten raken in zwang. In de Verenigde Staten schrijft William F. Friedman, dé cryptoanalist van de klassieke systemen uit onze eeuw, een aantal standaardwerken over het construeren en analyseren van traditionele cryptografische systemen. Op basis daarvan ontwikkelt hij ook lesmateriaal, dat pas vanaf de jaren zestig gedeeltelijk door de tijd zal worden achterhaald.
In 1949 publiceert de informatie-theoreticus Claude E. Shannon een opzienbarend artikel in 'Bell System Technical Journal'. In dit artikel 'Communication theory of secrecy systems' legt hij de grondslagen voor een wetenschappelijke benadering van geheime sleutelsystemen. Shannon kon door toepassing van de Informatietheorie op cryptografische systemen bewijzen dat het klassieke systeem van Vernam, de 'one-time pad', onbreekbaar is[3].

[3] Op de 'one-time pad' wordt verderop in het artikel teruggekomen.

De Eerste Wereldoorlog is een keerpunt in de beoefening van de cryptologie. De militaire waarde van het onderscheppen en kraken van berichten wordt volledig onderkend. Echter, de groeiende complexiteit van cryptografische systemen maakt het kraken steeds moeilijker. Een succesvol resultaat kan alleen door georganiseerd groepswerk worden behaald.
In de Tweede Wereldoorlog spelen cryptografische technieken een grote rol in zowel de strijd binnen Europa als binnen Azië. Het Amerikaanse leger telt ongeveer 16.000 mensen die zich met cryptologie (met name cryptografie) bezighouden. Ook de Britten zijn zeer actief. Een groot succes wordt behaald door een team onder leiding van de Britse wiskundige Alan Turing dat de Duitse Enigma vercijfermachine weet te kraken. Belangrijke militaire informatie komt daardoor in handen van de geallieerden.

1950 tot heden. Het digitale tijdperk gaat gepaard met een explosieve opkomst van elektronische vercijferapparaten. Voor de crypto-analyse wordt steeds meer van computers gebruik gemaakt. De cryptologie krijgt ook in niet-militaire toepassingen zoals telecommunicatie een belangrijke rol. In de zeventiger jaren groeit de cryptologie uit tot een aparte wetenschap binnen onder meer de wiskunde.
In 1976 verschijnt de publicatie 'New directions in cryptography' van W. Diffie en M.E. Hellman. Voor de eerste maal wordt in de openbare literatuur over public-key technieken geschreven. Diffie en Hellman tonen aan dat vertrouwelijke communicatie (d.w.z. geheimhouding) mogelijk is zonder vooraf een geheime sleutel af te spreken. Hiervoor wordt de (trapdoor) one-way functie geïntroduceerd, die in de verdiepingsstof bij het tweede deel van dit artikel nader aan de orde komt. De inzichten van Diffie en Hellman vormen de basis van het welbekende RSA public-key algoritme, genoemd naar de uitvinders Rivest, Shamir en Adleman. Public-key technieken spelen een belangrijke rol bij toepassingen op het gebied van authenticatie, het zetten van digitale handtekeningen en elektronisch betalen.
In 1977 wordt het door IBM ontworpen DES-algoritme (Data Encryption Standard) gepubliceerd als Amerikaanse de-facto standaard[4]. De status van DES als Amerikaanse standaard wordt in de tachtiger jaren verlengd. Ook anno 1995 is het DES-algoritme nog steeds een officiële stan-

[4] *Data Encryption Standard*, National Bureau of Standards, FIBS PUB 46, Washington DC, January 1977.

daard, al was het alleen maar vanwege het strategische belang van deze vercijfertechnologie voor de bancaire wereld. De maatschappelijke betekenis van de cryptologie is inmiddels namelijk zo groot dat zaken als de regulering van het gebruik van cryptologie en de controle op export van cryptografische produkten door verschillende westerse overheden wordt afgedwongen.

Data Encryption Standard (DES)

Het DES-algoritme is ontworpen door IBM en werd door de Amerikaanse overheid als standaard geadopteerd. Deze werd voor het eerst in 1977 gepubliceerd als Federal Information Processing Standard (FIPS). In 1988 werd onder meer op aandrang van de banken de status als US-standaard verlengd. In Europa wordt DES voornamelijk gebruikt voor bancaire toepassingen.

DES is nog steeds een algemeen aanvaarde standaard voor cryptografische toepassingen. De enige serieuze kritiek op DES betreft de beperkte sleutellengte. Over het algemeen vindt men een sleutellengte van 56 bit te klein voor de nabije toekomst. De verwachting is dat het mogelijk zal zijn, of wellicht al mogelijk is, om in beperkte tijd met supercomputers of gedistrubeerde computersystemen de sleutel waarmee een tekst is vercijferd te vinden door eenvoudig alle mogelijke sleutels te proberen. Als alternatief wordt vaak triple-DES genoemd waarbij vercijfering plaatsvindt door driemaal met DES te vercijferen, daarbij gebruikmakend van verschillende sleutels.

Naast de kwaliteit van het vercijferalgoritme zijn ook de manier waarop de vercijfering wordt toegepast, de identificatiemethode, het bijbehorende communicatieprotocol, het (sleutel-) beheersysteem en het onderliggende informatieproces van belang.

Cryptologie en de overheid

De cryptografie is van oudsher het domein van kleine selecte groepen in de samenleving. In de oudheid zijn het speciaal de hogere klassen die zich met cryptografie bezighouden. Zij proberen hun toch al uitzonderlijke positie door de

toepassing van geheimschrift verder te versterken. Vanaf de renaissance zal het gebruik van de cryptografie, tot ver in onze eeuw, voornamelijk aan de overheid zijn voorbehouden. Met name in militaire en diplomatieke kring wordt driftig met versleuteltechnieken gewerkt.
Maar natuurlijk kunnen cryptografische systemen ook voor illegale doeleinden gebruikt worden. Dat is nu zo en was ook in het verleden het geval. In de geschiedenis zien we dan ook herhaaldelijk dat overheden pogingen doen om het gebruik van cryptografie tot die groepen te beperken die er een maatschappelijk aanvaardbare toepassing voor hebben. In onze moderne tijd is dat geen eenvoudige taak. De explosieve groei van informatie- en telecommunicatietoepassingen maakt dat steeds meer groepen in de samenleving op cryptografie zijn aangewezen. Bedrijven hebben cryptografische beveiliging nodig omdat anders hun informatie en bedrijfsprocessen te kwetsbaar zouden zijn voor inbraak en misbruik. Burgers stellen eisen aan de bescherming van hun privacy, wat vaak alleen met behulp van cryptografische produkten op een afdoende manier te realiseren is.

Nieuwe diensten zoals elektronisch betalen en teleshoppen via Internet kunnen zonder de toepassing van cryptografie niet veilig ingevoerd worden. Hetzelfde geldt voor allerlei smartcard-applicaties, waarbij vooral de nieuwe generatie multi-functionele cards bijzonder privacy-gevoelig is[5]. Niemand wil tenslotte dat de bank of verzekeringsmaatschappij zomaar in je medische gegevens kan kijken. Of dat een winkelier eenvoudig je banksaldo kan achterhalen.
Kortom, een steeds groter deel van de samenleving heeft met het gebruik van cryptografische technieken te maken. Ook krijgen steeds meer mensen kennis van hulpmiddelen die op dit terrein beschikbaar zijn. Voor de overheid ontstaat daarmee een aantal problemen. Een belangrijke vraag is bijvoorbeeld hoe kan worden voorkomen dat cryptografie voor allerlei onwettige doeleinden gebruikt wordt. Te denken valt dan aan de vercijfering van bedrijfsadministaties met het doel belastingfraude te verdoezelen of aan de vercijfering van racistisch of pornografisch materiaal om dit onmerkbaar elektronisch te kunnen verspreiden. En waar moeten dan vervolgens de opsporingstaken van de overheid ophouden en komt de vrijheid van meningsuiting van burgers in het geding? Hoe dan ook staat vast dat cryptografie

[5] Voor een uitgebreide behandeling van de ontwikkeling van de kaarttechnologie verwijzen wij u naar het 'Themanummer Cards' dat het Studieblad in juni 1995 heeft uitgebracht.

een belemmering kan vormen voor de uitvoering van overheidstaken zoals het bestrijden van criminaliteit en het opsporen van verdachten.
Een apart probleem is de proliferatie van cryptografische technieken naar bepaalde landen in de wereld. Al geruime tijd trachten overheden dit door exportcontroles tegen te gaan. Diverse landen waaronder de Verenigde Staten, Frankrijk, Duitsland, Engeland en Nederland passen exportcontroles toe op cryptografische apparatuur. Dit betekent dat voor de uitvoer van dergelijke apparatuur een speciale vergunning moet worden aangevraagd. In de regel wordt die alleen afgegeven wanneer de beoogde toepassing als bonafide en controleerbaar wordt beoordeeld. Een recent voorbeeld van het weigeren van een exportvergunning is het uitvoerverbod van GSM-systemen met het Europese niveau van beveiliging naar landen in het Midden-Oosten en naar China.

Nationaal Bureau voor Verbindingsbeveiliging
In Nederland is het Ministerie van Economische Zaken formeel de beoordelende instantie voor het verlenen van exportvergunningen. In geval van cryptografische produkten vraagt dit ministerie advies van het Nationaal Bureau voor Verbindingsbeveiliging (NBV), dat fungeert als uitvoerend orgaan van de Nationale Verbindingsbeveiligingsraad (NVBR). De Raad is per gezamenlijke beschikking van de Ministeries van Defensie en Buitenlandse Zaken in 1984 ingesteld. Zij stelt het overheidsbeleid op het gebied van de verbindingsbeveiliging vast, ook ten behoeve van de Nederlandse stellingname in internationale samenwerkingsverbanden. De raad ontvangt beleidsaanwijzingen van beide direct betrokken Secretarissen-Generaal alsmede van de SG's van andere ministeries die bij verbindingsbeveiligingsvraagstukken zijn betrokken.
De advisering ten aanzien van exportvergunningen is overigens slechts een van de taken van het Nationaal Bureau voor Verbindingsbeveiliging. Het Bureau houdt zich daarnaast bezig met het geven van aanwijzingen, samenstellen van voorschriften, goedkeuringsdocumenten etc. ten behoeve van de Rijksoverheid op het gebied van de verbindingsbeveiliging. Dit ongeacht of

de beveiliging via afzonderlijke systemen of geïntegreerd in geautomatiseerde systemen en netwerken wordt gerealiseerd. In internationaal verband en dan met name binnen de NAVO vertegenwoordigt het NBV Nederland op verbindingsbeveiligingsgebied. Ook maakt het NBV deel uit van delegaties die Nederland vertegenwoordigen op het gebied van computerbeveiliging.

De regulering van de export van cryptografische produkten heeft maar een zeer beperkte invloed op de toepassing van cryptografie binnen de landsgrenzen. Beschrijvingen van cryptografische algoritmen worden algemeen verspreid (bijv. via Internet) en de nieuwste standaarden voor telecommunicatiediensten en -systemen bevatten in de regel hoofdstukken over cryptografische technieken. Alhoewel leveranciers van cryptografische produkten op basis van met de overheid gesloten gentleman's agreements niet zomaar aan iedereen hun systemen verkopen, geeft de beschikbaarheid bij vele Internetgebruikers van een programma als Pretty Good Privacy (PGP) wel aan dat de toepassing van cryptografie niet uitsluitend aan een geregistreerd gebruik verbonden is. Datzelfde blijkt bijvoorbeeld ook uit de gemakkelijke beschikbaarheid van cryptografische produkten voor het niet-afluisterbaar maken van gesprekken over analoge draadloze telefoons.

De overheid heeft daarom de laatste jaren naar andere middelen moeten zoeken om het binnenlands gebruik van cryptografie onder controle te krijgen. Enkele jaren geleden heeft de Amerikaanse overheid het idee van een zogenaamde 'key escrow' (escrow = schriftelijke verbintenis) voor telecommunicatie geïntroduceerd. De essentie van dit voorstel is dat de overheid via een ingebouwd mechanisme in staat is voor onder andere het aftappen van individuele telefoongesprekken de sleutels bij een onafhankelijke instantie te achterhalen. De sleutels zouden alleen na een gerechtelijk bevel worden afgegeven.

Het specifieke Amerikaanse voorstel bekend onder de naam 'Clipper' gaf aanleiding tot een uitgebreide maatschappelijke discussie, met als resultaat dat het voorstel vooralsnog in de ijskast lijkt te zijn gezet. Toch is het laatste woord over key escrow niet gesproken. In diverse Europese landen

duikt het idee regelmatig in verschillende verschijningsvormen op.

Inmiddels is de toepassing van cryptografie in telecommunicatiestandaarden als een speciaal probleemgebied onderkend. Na de invoering van GSM ontdekten diverse Europese landen dat legale interceptie ('aftappen') van gesprekken voor justitie zeer moeilijk of zelfs onmogelijk was. Van een aantal GSM-operators werd toen alsnog geëist GSM aftapbaar te maken. In Nederland is vanwege deze aftapbaarheid van GSM op 23 november 1995 de Wet op de Telecommunicatie Voorzieningen (WTV) gewijzigd.
Inmiddels wordt algemeen onderkend dat, zoals nieuwe telecommunicatiestandaarden internationaal worden afgesproken, de legale interceptie van gesprekken binnen telecommunicatienetwerken een kwestie is die een internationale aanpak verdient. In Europees verband werken overheden samen om gemeenschappelijk de grondslagen voor beleid op dit gebied te formuleren. In januari 1995 heeft de Europese Commissie een resolutie gepubliceerd, getiteld 'International Requirements for the Lawful Interception of Telecommunications'. In die publicatie zijn de functionele eisen vastgelegd die overheden aan de interceptie van telecommunicatiediensten en -systemen stellen.
Waarschijnlijk zullen in de toekomst de eisen voor legale interceptie al bij het opstellen van de standaards worden meegenomen, nu gebleken is dat implementatie van dergelijke eisen achteraf een zeer kostbare zaak kan zijn.

Techniek van de cryptologie: klassieke systemen

Oorspronkelijk werden cryptografische algoritmen alleen gebruikt voor het vercijferen van gewone taal. De klassieke technieken (tot en met WO II) zijn dan ook gericht op het bewerken van bepaalde taalelementen. Als eerste komen hiervoor de kleinste elementen van een taal in aanmerking: de letters. Andere veel gebruikte bewerkingsmethodes hebben te maken met het gelijktijdig aanpakken van hele woorden of combinaties van letters en het veranderen van de volgorde in de 'klare' tekst.

- Een veel toegepaste methode is de *substitutie*, het volgens een bepaalde sleutel vervangen van letters door andere let-

ters. Het meest elementaire substitutiesysteem ('mono-alfabetische substitutie') werd al door Julius Caesar gebruikt. Hij vercijferde zijn teksten door iedere letter te vervangen door een letter die drie plaatsen verderop in het alfabet stond. Bijvoorbeeld:

Klare tekst	jacta alea est
Vercijferde tekst	kdfwd dohd hvw

Hoewel dit systeem van mono-alfabetische substitutie eeuwenlang in allerlei vormen is toegepast, kan het toch niet echt veilig worden genoemd. De zwakte van het systeem is dat de statistiek van de vercijferde tekst, dat wil zeggen het aantal malen dat verschillende letters voorkomen, hetzelfde is als die van de klare tekst. In een taal is de frequentie waarmee verschillende letters voorkomen namelijk niet gelijk verdeeld. Wanneer voldoende vercijferde tekst beschikbaar is, kan met behulp van de statische kenmerken van een taal gemakkelijk bepaald worden welke vercijferde letter bij welke klare letter hoort. De factor van de verschuiving (de sleutel) is met andere woorden vrij eenvoudig vast te stellen. Een moeilijker variant van de mono-alfabetische substitutie ontstaat door de letters niet eenvoudig op te schuiven, maar deze in een willekeurige volgorde te vervangen. Ook dan zal de statistiek van de klare taal echter nog steeds in de vercijferde tekst terug te vinden zijn. Andere varianten zoals 'bigram-substituties', het vervangen van paren letters door andere letterparen, en het gebruik van 'code-boeken', het vervangen van begrippen en woorden (of delen daarvan) door codes, lijden in meerdere of mindere mate aan dezelfde zwakte.

• Pas in de vijftiende en zestiende eeuw slagen cryptografen erin de substitutiemethode structureel te verbeteren. Deze verbeteringen staan bekend onder de verzamelnaam *poly-alfabetische substitutie*. Het bekendste algoritme in deze categorie is uiteindelijk vernoemd naar de Franse cryptograaf Blaise de Vigènere, alhoewel meer mensen aan de totstandkoming hebben bijgedragen. Het idee bestaat eruit om op de achtereenvolgens te vercijferen letters steeds een andere Caesar-substitutie toe te passen. Bijvoorbeeld een verschuiving van 4 voor het eerste teken, 12 voor het tweede, 7 voor het derde etc. Tot rond 1860 geloofde men dat het Vigènere-algoritme veilig was. De Duitse crypto-analist

▲ Afb. 4
Julius Caesar was een van de beroemdste gebruikers van de (mono-alfabetische) substitutiemethode.

Kasiki hielp deze gedachte echter om zeep toen hij een methode ontwikkelde waarmee de sleutellengte kon worden achterhaald. Vervolgens is het natuurlijk niet zo moeilijk meer om het Vigènere-systeem te kraken, omdat de puzzel is teruggebracht tot het bepalen van de toegepaste letterverschuivingen (Caesar-substituties). Hoe eenvoudig dat laatste is, kunt u zelf vaststellen aan de hand van het cryptospel dat op de diskette bij dit nummer is gevoegd.

Van het Vigènere-algoritme zijn verschillende varianten bekend. De meest elementaire is een sleutelwoord te kiezen en op basis daarvan de opschuiving te bepalen. Dit wordt hieronder geïllustreerd aan de hand van de sleutel 'water'.

Klare tekst	we starten vandaag
Sleutel	wa terwate rwaterw
Vercijferde tekst	se lxrntxr mwnwerc

De opschuiving van de letters in de klare tekst is als volgt bepaald: bij een sleutelletter 'a' is de opschuiving nul, bij

een sleutelletter 'b' is de opschuiving één (bijvoorbeeld een 'a' wordt een 'b' en een 'k' een 'l'), bij een sleutelletter 'c' is de opschuiving twee (bijvoorbeeld een 'd' wordt een 'f' en een 't' een 'v') etc. Bij de sleutelletter 'w' in het voorbeeld is de opschuiving dus tweeëntwintig, waardoor de 'w' een 's' wordt, de 'r' een 'n', de 'a' een 'w' en de 'g' een 'c'.
Ondanks de toenmalige, hoge mate van betrouwbaarheid zal het Vigènere-algoritme pas vanaf de negentiende eeuw op grote schaal gebruikt gaan worden. De kraakbestendigheid van dit algoritme hangt sterk af van de gekozen sleutel, in het bijzonder van de sleutellengte. Bij het gebruik van korte sleutels, zoals in het voorbeeld, is het algoritme tamelijk eenvoudig tot een reeks mono-alfabetische substituties te herleiden, zoals Kasiki heeft aangetoond. Langere sleutels verdienen dus de voorkeur. In de praktijk worden deze bijvoorbeeld verkregen door bepaalde zinnen uit boeken als sleutel te nemen.

Voor een zeer belangrijk bericht komt als sleutel ook een zich niet-herhalende letterreeks (langer dan de te vercijferen tekst) in aanmerking. Wanneer zo'n reeks eenmalig gebruikt wordt spreekt men van een 'one-time pad'. Alhoewel een dergelijk systeem theoretisch onkraakbaar kan zijn, is het sleutelbeheer in de praktijk echter te gecompliceerd[6].
Daarom is naar praktische methodes gezocht om uitgaande van een korte sleutel gemakkelijk lange sleutelreeksen te kunnen genereren. Bijvoorbeeld 'rotorsystemen' ontlenen hun kracht aan een zeer lange sleutel op basis van poly-alfabetische substitutie. Ze zijn ontwikkeld aan het einde van de Eerste Wereldoorlog en op grote schaal gebruikt tijdens WO II. De bekendste rotormachine is de Enigma, die rond 1923 door A. Scherbius werd bedacht. Het Duitse leger zou de machine verder ontwikkelen en in de Tweede Wereldoorlog als standaard cryptomachine inzetten. In een vorig artikel heeft u al kunnen lezen dat de vercijferde berichten door de Geallieerden vaak konden worden gekraakt.
In de dertiger jaren ontwierp Boris Hagelin een vergelijkbare cryptomachine. Van deze succesvolle Hagelin-machine is een groot aantal versies vervaardigd, variërend van kleine draagbare types voor gebruik in het veld tot elektrisch aangedreven machines voor een vaste opstelling. Een van de meest succesvolle types was de M-209. Deze machine is als 'medium level' cryptografisch systeem onder andere door

[6] Aan het slot van de paragraaf 'Begrippen en methodes' gaan we nader op de one-time pad in.

de Amerikanen gebruikt tijdens de Tweede Wereldoorlog. Tot in de jaren vijftig heeft het Nederlandse leger de M-209 ingezet. Dit wonder der techniek genereert een sleutelreeks met een lengte van 26*25*23*21*19*17 = 101.405.850 letters.

