Basismethoden Cryptografie

Omslag: voor- en achterzijde van de Schijf van Phaistos (2000 - 1600 v. Chr.).
Gevonden in 1908 in het tempelcomplex te Phaistos aan de zuidkust van Kreta. Kleitablet (diameter 16,5 cm) met ingedrukte Kretenzische hiërogliefen. Tot op heden nog niet ontcijferd. Veronderstellingen variëren van een overwinningslied of lofzang tot een handleiding voor tempelgebruik. Het origineel bevindt zich in Museum van Herakleion op Kreta.
(Tekening: A.P.H. Berbers, Grafisch Museum Drenthe.)

Basismethoden Cryptografie

J.C.A. van der Lubbe

Vakgroep Informatietheorie
Technische Universiteit Delft

VSSD

Eerste druk 1994
Tweede druk 1997

Uitgegeven door:
VSSD
Leeghwaterstraat 42, 2628 CA Delft
tel. +31 15 278 2124, telefax +31 15 278 7585, e-mail: hlf@vssd.nl
internet: http://www.vssd.nl/hlf
URL over dit boek: http://www.vssd.nl/hlf/informatie.html

ISBN 978-90-407-1256-2

Voorwoord

Door de voortschrijdende technologische ontwikkelingen heeft de automatisering in alle lagen van onze maatschappij zijn intrede gedaan, alsmede zijn onze communicatiemogelijkheden steeds groter geworden. Op grote schaal wordt er gebruik gemaakt van methoden voor geautomatiseerde gegevensverwerking en datacommunicatie. Voorbeelden zijn er te over: medische en fiscale computerbestanden, automatisch betaalverkeer, beeldtelefoon, abonnee-tv, fax-verkeer, teleshopping, wereldwijde computernetwerken etc. etc. Bij al deze voorbeelden is er sprake van een toenemende behoefte voor de beveiliging van opslag en transport van informatie. De redenen voor het optreden van deze behoefte zijn van velerlei aard. Beveiliging kan noodzakelijk zijn om economische belangen te beschermen, om fraude tegen te gaan of om de privacy van de burger te waarborgen etc.
Cryptografie is de wetenschap die zich in meest algemene zin bezighoudt met methoden voor de beveiliging van opslag en transport van informatie.
In het voor u liggende boek zal aandacht besteed worden aan de basismethoden voor de beveiliging van opslag en transport van informatie, zoals deze momenteel ontwikkeld zijn en gehanteerd worden. Het is het doel van dit boek de lezer vertrouwd te maken met de diverse mogelijkheden die cryptografie biedt, maar zeker ook met de onmogelijkheden van en de randvoorwaarden voor het gebruik van cryptografie.
Het boek is bedoeld voor een ieder die op een of andere manier betrokken is bij beveiliging en beveiligingsaspecten van gegevensverwerking en communicatie: ingenieurs, systeemontwerpers, applicatieprogrammeurs, informatie-analisten, security officers, EDP-auditors etc.

Het boek is ontstaan uit colleges die de schrijver de laatste jaren heeft gegeven aan studenten van de Faculteiten Elektrotechniek, Technische Wiskunde en Informatica, Technische Bestuurskunde en Technische Natuurkunde van de Technische Universiteit Delft en op basis van de bankgerichte cursus Cryptografie verzorgd door TopTech Studies, welke verantwoordelijk is voor het postdoctorale onderwijs van de Technische Universiteit Delft, en waaraan de schrijver als directeur van genoemde cursus is verbonden.
De schrijver wil van de gelegenheid gebruik maken dr.ir. J.H. Weber te bedanken, met wie hij gedurende een aantal jaren de colleges Cryptografie aan de Technische Universiteit Delft heeft verzorgd. Verder zou ondergetekende alle collega's van de

TopTech cursus Cryptografie willen bedanken, in het bijzonder ir. R.E. Goudriaan van de Internationale Nederlanden Bank, omdat ze schrijver dezes veel geleerd hebben ten aanzien van de praktische aspecten van het gebruik van cryptografie.

J.C.A. van der Lubbe
januari 1994

Voorwoord bij de tweede druk

In deze nieuwe druk zijn paragrafen over IDEA (International Data Encryption), openbare-sleutelsystemen gebaseerd op elliptische curven, DSA (Digital Signature Algorithm) en fair cryptosystemen toegevoegd. Voorts is een aantal kleine verbeteringen aangebracht.

