YUNIBESITI YA BOKONE-BOPHIRIMA
NORTH-WEST UNIVERSITY
NOORDWES-UNIVERSITEIT

**WETENSKAPLIKE BYDRAES**
**REEKS H: INOUGURELE REDE NR. 205**

# DIGITALE INFORMASIEOORDRAG IN VYANDIGE OMGEWINGS

**Prof ASJ Helberg**

**Inougurele rede gehou op 30 Augustus 2002**

Navrae in verband met *Wetenskaplike Bydraes* moet gerig word aan:

Die Registrateur
Noordwes-Universiteit
2520 POTCHEFSTROOM



**ISBN** 1-86822-471-6

## Digitale Informasieoordrag in Vyandige Omgewings

**ASJ Helberg**

**Opsomming**
Hierdie rede word aangebied aan die personeel en nagraadse studente van die Potchefstroomse Universiteit vir CHO asook aan genooide gaste uit die akademie. Die doel van die rede is om beginsels van en om my belangstellingsveld aan te bied, wat in hierdie geval breedliks die oordrag van digitale informasie in verskeie, dalk vyandige, omgewings behels. Die rede word gelewer voor 'n breër gehoor met verskeie agtergronde, tog sal ek poog om die beginsels so oor te dra dat beide die leek en die cognici (kenner) iets interessants sal saamneem.

### 1. Agtergrond

As agtergrond is dit belangrik om die milieu te skets waarin informasie en die oordrag daarvan vandag plaasvind.

Daar word baie gepraat van verskillende era's waarin die breër gemeenskap hulle bevind, en die keuse van die heersende era word baie gemaak uit die oog van die aanskouer. Uit 'n tegnologiese standpunt is ons bekend met verskeie era's, bv die ruimte era, rekenaar era, internet era, en ook die informasie era. Die informasie era word gekenmerk deur die vrye beskikbaarheid van rekenaarstelsels en 'n kommunikasieinfrastruktuur tussen hulle. Waar die besit van 'n sekere tegnologie 'n instansie in die verlede 'n voorsprong gegee het teen sy teenstanders, het die situasie nou so verander dat die voorsprong nou verkry word deur die verwerking van inligting vir besluitsteunstelsels. Dus, die voordeel lê nou by die persoon wat beter weet wat aan die gebeur is as sy teenstander.

Hierdie gesogte inligting het 'n oorsprong en moet van hierdie oorsprong versamel word en versend word na die punte waar die inligting oral van belang is. Hierdie kommunikasie vind plaas op verskeie maniere en loop die risiko om in die proses beskadig of onderskep te word.

Dit is egter ook so dat die informasie era 'n verskynsel is waarby ontwikkelende lande al hoe vinniger agter raak. Die koste van infrastruktuur neem eksponensieel toe en die kennis en vermoë om die infrastruktuur te ondersteun dra ook by tot hierdie koste. Daarbenewens is daar 'n opvoedingsdrempel wat oorkom moet word voordat hierdie infrastruktuur benut kan word. Suid Afrika het die probleem van die digitale kloof erken en daar is verskeie inisiatiewe om die probleem aan te spreek. Die 2002 SATNAC konferensie het as hooftema "Bridging the Digital Divide" en die Nasionale Navorsing Stigting (NRF) ondersteun tans as 'n navorsingsfokusarea die ontwikkeling en toepassing van Informasie en Kommunikasie Tegnologiee in Suid Afrika.

Die ontplooiing van eerstewêreld tegnologieë in 'n derdewereld omgewing is egter nie voorspelbaar nie. Die sosiale struktuur speel 'n bepalende rol in die aanvaarding al dan nie van 'n gevorderde tegnologie. As voorbeeld die ingebruikneming van die GSM selfoon tegnologie wat selfs meer gevorderd is as wat in Amerika in gebruik was. (die VSA het intussen begin oorskakel na GSM). Aanvanklik is veronderstel dat die tegnologie meestal gebruik sal word deur tegnologies geletterde groepe en dat hierdie groepe hulle meestal sal verbind tot korttermyn kontrakte vir die GSM diens. Tot verbasing het die mark uitermatig gegroei en veral byval gevind by persone wat nie 'n vaste heenkome het nie. Hierdie tendens is veral versterk deur die beskikbaarheid van voorafbetaalde GSM dienste.

### 1.1 Definisie van Terme

Deesdae word alle informasie "digitaal" voorgestel. Maar wat word bedoel met die terme digitale informasie oordrag? Digitale inligting staan ook bekend as versyferde inligting. Enige gemete hoeveelheid kan as 'n syfer voorgestel word. Verder, as ons in rekenaarterme praat, word bedoel dat hierdie waardes voorgestel word deur die binêre getalle 0 en 1. In hierdie rede word enige versyferde waarde meestal aangedui as 'n binêre syfer, hoewel die waarde in enige ander grondtal voorgestel kan word.