3	1	5	2	6	4
w	e		s	t	a
r			t		e
n	v				a
n	d	a	a	g	
m			e	t	d
e	a	k	t	i	e

◀ Afb. 5
Transpositie-rooster (ook wel Route Transpositie genoemd)

• Een andere klassieke methode is de *transpositie* of *permutatie* van letters. Hierdoor wordt de volgorde van de letters veranderd. De meest elementaire vorm van deze techniek bestaat uit het in de kolommen van een bepaald grid (roos-ter) schrijven van de klare tekst, waardoor in de kolommen versluierde 'woorden' in de vorm van willekeurige letter-combinaties ontstaan. Voor het lezen wordt de vercijferde tekst weer in de juiste volgorde in het rooster teruggezet. Het transpositiesysteem is in deze elementaire vorm gemakkelijk te kraken aan de hand van specifieke eigenschappen van de taal. Het volgende voorbeeld, een transpositie-rooster met gaten, is echter veel moeilijker te kraken.

De sleutel, dat wil zeggen de volgorde van uitlezen van de kolommen, is in dit voorbeeld: *3 1 5 2 6 4*. In vercijferde vorm ziet de tekst er als volgt uit: *evdas taetw rnnme aeade aktgt i.*
Dergelijke voortdurend wisselende roosters waren een onderdeel van de cryptografische algoritmen die Japan in de Tweede Wereldoorlog benutte. Ze stelden de Amerikaanse crypto-analysten voor grote problemen[7]. Ten slotte willen

[7] Door het geringe aantal mogelijke roosters biedt de transpositie- of permutatie-methode op zichzelf een niet al te grote bescherming. Maar door nog een tweede vercijfermethode te gebruiken (confusie of diffusie) kan het ontcijferen/kraken een stuk moeilijker worden gemaakt. Het oplossen van bijvoorbeeld een kolomtranspositie wordt gemakkelijk gemaakt door dezelfde lengte van de kolommen. Er kan ook zoals in afbeelding 5 met kolommen van ongelijke lengte worden gewerkt. Een sterker systeem ontstaat bijv. wanneer twee kolomtransposities met ongelijke lengte achter elkaar worden toegepast.

we nog noemen dat heel wat klassieke systemen geënt zijn op een combinatie van substituties en transposities. In deze systemen worden de volgorde van een combinatie van letters èn de combinaties van letters zelf bewerkt. De populariteit van dergelijke hybride geheimschriften zou tot na de Tweede Wereldoorlog voortduren.

Eigenschappen van talen

In de Nederlandse taal komen de letters *e*, *t* en *n* zeer vaak voor. De letters *q*, *x* en *j* worden daarentegen sporadisch gebruikt. Evenzo blijkt dit voor combinaties van letters te gelden. De combinatie *en* komt vaak voor, *qn* echter niet. Het blijkt dat door gebruik te maken van deze kenmerken, die afhankelijk zijn van de gebruikte taal, bij het analyseren van een 'cryptogram' soms de oplossing gevonden kan worden. Dit komt doordat het vercijferalgoritme deze taalkenmerken niet of onvoldoende versluiert. Vooral de oudere (klassieke) systemen gaan hieronder gebukt.

Een sterk algoritme kan worden verkregen door via verschillende sleutels herhaaldelijk en afwisselend substituties en transposities toe te passen. Het nagestreefde doel is de specifieke taalkenmerken volledig te laten verdwijnen, zodat de vercijferde tekst op een willekeurige tekst lijkt.

Met deze kennis in het achterhoofd lijkt het wellicht handig om een tekst twee of nog meer malen via dezelfde vercijfermethode te versluieren bij gebruikmaking van verschillende sleutels. Helaas wordt de veiligheid op deze manier niet altijd verhoogd. Dit is gemakkelijk duidelijk te maken aan de hand van het volgende substitutievoorbeeld: wanneer een letter *a* vervangen wordt door een *c* en deze *c* vervolgens door een *k*, dan is dit in wezen gelijk aan het in één keer vervangen van de letter *a* door een *k*. Door een ongelukkige keuze van de sleutel kan het zelfs voorkomen dat de originele tekst weer ontstaat. We moeten dus oppassen bij het herhaald vercijferen van een tekst.

Om praktische redenen kan het soms toch gerechtvaardigd zijn dubbele of triple vercijfering toe te passen. De vercijfermethode moet dan echter wel aan bepaalde

wiskundige eisen voldoen. Helaas is het ondoenlijk om te bewijzen of een vercijfermethode aan alle voorwaarden voldoet en niet gekraakt kan worden.

Techniek van de cryptologie: moderne systemen

Met de komst van het binaire tijdperk, computers en digitale snelwegen is het gezicht van de cryptologie ingrijpend veranderd. De meeste klassieke (hand)systemen kunnen met behulp van computers eenvoudig gekraakt worden. Daarnaast hebben de vertrouwde letters plaats moeten maken voor bits en bytes en is er nu behoefte aan andere cryptografische algoritmen. Onveranderd is dat substituties en permutaties nog altijd de belangrijkste bouwstenen vormen voor het ontwerpen van cryptografische systemen, nu echter toegepast op bits of groepen van bits.
Het aantal toepassingen van de cryptologie is de laatste jaren zeer sterk toegenomen. Tegenwoordig heeft bijna iedereen, al dan niet bewust, met de vele facetten van de cryptologie te maken. Dat komt vooral door de toename van telecommunicatie- en informatiediensten. Diensten waarvoor speciale voorzorgsmaatregelen noodzakelijk zijn om te voorkomen dat belangrijke informatie, ook van persoonlijke aard, onder het bereik van derden komt. Daarnaast worden vitale bedrijfsprocessen steeds meer afhankelijk van computer- en telecommunicatiesystemen. Beveiliging van informatie en informatie-/communicatiestromen is een essentieel aspect om deze systemen verantwoord te kunnen toepassen.
We zien dan ook dat de cryptologie in onze tijd voor zeer uiteenlopende doeleinden wordt ingezet. De banken gebruiken cryptografische technieken bijvoorbeeld in hun betalingssystemen voor het automatisch opnemen van geld. Een andere toepassing is het in computers in vercijferde vorm opslaan van vertrouwelijke informatie om ongewenste inzage tegen te gaan. In moderne telecommunicatiesystemen worden vercijferalgoritmen onder meer toegepast om informatie over de radioweg te beveiligen en op die manier afluisteren tegen te gaan. Een bekende toepassing is ook het gebruik van cryptologie in toegangsverleningssystemen. Daarmee wordt voorkomen dat iedereen zomaar een bepaald gebouw of ruimte kan binnengaan of zomaar van

iemands zaktelefoon gebruik kan maken. Een steeds populairder wordende toepassing die we als laatste voorbeeld willen noemen is de beveiliging van E-mail op het Internet met behulp van het softwarepakket PGP (Pretty Good Privacy).
Al met al zijn er dus heel wat oogmerken om van beveiligingstechnieken gebruik te maken. Een van oudsher bekend doel is de bescherming van informatie tegen ongewenste inzage of afluisteren. Bij toegangscontrole speelt daarentegen de identiteitsvaststelling via bijvoorbeeld een magneetkaart en pincode een belangrijke rol. En in het betalingsverkeer is onder andere de echtheid van de data en de identificatie belangrijk: wordt een bedrag op de rekening gestort of ervan afgeboekt, om welke hoeveelheid geld gaat het en wie zet de transactie in gang.
Kort op een rijtje gezet kunnen we uit het voorgaande in ieder geval drie beveiligingsdoeleinden afleiden waarvoor een cryptografisch systeem kan worden ingezet:
- geheimhouding
- identificatie
- data-integriteit.

Geheimhouding. Bij geheimhouding gaat het erom dat informatie alleen toegankelijk is voor personen die daartoe gemachtigd (geautoriseerd) zijn. Meestal is datavercijfering in combinatie met een authenticatieprocedure een afdoend middel.
Identificatie. Hierbij speelt het in bezit hebben van bepaalde informatie (kenmerken) een belangrijke rol. Identificatie kan op verschillende manieren plaatsvinden. Denk maar aan het herkennen van een vingerafdruk (fysieke eigenschap), het moeten gebruiken van een password (kennis), het tonen van een paspoort (bezit) of het invoeren van een magneet- of smartcard en pincode in een kaartlezer (bezit + kennis). Omdat identificatie nooit 100% waterdicht kan zijn, moet bij de keuze van een identificatiemethode vooraf een geoorloofde foutkans (de kans op foutieve identificatie) worden vastgesteld. Naast deze onzekerheid geldt bovendien dat de identificatie slechts een momentopname in de tijd is. Bij informatie-overdracht zal de identificatie van de afzender en/of ontvanger daarom niet de enige veiligheidsmaatregel zijn. Om te voorkomen dat er na de identificatie alsnog inbreuk op de vertrouwelijkheid wordt gedaan, zal

tijdens de identificatiefase tussen zender en ontvanger een vercijfersleutel worden afgesproken voor het afschermen van de informatiestroom.

Praktijksituatie: voetbal

Aan de hand van een praktijkvoorbeeld willen we verschillende identificatiemethoden voor u demonstreren. Gekozen is voor de voetbalwereld waarin identificatie een steeds belangrijker rol speelt.

Al vele jaren wordt bij het voetbal gebruik gemaakt van toegangskaartjes. Je betaalt aan de kassa en krijgt een toegangsbewijs voor de gewenste wedstrijd. Bij het binnenkomen van het voetbalstadion wordt de controlestrook van het kaartje afgescheurd; een vorm van ongeldig maken. Om het fraudeurs niet al te eenvoudig te maken zijn vele kaartjes zo gemaakt dat de kosten van (goede) namaak niet opwegen tegen de opbrengsten die met valse kaartjes kunnen worden behaald. Slecht nagemaakte kaartjes zullen bij de toegangscontrole door de mand vallen.

Het identificatieproces bij een voetbalwedstrijd richt zich momenteel nog vrijwel geheel op het betaald hebben voor de wedstrijd. Door sommige voetbalclubs worden echter ook speciale pasjes gebruikt om ongewenste 'supporters' te weren. Hoe je het echter ook wendt of keert, het ongewenst binnendringen van een stadion kan nooit geheel worden voorkomen. Dat begint al met de fysieke beveiliging van het stadion waar mensen overheen kunnen klimmen. Daarnaast zal de wedstrijd met een goed nagemaakt toegangsbewijs en/of pasje altijd gezien kunnen worden. Hierbij geldt dat hoe hoger de entreeprijs is, hoe groter de kans wordt dat namaak van toegangsbewijzen loont. Of, hoe liever 'supporters' de wedstrijd willen verstoren, hoe meer moeite zij zullen doen om aan een vals pasje te komen. Voor een voetbalclub zijn dit belangrijke overwegingen om vooraf rekening mee te houden. De kwaliteit van de identificatie, dat wil zeggen de mate van waterdichtheid van het systeem, wordt er uiteindelijk door bepaald.

Data-integriteit. Bij data-integriteit moet de echtheid van de data worden gewaarborgd. We moeten met andere woorden in staat zijn om al dan niet moedwillige modificaties, tussenvoegingen, weglatingen of herhalingen in de data te ontdekken. Naast deze functies biedt een cryptografisch systeem soms ook de mogelijkheid tot:
- bewijs van echtheid,
- bewijs van herkomst,
- bewijs van ontvangst.

Die laatste drie beveiligingsfuncties zijn bijvoorbeeld van belang bij elektronische post (E-mail). Ze dienen ter vervanging van het 'aangetekend verzenden' van informatie, zodat in een later stadium (eventueel voor een rechtbank) kan worden aangetoond dat de informatie-uitwisseling heeft plaatsgevonden.

Begrippen en methodes in de moderne cryptologie

Geheimhouding en authenticatie zijn twee onafhankelijke begrippen die aan de basis staan van moderne cryptografische systemen. Afhankelijk van de toepassing, namelijk of een boodschap of identiteit moet worden beveiligd, spreken we achtereenvolgens van privacy of anonimiteit en van integriteit of identificatie.

• Geheimhouding:	
van boodschap	privacy/confidentialiteit
van identiteit	anonimiteit
• Authenticatie:	
van boodschap	integriteit
van identiteit	identificatie.

We wijzen hier zo nadrukkelijk op het onderscheid tussen deze begrippen omdat ze een belangrijke plaats innemen in de vakliteratuur. Ook in dit artikel speelt dit begrippenkader een belangrijke rol. Kort samengevat komt het erop neer dat afhankelijk van de toepassing de onafhankelijke begrippen 'geheimhouding' en 'authenticatie' vaak een andere naam en een specifieke betekenis krijgen.

Ook is het belangrijk te weten dat in een cryptografisch systeem drie belangrijke onderdelen worden onderscheiden:
- de vercijfermethode,
- de ontcijfermethode,
- de sleutel.

Vercijfer-/ontcijfermethode. Op basis van de vercijfer- en ontcijfermethode zal een cryptografisch systeem informatie onleesbaar en opnieuw leesbaar maken. Dit algemene principe voor het ver- en ontcijferen van informatie noemen we meestal het cryptografisch algoritme. Het algoritme vormt de grondslag – het rekenschema – waarop de werking van het systeem is gebaseerd.
Sleutel. De cryptografische sleutel bepaalt uiteindelijk hoe de informatie precies wordt ver- en ontcijferd. Is de methode (het cryptografisch algoritme) dus een soort rekenschema, de sleutel geeft aan hoe de berekening moet worden uitgevoerd. Bij gebruik van het algoritme, dat altijd vast is, èn dezelfde 'klare' tekst zal een wisseling van sleutel daarom voor een wisselend resultaat zorgen en dus de veiligheid van het systeem aanzienlijk vergroten.

Voorbeeld vercijfer-/ontcijfermethode en sleutel: Caesar
Het meest elementaire voorbeeld van het gebruik van een vercijfer-/ontcijferalgoritme en een cryptografische sleutel is de manier waarop Julius Caesar ruim tweeduizend jaar geleden zijn vertrouwelijke berichten verstuurde. Deze al eerder beschreven vercijfermethode bestaat uit het vervangen van elke letter in de boodschap door een andere letter. Bij het ontcijferen worden de versluierde letters weer in 'klare' letters teruggezet. De sleutel bepaalt welke letter een boodschapletter vervangt en omgekeerd. Zo zal bij een sleutel *4* de 'a' een 'd' en de 'b' een 'e' worden. Aldus zet het cryptografisch systeem de boodschap (klare tekst) om in een 'cryptogram' en vice versa.

Cryptografische ideeën in de muziek: 'Toestand'
'Toestand' is een compositie van Guus Jansen
Première 1996 door Orkest De Volharding
Stel u een tekening voor en leg hier vellen papier overheen waarin steeds andere gaten zijn geknipt. Het resultaat zal voortdurend verschillend zijn, terwijl de onderliggende tekening hetzelfde blijft.
Precies dit is wat er gebeurt in 'Toestand'. De tekening is nu een akkoordenschema dat de hele maat vult. Dit schema wordt het hele stuk door iedere maat herhaald.

De muziek ontstaat in feite door alle akkoordnoten die *niet* klinken (analoog aan de papieren vellen). Pas aan het eind van het stuk klinkt het volledige akkoordenschema als een ratelend aflopende wekker.

In moderne cryptografische systemen wordt dan ook voortdurend van andere sleutels gebruik gemaakt. De tijdens een bepaalde sessie te gebruiken sleutel zal via een op voorhand afgesproken manier uitgewisseld worden. Die uitwisseling van sleutels wordt vaak het sleutelprotocol genoemd. Ook kunnen de sleutels door een zogenaamd sleutelbeheercentrum worden geleverd. Uiteraard moet de sleuteluitwisseling over een veilig kanaal plaatsvinden, omdat de betrouwbaarheid van het cryptosysteem uiteindelijk staat of valt met de manier waarop in de praktijk met de sleutel wordt omgesprongen. Verderop in het artikel komen we op deze en andere kwesties rond het sleutelbeheer uitgebreid terug.
Voorlopig gaan we er echter vanuit dat het sleutelbeheer waterdicht geregeld is en dat alle gebruikers de veiligheidsafspraken strikt naleven. Wat kan binnen deze context dan een veilig systeem worden genoemd? Allereerst is een cryptografisch systeem veilig te noemen wanneer het theoretisch onbreekbaar is. Uit deze constatering mag overigens niet automatisch worden afgeleid dat een theoretisch breekbaar systeem ook praktisch breekbaar zal zijn. Zo kan het kraken van een theoretisch niet geheel veilig systeem de snelste computer ter wereld nog altijd enkele eeuwen rekentijd kosten. Beter dan alleen de theoretisch onbreekbare systemen veilig te noemen, is het daarom de veiligverklaring uit te breiden tot cryptografische systemen die praktisch onmogelijk breekbaar zijn. Ook deze definitie zal mensen uit de beveiligingspraktijk echter maar weinig aanspreken, omdat tot nu toe volledig aan financiële argumenten voorbij is gegaan. Omdat kosten/baten-overwegingen bij de aanschaf van een cryptografisch systeem wel degelijk een rol spelen, zal de definitie van wat veilig is verder moeten uitgewerkt. Een voorbeeld daarvan hebben we hiervoor al gegeven aan de hand van de voetbalwereld. Wat uit dit voorbeeld duidelijk blijkt, is dat veiligheid sterk afhangt van de omgeving van het cryptografisch systeem. En dan is er natuurlijk ook nog zoiets als het van tevoren door het management bewust nemen van bepaalde risico's (calculated risks).

In feite is het dus ondoenlijk om in de vorm van een eenvoudige definitie te bepalen of een systeem al dan niet veilig mag worden genoemd. Een oplossing die voor het ene bedrijf veilig is, kan voor een ander bedrijf risicovol zijn. Ook kunnen binnen één bedrijf voor verschillende toepassingen verschillende definities van veilig gelden. Sterker nog, dit kan zelfs gelden voor één toepassing op verschillende locaties van een bedrijf. De gebouwbeveiliging van een onderzoekslaboratorium of strategie-afdeling stelt bijvoorbeeld heel andere eisen dan de toegangsbeveiliging van een produktiehal of kantorencomplex.
Naast het maken van een nauwgezette kosten/baten-analyse speelt ten slotte de factor tijd een belangrijke rol bij het veilig zijn van een cryptografisch systeem. Zo mag een vercijferde boodschap ('cryptogram') die slechts één dag geheim hoeft te zijn, best in twee dagen worden gekraakt.
In het vervolg van dit artikel blijven dergelijke sterk contextafhankelijke redeneringen buiten beschouwing. Wij volstaan met de constatering dat er vele goede cryptosystemen ontwikkeld zijn en dat er een theoretisch onbreekbaar systeem bestaat: de zogenaamde one-time pad.

