De rol van de cryptologie en de digitale handtekening inzake de veiligheid van elektronische informatie-uitwisseling

Philippe SCHRAEPEN

promotor :
Prof.dr.ir Frans LEMEIRE

Eindverhandeling voorgedragen tot het bekomen van de graad
Handelsingenieur major accountancy en financiering

universiteit hasselt

Woord vooraf

Deze eindverhandeling wordt voorgedragen voor het beëindigen van mijn studies Handelsingenieur in accountancy en financiering met een verdiepende minor in financiering aan de Universitair Hasselt. Het schrijven van deze eindverhandeling zou echter nooit mogelijk geweest zijn zonder de hulp en steun van anderen. Zonder hun advies zou deze opdracht nooit tot stand zijn gekomen.

Op de eerste plaats zou ik graag een woord van dank richten tot Prof. dr. ir. Frans Lemeire voor zijn tijd, vakkennis en goede begeleiding tijdens het voltooien van deze eindverhandeling. Ik ben hem dankbaar voor zijn richtlijnen waarbij hij steeds ruimte liet voor een eigen inbreng.

Verder dank ik alle personen die hun tijd vrijmaakten voor een interview en dank ik alle bedrijven die zo vriendelijk waren mijn vragenlijst in te vullen. Tenslotte bedank ik mijn ouders voor hun steun gedurende mijn ganse studiejaren.

Samenvatting

Steeds meer van de huidige informatie-uitwisseling en communicatie gebeurt elektronisch. Hoogstwaarschijnlijk zal deze evolutie zich in de toekomst voortzetten. Nagenoeg altijd zorgen nieuwe technologieën voor vooruitgang (meer praktisch, efficiënter, veiliger,…), daarom is het belangrijk dat ze zo snel mogelijk aanvaard worden. Deze aanvaarding zal er echter pas komen wanneer men vertrouwen heeft in de nieuwe technologieën. Dit vertrouwen is op zijn beurt afhankelijk van de veiligheid van de nieuwe systemen. Men wil zeker zijn dat elektronische documenten confidentieel blijven; dat wanneer men ze verstuurt, ze niet gewijzigd kunnen worden; dat men zeker weet wie in de transactie participeert; en dat men ook nadien nog kan aantonen wie participeerde. De bedoeling van dit eindwerk is op zoek te gaan naar enkele mogelijke technieken die deze veiligheid kunnen verschaffen.

Een eerste, belangrijke techniek is cryptografie. Cryptografie zorgt ervoor dat een boodschap omgetoverd wordt tot een geheimschrift zodat enkel de personen in het bezit van de juiste sleutel uit het geheimschrift de correcte boodschap kan terughalen. Deze techniek zorgt dus voor de confidentialiteit. Er zijn verschillende klassen van cryptografie. Een belangrijk onderscheid is het symmetrisch versleutelen enerzijds, en het asymmetrisch versleutelen anderzijds. Bij symmetrische versleuteling gebruikt men zowel voor het versleutelen als het ontsleutelen van de boodschap dezelfde sleutel, terwijl bij asymmetrische versleuteling twee verschillende sleutels worden gebruikt, een publieke (waarmee men versleutelt) en een private (waarmee één iemand kan ontsleutelen). Beide methode hebben hun voor- en nadelen, en hun eigen specifieke toepassingen. Zo maakt onder andere de digitale handtekening gebruik van asymmetrische versleuteling, zij het wel in de omgekeerde richting. In dit eindwerk worden verschillende symmetrische cryptosystemen zoals de klassieke handcijfers, DES, IDEA, RC5, RC6 en AES belicht. Verder behandelen we de wiskundige principes die de basis vormen van de asymmetrische cryptosystemen en worden asymmetrische cryptosystemen zoals de Diffie-Hellman sleuteldistributie, RSA, ElGamal, Schnorr, DSA en ECC besproken.

Nu dat er een techniek gevonden is om de confidentialiteit van boodschappen te waarborgen gaan we verder in het eindwerk op zoek naar een manier om de andere vereisten voor veiligheid, die hierboven zijn aangehaald, tegemoet te komen. Hiervoor komen verschillende technieken in aanmerking, waaronder wachtwoorden, biometrie etc. maar de Wet van 9 juli 2001 stelt dat enkel de geavanceerde digitale (elektronische) handtekening met gekwalificeerd certificaat voldoet en hierdoor gelijke rechtsgeldigheid als een handgeschreven boodschap geniet. Een digitale handtekening zorgt ervoor dat men weet wie in de transactie van de boodschap participeert en dat deze boodschap ongewijzigd is. Verder is de transactie onweerlegbaar waardoor men ze nadien niet meer kan ontkennen.

Het creëren van een digitale handtekening gebeurt door een message digest van de oorspronkelijke boodschap te vercijferen met de eigen private sleutel. Een message digest is een met behulp van de hash-functie 'verkapte' versie (met een vast aantal bits) van de boodschap (van willekeurige grote). Door de kleinere message digest te gebruiken zal de asymmetrische versleuteling sneller verlopen. Na de creatie verstuurt de afzender de digitale handtekening samen met de oorspronkelijke boodschap op. De ontvanger zal ter verificatie dezelfde hash-functie gebruiken om een message digest van de boodschap te creëren. Verder gebruikt de ontvanger de publieke sleutel van de afzender voor het ontsleutelen van de digitale handtekening, wat op zijn beurt een message digest voortbrengt. Wanneer deze twee message digests gelijk zijn kan de ontvanger er zeker van zijn dat het bericht ongewijzigd en afkomstig is van de afzender. In deze eindverhandeling wordt deze techniek in detail besproken. Ook besteden we aandacht aan de codetheorie die extra bits aan de boodschap toevoegt waardoor de boodschap beschermd is tegen transport over een kanaal met een zekere kans op fouten. De codetheorie zorgt ervoor dat deze fouten worden opgespoord en gecorrigeerd.

De digitale handtekening zorgt wel niet voor geheimhouding van de boodschap, hiervoor zal men beroep moeten doen op de cryptografie. Een veilig bericht verzenden kan dus door de boodschap te voorzien van een digitale handtekening, waarna men de boodschap + de digitale handtekening versleutelt met een cryptosysteem. De bestemmeling ontsleutelt het geheel en verifieert het hierna aan de hand van de digitale handtekening.

Een toepassing van elektronische informatie-uitwisseling is het elektronisch versturen van facturen. Elektronische facturatie zit duidelijk in de lift, dit is zeker te merken aan de interviews en online bevraging. Vooral de grote bedrijven stellen dat de implementatie van elektronische facturatie niet kan uitblijven om op lange termijn competitief te blijven. Bij de kleinere bedrijven loopt het nog niet zo'n vaart, hoewel ook zij beseffen dat er heel wat voordelen gepaard gaan met elektronische facturatie. De hoofdreden voor het uitblijven van de implementatie bij kleinere bedrijven is de te kleine vraag vanwege hun partners, maar de meeste bedrijven verwachten in de toekomst wel dat ze elektronische facturatie zullen implementeren. Verder blijkt uit het onderzoek dat de bedrijven die momenteel het systeem gebruiken over het algemeen tevreden zijn. Het is gebruiksvriendelijk en tijdsbesparend. Een echte kostenbesparing biedt het echter voorlopig nog niet omdat de implementatiekost in de backoffice en informatica-infrastructuur voorlopig nog doorweegt ten opzichte van papierbesparing etc. Wel verwachten de bedrijven op lange termijn een kostenbesparing. Wat betreft de veiligheid zijn nagenoeg al de bedrijven het erover eens dat de digitale handtekening en de gebruikte encryptiemethodes, aangeboden door de certificaatautoriteiten, voldoende bescherming bieden. Hoewel de kennis over de beveiligingstechniek zeer beperkt is, heeft men voldoende vertrouwen in de veiligheid ervan.