'n Gepaste voorbeeld is die versyfering van 'n spanning. Die spanningswaarde word op gegewe tydstippe op 'n gereelde basis gemonster. Die spanningswaarde word dan as 'n syfer voorgestel. Hierdie monsterwaardes en tydstippe kan dan gebruik word om die sein te herkonstrueer.
Beginsel: Die sein moet gemonster word teen ten minste twee keer die hoogste frekwensie komponent teenwoordig in die sein. (Nyquist beginsel)

Die term informasie word gebruik in teenstelling met die term data om die verskil aan te toon. Met data word enige brokkie kennis of feit bedoel. Die waarde van enige twee feite/data verskil dan na gelang van die gebruiker. Die informasie inhoud van 'n boodskap is gekoppel aan die waarskynlikheid van voorkoms van die boodskap/boodskapsimbole. 'n Voorbeeld is die voorkoms van die letters q en u in 'n boodskap. Indien die letter q voorkom in 'n engelse boodskap, dan dra die volgende letter u geen inligting nie omdat u altyd op 'n q volg in engels. Die simbool dra dus geen inligting aan die ontvanger oor nie.

Beginsel: Die hoeveelheid informasie in 'n boodskap is omgekeerd eweredig aan die waarskynlikheid van die voorkoms van die boodskap. Dus, $I_j = log_2\ (1/P_j)$ bisse, waar $Pj$ die waarkynlikheid van die voorkoms van boodskap $j$ is. Die eenheid, bisse, word bepaal deur die grondtal van die log-funksie.

Informasie oordrag is dan die "vervoer" oordrag van 'n boodskap met een of ander infornasie inhoud van 'n bron na 'n bestemming. Hierdie oordrag vind plaas oor een of ander kanaal en moet op so 'n manier oorgedra word dat die ontvanger van die boodskap dit nie kan verwar met 'n ander geldige boodskap nie. Dit staan bekend as die eenduidigheidsbeginsel in kommunikasie. Die gebrek aan eenduidigheid is veral opmerklik by tale en verbale en skriftelike kommunikasie tussen mense. In digitale telekommunikasie word alle stelsels so ontwerp dat aan die eenduidigheidsbeginsel voldoen word.

**2. Digitale kommunikasie**

Digitale kommunikasie vind plaas in verskeie omgewings waarvan elk 'n bepaalde impak het op die oordrag.

Natuurlike faktore stel die faktore voor wat uit die natuurlike omgewing die kommunikasie beinvloed.
Derde party inmenging daarenteen is wanneer mense die kommunikasie tussen twee partye wederregtelik benadeel.

Wanneer kommunikasie aan die hand van netwerke plaasvind is daar 'n unieke stel probleme wat voorkom. Op 'n makroskaal kan die beperkinge van tegnologie ook beperk wat oorgedra kan word net soos wat die ontwikkeling van gepaste infrastruktuur bepaal word deur sosio ekonomiese faktore.

Hierdie rede konsentreer op die ingenieursbeginsels van die eerste twee gevalle. Om hierdie beginsels te verduidelik is dit nodig om eers 'n model te skep van 'n kommunikasiekanaal.

Die sender stuur sy boodskap aan die ontvanger oor die kommunikasiekanaal. In die geval van digitale kommunikasie word die sein eers versyfer by die sender en dan soortgelyk by die ontvanger word die digitale waardes weer omgeskakel na 'n sein. In sekere stelsels word oortollige inligting uit die boodskap uitgehaal om die oordragtempo te verhoog deur gebruik te maak van kompressietegnieke. Die boodskap word dan oor die fisiese kanaal gestuur. Wanneer die boodskap in die kanaal is is dit geheel en al buite beheer van beide die sender en die ontvanger. Dit is dan juis tydens hierdie fase wat sekere "vyandige" aspekte die boodskap kan beinvloed en die oordrag kan benadeel.

**2.1 Natuurlike faktore**

Natuurlike faktore wat die transmissie nadelig beinvloed volg verskeie meganismes en het verskillende gevolge vir die boodskap se inhoud. Indien ons die boodskap beskou as 'n lang ry nulle en ene wat deur die kanaal beweeg dan kan die gelyste faktore op verskeie maniere manifesteer in die rye binere sysfers:

So kan 'n swak sein lei tot foute soos wanvoorstelling van ene as nulle,'n verlore sein lei tot verlies van ene en nulle en 'n inmengende sein kan lei tot gesamentlike groeperings van foute (sarsies van foute).
Die fisiese aspekte werk saam, en alle meganismes kan voorgestel word as of die *verandering*, of die verlies van *waarde* of die verlies van *waarde en posisie* van nulle en ene. Verder kan die voorkoms van foute statisties gekoppel of onafhanklik wees.