Een theoretisch onbreekbaar cryptosysteem: de one-time pad

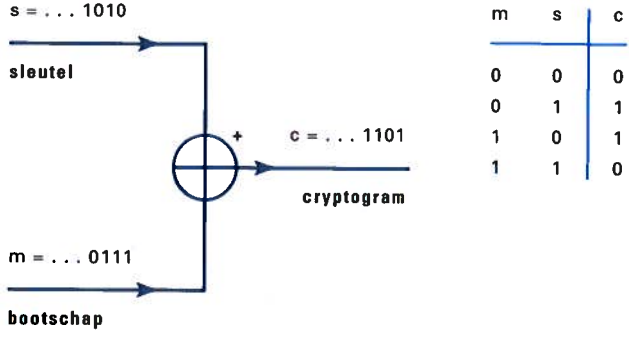
De vercijfermethode van de one-time pad is gegrond op het volgende kruis-of-munt principe: de uitkomst (één of nul) van een worp met een geldige munt opgeteld (modulo 2) bij de uitkomst van een worp met een valse munt heeft toch een willekeurige (random, niet voorspelbare) uitkomst als resultaat. Anders gezegd, willekeurig + niet-willekeurig = willekeurig! Dit principe is toegepast door Vernam. Hij telde bij een boodschaprij een willekeurige sleutelrij op, waardoor een willekeurige cryptogramrij wordt verkregen. Shannon bewees dat in Vernam's cryptosysteem de boodschap perfect verborgen blijft, mits de willekeurige sleutelrij tenminste even lang is als de boodschaprij en slechts éénmaal wordt gebruikt (one-time pad). Voor een lang bericht leidt dit al snel tot niet-handelbare systemen die voor toepassing in de telecommunicatie onpraktisch zijn. Gewoonlijk wordt een lange sleutelrij daarom afgeleid van een vele malen kleinere willekeurige sleutelrij (64

bits of meer). De verkregen lange sleutelrij is echter niet meer volstrekt willekeurig en wordt zodoende vaak een pseudo-random rij genoemd. Afhankelijk van de te gebruiken vercijfermethode kan een zeer lange pseudo-willekeurige sleutel worden samengesteld of een enorm grote substitutietabel opgesteld. De pseudo-random rij zal niet alleen goede statistische eigenschappen (gelijkverdeelde letter-/symboolfrequenties, geen of een uniforme correlatie tussen de symbolen etc.) moeten bezitten, maar dient ook cryptografisch sterk te zijn. Dit komt erop neer dat het ondoenlijk moet zijn een cryptografisch sterke pseudo-random rij van een echte willekeurige rij te onderscheiden.

Stroom- en blokvercijferaars

De vercijfering van een bericht kan in hoofdlijnen op twee manieren worden bewerkstelligd. Allereerst kan de versluiering teken voor teken plaatsvinden. Ten tweede kan de klare tekst bloksgewijs worden aangepakt. Afhankelijk van de gekozen methodiek spreken we respectievelijk van:
- stroomvercijfering
- blokvercijfering.

Stroomvercijfering (stream cipher). Bij stroomvercijfering vindt de versluiering op teken- of symboolniveau plaats. Dat wil zeggen dat de te vercijferen boodschap als een stroom tekens wordt beschouwd, die alle afzonderlijk vercijferd moeten worden. Dat het daarbij niet om letters gaat, maar om 'enen' en 'nullen' die versluierd moeten worden, spreekt

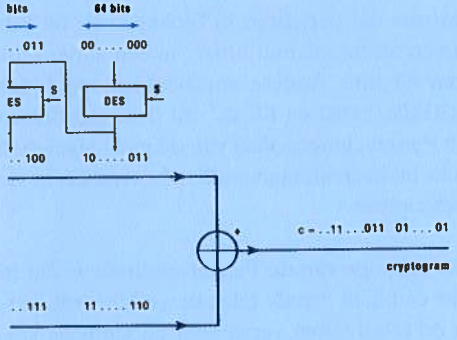


▶ Afb. 6
Stroomvercijfering met een binaire opstelling

in het digitale tijdperk eigenlijk voor zich. De tekenstroom is dan ook feitelijk een bitstroom, waarbij versleuteling plaatsvindt door de inkomende bitstroom te combineren met een stroom sleutelbits. Uit bijvoorbeeld een binaire optelling ontstaat zo de uitgaande vercijferde bitstroom. In afbeelding 6 is dit weergegeven.
Het is nu de kunst om vanuit een kleine willekeurig gekozen sleutel een zeer lange pseudo-willekeurige sleutelrij af te leiden.

Blokvercijfering (block cipher). Bij een blokvercijfering wordt de boodschap in een aantal groepen (blokken) van een vaste lengte verdeeld. Ieder blok wordt als geheel vercijferd. Een voorbeeld van een blokvercijferalgoritme is de Data Encryption Standard (DES) die ingebakken in een speciale chip (IC-vorm) te koop is. Een dergelijke hardware-matige aanpak van het cryptografische proces verdient de voorkeur omdat de ver- en ontcijfering dan veel sneller verloopt dan langs software-matige weg[8].

Voorbeeld: stroomvercijfering met behulp van een blokvercijferalgoritme



Afb. 7 Stroomvercijfering met behulp van een blokvercijferaar (DES).

Met blokvercijferaars kan op verschillende manieren een stroomvercijferaar gemaakt worden. Stel dat we als blokvercijferalgoritme voor DES kiezen. Bij aanvang kiezen we een sleutel S van 56 bits en een beginwaarde

[8] De praktijk heeft uitgewezen dat blokvercijferaars op verschillende manieren (Modes of Use) gebruikt kunnen worden. In het tweede deel van dit artikel geven we hier voorbeelden van. Bekende toepassingen van blokvercijferalgoritmes zijn: Electronic CodeBook (ECB), Cipher Block Chaning (CBC), Output FeedBack (OFB) en Cipher FeedBack (CFB).

BV van 64 bits. De beginwaarde *BV* kan eventueel vast gekozen worden, bijvoorbeeld allemaal nullen. Na de eerste vercijferslag zijn 64 vercijferde bits beschikbaar. Deze vercijferde bits worden gebruikt voor de eerste 64 bits van de stroomvercijfersleutel. Echter, we voeren deze 64 bits ook naar de ingang van het DES-systeem terug.
Vervolgens wordt weer een vercijferslag uitgevoerd met dezelfde DES-sleutel *S* en krijgen we 64 andere vercijferde bits. Deze vercijferde bits worden de volgende 64 bits van de stroomvercijfersleutel. Ook deze 64 bits worden weer naar de ingang van het DES-systeem gebracht etc.
De aldus verkregen stroomvercijfersleutel wordt net als in afbeelding 7 bij de te vercijferen boodschap opgeteld. Zolang gewaarborgd kan worden dat de stroomvercijfersleutel zich niet snel gaat herhalen, wat bij DES het geval is, kan een zeer lange pseudo-willekeurige sleutelrij worden verkregen uit de slechts 56 bits tellende DES-sleutel.

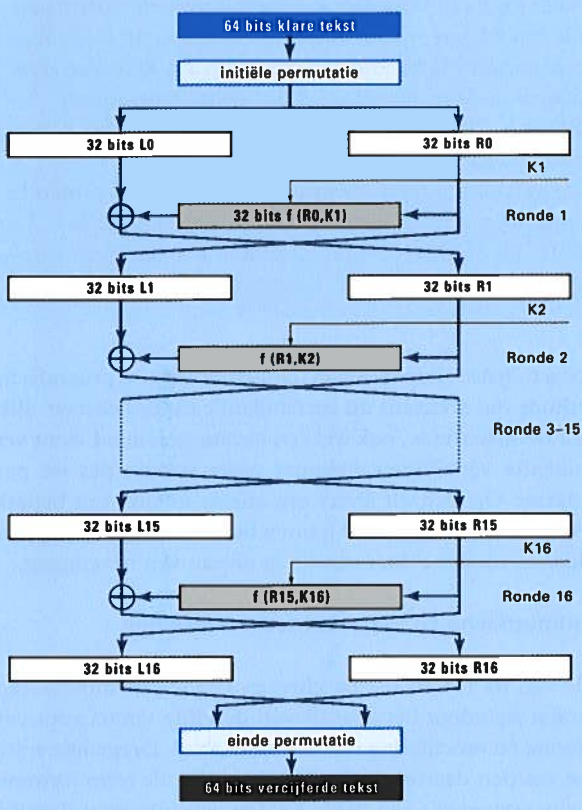
Feistel en product ciphers

DES is een algoritme dat berichten in blokken van 64 bits met behulp van een 56-bits sleutel omzet in een ander blok (cryptogram) van 64 bits. Andere voorbeelden van block ciphers zijn LUCIFER, LOKI en FEAL[9]. Al deze algoritmen zijn zogenaamde Feistel ciphers. Veel van de in de afgelopen jaren ontwikkelde blokvercijferaars vallen bovendien in de categorie product ciphers.

[9] Zie voor een nadere toelichting: Bruce Schneider, *Applied Crytography*, New York, 1966 (2nd ed.).

Feistel cipher. Het principe van de Feistel-methode is dat in elke ronde slechts één helft van de tekst bewerkt wordt, vervolgens worden de teksthelften verwisseld en vindt de volgende vercijferronde plaats. Een voordeel van deze procedure is dat de manier van ontcijfering overeenkomt met de vercijfering. In afbeelding 8 wordt het principe van een Feistel cipher geïllustreerd aan de hand van de rondestructuur van het DES-algoritme.

Voorbeeld van Feistel cipher



Afb. 8 Rondeschema van het DES-algoritme

De 64-bit klare tekst ondergaat een initiële permutatie en wordt dan gesplitst in twee 32-bit blokken L0 en R0. Hieruit worden twee nieuwe 32-bit blokken L* en R* afgeleid volgens:

L1 = R0 en R1 = L0 ⊕ f (R0, K1);
L2 = R1 en R2 = L1 ⊕ f (R1, K2);
L3 = R2 en R3 = L2 ⊕ f (R2, K3);
. . . . . .
L16 = R15 en R16 = L15 ⊕ f (R15, K16).

Hierbij zijn K1, K2, ... K16 rondesleutels met een lengte van 48 bits die worden afgeleid van de oorspronkelijke

56 bits DES-sleutel. Het symbool ⊕ geeft de bitgewijze optelling modulo 2 van twee 32 bit variabelen weer. Het symbool *f* staat voor een cryptografische functie die uit een 32 bits waarde onder invloed van 48 sleutelbits een nieuwe 32 bit waarde berekent. De kern van deze functie wordt gevormd door acht zogenaamde 'S-Boxen'. Elke S-Box is een substitutie waarbij 6 bits door 4 bits worden vervangen.
De vercijferde tekst ontstaat door L16 en R16 samen te voegen en een eindpermutatie te laten ondergaan.
N.B. De initiële en slotpermutatie hebben geen cryptografische waarde.

Product cipher. Een product cipher is een cryptografische methode die eveneens uit verschillende rondes bestaat. Elke afzonderlijke ronde, ook wel een iteratie genoemd, kent verschillende vercijferingsoperaties zoals substituties en permutaties. Op zichzelf levert een enkele iteratie een beperkt niveau van beveiliging op. Samen bewerkstelligen de opeenvolgende rondes echter een hoog niveau van beveiliging.

Symmetrische en asymmetrische systemen

Vele van de tot nu toe beschreven vercijfermethoden kenmerken zich door het gebruik van dezelfde sleutel voor vercijfering en ontcijfering van de boodschap. Dergelijke systemen worden daarom vaak aangeduid met de term 'symmetrische systemen': aan beide kanten gebruikt men dezelfde sleutel. Een belangrijk kenmerk van zo'n symmetrisch systeem is dat het absoluut noodzakelijk is dat zender èn ontvanger de gebruikte sleutel geheim houden. En omdat iets meestal maar heel kort geheim kan blijven, is het bovendien noodzakelijk veelvuldig van sleutel te wisselen. Dit betekent dat de sleutel voorafgaand aan een bepaalde sessie op een uiterst veilige manier moet worden uitgewisseld.
Naast de symmetrische systemen bestaan er sinds 1976 dankzij Whitfield Diffie en Martin Hellman ook 'asymmetrische systemen', dat wil zeggen systemen waarin de sleutel aan de vercijferkant een andere is dan die aan de ontcijferkant. Door de asymmetrie in het sleutelgebruik is het niet meer nodig om volledige geheimhouding van beide sleutels te handhaven. We kunnen met andere woorden één sleutel

openbaar maken. Dergelijke systemen worden ook (en correcter) publieke sleutelsystemen of public-key cryptosystems genoemd. De symmetrische systemen noemt men in tegenstelling daarmee soms geheime sleutelsystemen of secret-key cryptosystems.
Vooral in het handels- en financiële verkeer is het gebruik van asymmetrische systemen populair. Ze worden onder andere gebruikt voor het zetten van digitale handtekeningen en het uitvoeren van betalingstransacties. Een toekomstige toepassing van asymmetrische systemen zou anonieme televoting (telestemmen) kunnen zijn.

Een nadere uitleg van de werking van symmetrische en asymmetrische systemen vindt u in de verdiepingsstof aan het slot van dit artikel. Wel zal ondertussen het belang van de asymmetrische techniek duidelijk zijn. Een bekend asymmetrisch algoritme dat alle belangrijke eigenschappen bezit is het al eerder genoemde algoritme van Rivest, Shamir en Adleman oftewel het RSA-algoritme.

Sleutelbeheer

Het sleutelbeheer is een van de meest verwaarloosde onderwerpen in overzichtsartikelen over cryptologie. Helaas komt het sleutelbeheer in verband met de beschikbare ruimte er ook in dit artikel tamelijk bekaaid vanaf. Een volledige beschrijving van het sleutelbeheer vraagt namelijk om een toelichting van zeer uiteenlopende methoden. Daarnaast wordt het sleutelbeheer sterk door de omgeving/toepassing van een cryptografisch systeem bepaald. Zo maakt het voor het sleutelbeheer nogal wat uit of cryptografie wordt gebruikt binnen een toegangscontrole-, elektronisch post- of satellietcommunicatiesysteem. In deze paragraaf zal daarom, hoe belangrijk het onderwerp sleutelbeheer ook is, met enkele algemene opmerkingen moeten worden volstaan.
Maar hoe zit het dan met het algoritme, vraagt u zichzelf nu misschien af? Hoe vreemd en onnatuurlijk het mag klinken, in de cryptologie wordt er altijd vanuit gegaan dat het cryptografisch algoritme bekend is (Kerckhoffs principe). De geheimhouding van een nieuw algoritme verhoogt de veiligheid namelijk slechts gedurende een korte periode. Dit is niet alleen te wijten aan lekken in de organisatie, maar soms ook aan de inventiviteit van de crypto-analist. Deze vindt

vaak heel andere, eigen wegen om het geheimschrift te breken. Hoe dat in de praktijk ongeveer gaat, kunt u zelf ondervinden aan de hand van de bij dit dubbelnummer van het Studieblad gevoegde diskette met enkele crypto-analytische raadsels. Een roemrucht voorbeeld uit de rijke geschiedenis van de crypto-analyse is het Japanse cryptografische systeem 'Purple' dat zonder veel voorkennis van het systeem toch kon worden gebroken.
Alles draait dus in de cryptologie om de sleutel. Het sleutelbeheer speelt een bijzonder belangrijke rol bij de keuze van de sleutel. Ook moet de integriteit van de sleutel worden gewaarborgd. Bij zogenaamde symmetrische systemen, systemen waarin voor het ver- en ontcijferen dezelfde sleutel wordt gebruikt, is geheimhouding van de gebruikte sleutel uiteraard cruciaal voor de betrouwbaarheid van het systeem. Het veiligste is in deze situatie om de gebruikte sleutel direct na het vercijferen van de ontvangen boodschap te vernietigen. 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.

Zoals u ontdekt wanneer u de raadsels op de diskette probeert op te lossen, wordt de crypto-analyse in het algemeen bemoeilijkt naar mate minder vercijferde tekst beschikbaar is. We mogen hieruit concluderen dat het gebruik van slechts een enkele sleutel de crypto-analist sterk in de kaart speelt, omdat daardoor in de loop van de tijd steeds meer op dezelfde manier vercijferd materiaal beschikbaar komt. Het wisselen van de sleutel is dus een goed gebruik. Het *sleutelprotocol* zorgt daarvoor en houdt tevens nauwgezet bij welke sleutel gebruikt wordt en wanneer deze moet worden vervangen.
Het vervangen van de sleutel kan door verschillende omstandigheden in gang worden gezet, te weten:
- tijd,
- hoeveelheid vercijferde data,
- ontvanger,
- soort boodschap.

Met tijd wordt de vercijfertijd bedoeld. Na liefst een willekeurig aantal seconden dient de sleutel vervangen te worden. Ditzelfde geldt na een willekeurige hoeveelheid vercij-

ferde data. Dat we de sleutel moeten vervangen wanneer er van ontvanger wordt gewisseld, spreekt eigenlijk vanzelf. Los van de factoren tijd en hoeveelheid staat de boodschapklasse, waarmee aangegeven kan worden hoe belangrijk de te vercijferen informatie is. Als gevolg van de soort boodschap kan een bepaald cryptografisch algoritme worden gekozen. Hoe belangrijker geheimhouding van de boodschap is, des te hoger zal over het algemeeen het niveau van cryptografische beveiliging zijn. Zo zal de Amerikaanse NSA (National Security Agency) alleen de meest geavanceerde cryptografische produkten voor regeringsgebruik aanbevelen.

Een van de eenvoudigste methoden om sleutels over een lijnverbinding te verwisselen is door het definiëren van een *sleutelhiërarchie*. Met behulp van bijvoorbeeld een lijnsleutel *LS* wordt steeds een nieuwe sessiesleutel *SS* geïnstalleerd. *SS* wordt vervolgens gebruikt voor de datavercijfering en *LS* alleen voor het installeren van een nieuwe vercijfersleutel. Omdat *SS* steeds een willekeurig getal is, kan de crypto-analist de lijnsleutel *LS* niet breken op grond van taalkenmerken. Dit verhoogt de veiligheid van het systeem aanzienlijk. Het is overigens belangrijk op te merken dat de lijnsleutel *LS* niet op dezelfde manier te breken mag zijn als de vercijfersleutel *SS*, omdat anders een zogenaamd domino-effect ontstaat. Het domino-effect houdt in dat wanneer we *SS* kunnen breken, we ook in staat zijn om de cruciale lijnsleutel *LS* te breken. *LS* moet zich dan ook op een hoger beveiligingsniveau bevinden dan *SS*. Dit kan bijvoorbeeld worden gerealiseerd door de lijnsleutel *LS* langer te maken dan *SS*. Of door een sterkere vercijfermethode voor het overbrengen van *LS* te kiezen dan voor het coderen van de data. We stuiten hiermee op algemene problemen als 'Wat is sterker?' en 'Na hoeveel tijd moet de sleutel worden vervangen?'. Dit zijn beslist geen triviale vragen!

Naast het leveren van nieuwe sleutels, is het ook van belang te weten of de te gebruiken sleutel echt is. We moeten anders gezegd een soort waarmerk van herkomst hebben. Dit waarmerk kan bijvoorbeeld door gebruikmaking van een asymmetrisch algoritme worden verkregen, zoals in de verdiepingsstof is toegelicht. Maar daarmee zijn we er niet. We kennen nu weliswaar de herkomst van de sleutel, maar

zijn er nog altijd onzeker van of de te gebruiken publieke sleutel niet vals is of tijdens het transport vervormd is geraakt. Bij het noodzakelijk zeer frequente wisselen van sleutel zou je dan ook bij wijze van spreken tot in het oneindige met het uitvoeren van veiligheidsprocedures moeten doorgaan om volledige zekerheid te verkrijgen. Het moge duidelijk zijn dat dit praktisch niet haalbaar is en dat we ergens iemand of een bepaalde instantie moeten vertrouwen. Zo'n instantie zou een telecomoperator kunnen zijn die er als 'trusted third party' voor zorgt dat partijen met wederzijds vertrouwen een verbinding kunnen opzetten. De link-to-link beveiliging, foutcontrole en dergelijke die in het datacommunicatienetwerk van de operator zijn aangebracht, scheppen hiervoor de basis.

Cryptologie en telecommunicatie

De ontwikkelingen in de cryptologie hebben ook hun weerslag gehad op de telecommunicatie, zoals het bovenstaande voorbeeld van link-to-link beveiliging duidelijk laat zien. Maar er zijn nog heel wat meer voorbeelden te noemen. De toepassing van cryptografische technieken in de telecommunicatie is de afgelopen tien tot vijftien jaar namelijk sterk gestegen. Vooral de ontwikkelingen in de werelden van datacommunicatie en mobiele telefonie zijn sterk door de mogelijkheden op cryptologisch gebied bepaald.

De belangrijkste oorzaken voor de sterke toename van cryptografie in de telecommunicatie zijn:
- er wordt steeds meer gebruik gemaakt van digitale communicatie-protocollen, waardoor cryptografische technieken gemakkelijk toe te passen zijn,
- met het toenemen van de intensiteit en de (inhoudelijke) 'waarde' van het telecommunicatieverkeer en daarmee het aantal pogingen tot misbruik, ontstaat steeds meer behoefte aan een strenge beveiliging van communicatiediensten/-stromen.