Inhoudsopgave

1. Probleemstelling en onderzoeksvragen

1.1 Inleiding en probleemschetsing

Het is al een hele tijd aan de gang, maar de laatste jaren kunnen we spreken van een ware revolutie: computer, gsm, bankkaarten, het web, etc. Een vloed van informatie- en communicatietechnologieën geeft ons leven een nieuwe vorm. Voorspeld wordt dat na een twintigtal jaren de digitale en draadloze samenleving een feit zal zijn. De digitale samenleving is geen Science Fiction verhaal meer, maar staat volop in de steigers.

Uiteraard zullen al de innovaties niet ineens gebeuren, kijk naar de kinderziekten van "tax on web", maar over twintig jaar belooft onze samenleving er toch heel anders te zullen uitzien. Zo zal cash geld minder gebruikt worden en wordt e-money de regel. *(De standaard, 2005)*

De digitale revolutie zal ons de komende decennia dwingen om onze hele cultuur opnieuw te definiëren. Is een virtuele gemeenschap een echte gemeenschap of valt onze samenleving uit elkaar? Wat met de privacy in een wereld volgepropt met elektronische apparatuur? Maakt de digitalisering ons niet extra kwetsbaar voor aanslagen van cyberterroristen? Wie heeft waar en wanneer toegang tot welke informatie? *(De standaard, 2005)*

De moeilijkheid bij de mensheid is dat nieuwigheden altijd hebben geleid tot onzekerheid, maar ook tot curiositeit en vooruitgang. Het wegwerken van deze onzekerheid en creëren van vertrouwen zal een belangrijke uitdaging van het digitale tijdperk zijn, zodat tal van nieuwe technologieën de vooruitgang kunnen stimuleren. In deze eindverhandeling worden enkele technieken behandeld die er voor zouden moeten zorgen dat de mens meer vertrouwen krijgt in de veiligheid van de digitale en draadloze toepassingen. De belangrijkste technieken hierbij zijn de cryptologie en de digitale handtekening.

1.2 Onderzoeksdoelen en –vragen

Het uitgangspunt van deze eindverhandeling is een onderzoek uit te voeren naar enkele mogelijkheden en technieken die voor confidentialiteit, integriteit, authenticiteit en onweerlegbaarheid kunnen zorgen in dit digitale en draadloze tijdperk. Zo trachten we een beeld te schetsen van cryptologie in het algemeen en zullen we nagaan welke principes van de cryptografie aan de basis liggen van de digitale handtekening. Verder gaan we in op de eigenschappen en wettelijkheid van de digitale handtekening en bespreken we enkele wiskundige begrippen zoals de one-way trap functie, de hash-functie en de codetheorie om zo tot een beter inzicht te komen van de achterliggende techniek die wordt toegepast.

Nadat we deze theoretische concepten hebben verduidelijkt richten we ons op een concrete toepassing waarbij cryptologie en de digitale handtekening gebruikt worden. We zullen ons toespitsen op de elektronische factuur en zullen trachten een antwoord te formuleren op de vraag of elektronisch factureren werkelijk voor een revolutie in de bedrijfswereld zal zorgen. Verder zal er aan de hand van een praktijkonderzoek worden nagegaan in welke mate elektronische facturatie vandaag de dag al in gebruik is, waarom bedrijven deze techniek implementeren of waarom niet, welke voor- en/ of nadelen het systeem met zich mee brengt en bespreken we de economische haalbaarheid en motivatie.

Toch willen we even aanstippen dat het opzet van deze eindverhandeling geen allesomvattende studie van cryptologie en de digitale handtekening betreft. Wel trachten we, op basis van wetenschappelijke onderzoeksmethodes, een zo volledig mogelijk beeld te schetsen omtrent dit onderwerp .
We kunnen het doel van dit onderzoek samenvatten in de volgende onderzoeksvraag:

“Welke technieken kunnen zorgen voor een verhoging van het vertrouwen in elektronische informatie-uitwisseling?”

Verder stellen we de volgende deelvragen:

- Wat is cryptologie?
- Wat zijn one-way trap functies?
- Welke rol speelt de hash functie?
- Hoe draagt de codetheorie bij tot een efficiënter transport van data?
- Hoe functioneren de verschillende cryptosystemen?
- Welke voornaamste wiskundige principes worden toegepast in de cryptografie?
- Wat zijn mogelijke technieken voor authenticatie?
- Wat is een digitale handtekening?
- Wat zijn de kenmerken van de digitale handtekening?
- Hoe functioneert de digitale handtekening?
- Wat zijn certificaat autoriteiten?
- Wat is de wettelijke regeling voor de digitale handtekening?
- Wat is elektronische facturatie?
- Welke wettelijke regelingen zijn er voor elektronische facturatie?
- Hoe slaat het concept ‘elektronische facturatie’ aan bij bedrijven?

1.3 Onderzoeksmethodologie

Voor deze eindverhandeling is gebruikt gemaakt van een literatuurstudie en een praktijkgedeelte. Voor de literatuurstudie waren de literatuurlijsten uit gerelateerde eindverhandelingen van de vorige jaren zeer bruikbaar. Hierna zijn we dieper gaan graven in de database van verschillende bibliotheken en ook in de digitale persdatabank ‘Mediargus’. Verder is er veel gebruik gemaakt van een haast onuitputtelijke bron, het Internet. Wel zijn we steeds kritisch gebleven en hebben we vrijwel altijd geverifieerd of de informatie van het Internet wel waarheidgetrouw was.

Voor het praktijkgedeelte betreffende de elektronische factuur hebben we twee methodes gebruikt, enerzijds door een bevraging van bevoorrechte getuigen en ervaringsdeskundigen, anderzijds door middel van een korte elektronische enquête gericht aan specifieke bedrijven. De enquête werd gezien als middel om de in de literatuur en op internet aangehaalde argumenten te toetsen naar waarheid en om eventuele aanvullingen op de materie op te wekken. Bij de interviews (die soms telefonische, soms per mail werden gepleegd) werd getracht vragen te bespreken over aspecten die nog niet duidelijk waren en wat dieper op verschillende punten in te gaan.

2 Cryptologie

2.1 Wat is cryptologie – cryptografie – crypto-analyse

Van Dale: Cryptologie is de leer van het geheimschrift.

In de cryptologie houdt men zich bezig met het geheimschrift. Wanneer we leesbare informatie omzetten in onleesbare informatie noemen we dit cryptografie. Een cryptografisch algoritme onderzoeken op zwakheden heet crypto-analyse.

Cryptografie komt van twee Griekse woorden: *'krypto' en 'graphe'* . Deze woorden betekenen respectievelijk 'verborgen, geheim' en 'schrijven'. Cryptografie betekent dus letterlijk: 'geheimschrijven'. Hiervan kan de volgende definitie worden afgeleid: "Cryptografie is de wetenschap die zich bezighoudt met het versleutelen en ontcijferen van al dan niet versleutelde informatie." *(Tielman, Vernooij, 2002)*

In de cryptografie houdt men zich bezig met verschillende technieken voor het zodanig versleutelen van te verzenden informatie, dat het voor een cryptoanalist, een persoon die toegang heeft tot het kanaal tussen zender en ontvanger, en dus tot hetgeen wat verzonden wordt, onmogelijk is om tegen aanvaardbare inspanning uit de getransporteerde data af te leiden welke informatie er door de zender was verzonden. Enkel de zender en ontvanger beschikken over de juiste sleutel om de gegevens terug om te zetten in hun originele vorm. Cryptografie wordt voornamelijk gebruikt om gegevens over te dragen die onderweg niet leesbaar mogen zijn door andere partijen, maar verschillende principes van de cryptologie zijn bruikbaar voor andere toepassingen, zoals voor de digitale handtekening. (*http://nl.wikipedia.org/wiki/Cryptografie)*

Cryptografie vindt zijn oorsprong vooral als militaire toepassing. In tijden van oorlog moeten boodschappen kunnen doorgegeven worden zonder dat de vijand ze kan begrijpen. Omgekeerd

wil men zoveel mogelijk informatie van de vijand onderscheppen en ontcijferen. Het is altijd een belangrijke bezigheid geweest van geheime diensten om enerzijds onkraakbare codes te ontwerpen en anderzijds te proberen de codes van de tegenstanders te kraken.