Die invloed van die natuurlike faktore op die ry nulle en ene wat die boodskap vertweenwoordig kan voorgestel word met kanaalmodelle wat die gedrag van die voorkoms van foute simuleer. Dus is dit nie nodig om 'n fisiese kanaal ten alle tye te gebruik nie. Die proses van kanaalmodelering is 'n dissipline van sy eie in telekommunikasie.

Kanale kan geklassifiseer word as geheuelose kanale en kanale met geheue. 'n Voorbeeld van die eerste tipe kanaalmodel is die bekende binêr simmetriese kanaal. Hierdie model het geen geheue nie en modeleer 'n (teoretiese) kanaal waar die voorkoms van additiewe foute (dus 'n nul i.p.v. 'n een of andersom) plaasvind met een of ander waarskynlikheid *p*. Die waarskynlikheid van die voorkoms van 'n fout het geen afhanklikheid van die voorkoms van 'n vorige fout nie.

Dit is egter so dat meeste praktiese kanale een of ander geheue effek toon. Hierdie effek word gemodeleer deur 'n toestandsdiagram waar die kanaal se "goeie" en "slegte" toestande voorgestel word. Indien die kanaal dan 'n sekere toestand betree, dan is daar 'n waarskynlikheid dat daar in daardie toestand gebly sal word. Gevolglik word meer foute in slegte toestande gegenereer en minder foute in "goeie" toestande. Met hierdie model is dit moontlik om groeperings met hoër foutdigthede (sarsies) te modelleer.

Kanaalmodelle bestaan ook wat die voorkoms van ander tipe foute (soos bv die weglating/invoeging van bisse) modelleer. Dit is 'n aktiewe navorsingsgebied omrede daar soveel verskillende tipes kanale en foute is.

Die vraag wat nou gevra kan word is of dit moontlik is om 'n boodskap foutloos oor te dra al is daar ruis op die kanaal. Claude Shannon, die vader van die informasie teorie, het in 1948 'n stelling gemaak wat bewys het dat dit wel moontlik is om in die teenwoordigheid van ruis 'n sein foutloos oor te dra, onder sekere voorwaardes. Shannon het bewys dat die kapasiteit van 'n kanaal bereken kan word sodat indien die informasie tempo *R* minder as hierdie kanaalkapasiteit, *C*, is, dit moontlik is om die boodskap foutloos oor te dra. Vir die Binêr simmetriese kanaal, wat Gaussiese verspreide ruis voorstel is $C = B \log 2 (1 + S/N)$ waar *B* die bamdwydte van die kanaal in Hz is en *S/N* die sein tot ruis verhouding in watts/watts is.

**2.2 Foutkorreksie**

Met die kennis van die kanaal en die tipe foute wat voorkom en veral met die wete dat dit moontlik is om foutlose kommunikasie te bewerkstellig nieteenstaande die natuurlike vyandige omgewing, is dit nou moontlik om digitale foutkorreksietegnieke op die boodskap/kanaal toe te pas om degradering weens die natuurlike faktore tee te werk.

Die eenvoudigste metode van korreksie is om enige boodskap gedeelte met 'n fout weg te gooi en dan die sender te vra om dit weer te versend. Dit staan bekend as ARQ: Automatiese Hersend Aanvraag (Automatic Retransmission Request)

Die meer intelligente tegniek is om gebruik te maak van VFK: Vorentoe foutkorreksie. VFK werk op die beginsel dat ekstra inligting by die boodskap gevoeg word om die verwagte foute teë te werk. Op die minste is dit die byvoeging van een bis om 'n fout aan te dui sonder dat dit reggemaak word (pariteitsbis) tot die geval waar dele van die boodskap (inligtingswoorde) afgebeeld word op kanaalwoorde. Hierdie kanaalwoorde (foutkorreksiewoorde) word dan spesiaal ontwerp om die verwagte kanaalfoute teen te werk en te korrigeer by die ontvanger. Hierdie spesiale ontwerpte woorde sal nog steeds na die kanaal sekere( verwagte) foute daarin veroorsaak het uniek herkenbaar wees as afkomstig van die oorspronklike versende woord. Die inligtingswoord word dan verkry deur 'n truwaartse afbeelding vanaf die kanaalwoord na die inligtingswoord te maak. Dit is belangrik om te let dat daar in die VFK proses oortollige inligting by die boodskap gevoeg word asook meer kompleksiteit by beide die sender en die ontvanger. 'n Mate van die effektiwiteit van 'n kode is dan die datatempo wat die verhouding van inligtingsimbole tot kanaalsimbole is. Dit kan verder gemeet word deur te bepaal hoe naby *R* aan *C*, die teoretiese bo-perk van die informasietempo is.