De eerste telecommunicatiesystemen waarvan duidelijk werd dat misbruik mogelijk was waren de mobiele telecommunicatiesystemen. In het begin van de jaren tachtig werd een aantal westerse landen geconfronteerd met een groeiend aantal gevallen van inbraak (bellen op andermans kos-

ten) en afluisteren van de toenmalige autotelefoonsystemen. Cryptografische technieken, met name identificatie- of ID-protocollen, bieden effectieve bescherming tegen inbraak. In enkele landen zijn deze technieken alsnog in bestaande mobiele communicatiesystemen ingebouwd om aan het verschijnsel inbraak een halt toe te kunnen roepen. Nederland liep hierbij voorop met de beveiliging van het ATF1- en ATF2-systeem. Het ATF3-systeem[10] dat al in Scandinavië werd gebruikt, zou pas in Nederland geïntroduceerd worden nadat een secret-key ID-protocol aan de specificaties was toegevoegd. Om uw geheugen nog even op te frissen, zo'n geheime sleutel of secret-key cryptosysteem valt onder de categorie symmetrische cryptosystemen.

Een cryptografische beveiliging tegen afluisteren is in de ATF2- en ATF3-systemen echter moeilijk te realiseren omdat de spraak nog analoog wordt overgebracht. Anders is dit bij GSM, het pan-Europese mobiele communicatiesysteem. Doordat de spraak hier gedigitaliseerd over de radioweg wordt verzonden, kan het spraaksignaal gemakkelijk vercijferd worden. In het tweede deel van het artikel zal in detail beschreven worden welke cryptografische technieken binnen GSM precies een rol spelen.

De GSM-beveiliging heeft tevens als basis gediend voor de beveiliging van een aantal andere systemen. Voorbeelden zijn DECT (Digital European Cordless Telecommunications) dat gebruikt wordt voor draadloze telefonie en lage snelheid radio-LAN's en TETRA (Trans European Trunked Radio) dat een nieuwe Europese standaard vormt voor digitale mobilofonie. De TETRA-standaard wordt naar verwachting in 1996 afgerond. Aan zowel DECT als TETRA zijn extra cryptografische functies toegevoegd. Dit is niet verwonderlijk gezien hun uitgebreidere functionaliteit. Bovendien geldt voor TETRA dat dit systeem ook door Europese politie-organisaties gebruikt gaat worden die extra eisen stellen aan de beveiligingsmogelijkheden[11].

Maar tegenwoordig is ook bij de specificatie van niet-mobiele communicatiesystemen de toepassing van cryptografie een noodzakelijkheid. In het kader van onder meer Universele Persoonsgebonden Telecommunicatie (UPT), Intelligente Netwerken (IN), betaal-TV en multimediadiensten zijn diverse cryptografische functies gestandaardiseerd. Onderzoek, vaak in internationaal verband, wordt verricht

[10] ATF2 wordt tegenwoordig NMT450 genoemd, terwijl ATF3 nu bekend staat als NMT900. De ontwikkeling van de mobiele communicatie komt aan de orde in: J. Caspers, *Mobiele communicatie in historisch perspectief: de wereld van vóór de handhelds*, PTT Telecom Studieblad, (1995) pp. 727-741.

[11] Aan TETRA zal in een toekomstig nummer van het Studieblad aandacht worden besteed. Voor DECT zie: S. Wobben, *Draadloos communiceren in het bedrijf en de woonomgeving*, PTT Telecom Studieblad, (1991) pp. 735-741; G. Klein Wolterink, *DECT draadloze telecommunicatie voor de toekomst*, PTT Telecom Studieblad, (1992) pp. 44-51; B.J. Busropan, G.J. de Groot, W. Hollemans, E.C. den Toom, A. Verschoor, *Radio-LANS in de praktijk*, PTT Telecom Studieblad, (1994) pp.5-27; D.N.M. Dijkstra en Y.M. van der Veen, *Vox Cordless: draadloze communicatie binnen bedrijven*, PTT Telecom Studieblad, (1994) pp. 577-618.

naar de toepassing van cryptografie voor de beveiliging van elektronisch betalen, ATM, Internet-diensten en electronic mail. Verder gebruiken diverse service providers op individuele basis cryptografische technieken om hun telecommunicatiesystemen en -diensten (bijvoorbeeld ISDN en telefoonkaarten) te beveiligen[12]. De verwachting is dat een goede beveiliging door cryptografische technieken in de toekomst een belangrijk aspect zal vormen bij het op de markt zetten van telecommunicatiediensten.

In de meeste van de genoemde voorbeelden worden de cryptografische functies gestandaardiseerd als onderdeel van de betreffende ETSI-standaard. Dit gebeurt vanwege het specialistische karakter door speciale Security Expert Groups. Voor het ontwikkelen en specificeren van breed toepasbare cryptografische algoritmen is voor ETSI daarnaast een aparte groep opgericht: SAGE (Security Algorithms Group of Experts). Deze groep heeft onder andere standaard cryptografische algoritmen ontwikkeld voor toepassing binnen GSM, DECT, TE9 (multi-applicatie smartcard), videoconferencing en UPT. In 1996 zal de groep de specificatie afronden van een secret-key cipher dat Europese telecomoperators (PNO's) kunnen gebruiken voor de beveiliging van hun beheersystemen. Daarnaast zullen in 1996 standaards van secret-key ciphers worden ontwikkeld voor TETRA en HIPERLAN (een hoge snelheid radio-LAN dat in 1995 door ETSI is gespecificeerd)[13].

Naast de al genoemde ATF- en chipcardsystemen heeft KPN/PTT Telecom zelf ook andere systemen ontwikkeld waarin cryptografie gebruikt wordt. Zo maakt het TOBIAS-toegangsysteem waarmee de meeste KPN-gebouwen beveiligd zijn gebruik van een public-key algoritme en is het TIRO-systeem dat wordt gebruikt voor de toegangsbeveiliging via telefoonlijnen tot computer- en beheersystemen uitgerust met een secret-key stream cipher[14].

[12] PTT Telecom besteedt bijzonder veel aandacht aan de beveiliging van chipcards, zoals u heeft kunnen lezen in het Studieblad van juni 1995, 'Themanummer Cards', met name pp. 398 e.v.

[13] Zie: B.J. Busropan, G.J. de Groot, W. Hollemans, E.C. den Toom en A. Verschoor, *Radio-LANS in de praktijk*, PTT Telecom Studieblad, (1994) pp. 5-27.

[14] TIRO komt aan de orde in: E.J. Boessenkool, *Informatiebeveiliging*, PTT Telecom Studieblad, pp. 183-192.

Verdiepingsstof: symmetrische en asymmetrische systemen

In het kort zullen we in deze verdiepingsstof aan de hand van een voorbeeldsituatie uitleggen hoe symmetrische en asymmetrische cryptosystemen werken.

Symmetrisch systeem. Ter illustratie: noem de boodschap **B**, het cryptogram **C** en de sleutel **S**, dan kan de vercijferprocedure V worden genoteerd als

$\mathbf{C} = V(\mathbf{B},\mathbf{S})$.

Omdat de sleutel vooraf bekend is bij de gebruiker en niet voor iedere boodschap anders is, wordt vaak de voorkeur gegeven aan de notatie $V_S(\mathbf{B})$ in plaats van de standaard notatie $V(\mathbf{B},\mathbf{S})$. De ontcijferprocedure O is als volgt:

$O_S(\mathbf{C}) = O_S(V_S(\mathbf{B})) = \mathbf{B}$.

Asymmetrisch systeem. Noteer de publieke vercijfermethode voor een gebruiker A als E_A (Encryptie) en de geheime vercijfermethode als D_A (Decryptie). Voor een publiek sleutelsysteem geldt nu:

$\mathbf{C} = E_A(\mathbf{B})$ en $D_A(\mathbf{C}) = D_A(E_A(\mathbf{B})) = \mathbf{B}$.

Openbaar maken van E_A betekent dat iedereen een bericht kan vercijferen en toezenden aan de eigenaar die het geheime ontcijferalgoritme D_A bezit. We kunnen dat vergelijken met een telefoonboek waar achter de naam, het adres en het telefoonnummer van persoon A, nu ook het publieke vercijferalgoritme E_A staat dat moet worden gebruikt. Een niet te verwaarlozen probleem hierbij is hoe de integriteit van het telefoonboek kan worden gewaarborgd. We gaan er hier vanuit dat dit kan en in de praktijk gebeurd is. Doordat alleen de geadresseerde de sleutel D_A bezit, kan alleen hij of zij het bericht (dat met E_A vercijferd is) ontcijferen.
Merk op dat op deze manier ook een geheime sleutel kan worden uitgewisseld. Een andere leuke eigenschap van het asymmetrische systeem doet zich voor wanneer de vercijfer- en ontcijfervolgorde mogen worden verwisseld (gecommuteerd):

$D_A(E_A(\mathbf{B})) = E_A(D_A(\mathbf{B}))$.

De zender A kan zijn bericht **B** met de geheime sleutel D_A vercijferen als $\mathbf{C} = D_A(\mathbf{B})$. Iedereen kan het dan ontvangen en het vercijferde bericht met sleutel E_A ontcijferen:

$E_A(\mathbf{C}) = E_A(D_A(\mathbf{B})) = D_A(E_A(\mathbf{B})) = \mathbf{B}$.

Omdat in principe iedereen hiertoe in staat is, kan de privacy of geheimhouding niet gewaarborgd worden. De ontvanger is echter wel verzekerd van de herkomst, want alleen de bezitter van E_A kan het bericht vercijferd hebben. Een toepassing ligt voor de hand, namelijk de zogenaamde alternatieve of 'digitale handtekening'. Een contract of order kan op deze manier ondertekend respectievelijk bevestigd worden.
Om de kracht van dit systeem te illustreren het volgende voorbeeld: privacy + handtekening.
Persoon A bezit de sleutels E_A en D_A, evenzo beschikt B over de sleutels E_B en D_B. Zowel A als B maken de sleutels E_A respectievelijk E_B publiek bekend. Als A een door hem ondertekende boodschap $D_A(\mathbf{B})$ naar B wil sturen, versluiert hij dit bericht met de publieke sleutel E_B van B. De zender A is er nu van verzekerd (handtekening), dat alleen B het bericht

$\mathbf{C} = E_B(D_A(\mathbf{B}))$

kan ontcijferen, omdat alleen B de geheime sleutel D_B kent. Na ontcijferen zoekt B de publieke sleutel van A op en ontcijfert als volgt:

$\mathbf{B} = E_A D_B(\mathbf{C})$ met $D_B(\mathbf{C}) = D_B E_B(D_A(\mathbf{B})) = D_A(\mathbf{B})$.

Persoon B is nu in staat om de boodschap **B** te lezen en bezit tevens het bewijs dat het van A afkomstig is. Ook geldt zolang A en B de inhoud van de bood-

te voorzien[1]. Gaat het om de in deel 1 van dit artikel beschreven 'trusted third party'-rol van telecomoperators, dan speelt dit alles zich binnen de communicatiegerichte lagen van het OSI-model af (verg. afb. 1). Dit geldt onder meer voor datacommunicatie via een beveiligd X.25-netwerk zoals Datanet-1 van PTT Telecom. Willen partijen daarbovenop zelf nog extra beveiligingsmechanismen realiseren dan bieden de applicatiegerichte lagen daarvoor mogelijkheden. Wanneer gebruik wordt gemaakt van een netwerk als het Internet waarbinnen de communicatiestromen niet zoals in X.25-netwerken verregaand beschermd zijn, dan is dit op (eind)gebruikersniveau treffen van veiligheidsmaatregelen sterk aan te raden. Dat geldt zeker wanneer het om de verzending van strategische of privacygevoelige informatie gaat, bijvoorbeeld creditcardnummers. Overigens moet worden vermeld dat wanneer het gaat om het doen van betalingen via Internet op dit moment druk gewerkt wordt aan veilige oplossingen. Zo genieten de elektronische betalingsmechanismes van het in Nederland gevestigde bedrijf DigiCash inmiddels wereldwijde bekendheid[2]. Belangrijk is onder meer de internationale proef met 'ecash' waar duizenden Internet-gebruikers bij betrokken zijn. Ecash is een flexibel, op software gebaseerd systeem voor elektronisch betalen via e-mail of het Internet. Systemen als ecash zullen in de toekomst gebruikt kunnen worden om toegang tot commerciële databases te krijgen, software aan te schaffen, een klein geldbedrag naar een vriend of familielid te sturen of een pizza te bestellen. Even gemakkelijk (en anoniem) als we nu in de winkel met papier- of muntgeld betalen, zullen we straks met digitaal geld ('Cyberbucks') kunnen afrekenen. Speciaal ontwikkelde public-key functies zorgen ervoor dat dit op een veilige manier kan gebeuren.

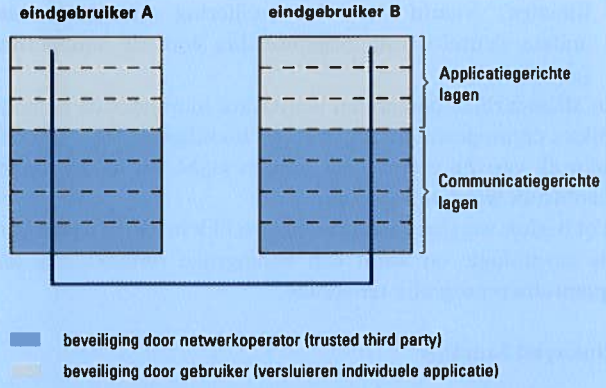
[1] Aan het OSI-model, Open Systems Interconnection, heeft het Studieblad een speciale artikelenreeks gewijd: (1990) pp. 204-216, 324-33, 580-591; (1991) pp. 76-83, 273-285; (1992) pp. 5-19. Zie bovendien de zevendelige serie 'Datacommunicatie' die Opleidingen Telecom (OT) in samenwerking met Samson bedrijfsinformatie heeft uitgegeven.

[2] Digicash is een bedrijf dat systemen ontwerpt op onder meer het gebied van elektronisch betalen, rekeningrijden en elektronische portemonnees. Het bedrijf werkt o.a. samen met KPN, IBM, VISA etc. Meer informatie over Digicash en elektronisch betalen vindt u op Internet: *http://www.digicash.com/*.

Beveiliging en het OSI-model

Communicatiegerichte lagen – integriteit, authenticiteit en versluieren gehele datastroom

- link-to-link; valt in de regel onder de business van een netwerkoperator
- geen effect op bestaande protocollen
- is basis voor het vertrouwen van gebruikers in de veiligheid van een netwerk ('trusted third party'-rol)



Afb. 1 Het OSI-model

Applicatiegerichte lagen – integriteit, authenticiteit en versluieren individuele applicatie

- end-to-end; is meestal een zaak van de eindgebruikers
- te gebruiken bij minimaal vertrouwen in de veiligheid van een netwerk (bijv. PGP op Internet)
- vorm van aanvullende beveiliging in het geval van reeds beveiligde communicatiestroom via netwerk van 'trusted third party' (extra overhead)
- afhankelijk van het belang van een applicatie is selectieve extra beveiliging mogelijk

Om aan de eisen van dit moderne gebruik van de cryptologie tegemoet te komen, zijn in de afgelopen jaren verschillende zogenaamde cryptografische *primitieven* ontwikkeld[3]. Deze cryptografische primitieven worden op basis van het sleutelgebruik in een drietal hoofdgroepen onderverdeeld. In afbeelding 2 is deze onderverdeling van cryptografische primitieven schematisch weergegeven[4].

- Binnen de eerste hoofdgroep van zogenaamde 'unkeyed functies' wordt, zoals de naam al zegt, geen geheime sleutel toegepast.
- De methodes uit de tweede hoofdgroep zijn wel op het gebruik van zo'n geheime sleutel gebaseerd en heten dan ook 'secret-key functies'.
- Ten slotte kennen we nog een derde hoofdgroep van cryptografische primitieven, de zogenaamde 'public-key

[3] Cryptografische primitieven worden ook wel cryptografische functies, cryptografische procedures of cryptografische protocollen genoemd. In de Engelstalige literatuur komen we onder meer de term 'security models' tegen.

[4] Zie ook: A. Bosselaers, B. Preneel (eds), *Integrity Primitives for Secure Information Systems*, Final RIPE report of RACE integrity primitives evaluation (RACE R1040), Springer Verlag, Berlin/Heidelberg/New York.

functies', waarin voor de vercijfering (encryptie) een andere sleutel wordt toegepast dan voor de ontcijfering (decryptie).

In afzonderlijke paragrafen lichten we hieronder de belangrijkste cryptografische functies per hoofdgroep toe[5]. Op het gebruik van de cryptologie binnen GSM zal in een apart hoofdstuk worden ingegaan.

Tot besluit werpen we nog een korte blik in de toekomst van de cryptologie en komt een belangrijke ontwikkeling als quantumcryptografie ter sprake.

[5] Om te voorkomen dat voor elke toepassing uitgebreide nieuwe onderzoeken nodig zijn, proberen cryptografen functies te ontwikkelen die in vele applicaties werken en die bovendien binnen een bepaalde toepassing gemakkelijk gecombineerd kunnen worden. Hierdoor is het mogelijk om op een kosteneffectieve manier in uiteenlopende beveiligingseisen van een toepassing te voorzien. Denk aan X.400-systemen waar zowel confidentialiteit, authenticiteit, sleutelbeheer als juridische betrouwbaarheid belangrijk zijn.

[6] N.B. niet te verwarren met het in deel 1 beschreven 'one-way pad' van Vernam, dat is gebaseerd op het principe: willekeurig + niet-willekeurig = willekeurig! Vernam's idee komt erop neer dat bij een boodschaprij een willekeurige sleutelrij opgeteld wordt, waardoor een willekeurige cryptogramrij ontstaat.

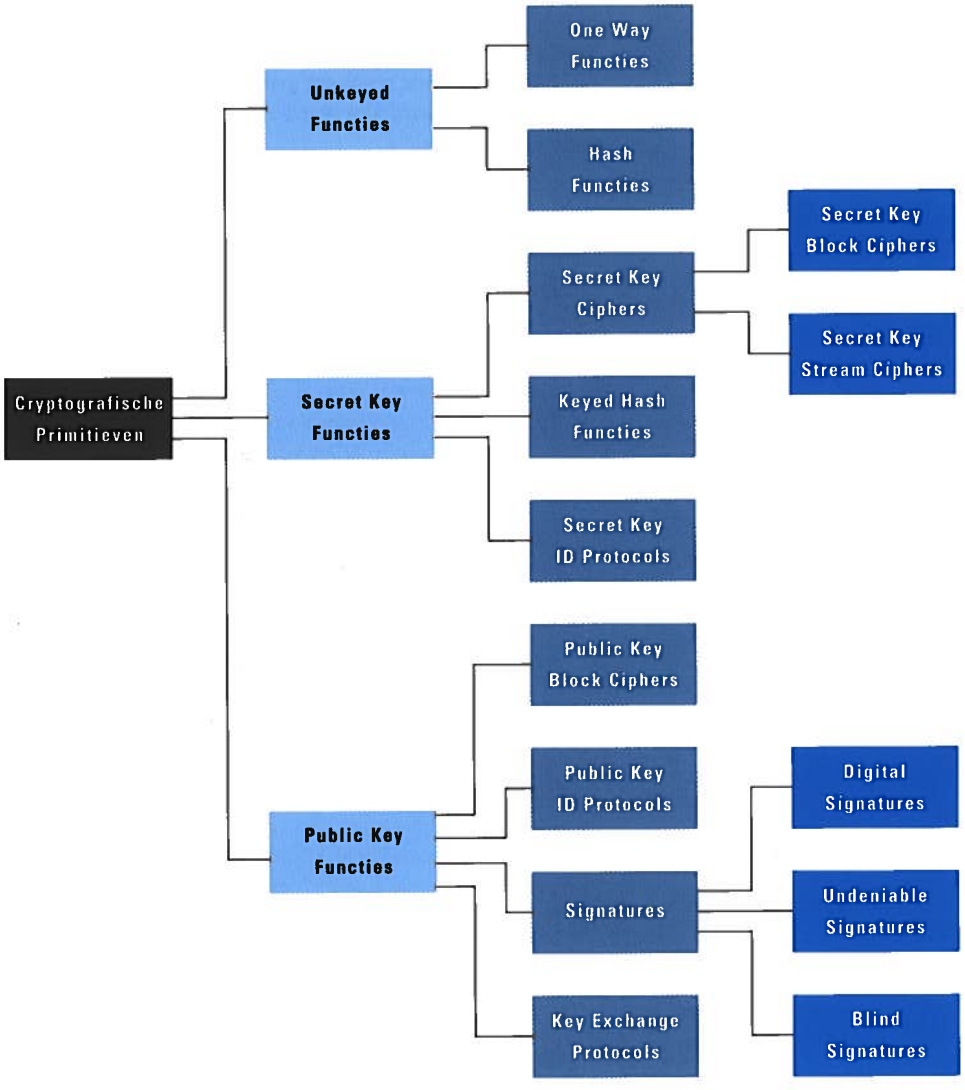
Unkeyed functies

In informatiebeveiligingssystemen is het gebruik van een sleutel niet altijd nodig. Zo worden passwords meestal beschermd door ze met behulp van een sleutelloze of unkeyed functie in een centraal computersysteem op te slaan. Twee bekende unkeyed functies zijn de:

- one-way functie[6],
- hash functie.