J.C.A. van der Lubbe
januari 1997

Inhoud

Beknopte inhoud

In Hoofdstuk 1 wordt vooral aandacht besteed aan de rol die cryptografie speelt binnen de totale beveiligingsproblematiek. De verschillende doelen van beveiliging worden beschouwd alsmede wordt een eerste overzicht gegeven van de cryptografische methoden die daarvoor gehanteerd kunnen worden.
In Hoofdstuk 2 komen de meer klassieke cijfersystemen aan de orde, zoals transpositie en substitutiecijfers. Tevens wordt enige aandacht besteed aan de methoden die cryptanalisten ('krakers') toepassen om genomen beveiligingsmaatregelen te doorbreken.
In vele gevallen valt of staat de sterkte van cryptografische algoritmen met de mate waarin veiligheid bereikt kan worden. Het begrip veiligheid zelf is echter verre van eenduidig. In Hoofdstuk 3 wordt met behulp van informatietheorie nagegaan wat er met veiligheid bedoeld wordt en hoe deze bereikt kan worden.
Een van de thans meest toegepaste cryptografische algoritmen, gebaseerd op vercijfering op basis van geheime sleutels, is het DES-algoritme. De principes van dit algoritme worden gegeven in Hoofdstuk 4.
In Hoofdstuk 5 wordt aandacht geschonken aan schuifregisters voor het opwekken van pseudo-random reeksen, welke laatste gebruikt kunnen worden voor het genereren van sleutels dan wel voor het vercijferen van bitstromen. Het begrip randomness wordt zelf ook nader bestudeerd.
Hoofdstuk 6 is gewijd aan de zogenaamde openbare-sleutel systemen; cryptografische algoritmen waarbij sprake is van een geheime en openbare sleutel. Het RSA-algoritme is hier een belangrijk voorbeeld van.
Hoofdstuk 7 is betrokken op andere soorten van beveiliging, te maken hebbend met authenticatie en integriteit. Het gaat hierbij om technieken op basis waarvan men zich ervan kan gewissen dat een verzonden bericht ongeschonden is en dat een door zeg A verzonden bericht inderdaad van A afkomstig is etc. De verschillende methoden passeren de revue, waarbij ook digitale handtekeningen en zerokennistechnieken aan de orde komen.
In het algemeen geldt dat hoe goed de cryptografische algoritmen ook zijn, de overall veiligheid valt of staat vaak met de mate waarin de geheime sleutel geheim gehouden wordt. In Hoofdstuk 8 wordt aandacht besteed aan sleutelbeheer, dat zich bezighoudt met het veilig genereren, distribueren etc. van sleutels, alsook aan de specifieke aspecten van beveiliging van netwerken.
Ter afsluiting zijn twee bijlagen toegevoegd. Bijlage A handelt over de informatiemaat van Shannon en is bedoeld voor degenen die met het oog op Hoofdstuk 3 onvoldoende vertrouwd zijn met de informatietheoretische basisbegrippen. Bijlage B behandelt enige specifieke technieken voor het vercijferen van beelden.

Notaties

A_d	Aantal residuklassen met d elementen
C	Cijfertekst
$C(\tau)$	Autocorrelatie
CI	Coïncidentie-index
CI'	Zuivere schatter van CI
d	Deel van geheime sleutel bij RSA; aantal elementen van residuklasse
δ	Hamming-afstand
DK(.)	Ontcijfering door symmetrisch algoritme met sleutel K
$dS_X(.)$	Ontcijfering door asymmetrisch algoritme met geheime sleutel S_X
D_L	Redundantie in tekst ter lengte L
e	Deel van openbare sleutel bij RSA of elliptische curve-algoritme
E	Expansie-operatie DES
$E(.)$	Verwachting
$EK(.)$	Vercijfering door symmetrisch algoritme met sleutel K
$eP_X(.)$	Vercijfering door asymmetrisch algoritme met openbare sleutel P_X
ε	Aantal elementen van alfabet
ϕ	Euler totiënt functie
$f(.)$	Karakteristiek polynoom
$f(.,.,.)$	Terugkoppelfunctie schuifregister
$F(.,.)$	Cijferfunctie DES
F	Elliptische curve
$G(.)$	Genererende functie
χ	Chi-test
$h(.)$	Hash-code
H	Hypothese
$H(.)$	Marginale informatiemaat
$H(K/C)$	Sleutelequivocatie
$H(M/C)$	Boodschapequivocatie
$H(K/M,C)$	Key appearance equivocatie
I	Identificatiereeks
IP	Initiële permutatie
IV	Initiële vector
J	Jacobi-symbool
K	Geheime sleutel bij symmetrisch algoritme
kDES	Eerste k bits van resultaat van vercijfering met DES
K_i	Subsleutel DES
K_{ij}	Sleutel Diffie-Hellmann-protocol