Een van die eerste tipe foutkorreksiekodes is die blokkodes. Blokkodes is geheueloos en die uitset word slegs bepaal deur die inset tot die kodeerder. Kodes met geheue kan ook geskep word en volg dan een of ander toestandsdiagram of boom-voorstelling om te onthou wat die vorige waardes was. Konvolusiekodes is voorbeelde van kodes met geheue.

Tabel 1: Voorbeeld van 'n blokkode

| Informasie | Kode |
|---|---|
| 00 | 00100 |
| 01 | 01010 |
| 10 | 11101 |
| 11 | 10110 |

'n Voorbeeld van 'n blokkode word getoon in Tabel 1 om die beginsels van foutkorreksie en deteksie te demonstreer. In hierdie kode word twee informasie bisse afgebeeld op 5 kodebisse, dus is die informasie tempo $R = 2/5$. Dit lyk op die eerste oogopslag sleg omdat twee en 'n halfkeer meer bisse op die kanaalversend word as wat daar inligting is. Hoe langer die kodewoorde hoe meer effektief raak die informasieoordrag tempo, maar hoe groter raak die waarskynlikheid dat die foutkorreksievermoë van die kode oorskry kan word. As mens dit egter met 'n hersend stelsel vergelyk, dan is daar wel 'n wins. 'n ARQ stelsel moet die fout kan optel. Daarvoor moet 'n enkele bis bygevoeg word by elke boodskap. Dus 3 bisse word versend per boodskap. Dus, as daar 'n fout voorkom moet die 3 bisse weer versend word, dus 6 bisse in totaal, waar die VFK geval slegs 5 versend het. Maar die ARQ stelsel versend net nou en dan die boodskap twee keer, dus is die datatempo afhanklik van die aantal foute op die kanaal. Indien die kanaal baie foute het, dan vaar die VFK beter, andersins die ARQ stelsel. Daar is egter die gevalle waar ARQ onprakties is (kanale met hoë vertraging) waar dit beter is om die boodskap met VFK te versend.

Verder is die kode sistematies, dws dat die informasiebisse altyd op dieselfde posisie in die kode voorkom, soos aangedui met die onderstreepte karakters.

Hierdie kode het 'n minimum Hammingafstand van 3 en kan een additiewe fout korrigeer of twee foute onderskei.

Die Hamming afstand is die aantal posisies waarin twee kodewoorde verskil. Dit word eenvoudig bereken vir die binêre geval deur die twee woorde eksklusief-of bymekaar te tel. Die minimum Hammingafstand tussen enige twee woorde van 'n kodeboek bepaal die additiewe foutkorreksie vermoë van die kode. Additiewe foute word so genoem omdat die foutmeganisme in die bisstroom manifesteer asof 'n foutvektor **e** by die geldige boodskap getel is. Hierdie foute vertoon aan die ontvanger asof 'n binere een in 'n nul verander het, of andersom. Die krag van die kode is dan die vloerfunksie van helfte van die minimum Hammingafstand van die kode minus 1. Dus 'n kode met $dmin = 3$ kan $\lfloor(3-1)/2\rfloor = 1$ additiewe fout korrigeer, en 2 foute onderskei.

'n Ander tipe fout wat in die bisstroom kan voorkom is die weglating of byvoeging van bisse. Hierdie tipe foute word veral veroorsaak wanneer die sinkronisasie tussen die sender en die ontvanger verskil en daar dan meer of minder bisse uit die boodskap gelees word as wat daar gestuur is. Hierdie tipes foute is heelwat moeliker om te korrigeer omdat beide die *waarde* en die *posisie* van die korrekte bis verlore gaan. (Vir additiewe foute is dit net nodig om die posisie te bepaal.)

Levenshtein het 'n koderingsmetode voorgestel wat een weglating of byvoeging kan korrigeer. Hierdie werk is later uitgebrei en is daar verskeie maniere om kodes te konstrueer om 1 of meer byvoegings of weglatings van simbole te korrigeer. Die voorbeeld in tabel 2 toon 'n *s=1* kode, dws 'n kode wat 1 weglating of byvoeging kan korrigeer. Die kode het *dmin = 2* en kan dus 1 additiewe fout onderskei. Hierdie kode is ook sistematies en het 'n informasietempo van 0.5 bisse per sekonde.