One-way functie. Van de instrumenten die cryptografen in de afgelopen decennia hebben ontwikkeld is de one-way functie waarschijnlijk de belangrijkste. De one-way functie staat voor een wiskundige procedure die uit een bepaald input-getal (van beperkte lengte) een zodanig resultaat berekent dat het ondoenlijk is om vanuit dit resultaat het input-getal te vinden. Een tweede voorwaarde is dat die berekening altijd op een simpele manier gemaakt moet kunnen worden. De volgende korte uitleg kan deze algemene omschrijving verhelderen.

Normaal gesproken is een functie, aangeduid met de letter f, een soort voorschrift of computerprogramma dat voor een toegestane invoer 'x' een resultaat of uitvoer 'y' berekent. Een functie f wordt een one-way functie genoemd wanneer de uitkomst 'y' bij een gegeven invoer 'x' eenvoudig te bepalen is. Als de uitkomst 'y' bekend is, moet het echter onmogelijk of ondoenlijk zijn om de invoer- of startwaarde 'x' vast te stellen. De uitkomst 'y' wordt vaak genoteerd als $f(x)$. Bijvoorbeeld als 'x' = 10111, dan is $f(x) = f(10111)$ = 'y' = 0. Het zal duidelijk zijn dat uit 'y' onmogelijk de startwaarde 'x' is te herleiden.



▲ Afb. 2
Overzicht van cryptografische primitieven

One-way functies worden, zoals gezegd, onder meer gebruikt voor de bescherming van passwords. Niet de passwords zelf worden opgeslagen, maar het berekende resultaat nadat op een password (herleid tot binaire informatie) de one-way functie is toegepast. Wanneer een gebruiker gedurende de toegestane gebruiksperiode vervolgens zijn/haar password invoert, berekent de one-way functie

vanuit de startwaarde iedere keer opnieuw het resultaat om dit met het opgeslagen resultaat te vergelijken. Dat uit het opgeslagen/berekende resultaat geen directe informatie over het gebruikte password kan worden afgeleid, laat het onderstaande voorbeeld zien.

Opslaan van passwords

Voor het in een computersysteem opslaan van passwords wordt een eenvoudige one-way functie gebruikt. Maar hoe werkt zoiets nu eigenlijk precies?

Wanneer u het password intikt, wordt de waarde 'y' = *f*(password) berekend. Het resultaat 'y' wordt vergeleken met de onder uw naam opgeslagen waarde van het password. De waarde 'y' mag daarbij bekend raken, omdat het onmogelijk of ondoenlijk wordt geacht om vanuit 'y' het originele password te bepalen.

Dit sluit helaas niet uit dat er een ander password kan bestaan dat dezelfde waarde 'y' oplevert. Het kan best voorkomen dat *f*(qvwbeb) = *f*(geheim). Overigens is het niet waarschijnlijk dat een eventuele indringer er binnen de drie toegestane inlog-pogingen in slaagt om zo'n toevalsresultaat te treffen. Niet alleen heeft hij hiervoor de juiste waarde 'y' nodig, maar in combinatie daarmee ook de gebruikersnaam. Vrijwel altijd zal bij een geslaagde inbraakpoging daarom van hulp van binnenuit of van laksheid sprake zijn. Een voorbeeld is dat in sommige situaties toegang kan worden gekregen tot de password-file, waarna met een eenvoudig zoekprogramma naar de resultaten 'y' kan worden gezocht van de meest voorkomende (waarschijnlijke) passwords. Wordt er op deze manier een 'y' gevonden, dan zoekt men de gebruikersnaam erbij en klaar is Kees. Men kan inloggen onder de gebruikersnaam en het met 'y' corresponderende password. Hoe goed een cryptografisch systeem ook is, tegen dergelijke inbreuken op de veiligheid helpen alleen andere veiligheidsmaatregelen en campagnes om het slordig omgaan met passwords te bestrijden. Echter hoe veilig bovengenoemd systeem in principe ook is, bij sommige toepassingen van one-way functies zal geëist worden dat toevalstreffers nooit en te nimmer mogen voorkomen. Gegeven een bepaald input-getal en het daarbij behorende resultaat zal er dus

geen ander input-getal te vinden mogen zijn dat hetzelfde resultaat geeft. Hoe dit technisch valt te realiseren komt in de verdiepingsstof aan het einde van dit artikel aan de orde. We verklappen u alvast dat het gebruik van een sleutel in combinatie met de one-way functie een belangrijke rol speelt bij dit definitief op slot doen van de deur.

Een eenvoudige toepassing van de one-way functie komen we ook tegen in de wereld van de datacommunicatie: de pariteitsfunctie. Het gaat er in dit geval om vast te stellen of tijdens de transmissie van een bericht verminking van data heeft plaatsgevonden. We kunnen dat realiseren door de waarde 'p' (een zogenaamd pariteitsbit) aan het bericht 'x' toe te voegen. De one-way functie betekent in dit geval dat iedere boodschap 'x' met daaraan toegevoegd het pariteitsbit 'p' een even aantal enen bevat, waardoor altijd geldt dat 'xp' = 0. Op deze manier kan eenvoudig worden geconstateerd of een boodschap verminkt is binnengekomen. Bijvoorbeeld als 'x' = 101101 dan is 'p' = 0 en 'xp' = 1011010, zodat f(xp) = f(1011010) = 0. Is de uitkomst van f(xp) = 1 dan kan het controlemechanisme in een (data)communicatienetwerk of bij de eindgebruiker (o.a. modem) direct zien dat het bericht onderweg een verandering heeft ondergaan en aan de zendende kant om heruitzending van de informatie vragen.

De toepassing van het pariteitsbit als speciale one-way functie maakt dus eenvoudige foutdetectie mogelijk. Voor een asynchroon of pakketgeschakeld netwerk waarin informatie teken-voor-teken wordt verzonden in de vorm van een pakketje van 7 informatiebits + 1 pariteitsbit, is dit een zinvolle oplossing. Maar natuurlijk heeft foutcontrole via het pariteitsbit ook z'n beperkingen. Het mechanisme veronderstelt namelijk dat in de boodschap maar één bit verminkt raakt. Zeker in situaties waarbij een grotere hoeveelheid informatie in één keer wordt verzonden zoals via het synchrone telefoonnet, zal de kans groot zijn dat er tijdens de transmissie meer dan één bit 'omvalt'. Het pariteitsbit verschaft dan onvoldoende zekerheid. Het gebruik van een andere pariteitsfunctie, de zogenaamde Cyclic Redundancy Code (CRC) kan nu een groter aantal foutpatronen helpen opsporen. Deze CRC ziet het te verzenden bericht als één lange

bitrij, dus als één groot getal. Dat getal wordt gedeeld door een bij de communicerende partijen bekende code, die in de telecommunicatiewereld gestandaardiseerd is (zgn. polynoom). De deling leidt tot een restgetal dat met de informatiebits wordt meegezonden. De ontvanger controleert het bericht door de afgesproken deling eveneens uit te voeren, waarna, als onderweg alles goed is verlopen, hetzelfde restgetal ontstaat[7].

[7] Wie belangstelling heeft voor deze materie verwijzen wij naar: R.L. Mattijssen e.a., *Computer, datacommunicatie en netwerken*, Academic Service, Schoonhoven, 1993, m.n. pp. 69-74.

Nadrukkelijk willen we hier opmerken dat foutcontrole altijd uit het toevoegen van redundantie aan een boodschap bestaat. Niet alleen is foutcontrole belangrijk bij het overdragen van gegevens via een telecommunicatie- of computernetwerk (LAN), maar ook bij het opslaan van belangrijke gegevens in een computergeheugen of bij de gegevensoverdracht van een in- naar een extern computergeheugen.

Hash functie. Een tweede type binnen de hoofdgroep van unkeyed functies is de zogenaamde hash functie. De hash functie berekent uit een invoerreeks van willekeurige lengte (de 'message') een waarde met een vaste lengte (de 'hash code'). Een hash functie geeft als het ware een vingerafdruk van de message en maakt het mogelijk de integriteit (echtheid) van een bericht met een te verwaarlozen onzekerheid vast te stellen.
De hash code, ook wel Message Authentication Code (MAC) genoemd, is meestal 128 of 160 bits lang. Dit betekent dat er bijvoorbeeld een gemiddelde kans van 2^{127} bestaat om bij een 128 bits hash code tot hetzelfde resultaat (collision) te komen[8]. Het is dan ook zeer onwaarschijnlijk dat twee verschillende boodschappen op dezelfde hash waarde uitkomen. Voor een hash functie geldt daarom dat:
- gegeven een hash code het uitgesloten is de boodschap te construeren die deze hash code oplevert,
- gegeven een boodschap en de bijbehorende hash code het ondoenlijk is een tweede message te vinden die dezelfde hash code geeft.

[8] Deze kans wordt 2^{64} voor het vinden van een willekeurige boodschap.

Secret-key functies

De veiligheid van secret-key functies is gebaseerd op het gebruik van een vertrouwelijke parameter, de secret-key of geheime sleutel. Zoals in het eerste deel is toegelicht,

gebruiken secret-key functies dezelfde sleutel voor het vercijferen en ontcijferen. We spreken daarom vaak van symmetrische cryptosystemen.
Drie belangrijke soorten secret-key functies worden onderscheiden:
- secret-key ciphers,
- keyed hash functie,
- secret-key identification (ID-)protocol.

Het bekendste secret-key algoritme is momenteel DES (Data Encryption Standard).

Secret-key ciphers. Een veel gebruikte soort secret-key functie zijn de zogenaamde secret-key ciphers of geheime sleutel algoritmen. Deze worden gebruikt voor de vercijfering van informatie. Dit kan via stroom- of blokvercijfering gebeuren, zoals we in deel 1 hebben laten zien. Wordt de klare tekst teken-voor-teken door een algoritme op basis van de secret-key vercijferd, dan is er sprake van een secret-key stream cipher. Wordt de klare tekst met de geheime sleutel blok-voor-blok vercijferd, dan spreken we van een secret-key block cipher.

Keyed hash functie. De keyed hash functie is een cryptografische functie die gebruik maakt van de hash functie in combinatie met een secret-key. Een dergelijke functie berekent van een message een (keyed) hash code. Deze hash code wordt aan de informatie toegevoegd en dient ervoor om sleutelafhankelijke redundantie aan de boodschap toe te voegen. Op deze manier kan de integriteit van een boodschap extra worden gewaarborgd. Alleen wie in het bezit is van de gebruikte secret-key kan de hash code en dus de getrouwheid van het bericht verifiëren.
Door een boodschap met een keyed hash functie te bewerken en de resulterende hash code door een one-way functie te halen, kan een 'expliciete' geheime handtekening aan een boodschap worden toegevoegd. De boodschap mag in dit geval in klare tekst over de lijn worden verstuurd, want het gaat om de digitale handtekening waarmee de boodschap is getekend. Deze 128 bits tellende handtekening is van degene die de geheime sleutel bezit en kan onder andere worden gebruikt om een op afstand gegeven commando te bekrachtigen. De Europese Satelliet Associatie (ESA) heeft deze cryptografische functie bijvoorbeeld gebruikt om comman-

do's mee naar satellieten te sturen. Maar natuurlijk zijn er veel meer situaties te bedenken waarin het veilig op afstand geven van (niet-confidentiële) commando's belangrijk is.

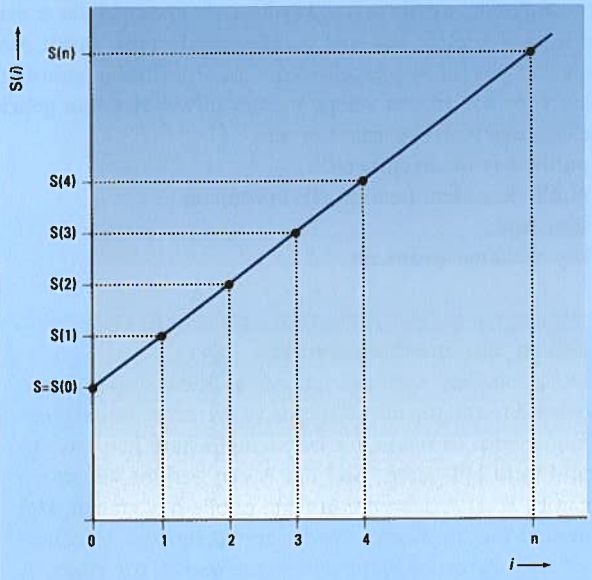
Secret-key identification (ID-)protocol. Bij een secret-key ID-protocol is er sprake van twee partijen die beide dezelfde geheime sleutel bezitten. Gebruikmakend van deze geheime sleutel en een cryptografisch authenticatie-algoritme vindt de uitwisseling van berichten plaats, waarbij steeds een van de partijen verifieert (authenticatie-procedure) of de andere partij in het bezit is van de secret-key: identificatie. Het protocol is er dus op gericht dat de ander aantoont dat hij in bezit is van de secret-key, zonder deze zelf over de lijn te hoeven sturen. Het moet uiteraard ondoenlijk zijn om de secret-key uit de uitgewisselde berichten te herleiden (one-way eigenschap).

Hoe deel je een geheim

De vertrouwelijkheid van een geheime sleutel is van essentieel belang voor de betrouwbare werking van een cryptografisch systeem. In een aantal gevallen zal daarom zelfs de bezitter van een sleutel niet vertrouwd worden, of beter gezegd mag de veiligheid van het systeem niet afhangen van slechts één gebruiker. We kunnen dit vergelijken met de situatie dat de kluis van een bank alleen in het bijzijn van tenminste twee personen mag worden opengemaakt.

De oplossing van dit probleem illustreren we aan de hand van een eenvoudig voorbeeld. Een rechte lijn wordt door slechts twee punten uniek vastgelegd. Kennen we deze twee punten dan kunnen we de lijn dus tekenen. In afbeelding 3 is de grafiek van een lijn getekend. De gebruikers zijn genummerd met 1, 2 ... n. De deelsleutels $S_i = S(i)$ corresponderen met een gebruiker i. Dus persoon 1 bezit deelsleutel S_1 en persoon 2 bezit deelsleutel S_2. Door nu $S_0 = S(0)$ 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 te bepalen, het punt $S = S(0)$. In de praktijk komt het erop neer dat een computer uit de ingevoerde gegevens

de sleutel S bepaalt, waarbij het onmogelijk is S te bepalen als er slechts één persoon participeert.



Afb. 3 Hoe deel je een geheim?

Public-key functies

Karakteristiek voor een public-key functie is dat de sleutel die voor het vercijferen wordt gebruikt een andere is dan de sleutel die bij het ontcijferen een rol speelt (zgn. asymmetrisch cryptosysteem). Een van de sleutels, de public-key of openbare sleutel, kan dus bekend worden gemaakt zonder dat de andere sleutel, de private-key of geheime sleutel, hieruit kan worden afgeleid. Het vercijferen van een bericht gebeurt met de openbare sleutel, voor het ontcijferen van het cryptogram is de geheime sleutel nodig. Public-key functies hebben het voordeel dat het sleutelbeheer eenvoudiger is dan voor secret-key functies geldt. De nadelen zijn dat de implementatie complex is en dat public-key functies relatief traag werken. Zeker in de rij voor de geldautomaat is het laatste een belangrijk bezwaar.

Public-key functies zijn gebaseerd op de ideeën van Diffie en Hellman. Het bekendste algoritme in deze groep is RSA,

ontwikkeld door Rivest, Shamir en Adleman[9]. De hoofdgroep van de public-key functies kan in een viertal typen worden onderverdeeld. Drie daarvan hebben een directe overeenkomst met de secret-key functies in de zin dat er een geheime sleutel in het spel is. Het vierde type wordt niet voor het vercijferen/ontcijferen van informatie gebruikt, maar voor het op een veilige manier uitwisselen van geheime sleutels. Kortweg gaat het om:

- public-key block cipher,
- public-key identification (ID-)protocol,
- signature,
- key exchange protocols.

[9] In de verdiepingsstof aan het slot van dit artikel wordt het principe van RSA aan de hand van een getallenvoorbeeld uit de doeken gedaan.

Beheer van openbare sleutels

De public-key van een gebruiker dient bij iedereen bekend te zijn die in vercijferde vorm met hem wil communiceren. In relatie tot het sleutelbeheer kan dat een probleem opleveren. Stel dat A een bericht wil sturen aan B. B zal A daarvoor om zijn public-key vragen. Het bericht met de sleutel wordt vervolgens door C onderschept, die een andere public-key aan A toestuurt. A vercijfert zijn bericht met deze laatste sleutel en verstuurt het. C kan het bericht nu onderscheppen en ontcijferen, tenminste wanneer de communicatie over een netwerk verloopt dat A geen zekerheid verschaft over de herkomst van de sleutel. Bij een dergelijk onbeveiligd netwerk zou een derde partij of 'trusted third party' de betrouwbaarheid van de sleutel kunnen garanderen. Dit alleen is echter niet voldoende, want naast de identificatie is ook de vaststelling van de integriteit van het bericht belangrijk en de op een niet-leesbare manier verzending daarvan. De integratie van bovengenoemde drie aspecten in Datanet-1 maakt dit netwerk van PTT Telecom tot zo'n betrouwbare communicatieweg.

Public-key block cipher. Als eerste type in de hoofdgroep van public key functies noemen we het public-key block cipher. Dit is een blokvercijferalgoritme dat gebruik maakt van een public-key/private-key sleutelpaar. Het algoritme kan als volgt worden gebruikt. De potentiële ontvanger van een bericht kiest een public-key/private-key sleutelpaar en

maakt zijn public-key bekend. Deze wordt vervolgens door de zendende partij gebruikt om het bericht mee te vercijferen. Alleen de ontvanger die in het bezit is van de private-key kan het bericht ten slotte ontcijferen.

Public-key identification (ID-)protocol. Een tweede type is het public-key ID-protocol, dat evenals het secret-key ID-protocol voor authenticatie wordt gebruikt. Het verschil met een secret-key ID-protocol is dat de betrokken partijen elk een (public-key/private-key) sleutelpaar bezitten. De public-keys worden tijdens een communicatiesessie bekend gemaakt en een protocol verifieert dat elk van de partijen in het bezit is van de bijbehorende private-key zonder deze bekend te hoeven maken.