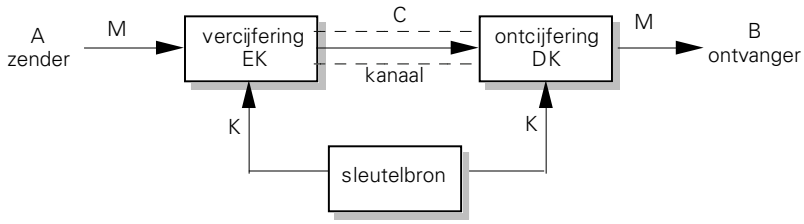
KS	Sessiesleutel
l	Lengte van een run
L	Lengte van een bericht
LC	Lineair-complexiteitsprofiel
m	Aantal secties schuifregister
mgK(.)	Resultaat van een MAC met sleutel K
M	Klare tekst, originele boodschap
MK	Master key
mod	Modulo-optelling
N	Lengte van (pseudo-)random reeks
oK(.)	Resultaat van eenrichtingsfunctie met sleutel K
p	Periode schuifregisterreeks; priemgetal
P_X	Openbare sleutel van X bij asymmetrisch algoritme
Pe	Foutkans
PeD	Foutkansafstand
q	Priemgetal
r	Totale aantal runs in binaire reeks
R	Random reeks
S	Knapzaksom; veiligheidssgebeurtenis
S_X	Geheime sleutel van X bij asymmetrisch algoritme
s_i	Element van schuifregisterreeks; geheim getal bij zerokennistechniek
T	Periode
T_K	Vercijferingstransformatie
TK	Terminal key
UD	Uniciteitsafstand
var	Variantie

1
Inleiding cryptografie

1.1. Cryptografie en cryptanalyse

In de titel van dit boek komt het woord *cryptografie* voor. Cryptografie is een onderdeel van wat men noemt de *cryptologie*. De term cryptologie is de samentrekking van twee Griekse woorden “cruptos” (= verborgen) en “logos” (= woord, leer). Het woord cryptologie betekent dan ook letterlijk de leer van het verbergen. In zoverre behelst het de ontwikkeling van methoden om boodschappen en signalen te *vercijferen* alsook de ontwikkeling van methoden om vercijferde boodschappen te *ontcijferen.*
Ten aanzien van cryptologie kan onderscheid gemaakt worden tussen twee deelgebieden: *cryptografie* en *cryptanalyse*.
In engere zin kan cryptografie opgevat worden als dat deel van de cryptologie dat zich bezighoudt met technieken om data te versluieren of te vercijferen, waarbij veelal gebruik gemaakt wordt van geheime sleutels. Alleen degene die over de geheime sleutels beschikt is in staat de vercijferde informatie te ontcijferen. Voor ieder ander is dit in principe ondoenlijk.
Cryptanalyse is dat deel van de cryptologie dat zich bezighoudt met technieken om de vercijferde data te ontcijferen zonder a priori volledige kennis over bijvoorbeeld de sleutel. Het gaat hier om wat in het dagelijks taalgebruik ook wel aangeduid wordt met de term “kraken”.

Het spreekt voor zich dat zowel cryptografie als cryptanalyse nauw met elkaar samenhangen. Zo zal een ontwerper van cryptografische algoritmen eigenlijk alleen maar in staat zijn goede (dat wil zeggen sterke) cryptografische algoritmen te ontwikkelen als hij voldoende kennis heeft met betrekking tot de methoden en gereedschappen die door cryptanalisten gehanteerd worden. Dit geldt ook voor degene onder wiens verantwoordelijkheid bepaalde beveiligingsmaatregelen geïmplementeerd worden. Ook hij zal op de hoogte moeten zijn van de technieken die een potentiële indringer kan hanteren.
Omgekeerd geldt natuurlijk dat cryptanalyse alleen maar succesvol kan zijn als men minimaal enige kennis heeft over de toegepaste cryptografische algoritmen en methoden.
In dit boek zal de nadruk vooral liggen op cryptografie.