Geheimschrift kan echter vandaag de dag ook voor andere doelen gebruikt worden, we evolueren immers naar i-City, de draadloze stad, waar iedereen met elkaar zal verbonden zijn. Het is belangrijk dat er in ons technologisch tijdperk gezorgd wordt voor veiligheid. Zo zorgt cryptografie ervoor dat derde geen toegang hebben tot vertrouwelijke informatie (bvb. bestanden op een harde schijf), dat communicatie tussen personen privé kan gehouden worden (bvb. e-mails), en dat men veilig financiële transacties kan uitvoeren over een onveilig kanaal, zoals het Internet. Belangrijk voor dit eindwerk is natuurlijk de toepassing van cryptografie bij de digitale handtekening en het veilig kunnen versturen van digitale facturen.

2.2 Begrippen

Onder **encryptie** wordt verstaan het versleutelen, het vercijferen, van de informatie door de zender, en **decryptie** is het weer ontcijferen van de informatie door de ontvanger. Afhankelijk van het gebruikte algoritme kunnen gegevensreeksen soms ook veel compacter worden opgeslagen. Een methode van vercijfering noemen we een **cijfer** (chiper). De leesbare tekst noemen we **klare tekst**, en de vercijferde of gecodeerde tekst noemen we **cijfertekst**. Het ontcijferen van versleutelde boodschappen die voor iemand anders bestemd zijn heet het **kraken** van een code. *(http://nl.wikipedia.org/wiki/cryptografie)*

In de cryptografische theorie worden sinds jaar en dag drie **personen** ten tonele gevoerd: Alice (=A =partij A), Bob (=B =partij B) en Eve, die gedrieën uitwisseling van geheime informatie naspelen.

→ Alice: Alice wil iets versturen aan Bob, bijvoorbeeld een geheime, een gesigneerde of een geheim en gesigneerde boodschap.

→ Bob : Bob ontvangt berichten van Alice (vertrouwenspersoon). Hij wil controleren of het bericht echt van Alice komt, hij wil het bericht kunnen lezen en hij wil kunnen zien of de boodschap onderweg is veranderd.

→ Eve : Eve is de spion. Zij wil de informatie die tussen Bob en Alice wordt uitgewisseld bijvoorbeeld kunnen lezen, manipuleren, of ze wil Bob berichten sturen die ze met 'Alice' ondertekent.

Een **onveilig kanaal** wil zeggen dat Eve alles kan horen wat Alice en Bob zeggen en dat zij bovendien allerlei informatie aan het gesprek toe kan voegen. Beide vormen van infiltratie moeten Alice en Bob voorkomen. Het maakt overigens niet uit dat Eve alles kan horen, als ze het maar niet kan verstaan; voor een geheim gesprek hoeven twee Chinezen in Vlaamse omgeving doorgaans niet te fluisteren.

2.3 Geschiedenis

De oorsprong van cryptografie gaat waarschijnlijk terug tot de begintijd van de menselijke beschaving, vanaf het moment dat mensen leerden te communiceren. Ze moesten continu zoeken naar middelen om er zeker van te zijn dat gecommuniceerde geheimen ook geheim bleven. Het eerste opzettelijke gebruik van technische middelen om berichten te coderen, is terug te vinden bij de Grieken. Reeds honderden jaren voor Christus werd bij hen een stok die "scytale" werd genoemd gebruikt. Degene die het bericht stuurde, bond een stuk papier om de stok en schreef er in de lengterichting een bericht op. Daarna haalde hij het papier van de stok en stuurde het naar de bedoelde ontvanger. Het decoderen van het bericht zonder kennis van de dikte van de stok – die hier de sleutel is - zou vrijwel onmogelijk zijn. *(Loidreau, 2002)*

Ook de Romeinen maakten al gebruik van cryptografie (de rotatievercijfering van Caesar). Zij gebruikten encryptie bij hun militaire communicatie en deden dit door de letters van het alfabet met een vaste factor te verschuiven. Julius Caesar was één van de meest prominente gebruikers van dit systeem en deze vorm van versleutelen staat dan ook bekend als Caesar-

cijfer systeem. Een met behulp van dit systeem geconstrueerde cijfertekst is in maximaal 26 pogingen te kraken en daarom niet erg veilig.

In de volgende 19 eeuwen zijn er meer en minder geavanceerde experimentele coderings-technieken verzonnen, waarbij de veiligheid afhing van de mate van vertrouwen dat de gebruiker er in had. Rond 1570 ontwikkelde de Fransman Blaise de Vigenère het Vigenèrecijfer, een aanzienlijke verbetering op de tot dan gebruikte substitutiecijfers. In de jaren 1700 had elke Europese grootmacht zijn eigen zogenaamde "Zwarte Kamer", een soort geheime dienst waar een team van codebrekers dagelijks geheime berichten ontcijferden. Met de komst van de elektrische telegraaf in 1843 ontstond ook de interesse van het grote publiek voor geheimschrift, om te vermijden dat de telegrafist alle bijzonderheden van het bericht zou meelezen. De komst van de radio rond 1900 maakte het versturen van berichten over grote afstanden gemakkelijker voor het leger, maar vereiste ook een verbetering van de encryptie, omdat de vijand op elk moment kon meeluisteren. In de 19e eeuw schreef Kerchoffs over de principes van de moderne cryptografie. Een van die principes zegt dat de veiligheid van een cryptografisch systeem niet afhangt van het gebruikte cryptografische proces, maar van de gebruikte sleutel.

Tot in de Eerste Wereldoorlog gebruikte men voor militaire toepassingen handcijfers, ook veldcijfers genoemd. Later ontstonden de eerste elektromechanische cijfers, waarbij machines gebruikt werden om de letters om te zetten in code. Een alom bekende codeermachine is de in 1920 in Duitsland ontwikkelde Enigma. Het was een zeer moeilijke code om te kraken maar uiteindelijk werd de code van de Enigma toch gekraakt door de Polen en de Britten door gebruik te maken van (primitieve) computers. Het ontcijferen van de Enigma-code heeft bijna zeker de nederlaag van de Duitsers versneld. Verder bezat Duitsland nog een andere code: de Lorenz-machine, die werd gebruikt voor de communicatie tussen Hitler en zijn generaals, en die nog moeilijker te breken was dan de Enigma-code. De Engelsen bouwden hiervoor een elektronische machine, de Colossus. Dit was tevens ook de eerste computer. Een code die in de Tweede Wereldoorlog nooit gebroken werd is er een van de Verenigde Staten die het Navajo, een indianentaal, gebruikte in de oorlog tegen Japan waarbij een team van Navajo's niets anders deden dan boodschappen via de radio aan elkaar door te geven. Nog een code uit

de Tweede Wereldoorlog is het one-time-pad versleutelmechanisme ontwikkeld door Gilbert Vernam. Deze methode kon door niemand ontcijferd omdat er geen spraken was van regelmatigheid bij de versleuteling.