**Tabel 2: Voorbeeld van 'n s=1 kode**

| Informasie | Kode |
|---|---|
| 00 | 0000 |
| 01 | 0110 |
| 10 | 1001 |
| 11 | 1111 |

'n Interessante verskynsel by hierdie spesifieke kode is die teenwoordigheid van nulle in die drywingspektraaldigtheid by beide gelykstroom en die Nyquist frekwensie. Hierdie verskynsel maak die versterking van die sein eenvoudiger en kan die spektrumbenutting verdubbel.

Net soos by additiewe kodes is daar ook 'n metriek wat bereken kan word om te bepaal wat die s-foutkorreksievermoe van 'n kodes is. Hierdie metriek word die Levenshtein afstand genoem en is die aantal posisies wat verander, weggeneem of bygevoeg moet word om een kodewoord in 'n ander geldige kodewoord te verander. In die voorbeeld kode is $d_l$ =2 en is dit dus 'n $s$=1 kode wat een weglating of een byvoeging kan korrigeer.

**3. Informasiesekerheid**

Tot dusver is beginsels bespreek wat van toepassing is op die oordrag van informasie in die teenwoordigheid van ruis (wat 'n natuurlike oorsprong het.) Ongelukkig is dit ook so dat natuurlike faktore nie die enigste faktore is wat kan verhinder dat 'n boodskap ongeskonde tussen sender en ontvanger oorgedra word nie. Die heel gevaarlikste bedreiging is 'n ander persoon. Hier verlaat ons die gebied van foutkorreksiekodering en betree die gebied van informasiesekerheid.

Informasiesekerheid is 'n veld van studie wat van die vroegste tye af beoefen is maar veral onlangs met die beskikbaarheid van telekommunikasienetwerke gesofistikeerd en tegnologies gevorderd geraak het.

Informasiesekerheid het ten doel die beskerming van drie hoofaspekte van informasieboodskap, naamlik die privaatheid en integriteit van die boodskap en die onweerspreekbare identifikasie van die sender en ontvanger van die boodskap.

Privaatheid het te doen met die versekering dat geen ander persoon die versende boodskap kon lees en verstaan nie.

Integriteit behels die versekering dat al kon geen ander persoon die boodskap lees nie, daar nogtans ook geen veranderinge aan die boodskap aangebring is nie.

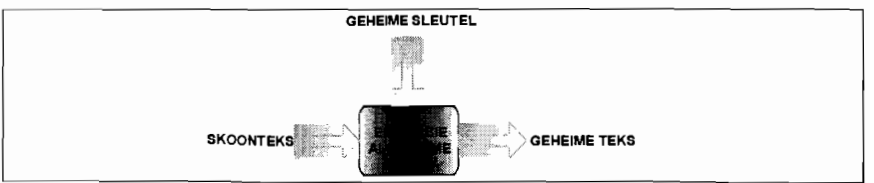
Identifikasie: Laastens is dit veral belangrik om te weet wie die sender/ontvanger van die boodskap is en dat daardie persoon aanspreeklik is vir die inhoud van die boodskap. Hierdie laaste vereiste van informasiesekerheid is tot onlangs die moeilikste om te bewerkstellig.

'n Ander aspek wat al hoe meer 'n belangrike rol speel by informasiesekerheid is of die "transaksie" of die oordrag van die boodskap, ouditeerbaar is. Ouditeerbaarheid het in hierdie geval nie te make met die boodskap self nie maar met die omstandighede waarin die boodskap versend word. Die hoofdoel is om inligting te versamel vir die kere wat daar wel fout gaan en die skuldige party aan te keer.

'n Derdeparty kan verskeie dinge doen aan die kommunikasie tussen twee partye. 'n Derdeparty kan gewoon die boodskap afluister om so die privaatheid van die boodskap te skend. Meer aktiewe vorms van inmenging is om die boodskap te verander, 'n vervalste boodskap te stuur deur een van die wettige partye na te boots, of om selfs net die kanaal tussen die wettige partye te versteur sodat die boodskap vertraag word of selfs verlore gaan. Die meganismes waarmee 'n derdeparty kan inmeng is menigvuldig en die stryd is permanent om metodes te kry om die nuwe vorms van inmenging te bestry. Dink gerus maar hoe gereeld 'n viruspakket opdateer moet word. (Laasgenoemde is 'n voorbeeld van inmenging met die doel om verlies of vertraging te veroorsaak en waar die rekenaarstoormedia beskou kan word as die kommunikasiekanaal tussen dieselfde persoon in tyd verplaas)

**3.1 Kriptografie**

Kriptografie is een van die metodes wat gebruik word om informasiesekerheid te bewerkstellig. .....