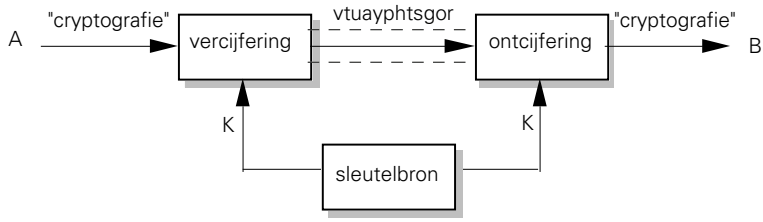
Figuur 1.1. Vercijfersysteem.

Om hier een eerste indruk te geven van wat een cryptografisch algoritme doet en tevens om enkele notaties te introduceren, beschouw de volgende situatie. Neem aan dat *A* (de zender) een bericht in vercijferde vorm, dat wil zeggen in geheimcode, wil versturen naar *B* (de ontvanger). Vaak wordt in de literatuur het originele bericht, ook wel genoemd de *klare tekst*, aangeduid met de letter *M* van het Engelse woord "Message", terwijl het vercijferde bericht, ook wel geheten de *cijfertekst*, wordt aangeduid met de *C* van het Engelse "Ciphertext". Een methode zou kunnen zijn, dat *A* daartoe gebruik maakt van een geheime sleutel *K* (van het Engelse woord Key) waarmee hij de boodschap *M* omzet in een cijfertekst *C*, welk bericht door *B* na ontvangst weer ontcijferd kan worden onder de aanname dat *B* ook beschikt over geheime sleutel *K*. Een en ander is weergegeven in figuur 1.1. *EK* geeft aan dat de boodschap vercijferd wordt met behulp van sleutel *K* (de letter *E* correspondeert met Encryptie (= vercijfering)); *DK* representeert de ontcijferoperatie (*D* van Decryptie (= ontcijfering). In het navolgende zullen we de volgende notaties hanteren:

$C = EK(M)$
(lees: klare tekst *M* wordt met sleutel *K* vercijferd tot cijfertekst *C*)

$M = DK(C)$
(lees: cijfertekst *C* wordt met sleutel *K* ontcijferd tot klare tekst *M*).

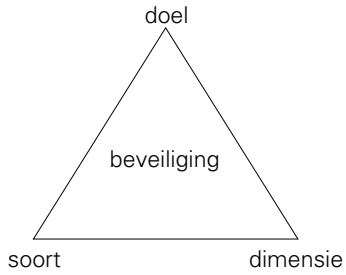
Figuur 1.2 geeft een eenvoudig voorbeeld van wat er aan zend- en ontvangzijde kan gebeuren. Het wordt aan de lezer overgelaten de gebruikte sleutel te achterhalen. Voor degene die gebruik maakt van tekstverwerkers zal dit niet al te moeilijk zijn.



Figuur 1.2. Voorbeeld van een vercijfering en ontcijfering.

1.2. Beveiligingsaspecten

Alvorens verder in te gaan op de methoden van de cryptografie zelf, is het hier nuttig enige aandacht te besteden aan de plaats en het gebruik van cryptografie binnen het totale beveiligingsconcept. Ten aanzien van beveiliging spelen drie aspecten een rol, welke zijn weergegeven in figuur 1.3.



Figuur 1.3. Beveiligingsaspecten.

De eerste vraag die men zich in de praktijk dient te stellen is welke het doel is van de beveiliging. Deze vraagstelling is onlosmakelijk verbonden met een adekwate dreigingsanalyse, die een nauwgezet antwoord moet kunnen geven op de vragen wat men wil beveiligen en waartegen men zich wil beveiligen.
Hierna komt de vraag aan de orde welke soorten middelen voor de beveiliging daartoe gehanteerd moeten worden. Hier gaat het dus om de vragen: hoe? waarmee?
Een derde aspect welke bij het creëren van beveiligingsmaatregelen een rol speelt is wat in de figuur aangeduid wordt met de term dimensie. Daarmee wordt bedoeld of beveiligingsmaatregelen preventief gericht moeten zijn dan wel corrigerend. We komen hier later nog op terug.