Met de komst van de computer werd het mogelijk de versleuteling zeer snel uit te voeren, en met een zeer groot aantal mogelijke sleutels. Men probeerde hierbij tot een standaard te komen, en een van de belangrijkste standaarden werd het DES-algoritme, een opvolger van het Lucifer-algoritme van IBM. *(http://nl.wikipedia.org/wiki/cryptografie)*

Het probleem bij deze techniek bleek het doorgeven van de sleutels bij veelvuldig gebruik. Whitfield Diffie en Martin Hellman ontwikkelden hiervoor samen in Amerika de Diffie-Hellman-procedure, die op een veilige wijze volledig elektronisch kan gebeuren, zelfs als de communicatie afgetapt wordt. Deze procedure legde de basis voor de later ontwikkelde asymmetrische systemen met publieke sleutels.

In 1948 en 1949 werd er een wetenschappelijke achtergrond opgesteld door Claude Shannon, hij schreef twee essays over het onderwerp: "A Mathematical Theory of Communication" en, nog belangrijker "The Communication Theory of Secrecy Systems". Deze artikelen maakte een einde aan hoop en vooroordelen. Shannon bewees dat Vernam's codering (het one-time-pad), die slechts een paar jaar eerder was voorgesteld, de enige onvoorwaardelijk veilige methode was die ooit zou kunnen worden ontwikkeld. Helaas echter is dit systeem in de praktijk onwerkbaar. Dit is de reden waarom evaluatie van de huidige systemen gebaseerd is op te berekenen veiligheid. Een geheime versleutelmethode is pas veilig als geen enkele bekende berekenmethode beter en sneller werkt dan een oneindig aantal pogingen tot de correcte sleutel gevonden is. *(Loidreau, 2002)*

2.4 Eigenschappen - doelen - van de cryptografische methoden

- **Geheimhouding** (confidentialiteit): Als Alice Bob een boodschap stuurt garandeert de eigenschap geheimhouding dat niemand behalve Bob de informatie kan lezen.

- **Data-integriteit** Als Bob een boodschap van Alice krijgt garandeert data-integriteit dat Eve geen informatie aan het bericht heeft toegevoegd of uit het bericht heeft verwijderd.

- **Authenticiteit** : Als Alice met Bob gaat praten, garandeert authenticiteit dat Bob niet stiekem Eve is die zegt dat ze Bob is (entiteit-authenticiteit). Ook garandeert authenticiteit dat Bob kan zien dat een boodschap die 'zegt' van Alice te komen ook echt van Alice komt (afzenderauthenticiteit).

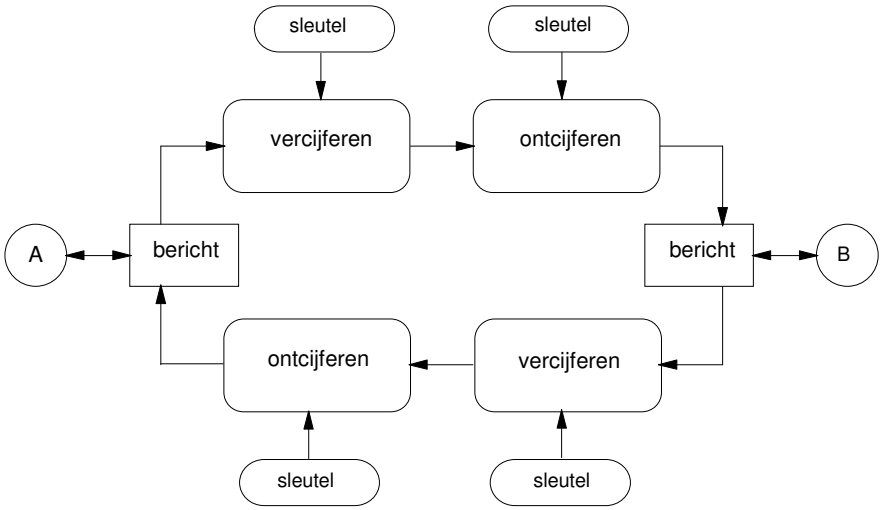
- **Erkenning** (onweerlegbaarheid): Als Alice een boodschap heeft verstuurd aan Bob en dit later ontkent garandeert erkenning dat Bob aan derden kan aantonen dat Alice en niemand anders deze boodschap aan hem heeft verstuurd.

Lang niet elk cryptografisch systeem voldoet aan deze doelstellingen. De cryptografische technieken zorgen wel voor geheimhouding, maar de andere drie eigenschappen worden enkel bereikt wanneer men gebruikt maakt van asymmetrische encryptiemethodes. Zie hiervoor de volgende paragraaf. Voor digitale handtekening algoritmen zijn data-integriteit, authenticiteit en erkenning van belang. In hoofdstuk 5 worden deze doelen uitgebreider behandeld.

2.5 Klassen van encryptie

2.5.1 Symmetrische encryptie (Private-key)

Bij symmetrische cryptografie wordt dezelfde sleutel gebruikt voor zowel het vercijferen van informatie als voor het ontcijferen. Op de volgende pagina vindt u een schematische voorstelling van symmetrische encryptie.



Figuur 1 : Schema symmetrische encryptie

Als A een bericht naar B wil sturen, vercijfert hij de boodschap met een sleutel, B ontcijfert deze vervolgens met dezelfde sleutel. Als B een bericht terug wil sturen dan doet hij hetzelfde.

Voordeel van symmetrische cryptografie is dat het minder rekenintensief en sneller is dan asymmetrische cryptografie (zie verder) waardoor het de voorkeur heeft voor grote bestanden of hoge datasnelheden.

Symmetrische systemen zijn echter minder geschikt voor groepen: zodra er drie partijen in het geding zijn, kan men niet meer vaststellen wie de verzender geweest is van het bericht: beide andere partijen hebben immers de verzendsleutel (die identiek is). Voor dergelijke authenticatie gebruikt men vaak asymmetrische cryptografie.

Een bijkomend nadeel is de hoeveelheid benodigde sleutels. Als bijvoorbeeld elk individu van een groep van 10 verschillende personen met ieder ander lid van de groep wil communiceren met behulp van een sleutel-combinatie, dan zijn er maar liefst 45 sleutels nodig. De formule voor het aantal vereiste sleutels (y): $y = n(n-1) / 2$.

Het aantal benodigde sleutels is in de volgende tabel uitgezet tegen het aantal deelnemers.

Tabel 1 : Benodigde sleutels per deelnemer bij symmetrische encryptie

Symmetrische Encryptie					
	Deelnemers	2	4	6	18
	Sleutels	1	6	28	120

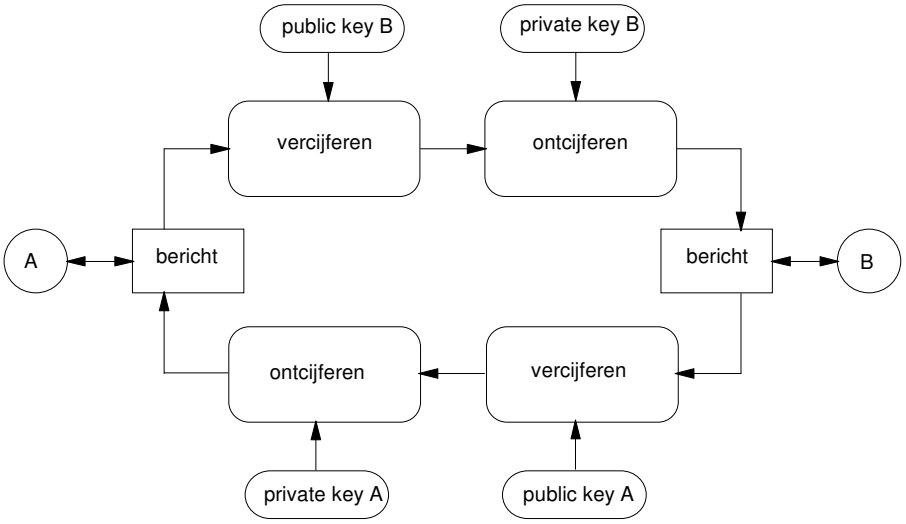
Hierin is goed zichtbaar dat het beheer van sleutels al snel onpraktisch wordt. *(Noorden, 2000)*

Voorbeelden van symmetrische systemen zijn bijvoorbeeld de klassieke handcijfers en de modernere computeralgoritmes DES, IDEA en RC4.