**Figuur 1: Skematiese diagram van enkripsieproses**

Figuur 1 toon 'n vereenvoudigde voorstelling van die enkripsieproses. 'n Skoonteks boodskap word tesame met 'n geheime sleutel as inset tot 'n kriptografiese algoritme gebruik om 'n geheimeteks

boodskap te skep. Hierdie geheimeteks boodskap word dan versend en die ontvanger voer die omgekeerde proses uit om die skoonteks te herwin.

Twee belangrike beginsels geld vir 'n kriptografiese enkoderings stelsel:

Beginsel: Die sekerheid van 'n kriptografiese stelsel mag nie staat maak op die geheimhouding van die algoritme nie, maar moet slegs berus op die geheimhouding van die sleutel. Hierdie beginsel verseker dat die stelsel versprei kan word sonder om informasiesekerheid prys te gee. Dit is veral belangrik met internet besigheid waar die transaksie vanaf enige plek en deur enige persoon sekuur afgehandel kan word.

Beginsel: Die doel van kriptografie is om die informasie inhoud in die boodskap so te versprei dat die loerbroer geen afleiding kan maak oor die boodskap se inhoud of die sleutel waarmee dit ge-enkodeer is nie. Hierdie beginsel probeer sorg dat statistiese aanvalle nie teen die boodskap gebruik kan word nie.

In enkelsleutelstelsels word dieselfde sleutel deur beide kommunikasiepartye gebruik om die boodskap te enkodeer en te dekodeer. Hierdie "geheime" sleutel staan bekend as 'n simmetriese sleutel en moet vooraf afgespreek word tussen die sender en ontvanger. Die probleem is egter dat om enigsens sekuur te kommunikeer moet die twee partye bymekaar uitkom en die sleutel afspreek of 'n derde party vertrou om die sleutel oor te dra. Hierdie probleem is eers effektief opgelos in 1975 met asimmetriese sleutelstelsels.

In asimmetriese stelsels word twee sleutels gebruik, die sogenaamde Privaat en Publieke sleutels. Gebruik enige een vir enkripsie, en dan die ander een vir dekripsie. Dieselfde sleutel kan nie gebruik word vir enkripsie en dekripsie nie.

Die sleutelruilingsprobleem word opgelos deurdat elke persoon een van sy twee sleutels publiseer in 'n gids, soortgelyk aan 'n telefoongids. Indien "adam" met "eva" wil kommunikeer soek hy eenvoudig haar publieke sleutel op en gebruik dit om sy boodskap aan haar te enkripteer met die versekering dat net sy die ooreenstemmende privaatsleutel het om die boodskap te dekripteer. Soortgelyk kan "Eva" dan antwoord deur "Adam" se publieke sleutel te gebruik. Asimmetriese sleutelstelsels word egter in die algemeen nie so gebruik vir lang boodskappe nie omdat dit berekeningintensief is en dus stadiger is as simmetriese sleutel stelsels. Dit is egter die ideale manier om so die geheime sleutel van 'n enkelsleutelstelsel oor te dra.

Met die omgekeerde proses is dit ook moontlik om die sender of ontvanger te outentiseer, om maw met redelike vetroue te besluit dat die kommunikasie wel van die korrekte party af kom, al het hulle mekaar nog nie ontmoet nie. Daar word as volg te werk gegaan. Adam enkripteer sy besonderhede met sy privaatsleutel. Daarna enkripteer hy hierdie geheime boodskap (dalk met kommentaar by) met die ontvanger "eva" se publieke sleutel. By ontvangs kan slegs Eva met haar privaatsleutel die ge-enkripteerde kommentaar lees, en daarna kan sy Adam se publieke sleutel gebruik om sy besonderhede te dekripteer en te verifieer teenoor die inligting van Adam wat in die sleutelgids staan.

Die een party is redelik seker dat die boodskap wel van die ander party kom, mits daar vertroue is in die sleutelgids publikasie maatskappy. Hiervoor is die Publieke Sleutel Infrastruktuur ontwikkel. 'n Derde party wat vertrouenswaardig is word gebruik om die identifikasie van 'n persoon en die uitreiking en publisering van sy publieke en privaatsleutels te doen. Dit is dieselfde konsep as die paspoort of id-dokument waar die regeringsdepartement die vertrouenswaardige derdeparty is.