Het interessante van figuur 1.3 is dat de driedeling zich ook op lagere niveaus laat doorzetten. Met betrekking tot het doel van beveiliging kunnen er een groot aantal zaken zijn, waartegen men zich wil beveiligen. Om een aantal voorbeelden te geven van waartegen men beveiligingsmaatregelen zou willen nemen:
a. uitlezen en afluisteren van data
b. manipuleren en modificeren van data
c. ongeoorloofd gebruik van (computer-)netwerk
d. aantasting van databestanden
e. verstoren van datatransmissie
f. verstoren van werking van apparatuur of systemen.

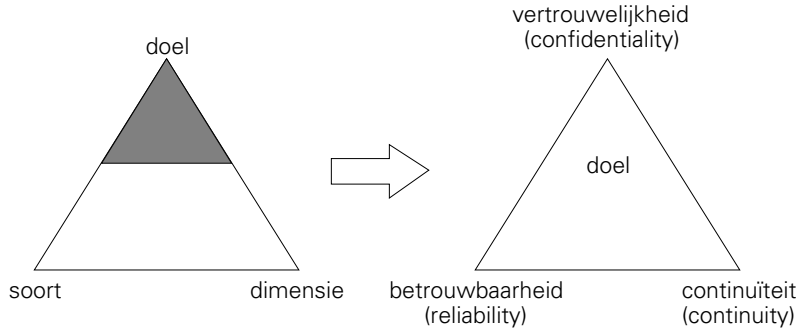
Bij a) gaat het primair om *geheimhouding*, *vertrouwelijkheid* (*confidentiality*). Van oudsher speelt geheimhouding een belangrijke rol bij diplomatieke en militaire aangelegenheden. Vaak is er daarbij, zoals we ook hebben gezien in de vorige paragraaf, sprake van opslag van informatie of overdracht van informatie van de ene

plaats naar de andere; informatie welke men verborgen zou willen houden voor de vijand of tegenpartij. Een ander voorbeeld waar men vercijfering toepast om geheimhouding te waarborgen is bij de communicatie tussen surveillerende politiepatrouilles en de centrale meldkamer. De gevoerde gesprekken worden omgezet in een vorm, die het buitenstaanders moeilijk maakt de relevante informatie eruit te kunnen extraheren. Het kan ook voorkomen dat het feit dát er een bericht verzonden wordt op zich al vertrouwelijk is. In dat geval moeten er regelmatig dummy berichten verzonden worden om de echte berichten te camoufleren.

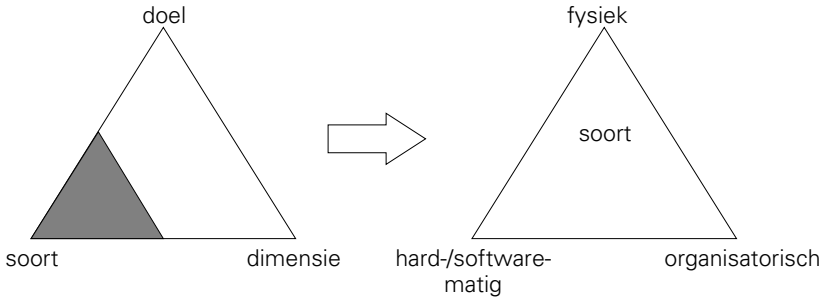
Nauw samenhangend met geheimhouding is het *sleutelbeheer* (*key management*). Het gaat hierbij om het genereren, distribueren en het opslaan van sleutels. Het is duidelijk dat hoe sterk cryptografische algoritmen ook mogen zijn, als er gewerkt wordt met geheime sleutels dan valt of staat de effectiviteit van het algoritme met de mate waarin de sleutel geheim gehouden kan worden. Een indringer die de sleutel weet te bemachtigen kan in principe de vercijferde berichten ontcijferen. Sleutelbeheer is dan ook een essentieel element in het gehele beveiligingsplan.