2.5.2 Asymmetrische encryptie (Public-key)

Asymmetrische cryptografie gebruik twee aparte sleutels: één sleutel wordt gebruikt om de informatie te coderen (vercijferen) en de tweede sleutel om de informatie weer te decoderen (ontcijferen). Dit in tegenstelling tot de hierboven besproken symmetrische cryptografie, waarbij één en dezelfde sleutel gebruikt voor zowel coderen als decoderen.

Het voordeel bij deze methode is dat men één van de twee sleutels gewoon publiek kan maken (bijvoorbeeld publiceren op een website of als ondertekening van een e-mail) Deze sleutel wordt de publieke sleutel van de set sleutels genoemd. Vanwege het publiceren van de geheime sleutel heet deze techniek ook wel "public key cryptography". Wanneer eender wie mij een bericht wil sturen dat geheim moet blijven kan men de publieke sleutel gebruiken om de informatie te vercijferen. Vervolgens wordt het bericht mij toegezonden. Het bericht kan nu enkel door mij ontcijferd worden, omdat ikzelf als enige de privé of geheime sleutel heb, benodigd om het bericht te ontcijferen. De anderen hebben dus een sleutel om te vercijferen, maar niet om te ontcijferen. Hierdoor blijft, behalve voor mij, het bericht onleesbaar voor iedereen die het kan onderscheppen.



Figuur 2 : Schema asymmetrische encryptie

Als A een bericht naar B wil sturen, dan zal hij eerst vragen of B zijn public key aan A wil sturen (de public key mag iedereen weten), en zijn bericht vercijferen met de public key van B, en vervolgens naar B sturen. Omdat dit bericht alleen maar met de private key van B gelezen kan worden (die B geheim houdt), kan niemand anders dit lezen. Als B een bericht terug wil sturen aan A, dan moet hij dit weer vercijferen met de public key van A, en kan dit bericht alleen met de private key van A gelezen worden

Andersom zou ik een bericht dat ik verzend kunnen voorzien van een controlegetal dat afhankelijk is van de inhoud. Door dat controlegetal met mijn geheime sleutel te vercijferen en het resultaat mee te sturen, geef ik iedereen de mogelijkheid om met mijn publieke sleutel het controlegetal te ontcijferen. Door opnieuw zelf een controlegetal van de inhoud te bepalen en het resultaat te vergelijken met de ontcijferde waarde, weet men vrijwel zeker dat het bericht van mij afkomstig moet zijn. Immers: alleen ik bezit de sleutel om die informatie te kunnen vercijferen (coderen).

Voordeel van de asymmetrische cryptografie is, dat men door het verstrekken van de ene dan wel de andere sleutel kan kiezen wie de versleutelde informatie kan lezen en ook wie allemaal informatie kan versleutelen.

Nadeel van public key cryptografie is dat het in feite zeer complex is. Voor public key encryption en decryption heeft de computer veel verwerkingscycli nodig: ongeveer 100 keer

zoveel cycli als bij symmetrische encryptie. De inefficiëntie van deze verwerkingslast is zo groot dat public key encryption alleen gebruikt kan worden om kleine berichten te versleutelen, zoals een hash bij de digitale handtekening (zie verder).

Omdat bij asymmetrische encryptie iedere deelnemer aan de communicatie over één publieke sleutel beschikt, is het mogelijk een persoon, van wie men de publieke sleutel heeft, een geheim bericht te sturen. Als we hier het aantal deelnemers uitzetten tegen de benodigde sleutelparen, zien we het volgende: *(Noorden, 2000)*

Tabel 2 : Benodigde sleutels per deelnemer bij asymmetrische encryptie

Asymmetrische Encryptie					
	Deelnemers	2	4	6	18
	Sleutels	2	4	6	18

De public key encryption-methode die op de meeste plaatsten gebruikt wordt, is RSA. Een nieuwe vorm van public key encryption, de elliptic curve cryptosystem (ECC), belooft gelijkwaardige bescherming met kleinere sleutels, en dus een kleinere verwerkingslast, te bieden.*(Panko, 2005)*

2.5.3 Blokcijfers - Stroomcijfers

De verschillende vercijferingsmethodes kunnen ook ingedeeld worden op basis van de manier waarop de input verwerkt wordt.

Bij blokcijfers gebeurt de vercijfering van de boodschap in vaste blokken (groepen karakters) met behulp van een vaste encryptietransformatie. Een blok gegevens wordt dus omgezet tot een geencrypteerd blok. De vaste lengte wordt blokgrootte genoemd, de meeste blokken hebben een lengte van 64 bits, zoals onder andere van toepassing bij RSA. Het is noodzakelijk dat de indeling van de blokken zo veilig en efficiënt mogelijk gebeurd.

Stroomcijfers daarentegen vercijferen de karakters één per één. Hierdoor zijn ze sneller dan blok cijfers en hebben ze een eenvoudiger hardwareschakelschema. Stroomcijfers zijn zeer

geschikt wanneer buffering gelimiteerd is (zoals in de telecommunicatie) of als karakters individueel verwerkt moeten worden bij ontvangst. Omdat ze geen of beperkte foutpropagatie hebben, zijn ze ook te verkiezen in situaties waarin transmissiefouten zeer veel voorkomen. *(Simons, 2005)*

2.6 Public key distribution van symmetrische sleutels

In feite kan public key distribution een bijdrage leveren aan symmetrische encryptie door symmetrische sessiesleutels veilig te verdelen.

- Partij A kiest zijn symmetrische sleutel
- Partij A versleutelt deze symmetrische sleutel met de publieke (asymmetrische) sleutel van B
- Partij A verstuurt het geëncrypteerde naar partij B
- Partij B ontsleutelt dit met zijn private sleutel
- Partij B is nu net als A in het bezit van de symmetrische sleutel, deze kunnen ze gebruiken om berichten vertrouwelijk te verzenden

De sleutel die op deze manier is uitgewisseld wordt een sessiesleutel genoemd, omdat deze alleen voor de communicatiesessie van dat moment gebruikt wordt (veiliger). Als de twee partijen naderhand weer met elkaar communiceren, genereren ze een nieuwe sessiesleutel.

Met deze techniek combineert men de veiligheid van de asymmetrische methode met de snelheid van de symmetrische methode. *(Panko, 2005)*

3 Wiskunde gebruikt in de cryptologie en de digitale handtekening

Vooraleer we overgaan tot de bespreking van enkele cryptosystemen en later de digitale handtekening is het noodzakelijk dat we enkele basisbegrippen en wiskundige principes nader toelichten.

3.1 Modulair rekenen

Modulair rekenen gaat over het rekenen met resten bij deling. Het basisidee is het volgende:

$a = c(\text{mod } b)$	waarbij,
$a = k \cdot b + c$	voor k = een willekeurig natuurlijk getal

Het voordeel voor cryptografen van modulair rekenen is dat het niet direct omkeerbaar is: dat is te zien aan de bovenstaande formule. Het getal 'k' kan immers alle natuurlijke getallen zijn, en is dus niet te vinden als men alleen beschikt over getal 'c'. Natuurlijk is het wel mogelijk om een modulo-bewerking om te keren, anders was het immers onbruikbaar voor cryptografie.