### 3.2 Vertroue

Kern tot die werking van 'n praktiese kriptografiese stelsel is die beginsel van vertroue. Ondanks die sekuriteit wat deur die wiskundige kriptografiese algoritmes verskaf word, is dit tog so dat baie toepassings van kriptografiese stelsels faal omdat 'n vertrouensverhouding êrens geskend word. Een van die eerste dinge waarmee die sender en ontvanger mee vertrou word is die geheimhouding van die sleutels, synde dit die enkel geheime sleutel is of die privaatsleutel in 'n asimmetriese sleutelstelsel. Indien hierdie sleutel bekend sou word is daar geen privaatkommunikasie moontlik nie. 'n Tweede aspek wat uitgeklaar moet word is die aanspreeklikheid vir inligting wat versend word. Wie is aanpreeklik vir beslissings wat geneem word op (vals) data wat ge-enkodeer is met die sender se privaatsleutel. Suksesvolle stelsels maak gebruik van waarde balanse waar die waarde van die sleutel se geheimhouding hoër is as die waarde van die inligting wat versend word. 'n Voorbeeld is bv om die

geheime sleutel te koppel aan 'n persoon se kredietkaartnommer wat genoegsame motivering behoort te wees om nie die sleutel te laat rondlê nie!

Dit is ook belangrik om te besef dat indien een van die partye 'n derde party vertrou, daar ook 'n vetrouensverhouding bestaan tussen al drie persone, al is dit indirek. Die suksesvolle implementering van internet handel berus op die vertroue van die publieke sleutel infrastruktuur. Hierdie partye is verantwoordelik vir die uitreiking van sleutels aan genoegsaam geïdentifiseerde partye, die bewaring van die meestersleutels en die publisering van sleutelgidse asook terugtrekkinglyste.

Informasie sekerheid is 'n baie aktiewe navorsingsveld wat amper daagliks met nuwe probleme te make het en nuwe toepassings bewerkstellig vir ou kennis. So is daar Steganografie wat die studie van die geheime boodskap is. Baie naby daaraan gekoppel is die nood aan digitale waarmerke om eiendomsreg van digitale materiaal soos musiek en beeld op die internet te beskerm deur 'n waarmerk/watermerk in die digitale lêer in te bou. Nog 'n interessante studie is die gebied van geheimverdeling. Met geheimverdeling word 'n geheim tussen partye so verdeel dat daar 'n sekere kworum benodig word om die geheim te ontsyfer.

Onbeantwoorde probleme is die gebruik van 'n enkeltransmissies met geselekteerde dekripsie, waar verskeie persone op 'n hiërargiese basis met 'n enkel sleutel meer of minder data kan ontsyfer na gelang van behoefte. Verder is daar nog die gebruik van slimkaarte en biometriese sleutels. 'n Biometriese sleutel het die voordeel dat mens dit nie kan verloor nie, maar die nadeel dat as iemand ontdek wat dit is, daar slegs 'n beperkte aantal nuwe sleutels is – 'n mens het net tien vingers!

Buiten die teorie van informasie oordrag en die beginsels wat daarmee gepaard gaan is 'n ingenieur veral gemoeid met die praktiese implementering van hierdie stelsels. In telekommunikasie het hierdie toepassingsgebied so groot gegroei dat dit sy eie teorie ontwikkel het en bekend staan as netwerke. Waar ons tot dusver net 'n enkele kommunikasiekanaal in isolasie beskou het, moet netwerke beskou word as die gedeelde infrastruktuur waarop 'n kommunikasiekanaal tussen enige twee partye bewerkstellig kan word. Let dat dit nie net 'n versameling van enkelkanale is nie.

**4. Strategiese belang**

Telekommunikasiediensverskaffers moet deur effektiewe netwerkbestuur beide hulle aandeelhouers en die streek en landsbehoeftes bevredig. Dit is duidelik dat daar geen sprake kan wees van 'n informasie era "of die sg Information highway" as daar nie telekommunikasiedienste bestaan nie.

Verder word telekommunikasie gesien as een van die kernbestandele tot die ontwikkeling van 'n land. Vergelyk byvoorbeeld die teledigtheid, d.i. die aantal telefone per 100 persone, van die ontwikkelde lande vs die ontwikkelende lande. Amerika het 'n teledigtheid van ongeveer 67% en Europa ongeveer 41%. In Afrika is die teledigtheid ongeveer 1,5% met sekere lande, soos die DRK met 'n teledigtheid van 0,3% (een foon per 300 mense). Volgens BMI-Techknowledge is daar 'n direkte korrelasie tussen die telekommunikasie digtheid en 'n land se BBP.

In Suid Afrika lyk die prentjie beter as in die res van Afrika. Huidiglik is daar meer as 13 miljoen selfoongebruikers in die land wat 'n teledigtheid van net oor die 30% gee. Hiervan is slegs ongeveer 80% aktiewe gebruikers. Dus is die praktiese teledigtheid nader aan 25%. Ongeveer 90% van selfoongebruikers maak van voorafbetaalde dienste gebruik. 'n Interessante newe effek is dat dit moeilik is om 'n markprofiel saam te stel van die gemiddelde selfoon gebruiker in die land. Daarteenoor is die landlyn teledigtheid in die land ongeveer een telefoon per 10 persone,(ongeveer 5 mil lyne vir die ongeveer 43 mil inwoners van Suid Afrika.) Hierdie mark is ongeveer R23 bill groot en is 'n groot werkverskaffer in die land. (Telkom alleen het oor die 40000 werknemers).