Bij b) t/m d) gaat het om *betrouwbaarheid* (*reliability*). Bij het elektronisch betaalverkeer zal de bank er zeker van willen zijn dat er niet met de data betreffende een financiële transactie geknoeid is, waardoor bijvoorbeeld ten onrechte hogere geldbedragen geïncasseerd kunnen worden. Men duidt dit ook wel aan met de term *integriteit*: het vaststellen van de ongeschondenheid van data. Ook zal men computernetwerken willen beveiligen tegen binnendringers en daartoe niet-geautoriseerde gebruikers. Als men een fax-bericht ontvangt van een persoon *A* dan zal men de zekerheid willen hebben dat het fax-bericht inderdaad van *A* afkomstig is en de persoon die zich voor *A* uitgeeft inderdaad *A* is. Feitelijk zijn dit vormen van *authenticatie*: het vaststellen van de identiteit van een zich als zodanig uitgevende persoon en het vaststellen van de herkomst van gegevens.

Boven gegeven voorbeelden zijn alle voorbeelden van beveiliging waarbij de betrouwbaarheid op de voorgrond staat.



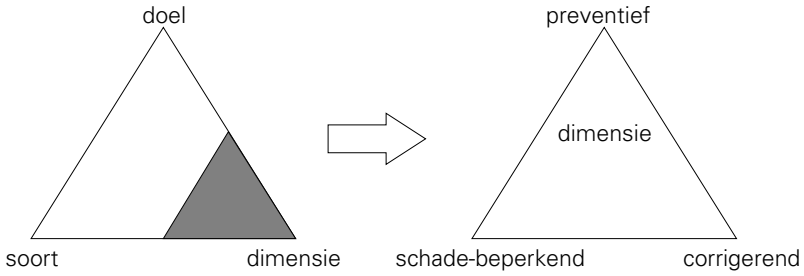
Figuur 1.4. Doelen van beveiliging.



Figuur 1.5. Soorten van beveiliging.

De punten e) en f) geven een ander doel van beveiliging weer, welke zich laat samenvatten met de term *continuïteit*. Dat wil zeggen dat men zich wil beveiligen tegen moedwillig aan te brengen verstoringen in de datacommunicatie en data-opslag.
Ten aanzien van het doel van de beveiliging zijn er dus drie groepen (vergelijk figuur 1.4).
Hetzelfde geldt ook ten aanzien van het soort beveiliging dat toegepast wordt (vergelijk figuur 1.5).
De termen spreken voor zich. Bij *fysieke beveiliging* gaat het om het treffen van maatregelen om het fysiek binnen dringen in systemen, waarin bijvoorbeeld geheime sleutels opgeslagen liggen, te bemoeilijken. Dit kan door het aanbrengen van beschermingen van metaal, toepassen van bepaalde kunststoffen, aanbrengen van temperatuurs- en trillingssensoren etc.
De *hardware- en softwarematige beveiliging* is hetgene waar het in dit boek omgaat; de cryptografische algoritmen en methoden.
Hoe goed men ook fysieke beveiliging en hardware/softwarematige beveiliging kan waarborgen, zonder organisatorische maatregelen hebben ze weinig zin. *Organisatorische beveiliging* houdt in dat er randvoorwaarden gecreëerd worden waardoor inderdaad de genomen fysieke en hardware/ software-matige beveiligingsmaatregelen effectief kunnen zijn. Als de genomen beveiligingsmaatregelen in de praktijk complex en ingewikkeld zijn, dan loopt men het risico dat de gebruikers niet altijd de gewenste zorgvuldigheid in acht nemen. Bedacht dient te worden, dat hoe ver er ook geautomatiseerd wordt, ergens altijd de mens in de keten zit.

Het laatste aspect wat hier beschouwd wordt betreft de dimensie van beveiliging. Ook hier is weer sprake van een driedeling (vergelijk figuur 1.6).



Figuur 1.6. Dimensies van beveiliging.