Voorbeeld van een publiek sleutelsysteem en de mogelijkheden

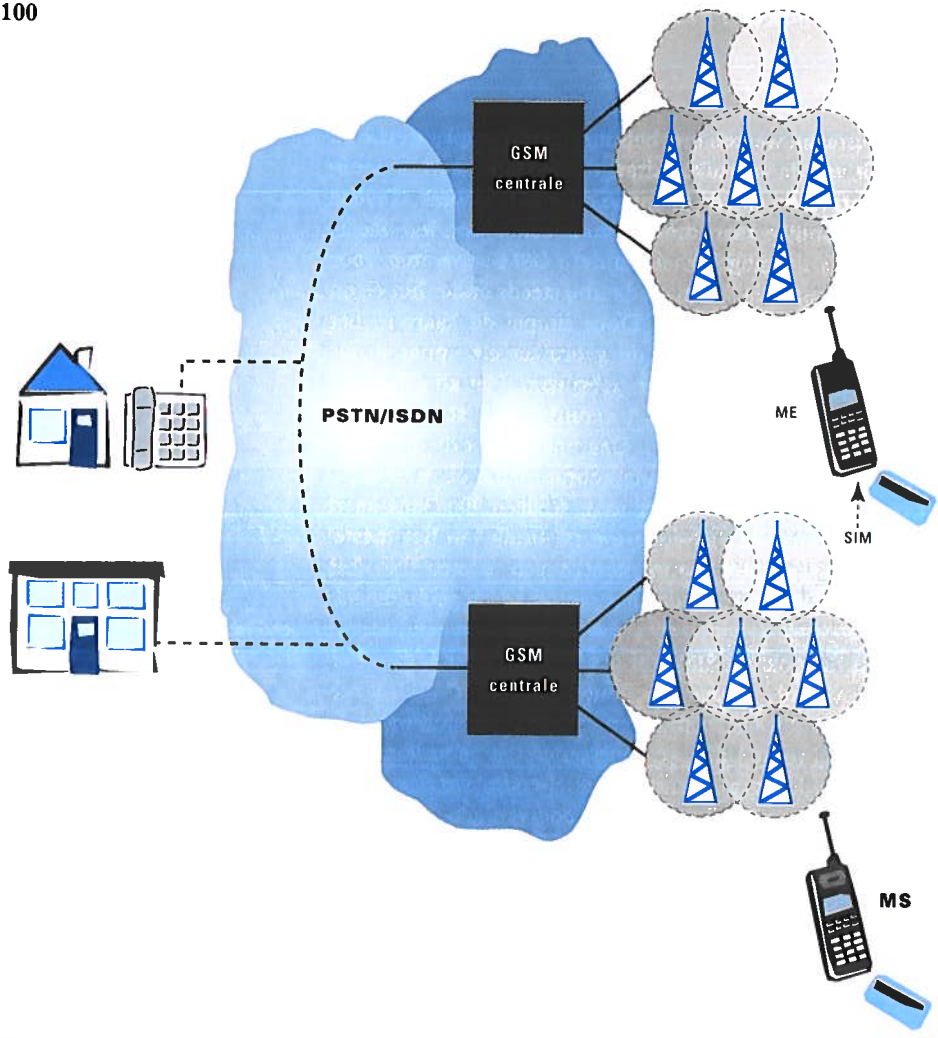
Methode

Publiek bekend vercijferalgoritme: E_A
Geheim ontcijferalgoritme: D_A
$D_A E_A(\mathbf{X}) = \mathbf{X}$
Ondoenlijk om vanuit E_A de inverse D_A te bepalen

Mogelijkheden

Alice stuurt een boodschap **X**:	**X**
Alice stuurt een vercijferde boodschap **X** naar **B**ob:	$E_B(\mathbf{X})$
Alice stuurt een boodschap **X** met een digitale handtekening:	$D_A(\mathbf{X})$
Alice stuurt een vercijferde boodschap **X** met een digitale handtekening naar **B**ob:	$E_B D_A(\mathbf{X})$

Signature. Als derde type is er de signature, als het ware het elektronische equivalent van de gewone handtekening. De signature maakt ook gebruik van een (public-key/private-key) sleutelpaar. Van de signature bestaan verschillende varianten. De meest voorkomende vorm is de 'Digital signature'. Een bericht wordt aan de hand van deze cryptogra-

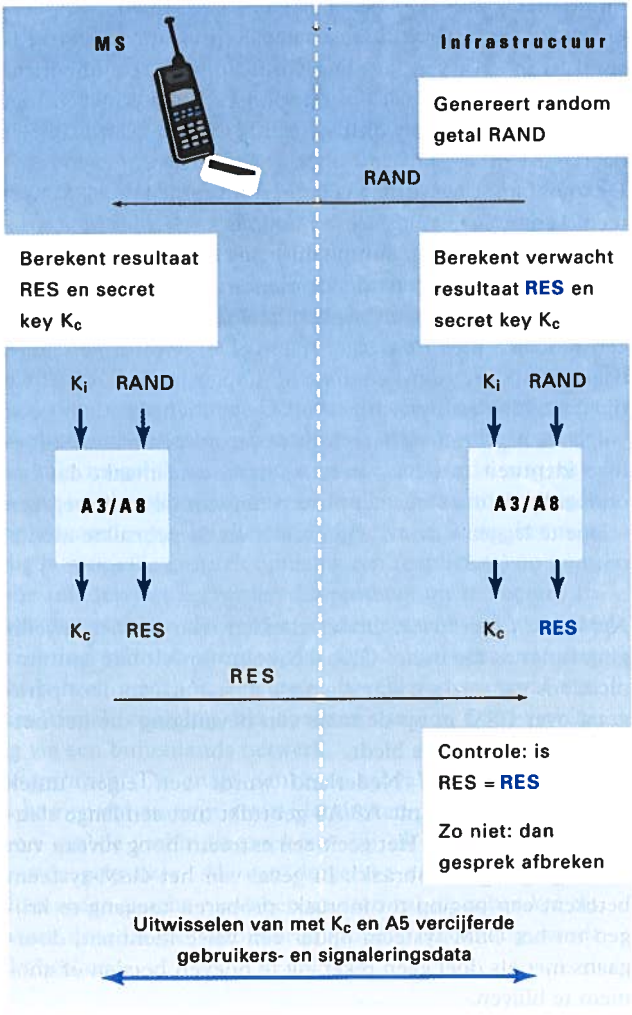


▲ Afb. 4
De GSM-architectuur

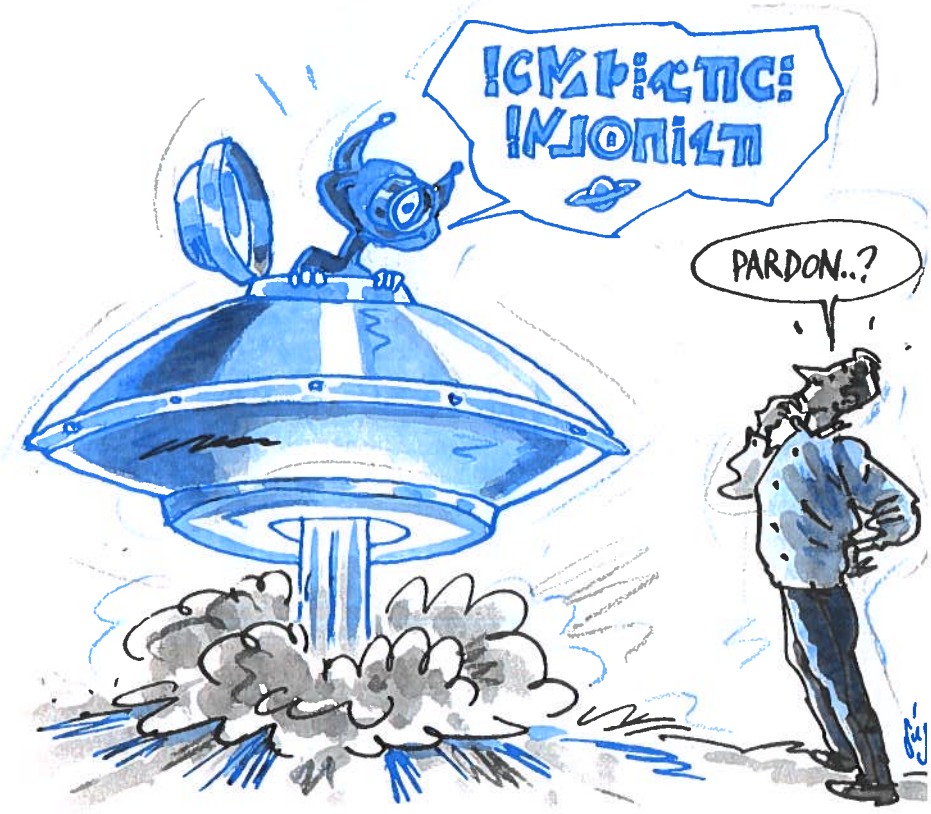
Beveiligingsfuncties in GSM. In GSM wordt standaard een viertal beveiligingsfuncties geboden:

- expliciete authenticatie; als onderdeel van de gespreksopbouw wordt de identiteit van de gebruiker gecontroleerd,
- vertrouwelijkheid; de gebruikersinformatie en bepaalde signaleringsdata wordt over de radioweg vercijferd,
- impliciete authenticatie; de in GSM gespecificeerde mechanismen voor realisatie van de expliciete authenticatie en vertrouwelijkheid zijn op een zodanige manier gekoppeld dat tijdens een gesprek de authenticatie impliciet wordt voortgezet,
- anonimiteit; de GSM-identiteit van de gebruiker wordt over de radioweg vercijferd.

In afbeelding 5 wordt het cryptografisch protocol geschetst dat voor realisatie van de beveiligingsfuncties zorgdraagt. Tijdens de opbouw van een gesprek tussen MS en Infrastructuur wordt een secret-key ID-protocol uitgevoerd waarbij de identiteit van de gebruiker wordt gecontroleerd. Dit gebeurt met behulp van een persoonlijke secret-key (de authenticatie-sleutel) van de gebruiker. Deze sleutel, K_i, is opgeslagen in de SIM en is ook bekend in de infrastructuur. Tijdens de afwikkeling van het protocol wordt tevens een



◀ Afb. 5
Schets van het authenticatie- en encryptieprotocol van GSM



▲ Afb. 6

Toekomstige ontwikkelingen

De opmars van de cryptografie is niet meer te stuiten. I
geldt zowel voor de ontwikkeling van nieuwe cryptogra
sche technieken als voor het aantal toepassingen waar
cryptografie een rol speelt. De explosieve groei van de te
communicatie is een belangrijke katalysator voor deze tc
name van de 'markt' voor cryptografie. De cryptografie
essentieel voor zowel de basisbeveiliging van de transmis
als voor de meer specifieke beveiliging van communicati
diensten en -toepassingen.
Op dit gebied tekent zich een duidelijke trend af. Voor nie
we telecommunicatiesystemen zullen de noodzakelij
cryptografische voorzieningen steeds meer in internationa
standaarden gerealiseerd worden. We kunnen dan denk
aan mobiele communicatiesystemen als TETRA
Inmarsat-P, hoge snelheid radio-LAN's, draadloze techni
ken in de 'local loop', Intelligente Netwerken (IN), ATM

multimediadiensten[12]. Wellicht zal ISDN het laatste telecommunicatiesysteem zijn waarvan de cryptografische beveiliging niet via de internationale standaard is geregeld.

Maar cryptografie is ook belangrijk voor allerlei klanttoepassingen die van communicatienetwerken gebruik maken. Voor de beveiliging van besturing-op-afstand, elektronisch betalen en financieel verkeer op het Internet zullen steeds betere en omvangrijker cryptografische protollen en algoritmen nodig zijn. Hetzelfde geldt voor de beveiliging van video-on-demand en betaaltelevisiesystemen, die om eigen cryptografische oplossingen vragen.
De beheermatige aspecten van beveiliging zullen in de toekomst eveneens belangrijker worden. Het is te verwachten dat cryptografische technieken als X.509-beveiliging op een steeds grotere schaal toepassing gaan vinden. Ook zullen Trusted Third Party (TTP-)systemen aan belang winnen.
Wat betreft de ontwikkeling van cryptografische technieken valt te verwachten dat de toepassing van public-key functies sterk zal groeien. Zij zullen de basis zijn voor verfijnde cryptografische technieken op het gebied van elektronische betaalsystemen, Internet-transacties, gedistribueerde systemen, CallCenters, direct-banking systemen, bescherming van software, CTI-toepassingen en betaal-TV[13].

Quantumcryptografie

Een interessante nieuwe cryptografische techniek is de zogenaamde quantumcryptografie. Hierbij vinden de cryptografische bewerkingen niet op het niveau van de symbolen plaats zoals in de klassieke cryptografie, of op het niveau van de bits en bytes zoals in de huidige cryptografie, maar op het niveau van de elementaire lichtpakketten (fotonen). De quantumcryptografie zou in de toekomst een zeer efficiënte techniek voor de beveiliging van optische communicatiesystemen kunnen zijn. Inmiddels zijn in Engeland en de Verenigde Staten al testopstellingen gerealiseerd waarmee quantumcryptografische technieken succesvol worden gedemonstreerd. In de oktobernummers 1995 van 'Scientific American', 'Science' en 'Physics Today' kunt u hier meer over vernemen.

[12] Zie: B.M. Franke en Y.M. van der Veen, *Technische ontwikkelingen: de gebruiker bepaalt de grenzen*, PTT Telecom Studieblad, december 1995, pp. 807-827.

[13] CTI staat voor Computer-Telephony Integration, het combineren van de mogelijheden van de PC met die van de telefoon. Zie: M.W. van der Schrier en M.T.A.M. Vijftigschild, *CAT: Computer Aided Telecommunications*, PTT Telecom Studieblad, juli/augustus 1992, pp. 420-431.

In een bredere context zijn er enkele ontwikkelingen die niet onbesproken mogen blijven. Sinds kort wordt er in internationaal verband gesproken over nu nog abstracte begrippen als de 'European Information Infrastructure' (EII) en de 'Global Information Infrastructure' (GII). Hoe deze netwerken in de praktijk uitgevoerd zullen worden, moeten we afwachten. Eén ding is op voorhand echter duidelijk: de succesvolle realisatie van nieuwe internationale communicatienetwerken is ondenkbaar zonder een adequate, op cryptografische technieken gebaseerde beveiliging.

Ook op politiek gebied zullen er ontwikkelingen plaatshebben. In de komende jaren zal worden beslist wat de rol van de overheid met betrekking tot cryptografie zal worden. Wordt zij een 'facilitator' voor cryptografie, bijvoorbeeld door de ontwikkeling van cryptografische produkten te stimuleren en eisen/richtlijnen voor de beveiliging van systemen te formuleren. Of zal de overheid haar beperkende rol van 'regulator' blijven benadrukken en eventueel verder uitbouwen door middel van export-beperkingen, eisen voor legale interceptie (aftappen) en toepassing van key escrow systemen. Op korte termijn lijkt de laatste rol het meest waarschijnlijk. Wat de verdere toekomst brengt zal afhangen van een bijna-niet-te-vermijden maatschappelijke discussie die in vele landen zal losbranden en gedeeltelijk al plaatsvindt. Denk aan de discussies in de Verenigde Staten rond key escrow ('Clipper'-debat, zie deel 1) en de Communications Decency Act. Deze laatste wet, die onderdeel uitmaakt van de nieuwe Amerikaanse telecommunicatiewetgeving, beoogt het publiek en met name minderjarigen te beschermen tegen 'onkies' gebruik van communicatienetwerken en -diensten. De internationale ontwikkelingen die uit dit soort overheidsbeslissingen voortvloeien, zullen de nationale keuzes onvermijdelijk beïnvloeden. Ook op cryptografisch gebied is de globalisering een onomkeerbaar proces. Of zoals vele vooraanstaande Amerikaanse bedrijven (o.a. AT&T, MCI en CompuServe) het in hun afwijzing van de key escrow-voorstellen formuleren: 'Een veilige, private en vertrouwenwekkende wereldwijde informatie-infrastructuur is essentieel om economische groei te bereiken en te voldoen aan de behoeften van de informatiemaatschappij. Concurrerende bedrijven hebben de behoefte aan cryptografie die hun bedrijfsgevoelige informatie beschermt als deze via wereldwijde netwerken verstuurd wordt[14].

[14] Geciteerd via: H.A.M. Luiijf, 'Regelgeving cryptografie staat in VS onder druk'. In: *Beveiliging*, (1996), jrg. 9, nr. 1.

Verdiepingsstof: een cryptografisch zesgangen menu

Wie na het lezen van dit artikel de tanden nog wat dieper in de cryptologie wil zetten, vindt in onderstaand zesgangen menu ongetwijfeld iets van zijn of haar gading.

Factoriseren

Een one-way functie die nog niet is behandeld, is het factoriseren van een groot getal. Deze aanpak kan een zeer hoog niveau van beveiliging bewerkstelligen (zie ook verderop de paragraaf over RSA).

Het is bijvoorbeeld eenvoudig om vanuit twee gegeven priemgetallen (getallen die alleen door 1 of zichzelf deelbaar zijn) het produkt te bepalen: 47 x 61 = 2867. Het is echter een stuk moeilijker om vanuit het getal 2867 de twee priemgetallen te bepalen. Naarmate een produkt groter wordt zullen we dit werk al snel aan de computer moeten overlaten. Het blijkt evenwel dat wanneer de getallen erg groot zijn, bijvoorbeeld 500 cijfers, het zelfs met behulp van de snelste computer ter wereld ondoenlijk wordt om de twee priemgetallen te bepalen. Dit kost letterlijk eeuwen computertijd!

Unieke one-way functies

In de situatie dat iedere gebruiker een unieke one-way functie moet bezitten, willen we op een eenvoudige manier kunnen bepalen welke gebruiker welke functie bezit. Om de juiste functie voor een gebruiker te selecteren kan bijvoorbeeld gebruik worden gemaakt van een gebruikerssleutel. Die gebruikerssleutel zal aangeven welke functie een gebruiker bezit. Dit kan eenvoudig worden gerealiseerd met behulp van een speciale one-way functie. Iedere gebruiker krijgt in dit geval een unieke sleutel toegewezen en houdt die geheim. Stel dat de geheime sleutel S opgedeeld kan worden in twee deelsleutels S_1 en S_2, dan kan volstaan worden met een enkele one-way functie en wel als volgt: $\mathbf{Y} = f(\mathbf{X}+S_1) + S_2$. Merk op dat de functie f publiek bekend mag zijn.

Meer algemeen staat hier:

$g_S(\mathbf{X}) = g(\mathbf{X},S) = f(\mathbf{X}+S_1) + S_2$

We noemen g_S daarom een sleutelafhankelijke one-way functie

Voorbeeld: mobiele communicatie. Bij mobiele communicatie kan van een sleutelafhankelijke one-way functie gebruik worden gemaakt om de identiteit van de abonnee vast te stellen. 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 (of beter zijn MS) bepaalt vervolgens dat $\mathbf{Y} = g_{\text{sleutel}}$(willekeurig getal) en stuurt het resultaat **Y** terug. De centrale verifieert dit ontvangen resultaat met het in de centrale berekende resultaat g(getal,sleutel). Afhankelijk van het resultaat van de vergelijking wordt de verbinding nu verbroken of opgebouwd.

Een belangrijke voorwaarde is natuurlijk dat een afluisteraar niet in staat mag zijn de geheime sleutel van de abonnee te bepalen uit de opgevangen **X** en **Y** en het bekend zijn van de functie g. Bij de vaststelling of de functie g voldoet, komt de crypto-analyse om de hoek kijken. Een tweede voorwaarde is dat het voor de illegale gebruiker niet lonend mag zijn naar de waarde **Y** te gokken. Met andere woorden de kans op succes bij gokken moet te verwaarlozen zijn. Bijvoorbeeld na gemiddeld een miljoen maal gokken mag hij een keer succes hebben. Roulette spelen is vergeleken hierbij meer winstgevend: kans 1/35. Een derde voorwaarde is dat het ondoenlijk moet zijn om een lijst op te stellen met corresponderende **X**- en **Y**-paren.

Achterdeurtjes

Er bestaat ook een aantal one-way functies waarbij het met wat extra informatie wel mogelijk is om vanuit het resultaat **Y** de waarde **X** te bepalen. Zonder de extra informatie blijft het echter onmogelijk of ondoenlijk om achter de waarde **X** te komen. Deze functies worden 'one-way trapdoor functies' genoemd. Er is als het ware een achterdeur in het leven geroepen om de juiste waarde van **X** te achterhalen.

Een bijzondere one-way trapdoor functie is de functie waarbij voor iedere toegestane invoer **X** het resul-

taat **Y** berekend kan worden en omgekeerd. Dat wil zeggen, als $g_S(\mathbf{A}) = g_S(\mathbf{B})$, dan is **A** = **B**. Wij zijn dit soort functies al eerder tegen gekomen bij de asymmetrische systemen. En dit is ook precies wat we met een publiek sleutelsysteem bedoelen. Door informatie achter te houden (private-key) is het voor een buitenstaander ondoenlijk om achter de boodschap te komen, echter wie in het bezit is van de extra informatie kan de boodschap wel bepalen.

Het Diffie en Hellman sleuteldistributieprotocol

Een andere belangrijke one-way functie in de cryptologie is de machtsverheffing modulo een priemgetal p:

$f(\mathbf{X}) = \mathbf{A}^{\mathbf{X}} \bmod p$.

Hierin is **X** een geheel getal tussen 0 en p.

A (1 < A <p) is een geheel getal waarvoor geldt dat:

$\mathbf{A}, \mathbf{A}^2, \mathbf{A}^3 \ldots \mathbf{A}^{p-1}$ modulo p.