Die Suid Afrikaanse telekommunikasie verskaffers is besig om die markte in die res van Afrika te help ontwikkel. MTN het bv meer as 500 000 gebruikers in Uganda. Afrikaleiers is aktief besig om die telekommunikasiebehoeftes van die streek aan te spreek. In 2001 is die Yaounde deklarasie onderteken om die probleem van die digitale kloof tussen stedelike en landelike gebiede aan te spreek. Die Yaounde deklarasie is opgeneem in die NEPAD inisiatief. NEPAD bestaan uit 'n versameling inisiatiewe waarvan een die oorbrugging van die infrastruktuur gaping t.o.v. informasie en kommunikasie tegnologie, energie, vervoer, water en sanitasie behels. In Maart 2002 is die Wereld Telekommunikasie Ontwikkelingskonferensie in Istanbul gehou waar Afrika gepoog het om die volgende te bereik:

- 'n toename in teledigtheid om as ekonomiese katalisator op te tree,
- Loodsing van proefprojekte,
- Meer gevestigde vervaardigers om meer gepaste tegnologiee te ontwikkel om teledigtheid te verhoog,
- Oombliklike toegang tot informasie vir alle afrikabewoners,
- Opleiding en menslike hulpbron ontwikkeling in informasie tegnologie.

Na afloop van die konferensie is 'n deklarasie en aksieplan onderskryf vir 2003 en 2004. Hierdie plan bevat ses programme om so veel as moontlik mense oor die digitale kloof te bring.

**4.1 Opleiding en navorsing**
Dit is juis met die taak van opleiding waarmee 'n universiteit en 'n dosent te doen het. Verder is dit ook so dat 'n universiteit ook getaak is met die skep van nuwe inligting wat deur navorsing moet plaasvind.

Hierin lê daar unieke geleenthede en uitdagings. By die PUK bestaan daar reeds sterk interaksie met die industrie. In telekommunikasie is daar ooreenkomste met Telkom en met Transtel om nagraadse studente op te lei. Entrepreneurskap word ook sterk ondersteun deur die inkubatorprogram waar daar geleentheid geskep word vir studente om 'n idee vanaf konsep tot produk te ontwikkel. Nagraadse ontwikkeling het ten doel dan om kennis in telekommunikasie te ontwikkel deur die grense van bestaande kennis verder te stoot. Daarbenewens is dit ook 'n doel van ingenieurs om praktiese probleme wat huidig bestaan op te los. Laastens is dit ook 'n doel om te sorg dat innovasie en bemarking van kundigheid ontwikkel word.

Die omgewing waarin onderrig plaasvind is een van die navorsingsbemiddelaars. 'n Gepaste klimaat en kultuur moet geskep word waarin dit vir studente moontlik is om bymekaar te leer en ondersteuning te kry. Die omgewing moet die gepaste hulpbronne daarstel, vanaf inligting tot apparaat. 'n Kultuur van innoverende, kritiesdenkende waardetoevoeging moet by elke navorser gekweek word. Die resultate van die navorsing moet dan ge-evalueer word op internasionale vlak deur middel van konferensiebydraes en veral joernaal artikels. In die geval van industrienavorsing word die kwaliteit verseker deur industrieaanvaarding van die voorgestelde oplossing en die toepaslike ouditmeganismes vir elke instansie.

**5. Ten Slotte**
Die tegnologie wat mense gebruik en ontwikkel is 'n uitbeelding van sy wêreldbeeld en visie. Daaruit kan mens bepaal wat 'n sekere kultuur se waardes is. Die volgende aanhalings uit Spreuke openbaar wyshede oor telekommunikasie in 'n tyd toe dit nog net kommunikasie was:

Oor die stuur van boodskappe:
Spr 26:6: As jy 'n dwaas met 'n boodskap stuur, kan jy net so wel nie 'n boodskap stuur nie.
Oor die bewaring van sleutels:
Spr 11:11 & 20:19'n Betroubare mens bewaar 'n geheim, iemand wat loop en skinder lap geheime uit
Oor ingenieurswese en navorsing:
Spr 19:2 Ywer sonder kennis deug nie, oorhaastigheid bring foute
Spr 13:6 Alles wat 'n verstandige mens doen word met kennis gedoen