In eerste instantie zal men bij het toepassen van cryptografie vooral *preventief* te werk willen gaan. Dat wil zeggen dat men de kans dat er iets gebeurt zal willen minimaliseren. Dit kan men bereiken door het toepassen van sterke cryptografische algoritmen en protocollen en het treffen van adekwate fysieke en organisatorische maatregelen. Echter *absolute beveiliging* is per definitie onmogelijk. De kans dat er iets gebeurt kan weliswaar geminimaliseerd worden, maar zal in de praktijk nooit gelijk aan nul zijn. Een ander aspect dat men dan ook met betrekking tot de dimensie van beveiliging kan onderscheiden is het *schade-beperkende* aspect van beveiliging. Dat wil zeggen, laat de kans dat er iets gebeurt niet gelijk aan nul zijn, men dient er in ieder geval voor te zorgen dat als er iets gebeurt de schade zo beperkt mogelijk blijft. Dit betekent dat als iemand in bijvoorbeeld een computerbestand weet door te dringen dat dit slechts in een klein deel van het bestand is. Of als een indringer over een geheime sleutel beschikt, hij slechts een deel van de boodschappen kan ontcijferen, maar nooit alle boodschappen etcetera.
Het laatste aspect is het *corrigerende*. Dit houdt in dat als er iets misgaat dit spoedig te herstellen moet zijn. Als bijvoorbeeld een niet-geauthoriseerde persoon over de geheime sleutel is komen te beschikken, dan moeten er eenvoudig en snel maatregelen genomen kunnen worden zodanig dat deze sleutel onbruikbaar is. Het houdt ook in dat als bijvoorbeeld vitale computerbestanden aangetast zijn deze gereconstrueerd moeten kunnen worden.

Het zal duidelijk zijn dat er in de praktijk ten aanzien van alle bovengenoemde beveiligingsaspecten een trade-off gemaakt moet worden.

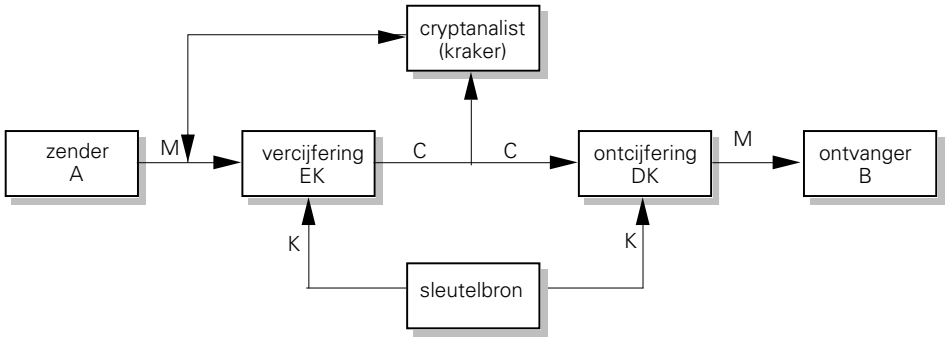
Een facet dat nog niet aan de orde is gekomen is het economische aspect van de toepassing van beveiligingsmaatregelen. Feitelijk gaat het hier om de relatie tussen gewenst beveiligingsniveau, de waarde van hetgeen beveiligd wordt of waartegen beveiligd wordt en de investering die er gedaan moet worden om de gewenste beveiligingsmaatregelen te nemen dan wel die een indringer nog geacht wordt bereid te zijn te doen teneinde de gewenste informatie te verkrijgen.