De inverse van een modulo wordt als volgt omschreven → voor inverse i van a, modulo m, geldt:

$(a \cdot i) = 1(\text{mod } m)$	deze formule kan ook als volgt worden omgeschreven:
$a \cdot i = m \cdot k + 1$	voor k = een willekeurig natuurlijk getal
	dit wordt ook wel genoteerd als:
$a^{-1} = i(\text{mod } m)$	

Er is niet altijd een oplossing voor dit soort problemen: een voorwaarde is dat i en m relatief priem zijn. Dit betekent dat ze geen gemeenschappelijke priemfactoren hebben, ofwel dat hun GGD (grootste gemene deler) gelijk is aan 1. De inverse van een modulo kan worden

berekend met het zogenoemde ‘uitgebreide Euclidische algoritme’, wat een uitbreiding is van het Euclidische algoritme waarmee GGD’s berekend worden (zie verder).

3.2 Priemgetallen

Een priemgetal is een getal groter dan 1, en alleen deelbaar door 1 en door zichzelf.

Bijvoorbeeld 15 is niet priem, want 15 = 3*5 maar 11 is wel priem. Er bestaan oneindig veel priemgetallen en met computers kost het weinig moeite om grote priemgetallen te bepalen. In de cryptografie worden priemgetallen van 512 bits (ongeveer 154 decimale cijfers) en 1024 bits (ongeveer 308 decimale cijfers) gebruikt.

3.3 Euler & Fermat

- Euler’s Phi functie: Een waarde waarmee gemoduleerd wordt, heet modulus. Bij elke modulus is er een restklasse: de mogelijke waarden van k(mod m) waarbij k een natuurlijk getal is en m de modulus. Behalve de gewone restklasse bestaat er ook een gereduceerde restklasse: de leden van de restklasse die relatief priem zijn ten opzichte van de modulus. Een voorbeeld: de restklasse van 12 is 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11; de gereduceerde restklasse van 12 is 1, 5, 7, 11 want deze getallen hebben geen factor gemeenschappelijk met 12. De ’Euler phi functie’ (geschreven als $\phi(n)$) is het aantal elementen in de gereduceerde restklasse. Bij 12 is dat dus 4, bij priemgetallen is dat altijd n − 1. Een bijzonder geval hiervan is als p en q priem zijn, en $n = p \cdot q$: dan geldt $\phi(n) = (p - 1)(q - 1)$. Dit is belangrijk voor asymmetrische cryptografie: vrijwel alle algoritmes maken er gebruik van.
- De kleine stelling van Fermat luidt: Als m een priemgetal is en a niet deelbaar door m, dan geldt: $\boxed{a^{m-1} = 1 (\text{mod } m)}$

- Volgens Euler's generalisatie van de kleine stelling van Fermat geldt: $a^{\phi(n)} = 1 (\text{mod } n)$

3.4 Algoritme van Euclides

Het 'standaard' algoritme van Euclides wordt gebruikt om de grootste gemene deler te berekenen van twee getallen. Het werkt als volgt: Neem twee getallen a en b waarvan de GGD uitgerekend moet worden en waarvoor geldt: $a > 0$ en $a \geq b \geq 0$.

Schrijf a als $k \cdot b + c$
Schrijf b als $l \cdot c + d$
Schrijf c als $m \cdot d + e$
. . .
Ga door tot $e = 0$, dan geldt: GGD(a, b) = d

Bewijs

Als $e = 0$, dan geldt:
$c = m \cdot d$
$b = (l \cdot m + 1) \cdot d$

Dus GGD(b, c) = d, omdat m en $l \cdot m + 1$ geen gemeenschappelijke factoren hebben. Nu kunnen a en b worden geschreven als:

$a = k \cdot (l \cdot m + 1) \cdot d + m \cdot d = d \cdot (k \cdot (l \cdot m + 1) + m)$
$b = d \cdot (l \cdot m + 1)$

Omdat $(l \cdot m + 1)$ en $(k \cdot (l \cdot m + 1) + m)$ geen gemeenschappelijke factoren hebben, geldt ook dat GGD(a, b) = d. Dit kan net zo vaak herhaald worden als nodig.

Voorbeeld

Er zijn twee mogelijkheden: a) GGD > 1; b) GGD = 1

Mogelijkheid b) impliceert dat de getallen geen gemeenschappelijke deler hebben buiten 1, dus relatief priem zijn.

Bereken met het algoritme van Euclides GGD(654321, 123456).

$654321 = 5 \cdot 123456 + 37041$
$123456 = 3 \cdot 37041 + 12333$
$37041 = 3 \cdot 12333 + 42$
$12333 = 293 \cdot 42 + 27$
$42 = 1 \cdot 27 + 15$
$27 = 1 \cdot 15 + 12$
$15 = 1 \cdot 12 + 3$
$12 = 4 \cdot 3 + 0$

GGD(654321, 123456) = 3

3.5 Discrete logaritmen

Modulair machtsverheffen, en zijn inverse de discrete logaritme, was de eerste wiskundige invulling van het theoretische begrip one-way functie. Diffie en Hellman presenteerden behalve public-key cryptografie ook een sleuteldistributiesysteem gebaseerd op de discrete logaritme. De kracht van het systeem berust op het discrete logaritmeprobleem.

Logaritme

De wiskundige functie logaritme bepaalt voor een x en een grondtal g tot welke macht m je g moet verheffen om x te krijgen:

$$\log_g x = m, g^m = x.$$

Een bekend voorbeeld is de natuurlijke logaritme, $\ln = \log_e$.

De discrete logaritme is nu de logaritmische functie in een eindige, cyclische groep G. De cryptografisch interessante groepen zijn de multiplicatieve groepen Fq van het eindige lichaam Fq . In dit onderzoek wordt naar Fp , met p priem, gekeken.

Definitie discrete logaritmeprobleem

Het discrete logaritme-probleem (DLP) speelt zich af in een eindige, cyclische groep G van orde n met een voortbrenger α. Voor voortbrenger α en een groepselement $\beta \in$ G geldt de volgende equivalentie

$$\beta = \alpha^x , x = \log_\alpha \beta.$$

Het discrete logaritme-probleem is nu: Gegeven β en α, vind het unieke natuurlijk getal x, $0 \leq x \leq n \leq 1$, zodat $\alpha^x = \beta$

4 One-way functions

4.1 Algemeen

Een van de belangrijkste pijlers van een public-key cryptosysteem is de one-way functie. Een one-way functie(of eenswegsfunctie) is een wiskundige functie *f* waarbij er voor elke *x* in het domein van *f* er makkelijk *f(x)* kan berekend worden, maar waarbij het zeer moeilijk is voor alle *y* (mogelijke oplossingen) van *f* , *x* te vinden zodanig dat *y = f(x).* Met andere woorden: een one-way functie is een functie waarbij het vinden van de inverse van *f* zo goed als onmogelijk is. *(Wilschut, D.E., 2000)*

Voorbeeld: *(Simons, 2005)*
Stel $X = \{1; 2; 3; \ldots; 16\}$ en $y = f(x) = 3^x \bmod 17$ waarbij $x \in X$; Het is relatief eenvoudig om de waarde van y te berekenen voor een gegeven x, zelfs bij grote getallen. De inverse functie berekenen is al veel moeilijker, zelfs voor kleine getallen.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f(x)	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Wat is er cryptografisch dan interessant aan zulke functies? Deze functies zijn op zich voor de cryptografie niet bruikbaar vermits een vercijfering niet meer kan worden ontcijferd. Er bestaat echter een bijzondere klasse one-way functies namelijk de “trapdoor” one-way functies (zie paragraaf 4.2), die een sluiproute, trapdoor, in zich bergen. Als je wat extra informatie hebt is het ineens heel eenvoudig om vanuit f(x) x te bepalen. Het zijn deze kandidaat-functies die aan de basis liggen van public-key cryptosystemen.

We splitsen de one-way functions dus op in twee categorieën, enerzijds de functies zonder inverse, anderzijds de functies met inverse door de aanwezigheid van een “trapdoor”.

De one-way functies waarbij er geen inverse bestaat zijn echter niet totaal onbruikbaar. Een belangrijke toepassing is de hash-functie, die gebruikt wordt voor de generatie van de digitale handtekening.