De p-1 verschillende getallen liggen tussen 0 en p. De modulaire reductie vindt meestal plaats door gebruik te maken van een delingsalgoritme. Nemen we de modulus m als quotiënt en het te reduceren getal **X** als deeltal (X modulo m), dan geeft de rest **R** na deling het gewenste resultaat:

$\mathbf{X} = q.m + \mathbf{R}$.

Het probleem om **X** te bepalen wanneer $\mathbf{Y} = f(\mathbf{X})$ is gegeven, staat bekend als het 'discrete logaritme probleem'. De veiligheid van het in 1976 door Whitfield Diffie en Martin Hellman voorgestelde sleuteldistributieprotocol is gebaseerd op het vermoeden dat het nemen van de discrete logaritme van grote getallen een moeilijk probleem is. Het protocol verloopt als volgt:

- iedere gebruiker beschikt over een publiek getallenpaar (a,p),
- een gebruiker G kiest willekeurig een getal $\mathbf{X_G}$ (1< X_G <p) en houdt dit geheim. Evenzo kiest gebruiker H willekeurig een getal $\mathbf{X_H}$ (1< X_H <p) en houdt dit geheim. Vervolgens wordt $\mathbf{K_G} = a^{X_G} \bmod p$ en $\mathbf{K_H} = a^{X_H} \bmod p$ respectievelijk door gebruiker G en gebruiker H berekend.
- de twee gebruikers sturen de getallen $\mathbf{K_G}$ en $\mathbf{K_H}$ naar elkaar toe. Na ontvangst van $\mathbf{K_H}$ is G in staat om de met H gemeenschappelijke geheime sleutel **K** te berekenen: $\mathbf{K} = (\mathbf{K_H})^{X_G} = a^{X_G X_H} \bmod p$. Evenzo kan H na ontvangst van $\mathbf{K_G}$ de gemeenschappelijke sleutel **K** berekenen: $\mathbf{K} = (\mathbf{K_G})^{X_H} = a^{X_H X_G} \bmod p$.

Voor een *klein* getallenvoorbeeld kiezen we p = 13 en a = 2. De bijpassende logaritme-tabel is weergegeven in tabel 1. Gebruiker G kiest $\mathbf{X_G} = 9$ en berekent $\mathbf{K_G} = 5$. Evenzo kiest gebruiker H willekeurig het getal $\mathbf{X_H} = 5$ en berekent $\mathbf{K_H} = 6$. Na ontvangst van $\mathbf{K_H} = 6$ is G in staat om de met H gemeenschappelijke geheime sleutel **K** te berekenen:

$\mathbf{K} = (6)^9 \bmod 13 = 10077696 \bmod 13 = 5$

Op dezelfde manier kan H na ontvangst van $\mathbf{K_G} = 5$ de gemeenschappelijke sleutel **K** berekenen:

$\mathbf{K} = (5)^5 \bmod 13 = 3125 \bmod 13 = 5$

Het RSA-algoritme

De veiligheid van het naar de uitvinders Rivest, Shamir en Adleman genoemde RSA-algoritme is erop gebaseerd dat het 'factoriseren' van grote getallen bijzonder moeilijk is. Het RSA-systeem laat zich als volgt beschrijven. De modulus m is het produkt van twee grote priemgetallen p en q. Verder zijn er twee getallen e (encryptie exponent) en d (decryptie exponent) die geen gemeenschappelijke delers hebben en waarvoor geldt dat d.e = k.m + 1 voor een zekere k (ofwel d.e = 1 mod m). Het getallenpaar (e,m) wordt nu openbaar gemaakt (public-key) en het getal d wordt geheim gehouden (private key).

Een bericht wordt als volgt vercijferd:

$\mathbf{C} = \mathbf{B}^e \bmod m$.

Voor de ontcijfering geldt:

$\mathbf{C}^d \bmod m = \mathbf{B}^{ed} \bmod m = \mathbf{B}^{km+1} \bmod m = \mathbf{B}$.

Ten behoeve van een *klein* getallenvoorbeeld kiezen we p = 2 en q = 11, wat wil zeggen dat m = p.q = 22. Kiezen we vervolgens voor e = 7, dan is de bijbehorende d = 3, terwijl k = 2 (3.7 = 21; 21 = k.10 +1).

Laat de boodschap **B** = 19 zijn dan is de vercijfering:

$\mathbf{C} = 19^7 \bmod 22 = 893871739 \bmod 22 = 13 \bmod 22$,

zodat **C** = 13.

X	1	2	3	4	5	6	7	8	9	10	11	12
2^x mod 13	2	4	8	3	6	12	11	9	5	10	7	1

Tabel 1

Het bericht **C** = 13 kan nu als volgt worden ontcijferd: **B** = 13^3 mod 22 = 2189 mod 22 = 19 mod 22, waaruit de oorspronkelijke boodschap **B** = 19 volgt.

De populariteit van RSA heeft ervoor gezorgd dat het aloude probleem van het factoriseren meer dan ooit in de wiskunde leeft. Cryptografen zullen in de praktijk steeds alert moeten zijn op wat uit deze hernieuwde belangstelling voor factorisatie en/of equivalente problemen voortvloeit. De veiligheid van hun methodes kan er vanaf hangen. De Nederlandse familie Lenstra speelt een belangrijke rol in de actuele pogingen om het factorisatie-probleem te doorgronden. Bijvoorbeeld Arjen Lenstra heeft dankzij 'factoriseren per E-mail' belangrijke vooruitgang geboekt. Tevens zijn er ook nieuwe factoriseer-algoritmen ontwikkeld.

Zero-knowledge protocollen

Een interessante nieuwe ontwikkeling in de cryptografie zijn de zogenaamde zero-knowledge protocollen. Bijvoorbeeld: via een zero-knowledge protocol overtuigt Alice Bob ervan dat zij de factorisatie van een samengesteld getal kent, zonder de factorisatie zelf aan Bob bekend te hoeven maken. Bob kan er langs deze weg dus van overtuigd worden dat hij Alice kan vertrouwen, terwijl Alice de eigenlijke basis waarop dit vertrouwen berust niet hoeft prijs te geven. We kunnen het ook zo zeggen: nadat Bob ervan overtuigd is dat Alice de factorisatie van het samengestelde (grote) getal kent, zal hij met hetzelfde protocol niet iemand anders kunnen overtuigen. De factorisatie zelf kent hij immers niet!
Dit soort protocollen wordt in authenticatieprocedures toegepast om bijvoorbeeld de identiteit van een persoon of communicatiegebruiker vast te stellen.

Ir. G. Roelofsen studeerde Wiskunde aan de TU Eindhoven en trad daarna in dienst bij de Koninklijke Marine. In 1986 maakte hij de overstap naar KPN Research waar hij sindsdien aan een groot aantal projecten op het gebied van beveiliging heeft gewerkt (o.a. TIRO, GSM en DECT). Momenteel is hij binnen het werkveld Beveiliging en Kaartsystemen betrokken bij diverse interne KPN-projecten op beveiligingsgebied. Daarnaast is de heer Roelofsen voorzitter van de TETRA-beveiligingsgroep en van ETSI SAGE (Security Algorithms Group of Experts) en leidt hij het team dat een encryptie-algoritme ontwikkelt voor Europese Public Network Operators.

Dr.ir. J. van Tilburg studeerde Elektrotechniek aan de TU Delft. In 1986 trad hij in dienst bij KPN Research waar hij zich vooral bezighield met de beveiliging van informatie- en communicatiesystemen (TIRO, ATF). Na een korte periode werkzaam te zijn geweest bij de Koninklijke Marine, trad de heer Van Tilburg opnieuw in dienst bij KPN Research. Sindsdien is hij betrokken geweest bij diverse beveiligsprojecten en medeuitvinder van de TeleChipper. In 1994 promoveerde hij aan de TU Eindhoven op het gebied van de wiskunde (veiligheidsanalyse van een klasse van cryptosystemen gebaseerd op coderingstheorie). Momenteel werkt hij bij de afdeling Network & Service Control van KPN Research o.a. aan Intelligente Netwerken.

Explanatory notes

to gather	zich verzamelen, bijeenkomen
instance	geval, voorbeeld
to slim	afslanken
billing skills	geavanceerde betalingsmogelijkheden
diverse	ongelijksoortig, uiteenlopend
to nibble at	knabbelen aan
an incidental part	een bijkomstig deel
a host of other services	een groot aantal andere diensten
reach	bereik
converge	convergeren, samenkomen
interplay	interactie, wisselwerking
distinct	duidelijk, specifiek
glut	overvloed, oververzadiging
entry	toetreding, binnenkomst
simultaneous	gelijktijdig
to eavesdrop	afluisteren
clunky	rammelend
inexorably	onverbiddelijk
lavishly	kwistig
stake	aandeel
huge	enorm
basement	kelder, souterrain
premium products	duurdere produkten van hoge kwaliteit

Nortel op weg naar verkoop van 1 miljoenste MERIDIAN-1 lijn in 1995

Als gevolg van een groei van 26,9 procent in de PBX-verkoop in 1995, heeft Nortel (Northern Telecom) Europa in december de miljoenste Meridian-1 PBX-aansluiting van 1995 kunnen verkopen. Hiermee is het record van 1994 (788.000 aansluitingen) gebroken. Vrijwel alle Europese landen werkten mee aan deze belangrijke groei.
Ook in Nederland was de groei van het aantal Meridian-1 systemen aanzienlijk. Als gevolg van de distributie-overeenkomst die Nortel in het begin van 1995 sloot met PTT Telecom verdubbelde hier het aantal geïnstalleerde systemen. Daarnaast nam het marktaandeel in het Verenigd Koninkrijk met drie procent toe en voegden ook Nortel's Joint Ventures in Frankrijk en Duitsland een belangrijk deel aan de winst toe. In de voormalige Sovjetunie, waar eerder in 1995 een nieuw kantoor werd geopend, werd een groei van 75 procent behaald. Volgens Nortel Europe-topman Richard Reid hangt de groei in Europa samen met het herstel van de economische recessie.

(Bron: Persbericht Nortel, december 1995)

Vakantieservice PTT Post: Post naar tijdelijk adres

Vanaf 1 januari 1996 heeft PTT Post in haar dienstverlening de Vakantieservice opgenomen. De klant van deze dienst kan dan voor kortere of langere tijd zijn post laten doorsturen naar een tijdelijk adres in Nederland.
Tot dusverre konden klanten op verzoek hun post gratis laten nasturen naar een tijdelijk adres. Dat kan nu niet meer. De invoering van de Vakantieservice maakt deel uit van het streven van PTT Post om haar tarieven van produkten en diensten beter te laten aansluiten bij de kosten ervan. Overigens worden lopende afspraken nog (gratis) afgewerkt.
Voor de Vakantieservice geldt hetzelfde tarief als voor de Bewaarservice:
- *f* 25,– voor de eerste twee weken en
- *f* 3,50 voor elke volgende week.

PTT Post stuurt de post zo lang door als de klant wenst, met een maximum van één jaar.
Klanten die nadere vragen hebben over de Vakantieservice kunnen (gratis) bellen met PTT Post Klantenservice, 06-0417.

(Bron: Persbericht PTT Post, P 083/1995)

Boek 'De Verborgen Collectie' laat deel van kunstcollectie KPN zien

Op 29 november 1995 ontving Zijne Koninklijke Hoogheid Prins Claus, lid van de Raad van Commissarissen van KPN, het eerste exemplaar van het boek 'De Verborgen Collectie' uit handen van Ir. W. Dik, voorzitter van de Raad van Bestuur van KPN. Prins Claus ontving daarbij de 28 originele prenten van beeldende kunstenaars die zij in opdracht van KPN speciaal voor deze boekuitgave gemaakt hebben.
Het boek 'De Verborgen Collectie' laat hoogtepunten uit de kunstcollectie van KPN zien. De kunstcollectie van KPN bestaat uit ongeveer 15.000 kunstwerken die door het hele bedrijf verspreid te zien zijn. Het is daarmee de grootste bedrijfscollectie in Nederland.
'De Verborgen Collectie' verschijnt in het jaar dat de afdeling Kunst & Vormgeving van KPN vijftig jaar bestaat. Het boek is een relatiege-

schenk en is dus niet in de boekhandel te koop.
Het boek 'De Verborgen Collectie' laat een representatieve keuze zien uit de totale bedrijfscollectie. Het begrip 'verborgen' duidt op het gegeven dat de bezoeker van KPN nooit alle kunstwerken in één keer te zien zal krijgen. In 1994 is er in het PTT Museum een speciale tentoonstelling 'De Verborgen Collectie' met een aantal kunstwerken van KPN geweest.
Het boek heeft bijna 300 bladzijden en toont 250 afbeeldingen van kunstwerken van KPN en tevens afbeeldingen van de 28 speciaal in opdracht vervaardigde prenten.
'De Verborgen Collectie' bevat een bijdrage van de heer drs. Hein van Haaren, kunsthistoricus, over 50 jaar kunst en vormgeving van KPN. Dr. Wim Beeren, voormalig museumdirecteur, heeft de kunstcollectie van KPN in museaal perspectief geplaatst. De tekst en toelichtingen zijn in het Nederlands en Engels. De oplage is 2500 stuks.
Kunst & Vormgeving is binnen KPN verantwoordelijk voor de kwaliteit van kunstaankopen en -opdrachten en de vormgeving van de produkten en dienstverlening van KPN. De afdeling valt onder directe verantwoordelijkheid van de Raad van Bestuur. In die positie heeft Kunst & Vormgeving daarom ook een duidelijke betrokkenheid bij alle uitingen van de bedrijfsstijl en zorgt daarbij voor een constante en goede kwaliteit en juiste uitstraling van het concern.
De betekenis en het belang van een afdeling Kunst & Vormgeving is in 1945 onderschreven door de oprichting van de Dienst voor Esthetische Vormgeving voor het staatsbedrijf der PTT. De oprichting van deze dienst is gebaseerd op de mening van de heer mr. J.F. van Royen (1878-1942), destijds algemeen secretaris van het hoofdbestuur der PTT. Hij stelde dat een dienstverlenend bedrijf in de tijd zelf moest staan en zich moest bedienen van de instrumenten die de moderne techniek, maar ook de moderne kunst en vormgeving hem bood. Voor die tijd was dit een opmerkelijk progressieve stelling; voor deze tijd lijkt het een vanzelfsprekendheid.
KPN maakt gebruik van de meest geavanceerde technologie en weet zich ondersteund door een corporate culture, die niet alleen in een heldere bedrijfsstijl en in opvallende grafische en industriële produkten, maar ook in de kunstaankopen en kunstopdrachten is af te lezen.

(Bron: Persbericht KPN, H 116/1995)

Software telefooncentrale sneller en goedkoper gewijzigd

Voor de gebruikers van een Philips en Ericsson telefooncentrale is het wijzigen van de software-instellingen van de telefooncentrale een stuk eenvoudiger geworden. Op basis van het TeleMutatie Support abonnement verzorgt PTT Telecom namelijk op afstand de gewenste veranderingen in de software.
Het controleren van de systeemgegevens en het maken van back-up's kon al langer op afstand plaatsvinden. Met de introductie van TeleMutatie Support kunnen ook andere softwarematige faciliteiten op afstand worden gewijzigd. Het instellen van de chef/secretaresse-schakelingen en groepsschakelingen maar ook het instellen van de gebruiksrechten per toestel, het omzetten van nummers bij een interne verhuizing en het instellen van de geheugenplaatsen in de toestellen zijn enkele voorbeelden.
Door deze activiteiten uit te besteden hoeft niet langer een medewerker te worden opge-

leid. Die klopt, in de praktijk, bij meer complexe zaken toch voor advies en hulp bij de leverancier aan. TeleMutatie Support zorgt er voor dat het merendeel van de gewenste veranderingen binnen 24 uur zijn gerealiseerd. Maatwerkoplossingen en omvangrijke opdrachten vragen vanzelfsprekend meer tijd. De mutaties kunnen zowel overdag als 's nachts worden uitgevoerd, waardoor rekening kan worden gehouden met de pieken in het eigen telefoonverkeer. Een telefonische helpdesk ondersteunt de systeembeheerder bij vragen over software mutaties.
Met TeleMutatie Support wordt een aantal operationele problemen weggenomen, wijzigingen kunnen daardoor sneller worden geëffectueerd en de noodzakelijke kennis is verzekerd. Ook hoeft er niet meer geïnvesteerd te worden in opleidingen en spelen de geografische grenzen die gelden bij meerdere vestigingen, geen rol meer.
De kosten van het TeleMutatie Support abonnement bestaan uit een vast maandelijks bedrag en een bedrag per handeling.
De mogelijkheid bestaat om voor drie maanden een proefabonnement af te sluiten. Telefonische informatie wordt gegeven via het gratis telefoonnummer 06-0403.

(Bron: Persbericht Telecomnieuws, nr 37/1995)

BT chooses partners for its future intelligent network

BT has chosen Digital Equipment and Alcatel as its partners to develop a design for BT's next generation of intelligent network, called CORNICHE (customer oriented network intelligence and capability in a heterogeneous environment). The new network will be based on the telecommunications information networking architecture (TINA) model.
BT's current intelligent network provides services such as Advanced Freephone 800, Value Call 0891 and virtual private network services. CORNICHE, instead of using stand alone service control points, will put applications and services into a separate layer from the underlying network infrastructure – giving BT additional flexibility to offer services tailored to meet individual customer needs, by mixing and matching services.

(Bron: The ITU Newsletter, 9/1995)

Europe's telephone bills continue to fall

The second edition of the report *Cutting the cost: the falling price of telephony in Europe*, released last August by Analysys (telecommunications consultants) reveals that while most of Europe's business and residential customers continue to benefit each year from real cuts in what they pay for their telephone services, there is still a wide range between the cheapest and the most expensive countries.
According to Analysys, 'The competitive markets in Finland and the United Kingdom delivered another steep reduction in price over the last year. But bills in other countries – such as Germany and the Netherlands – stayed the same in real terms.'
Business customers in countries such as Italy and Ireland are now paying more than their competitors elsewhere in Europe. For residential customers, Finland, France, the Netherlands and the United Kingdom are delivering the best deals, with Italy and Ireland again lagging behind.

(Bron: The ITU Newsletter, 9/1995)

Postwijzer biedt op diskette informatie over tarieven, produkten en diensten van PTT Post

Vanaf 8 januari brengt PTT Post de Postwijzer uit, dat uitgebreide informatie over tarieven, produkten en dienstverlening van PTT Post op diskette bevat. Het computerprogramma is bestemd voor met name de zakelijke klanten (midden- en kleinbedrijf) die regelmatig het PTT Post tarievenboekje raadplegen. Op eenvoudige wijze geeft de Postwijzer informatie over bijvoorbeeld het voordelige tarief voor een bepaald soort zending.
De Postwijzer 1996 kost *f* 23,50 exclusief BTW. Zakelijke postbushouders krijgen in januari via een mailing van PTT Post de mogelijkheid de Postwijzer 1996 te bestellen. Ook is bestellen mogelijk via PTT Post Klantenservice Zakelijke Markt: 06-0430 (gratis).
Met de Postwijzer 1996 is het gemakkelijk tariefinformatie op te zoeken van alle soorten post voor binnen- en buitenland. De gebruiker kiest voor een soort zending, typt het gewicht en aantal in en geeft aan welke dienstverlening gewenst is. Het voordeligste tarief verschijnt dan op het beeldscherm. Het computerprogramma geeft de tarieven en voorwaarden van streekpost en partijenpost en belangrijke verzendingsvoorwaarden.
Naast een overzicht van alle PTT Post business-balies (zakelijke post), worden alle adressen en openingstijden van postkantoren vermeld. Ook staan de brievenbussen aangegeven die pas om 19.00 uur gelicht worden. De Postwijzer 1996 geeft eveneens aan welke postcodes tot een streekpostgebied horen. Een uitgebreid trefwoordenregister vergroot het gemak bij gebruik van dit computerprogramma.
De Postwijzer 1996 maakt het mogelijk om verschillende verzendmogelijkheden te vergelijken zoals bijvoorbeeld aangetekend en verzekerd vervoer. De gebruiker kan uitrekenen welke voordelige partijenposttarieven gelden bij bepaalde hoeveelheden post. Informatie over het verschil in prijs en overkomstduur naar het buitenland tussen lucht- en zeepost biedt de Postwijzer eveneens.
Voor de Postwijzer 1996 is minimaal een personal computer (IBM-compatible met 80386-processor) nodig. Het computerprogramma draait op Windows 3.1 of hoger. Tevens is ten minste een intern geheugen van 4 Mb nodig en 6 Mb vrije ruimte op de harde schijf.
De Postwijzer is door de zakelijke klant te bestellen via PTT Post Klantenservice Zakelijke Markt, telefoonnummer 06-0430 (gratis). Het tarievenboekje van PTT Post blijft gratis verkrijgbaar op het postkantoor, bij PTT Post business-balies of (telefonisch) bij PTT Post Klantenservice Zakelijke Markt.