Hierboven kwamen hier en daar al een aantal toepassingen van cryptografie ter sprake. De toepassingen kunnen ingedeeld worden naar twee groepen, te weten toepassingen met betrekking tot opslag en toepassingen te maken hebbende met transport van informatie.
Bij opslag moet vooral gedacht worden aan opslag in computersystemen; op schijf dan wel op magneetbanden etc. Vaak is hier de methode zelf volgens welke bijvoorbeeld gegevens, software etc. opgeslagen worden wel bekend en openbaar, maar de sleutel niet. Omdat deze gegevens vaak voor langere duur worden opgeslagen, is een cryptanalytische aanval aantrekkelijk. De cryptanalist heeft immers ruim de tijd de sleutel te vinden. Een relatief hoog beveiligingsniveau zou dan gewenst kunnen zijn.
Bij datacommunicatie (tv, satellietverbindingen) is de vercijferde boodschap, in tegenstelling tot wat bij opslag het geval is, slechts een zeer korte tijd voor de cryptanalist beschikbaar en wel op het moment van uitzenden. Er zal bovendien gemakkelijker gewisseld worden van sleutel dan in geval van opslag. De cryptanalist kan uiteraard de verzonden boodschap op een recorder of iets dergelijks opnemen, maar het ontcijferen van de boodschap is nog geen garantie dat daarmee ook andere vercijferde boodschappen ontcijferd kunnen worden; juist omdat er wellicht frequente sleutelwisseling plaatsvindt.
Daar komt nog bij dat bij datacommunicatie dikwijls sprake is van boodschappen, welke slechts gedurende een beperkte tijdsduur waarde hebben; bijvoorbeeld omdat na verloop van tijd de inhoud ervan verouderd is (denk aan nieuws, weersinformatie etc.).
In dergelijke omstandigheden waarbij er sprake is van een slechts momentane waarde van de beveiligde informatie, kan in het algemeen volstaan worden met een beperkter beveiligingsniveau en daardoor geringere investeringen.
Het kostenaspect speel ook nog op een andere manier een rol. Beschouw kabeltelevisie. Het is duidelijk dat de exploitant gebaat is bij een optimale beveiliging. Immers het bedrijf is er bij gebaat zoveel mogelijk illegaal kijken te voorkomen. Daar staat tegenover dat de kosten van het systeem bij de consument, dat er voor dient te zorgen dat het vercijferde signaal ontcijferd wordt, niet te hoog mogen zijn. Dit geldt voor de exploitant, maar ook vanuit het standpunt van de consument bezien. Immers de consumenten, waarvan het merendeel te goeder trouw geacht mag worden, zijn slechts in beperkte mate bereid een bijdrage te leveren aan beveiliging, waar zijzelf niet om gevraagd hebben. Verder hoeft het beveiligingsniveau slechts zodanig te zijn dat een potentiële zwartkijker om de programma's te kunnen zien een grotere investering moet doen dan het bedrag waarvoor hij op reguliere wijze tot het kabelnet toegelaten kan worden.

1.3. Cryptanalytische aanvallen

We beschouwen hier de situatie van een cryptografisch algoritme waarbij door betrokken partijen gebruik wordt gemaakt van een geheime sleutel. Vergelijk figuur 1.1. Er is sprake van een cryptanalytische aanval als de indringer anders dan alleen door proberen de klare tekst of de sleutel tracht te vinden. Het laatste, het vinden van de geheime sleutel, is vaak aantrekkelijker dan het incidenteel vinden van een klare tekst. Voordeel van het hebben van de geheime sleutel is dat dan mogelijkerwijs ook andere cijferteksten ontcijferd kunnen worden. Met betrekking tot het zoeken naar de sleutel is het natuurlijk mogelijk dat men alle mogelijke sleutels toepast op de cijfertekst totdat men de juiste gevonden heeft. Men spreekt dan van een zogenaamd *uitputtend sleutelonderzoek* (*exhaustive key search*). Toch is dit geen cryptanalytische aanval in de ware zin van het woord, omdat er bij een cryptanalytische aanval sprake moet zijn van "intelligenter" gedrag van de kant van de cryptanalist dan alleen maar proberen.
Met betrekking tot echte cryptanalytische aanvallen op cryptosystemen kunnen drie typen van aanvallen onderscheiden worden, samenhangend met de mate waarin de cryptanalist over informatie beschikt. Vergelijk ook figuur 1.7. Deze drie soorten van aanval zijn:

a. aanval op basis van alleen een cijfertekst: *alleen-cijfertekst-aanval* (*cipher-text-only-attack*)
b. aanval op basis van een gegeven klare tekst en de corresponderende cijfertekst: *gekende-klare-tekst-aanval* (*known-plaintext-attack*)
c. aanval op basis van een gekozen klare tekst en bijbehorende cijfertekst: *gekozen-klare-tekst-aanval* (*chosen-plaintext-attack*).



Figuur 1.7. Cryptanalytische aanvallen.

In geval van een aanval op basis van alleen cijfertekst, heeft de cryptanalist alleen de beschikking over de cijfertekst (het vercijferde signaal). Op basis hiervan moet hij, door middel van een analyse van de in de cijfertekst aanwezige structuur en eventuele statistiek, trachten de onderliggende boodschap (klare tekst) te ontcijferen of wat nog belangrijker is, trachten de sleutel te vinden. In geval van vercijferde spraak, afluisteren