4.2 De hash functie

Digitale handtekening schema's gebaseerd op asymmetrische cryptosystemen kunnen enkel relatief kleine berichten aan. Zo zal bijvoorbeeld een 160-bit bericht onder het gebruik van DSS getekend worden met een 320-bit handtekening. In het algemeen willen we veel grotere boodschappen kunnen tekenen. Zo zal bijvoorbeeld een juridisch document dikwijls vele megabytes groot zijn.

Een naïeve oplossing zou zijn de boodschap eerst op te splitsen in stukken van 160-bits, en dan elk stuk apart te gaan tekenen. Dit zou analoog zijn aan het encrypteren van een lange platte tekst door elke letter apart gaan te versleutelen met dezelfde sleutel.

Er zijn echter meerdere problemen wanneer we op deze manier digitale handtekeningen gaan creëren. Om te beginnen gaan we een enorme handtekening hebben bij lange boodschappen. Een tweede nadeel is dat de meeste beveiligingshandtekeningen traag zijn omdat ze gecompliceerde berekeningen uitvoeren. Maar het grootste tekort is dat wanneer er stukken boodschap worden verwijderd of gewijzigd, de resulterende boodschap nog steeds kan worden als correct geverifieerd. We moeten zorgen dat we de integriteit van de hele boodschap bewaren. Dit kan niet gebeuren door afzonderlijke stukken te tekenen. Bovendien wordt het kraken van de boodschap eenvoudiger wanneer men de afzonderlijke stukken telkens met dezelfde sleutel gaat vercijferen.

De oplossing is het gebruik van een snelle publieke cryptografische hashfunctie (ook wel klutsfunctie of hutsfunctie genoemd). Het woord *hash* komt uit het Engels en betekent hier *hakken*. Bij de hashfunctie zal een boodschap van eender welke lengte omgezet worden naar

een ‘message digest’ van een specifieke, te kiezen lengte (bijvoorbeeld 128 bits voor MD5, of 160 bits voor SHA-1). Men kan deze message digest beschouwen als een soort vingerafdruk van de originele boodschap.

Hashfuncties worden vooral gebruikt voor data integriteit in combinatie met digitale handtekeningen: eerst berekent men met een hashfunctie de message digest van de boodschap, en deze digest wordt vervolgens ondertekend. Bijvoorbeeld, wanneer Bob een bericht *x* wil tekenen, zal hij eerst de message digest g = *h(x)* construeren. Hierna zal hij g versleutelen tot *y* = *sigK(z).* Zoals men kan zien op onderstaande figuur zal een bericht van willekeurige lengte door enkele iteraties van de hashfunctie gecomprimeerd worden tot een vaste lengte waardoor het mogelijk wordt lange berichten te ondertekenen.

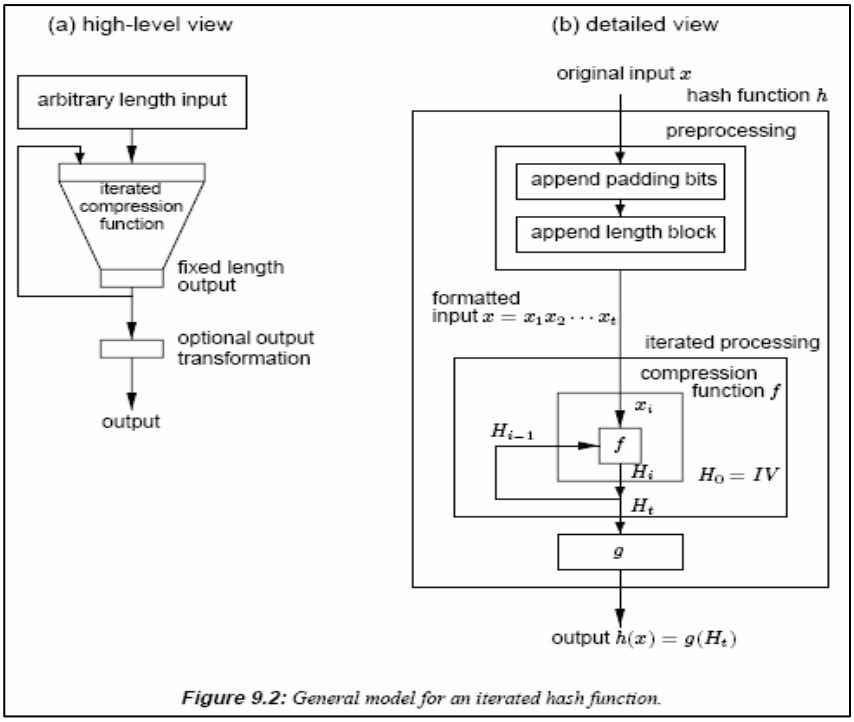


Figure 9.2: *General model for an iterated hash function.*

Figuur 3 : Schema hash-functie

4.2.1 Eigenschappen van de hashfunctie

Het gebruik van hash-functies in de cryptografie worden zo gekozen dat ze de volgende basis vereisten bezitten: *(http://www.x5.net/faqs/crypto/index.html)*

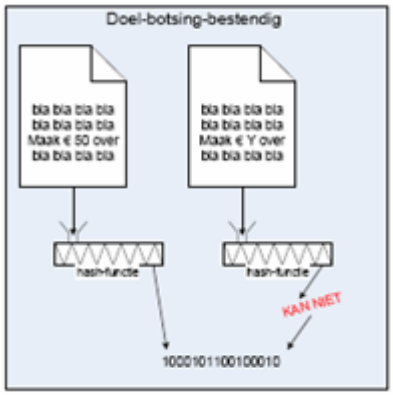
- de **input** mag van **eender welke lengte** zijn: dit is een groot voordeel aangezien men op deze manier eender welke tekst, hoe groot ook, een digitale handtekening kan verschaffen op basis van zijn hash-waarde.

- de **output** heeft altijd een **vaste lengte**

- $g = h(x)$ is relatief **gemakkelijk te berekenen** voor elke x

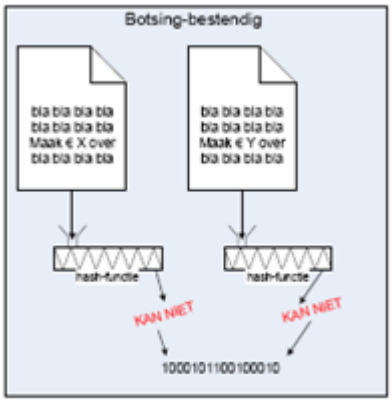
- $h(x)$ is een **'one-way' functie** : het is onmogelijk om uit een gegeven hashwaarde het oorspronkelijke bericht te achterhalen vermits er tijdens het 'hashen' heel wat informatie wordt weggelaten. De inverse van de hashfunctie bestaat niet. Hierdoor gebruikt men de hash-functie dus ook voornamelijk voor controledoeleinde. Wanneer twee (zinvolle) documenten dezelfde hashwaarde hebben zijn ze nagenoeg zeker identiek.