(Bron: Persbericht PTT Post, P 001/1996)

Chipkaartgebruikers geënquêteerd

In een enquête van Intomart onder 1125 van de eerste 20.000 kaartbezitters beoordelen de gebruikers de experimentele, multifunctionele chipkaart voor studenten met een 7,2. Het experiment met de kaart, die dient als collegekaart, OV-kaart, bibliotheekkaart, betaalpasje en communicatiemiddel met de IBG, werd ruim twee maanden geleden gestart aan de TU Twente, de RUG en de Hogeschool van Groningen. Grootste probleem is de herkenbaarheid. Eenvijfde van de gebruikers heeft wel eens te maken gehad met conducteurs of buschauffeurs die de kaart niet herkenden als

vervoerbewijs. Ook waren er nog veel informatiezuilen niet aangesloten. Kinderziektes, oordelen de initiatiefnemers. De 'papieren' OV-kaart heeft inmiddels dezelfde kleuren als de chipkaart en de technische problemen met de informatiezuilen zijn opgelost. Vrijwel niemand heeft problemen met dit nieuwe communicatiemiddel. Slechts acht procent van de kaartbezitters moest de hulp inroepen van de zogenaamde 'helpdesk'. Ruim de helft van de ondervraagden vindt de chipkaart een enorme verbetering en driekwart vindt haar zeer gebruikersvriendelijk, terwijl 85 procent aangeeft geen enkele functie van de kaart te willen missen. Ook uitbreiding met extra functies wordt als positief ervaren: 77 procent zou daar geen bezwaar tegen hebben. De combinatie van de functies maakt studenten wel bang voor verlies: 84 procent van de bezitters ziet dat als een probleem. Het consortium is blij met die uitslag. Het betekent dat studenten goed op de kaart zullen passen.
Conclusies over verdere verspreiding van de kaart worden nog niet getrokken. In december en februari hebben opnieuw onderzoeken plaatsgevonden. Na dit onderzoek komt ook de mogelijkheid aan de orde om met de chipkaart te betalen. Betalen met de chipkaart is pas sinds november 1995 mogelijk.

(Bron: Cursor 16-11-1995)

Infonet en Unisource breiden samenwerking uit

Infonet en Unisource zijn overeengekomen hun respectieve datanetwerken te koppelen. Voor Europese gebruikers betekent dit een aanzienlijke uitbreiding van de communicatiemogelijkheden. Unisource kan haar klanten door deze overeenkomst toegang bieden tot het volledige Infonet World Network dat 165 landen beslaat. Infonet kan haar klanten buiten Europa nu binnen Europa netwerkdiensten aanbieden via het pan-Europese netwerk van Unisource. De overeenkomst omvat wereldwijde X.25, SNA-, Virtual Private Data Network- en kieslijntoegangsdiensten. Beide partijen hebben de intentie uitgesproken om te investeren in gemeenschappelijke switching-apparatuur, zodat de beide netwerken optimaal zijn te integreren.
Unisource en Infonet zullen onafhankelijk van elkaar blijven opereren. Daartoe zijn gebruikersondersteuning en dienstverlening op logische wijze verdeeld. Om snel op vragen van klanten te kunnen reageren en problemen op te lossen hebben beide bedrijven standaard procedures vastgesteld. Voor de klanten van beide bedrijven heeft de overeenkomst geen gevolgen.

(Bron: Persbericht Telecom Nieuws '95)

ISDN Pakket Advanced: Fax- en modemverkeer met digitale en analoge gebruikers

ISDN, het Integrated Services Digital Netwerk, is met een snelle opmars bezig. Met dit digitale telefoonnet is het mogelijk informatie met een veel hogere snelheid tegen lagere kosten te verzenden.
Met name voor zakelijk gebruik wordt ISDN algemeen als opvolger van het huidige analoge telefoonnet gezien. De overgang naar ISDN is eenvoudig omdat gebruik wordt gemaakt van het bestaande kabelnet.

Computertechnologie speelt een grote rol bij de vele toepassingen van ISDN. Naast een ISDN-aansluiting is bij de verschillende toe-

passingen specifieke hard- en/of software vereist.
Met de introductie van het ISDN Pakket Advanced is het mogelijk zowel de oude (analoge) als de nieuwe (digitale) telecommunicatiewereld te bereiken. De gebruiksmogelijkheden nemen daartoe sterk toe en een soepele overgang van de analoge naar de digitale wereld ligt voor grote en kleine organisaties binnen handbereik.
De faciliteiten die het ISDN Pakket Advanced biedt zijn:

- File Transfer. Met behulp van Euro File Transfer worden bestanden via ISDN super snel uitgewisseld. Een floppy met 1,4 Mb aan informatie wordt in circa drie minuten verstuurd.
- Faxen. Met behulp van faxgroep-4 apparaten wordt via ISDN gefaxed op een snelheid die gemiddeld vijf keer hoger ligt dan bij een analoge verbinding.

Omdat nog niet iedereen over ISDN beschikt, biedt het ISDN Pakket Advanced ook de mogelijkheid voor analoge toepassingen:

- Modemcommunicatie via de eigen ISDN aansluiting met een analoge partner. Hierbij blijft de snelheid beperkt tot 2.400 Bps (in vergelijk met ISDN 64.000). De mogelijk heid om met de oude en de nieuwe wereld te communiceren blijft echter bestaan, terwijl de stap naar de moderne ISDN wereld is genomen.
- Faxen 3. Vanaf de PC faxen met andere Faxgroep-3 apparaten. De snelheid blijft hier op het bestaande niveau.

PTT biedt ook het ISDN Pakket Migratie aan, waarmee bestaande analoge apparatuur op het ISDN-net wordt aangesloten, terwijl ISDN-applicaties buiten deze adapter omgaan. Een belangrijke desinvestering wordt daarmee voorkomen.

De belangrijkste eisen die aan de PC worden gesteld om het ISDN-pakket Advanced goed te kunnen gebruiken zijn: 386/486 IBM compatable PC, ISA/EISA businterface, MS Dos>3.x of Windows>3.0, 4MB intern geheugen, 8 MB beschikbaar op harde schijf. De prijs van het ISDN Pakket Advanced bedraagt *f* 895,- exclusief BTW.

(Bron: Persbericht PTT Telecomnieuws, nr. 34-01/1995)

Onderzoekster KPN Research krijgt Europese prijs

Aan mevrouw J.M. Scarr MA, projectleidster bij KPN Research, is een belangrijke Europese prijs toegekend. Zij krijgt in het kader van het RACE-programma van de Europese Gemeenschap, de 'Award' voor 'The best young technologist in the RACE-programme'. De prijs is op 6 november jl. uitgereikt in Wenen, door de voorzitter van het Europese Parlement, Klaus Hänsch.
Josie Scarr (29) is gekozen uit de vele jonge mensen die in de loop der tijd hebben meegewerkt aan één of meer van de 180 RACE-projecten. De prijs gaat naar de persoon onder de 35 jaar die de beste innovatieve resultaten in RACE heeft geboekt. Van doorslaggevend belang bij de toekenning van de 'award' is de kwaliteit van het werk van Scarr en de kwaliteit van de innovatie.
RACE (Research in Advanced Communications in Europe) is in 1988 opgezet om de introductie van geavanceerde communicatie via onder meer breedbandnetwerken en ATM te versnellen. RACE loopt eind dit jaar af. ATM (Asynchronous Transfer Mode) is een techniek die breedbandtransmissie mogelijk maakt. Er deden meerdere landen binnen de

Europese Gemeenschap mee aan RACE, dat ook gedeeltelijk door de EG werd gesubsidieerd.
Josie Scarr, sinds 1988 werkzaam bij KPN Research, is leidster van het RACE-project Tribune. Tribune is gericht op het volledig specificeren, implementeren en testen van de interface tussen netwerk en gebruiker (de zgn. Broadband User Network Interface). Deze interface is een onderdeel van het ATM-netwerk en vormt het koppelvlak tussen netwerk en de apparatuur van de gebruiker(s). Bij KPN Research in Leidschendam staat een test- en demonstratie-opstelling van Tribune die nog altijd veel belangstelling trekt; in 1994 en dit jaar heeft KPN Research aan meer dan 500 mensen het netwerk en de toepassingen kunnen laten zien.

(Bron: Persbericht KPN, H 108/1995)

Traxys gebruiker eenvoudiger en goedkoper bereikbaar

Investering in twaalf maanden terug verdiend - Met de introductie van de Efcyphone TL door PTT Telecom wordt de bereikbaarheid voor Traxys gebruikers sterk vereenvoudigd en vooral goedkoper. De Traxys gebruiker is nu, zonder tussenkomst van de operator, direct telefonisch te bereiken. Het komt maar al te vaak voor dat de Traxys gebruiker, in de auto, bij klanten of zwervend door het eigen bedrijf opgeroepen moet kunnen worden zonder tussenkomst van de Traxys Vaste Post. Vooral buiten kantooruren doet die situatie zich voor. De Efcyphone T1 verzorgt de koppeling tussen een Traxys-vloot en een bedrijfstelefooncentrale of het openbare telefoonnet. Met de koppeling is het mogelijk om vanaf een telefoontoestel Traxys gebruikers op te roepen. Ook het omgekeerde is mogelijk, de Traxys gebruiker die rechtstreeks een telefoonnummer kiest binnen of buiten het eigen bedrijf. Via de bedrijfstelefooncentrale kunnen de gebruiksrechten per Traxys toestel worden vastgesteld. In de oude situatie was de gebruiker genoodzaakt een abonnement en eigen huurlijnen te nemen tussen de bedrijfstelefooncentrale en de Traxys centrale. Met de komst van de Efcyphone kan worden volstaan met een eenmalige aanschaf van het apparaat, t.w.v. *f* 6.995,- (exclusief BTW) en een abonnement ter waarde van *f* 19,- per maand. De terugverdienperiode bedraagt ongeveer 12 maanden.

(Bron: PTT Telecomnieuws, nr 33/1995)

A2000 en PTT Telecom sluiten contract voor levering radio- en tv-signalen

A2000, de nieuwe kabelexploitant van de regio Amsterdam, heeft met PTT Telecom een contract getekend over de levering van radio- en televisiesignalen. PTT Telecom verzorgt deze dienst, CableLink, via het Breedband Video Netwerk.
CableLink verzorgt de aanvoer, de directe ontvangst en de doorgifte tussen de aanbieders van televisie- en radioprogramma's en de kabelexploitant, die deze programma's weer aan de consument aanbiedt. A2000 gebruikt CableLink als aanvulling op de faciliteiten van het eigen ontvangststation. CableLink biedt een ruim en gevarieerd programmapakket aan, waaruit het programmapakket van A2000 wordt samengesteld. Het CableLink-pakket omvat onder meer BBC 1 en 2, zenders die kabelexploitanten in Nederland zelf niet kun-

nen ontvangen. Ook wordt via CableLink een toenemend aantal zenders rechtstreeks vanuit de studio aangeleverd. Dit zijn naast Nederland 1, 2 en 3 ook commerciële zenders als TV 10 Gold en Veronica.
A2000 heeft gekozen voor CableLink, omdat de aanvoer van een deel van deze programma's een kwaliteitsverbetering van het ontvangstsignaal voor de A2000-abonnees betekent; storingen door atmosferische invloeden kunnen niet meer optreden.

(Bron: Persbericht PTT Telecom,
T 110/1995)

Virtueel kunstwerk dankzij videoconferencing

De bezoeker die onderdeel is van een virtueel kunstwerk. Dat is realiteit in het Stedelijk Museum in Amsterdam en de Vishal in Haarlem, waar de kunstenares Kirsten Geisler tot en met 3 december haar virtuele kunstwerk 'Change' toont. Een voorbeeld waarbij de moderne techniek mensen dichter bij elkaar brengt.

De videoproduktie 'Change' toont het groeien van eenvoud naar complexiteit, de overgang van chaos naar structuur. Geprojecteerd op de muren van beide musea, geeft de produktie het beeld van neerdruppelend water. Deze rustige cadans verandert al snel in een chaotische stroom waarin een nieuwe ordening zichtbaar wordt. Plotseling verschijnen er menselijke figuren in beeld. Het blijken geen acteurs, maar de toeschouwers in het Stedelijk Museum en de Vishal te zijn.
Videoconferencing apparatuur van PTT Telecom brengt hen afwisselend als onderdeel van het kunstwerk in beeld. Gedurende enkele seconden worden daarbij de grenzen van ruimte en tijd overschreden en lopen 'echte' en virtuele werkelijkheid door elkaar.
Videoconferencing maakt het mogelijk om gelijktijdig met 2 tot ruim 25 lokaties beeld en geluid te versturen via het ISDN net, het snelle digitale netwerk van PTT Telecom.
De beelden worden opgenomen met een minicamera en weergegeven op een scherm, een grootbeeld monitor of de eigen PC. Niet alleen beeld, maar ook spraak en data signalen kunnen via ISDN gelijktijdig en met een veel hogere kwaliteit worden verstuurd.

(Bron: Persbericht Telecomnieuws,
nr 36/1995)

PTT Telecom verhuurt apparatuur voor korte perioden

Een tijdelijk tekort aan apparatuur komt in iedere organisatie voor. In een aantal gevallen is huren de oplossing. Gaat het om telecommunicatie-apparatuur dan biedt PTT Telecom daarvoor verschillende oplossingen. Huren komt vooral in aanmerking als het gaat om kortere perioden.

Een beursdeelname, een buitenlandse reis, werkzaamheden aan produktieapparatuur in fabrieken maar ook een verkoopactie veroorzaakt capaciteits- en daarmee bereikbaarheidsproblemen. Een extra mobiele- of autotelefoon, een fax, een semafoon of een portofoon netwerk is dan een goede oplossing en zorgt dat er bij deze tijdelijke pieken geen vertraging in de normale werkzaamheden ontstaat. Niet alleen deze apparaten maar ook complete telefooncentrales kunnen voor enkele dagen worden gehuurd. Zo kan bij een beurs die op een

ijdelijke locatie plaatsvindt, toch elke deelne-
ner zijn eigen aansluiting krijgen.
De zakenreiziger die tijdens zijn trip in het
uitenland telefonisch bereikbaar wil zijn, kan
ij het RentCenter op de luchthaven Schiphol
n Rotterdam Airport terecht. De evenemen-
enorganisator heeft meer baat bij de onder-
teuning door PTT Telecom Event. Daarnaast
iedt het Business Center voor het bedrijfsle-
en tal van mogelijkheden. Drie mogelijkhe-
len om snel informatie te krijgen. Apparatuur
s er meestal voldoende. Heeft de één het niet,
lan biedt de ander wel uitkomst.
Een simpel telefoontje met het Business
Center, het RentCenter of PTT Telecom
Event is voldoende om informatie over de
uurmogelijkheden te krijgen. Natuurlijk is
et mogelijk om de apparatuur te reserveren.
Bij mobiele telefoons is twee dagen vooraf-
aande aan de huurperiode het tijdelijke tele-
oonnummer bekend.

Bron: Persbericht PTT Telecomnieuws, nr.
5/1995)

Waddenvereniging en SOS-Kinderdorpen thema op telefoonkaarten

Op 8 november 1995 heeft PTT Telecom de
aarlijkse telefoonkaarten-serie gewijd aan cha-
itatieve instellingen uitgegeven. Dit jaar staat
eze serie in het teken van de Waddenver-
niging en SOS-Kinderdorpen.
De heer Ir W. Dik, voorzitter Raad van
Bestuur KPN, overhandigde de eerste exem-
laren aan Hare Koninklijke Hoogheid
Prinses Margriet, beschermvrouwe van SOS-
Kinderdorpen.
De ontwerper van de telefoonkaarten-serie is
Anthon Beeke. De serie bestaat uit telefoon-
kaarten met een waarde van één, vijf, tien en
vijfentwintig gulden. Voor verzamelaars is er
een speciaal mapje waarin zich de vier kaarten
bevinden. De oplage van deze set is 13.000
stuks. De één gulden kaart is alleen te verkrij-
gen door aanschaf van het verzamelmapje. De
oplage van de vijf gulden kaart is 800.000
stuks, de tien gulden kaart is 600.000 keer
gedrukt en de vijfentwintig gulden kaart
450.000 keer.
SOS-Kinderdorpen biedt overal ter wereld
hulp aan kinderen die als gevolg van oorlog,
aardbevingen en andere rampen vrijwel niets
of niemand meer hebben. De Waddenvereni-
ging vecht en waakt voor het behoud van het
wad (en voor de vele trekvogels die tijdelijk op
het wad leven). Anthon Beeke heeft hun acti-
viteiten gesymboliseerd door een vluchtheu-
vel. Op de voorzijde van de kaarten heeft
Anthon Beeke het geografische werkveld van
de beide instellingen weergegeven. Aan de
achterzijde van de kaarten heeft hij de doel-
groep van de beide instellingen weergegeven.
De telefoonkaarten van vijf, tien en vijfentwin-
tig gulden zijn te koop bij Postkantoor,
Primafoon en wederverkopers. De één gulden
kaart bevindt zich alleen in de set die verkrijg-
baar is bij Primafoon of via de Verzamelservice
Telefoonkaarten (06-0993360). De prijs van
de gehele set bedraagt vijfenveertig gulden.

(Bron: Persbericht PTT Telecom,
T 109/1995)

Boekbespreking

Titel: *De muren hebben oren...: een gids tegen het afluisteren*
Auteur: Stichting Backslash, Buro Janssen & Janssen, Stichting Hacktic
Amsterdam: Stichting Backslash, 1994
112 p. met diskette
ISBN 90-9007580-1

Het gebruik van afluistertechnieken heeft een hoge vlucht genomen. Zowel criminelen als politie gebruiken deze technieken. In dit boek worden verschillende communicatievormen beschreven en de manier waarop ze afgeluisterd kunnen worden. Het ontdekken, bemoeilijken, verhinderen en onbruikbaar maken van afluisteren wordt ook besproken.
Doel van het boek is om mensen praktische tips te geven zodat er een voorsprong op de eventuele afluisteraar ontstaat.
Eerst wordt ingegaan op de partijen die in Nederland afluisteren. Dit zijn – grofweg – politie, de BVD en het bedrijfsleven. De afluisterwetgeving in Nederland is vastgelegd in het Wetboek van Strafrecht en de Wet Computercriminaliteit. De gevolgen van de Wet Computercriminaliteit worden besproken.
Er zijn verschillende manieren om af te luisteren. In ruimtes kan men afluisteren door bijvoorbeeld richtmicrofoons en contactmicrofoons te gebruiken. Op hoofdlijnen wordt de werking van deze microfoons uitgelegd. Nagegaan wordt hoe tegenmaatregelen genomen kunnen worden tegen het afluisteren. Ook telefoonverkeer kan afgeluisterd worden. Naast 'gewone' telefoongesprekken kunnen ook gesprekken die via draadloze communicatie gaan worden afgeluisterd.
Verschillende oude en nieuwe methoden om gegevens te versleutelen worden kort besproken. Naast het versleutelen van data is ook het versleutelen van spraak mogelijk. Enkele technieken hiervoor worden behandeld.
Ook de rol die camera's kunnen spelen bij afluisteren wordt toegelicht. Op de diskette die bij het boek hoort staan een aantal programma's en algoritmen voor het versleutelen van gegevens.
Dit boek is bedoeld om leken bekend te maken met afluisteren en de daarbij behorende technieken. Geïnteresseerden kunnen met de gegevens op de diskette experimenteren.

Deze boekbespreking is samengesteld door Genoveva Geppaart, KPN Research BIDATA, in opdracht van de redactie van PTT Telecom Studieblad. KPN-medewerkers kunnen het boek onder vermelding van BIDATA-kenmerk 1076045 lenen bij: KPN Research, BIDATA, Gebouw SI, Postbus 30000, 2500 GA Den Haag, tel. 070 – 33 23172.