- $g = h(x)$ is **doel-botsing-bestendig** (target collision resistant, second pre-image resistant): het is praktisch gezien onmogelijk om uit een gegeven input-bitstring een tweede input-bitstring af te leiden met dezelfde hash-waarde;



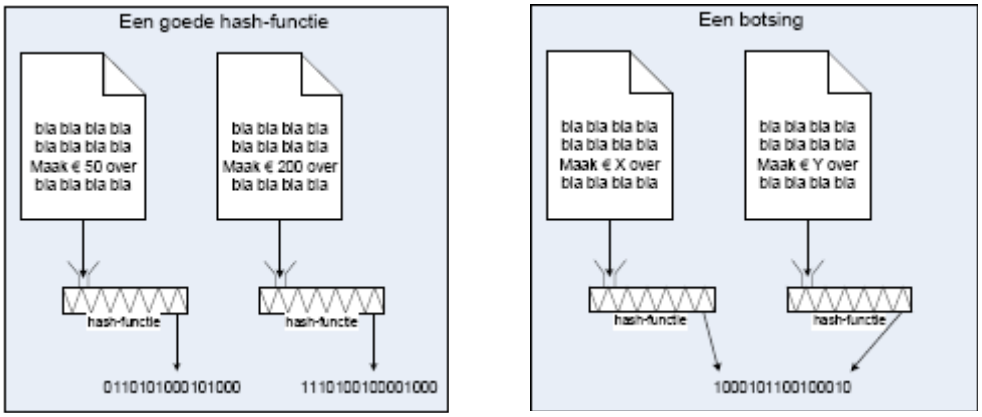
Figuur 4 : Doel-botsing-bestendigheid bij hash-functies

- $g = h(x)$ is **botsing-bestendig** (random collision resistant): het is praktisch gezien onmogelijk om twee input-bitstrings te vinden met dezelfde hash-waarde.



Figuur 5 : Botsing-bestendigheid bij hash-functies

Twee verschillende inputs die dezelfde hash-waarde hebben wordt een *botsing* genoemd, en dat moet vermeden worden.



Figuur 6 : Een goede hashfunctie en een botsing

Botsingsvrij wil zeggen dat het rekenkundig zo goed als onmogelijk is om twee verschillende inputs *x, x'* te vinden, die dezelfde hashwaarde als output hebben, zodat $h(x) = h(x')$. 'Zo goed als rekenkundig onmogelijk' moet men echter verstaan in zijn referentiekader. Zwak botsingsvrij zou men kunnen definiëren als oplosbaar in een polynomiale tijd en ruimte; hiermee wordt praktisch bedoeld als oplosbaar binnen een bepaald aantal machine operaties,

misschien wel seconden of milliseconden. Met een andere, meer specifieke definitie zoals de sterke botsingsvrije hash-functie wordt bedoeld dat deze functies een super-polynomiale inspanning vereisen. Hiermee bedoelt men een inspanning die meer vraagt dan er beschikbare bronnen zijn. Het is belangrijk dat we hashfuncties met een sterke botsingsvrij karakter kiezen voor het gebruik met de digitale handtekening om de veiligheid te verzekeren.

4.2.2 Veiligheid

Het is, zoals bovenvermeld, essentieel bij de hash functie dat ze 'one-way' en botsingsvrij is. Een basis aanval op de hash functie is het generen van verschillende inputs tot dat er een bepaalde input gevonden wordt die dezelfde target output waarde genereert (en hierdoor dus de 'one-way' eigenschap tegenspreekt). Een andere manier is twee inputs te vinden die dezelfde output generen (en hierdoor dus de botsingsvrije eigenschap tegenspreekt).

Stel dat we een hash functie hebben met een output bitlengte n. Omdat wanneer we opzoek zijn naar een input die een bepaalde output zal produceren, dan zullen er 2^n mogelijke inputwaardes zijn omdat elke output een gelijke kans tot voorkomen heeft.

Wanneer we op zoek zijn naar een botsing, dan verwachten we aan de hand van 'de verjaardagsparadox' een botsing na het testen van $2^{n/2}$ mogelijke inputwaardes. Van Oorschot en Wiener toonde aan hoe zulk een brute-kracht aanval moet geïmplementeerd worden.

Met het oog op het gebruik van hash functies bij digitale handtekeningen, stelde Yuval de volgende strategie voor op basis van de 'verjaardagsparadox'.

N is de lengte van de digest:

- De tegenpartij selecteert een boodschap die ze wil kraken en een onschuldige boodschap die de andere partij waarschijnlijk wel zal tekenen.
- De tegenpartij genereert $2^{n/2}$ variaties van de onschuldige boodschap (door bijvoorbeeld kleine editoriale wijzigingen aan te brengen), met alle dezelfde betekenis

en hun corresponderende message digests. Daarna genereert men evenveel variaties van de boodschap die ze wil kraken.

- De kans dat één van de variaties van het onschuldige bericht zal overeenkomen met één van de variaties van het kritieke bericht is groter dan ½ volgens de 'verjaardagsparadox'.
- De tegenpartij verwerft hierna de andere partij haar handtekening op de variatie van het onschuldige bericht
- De handtekening van het onschuldige bericht wordt nu verwijderd en verbonden aan de variatie van de echte boodschap met dezelfde message digest. De tegenpartij is er nu in geslaagd het oorspronkelijke bericht te vervalsen zonder de vercijferingssleutels te ontdekken.

Om zo een aanval te voorkomen moet men zorgen dat de output van de hash functie voldoende lang is.

4.3 "Trapdoor" one-way function

Een valfunctie (=trapdoor) is een one-way functie met het verschil dat de inverse richting gemakkelijk te vinden is wanneer men bepaalde informatie bezit (de 'trap door'), maar quasi onmogelijk (met een beperkte hoeveelheid rekenwerk) wanneer men deze informatie niet bezit. *(Menezes, 1997)*

Men gebruikt valfuncties voor public-key cryptosystemen (PKI). De publieke sleutel geeft de eigelijke functie; de private sleutel geeft informatie betreffende de 'trap door'. Diegene die de 'trap door' bezit kan de functie gemakkelijk in twee richtingen uitvoeren. Iemand die deze niet heeft kan de functie enkel uitvoeren in de voorwaartse richting. De voorwaartse richting wordt gebruikt voor encryptie en handtekening verificatie. De inverse richting wordt gebruikt voor decryptie en handtekening generatie.

De grootte van de sleutel bepaalt het aantal inputs tot de ‘one-way’ functie en dus de moeilijkheid tot vinden van de inverse voor iemand die de ‘trap door’ niet bezit. Opdat een digitale handtekening jaren veilig zou zijn is het nodig dat men een valfunctie gebruikt met een groot aantal inputs zodat iemand zonder de ‘trap door’ vele jaren zou nodig hebben om de inverse functie te berekenen.

5 Cryptosystemen

5.1 Handcijfers

Handcijfers vormen een klasse van verschillende vercijferingsmethodes die met behulp van een geheim sleutelwoord of een geheime zin een tekst omzetten in een onleesbare code. Synoniemen voor handcijfers zijn pen- en papiercodes of veldcijfers. De bedoeling van handcijfers is dat men een vercijferde tekst enkel kan ontcijferen indien men over dezelfde methode beschikt en in het bezit is van dezelfde geheime sleutel. In de loop der jaren ontwikkelde men verschillende succesvolle en betrouwbare technieken. Het grote voordeel van handcijfers is de eenvoudige toepassing zonder speciale toestellen. Daarom blijven deze handcijfers tot op vandaag nog steeds een interessant alternatief om een boodschap op eenvoudige wijze toch veilig over te brengen. We bespreken enkelen van de bekendste klassieke handcijfers.

5.1.1 De klassieke handcijfers

In deze paragraaf beschrijven we kort de bekendste handvercijferingsmethodes, in paragraaf 5.2 worden al deze cijfers verduidelijkt aan de hand van een voorbeeld.

- De rotatievercijfering van Caesar is een van de oudst gekende cijfers en werd gebruikt voor de communicatie tussen Romeinse veldheren. Deze vercijfering wordt ook wel rotatiecijfer of ROT genoemd.

- Het substitutiecijfer is een monoalfabetische substitutie. Hierbij wordt elke letter vervangen door een andere letter.

- Vigenère is een polyalfabetische substitutie, het vervangen van letters aan de hand van verschillende alfabetische reeksen in een tabel, het Vigenère-tableau.

- Autoclave is een verbetering van het Vigenèrecijfer. Hierbij vercijfert men, mits een kleine verschuiving door een sleutelwoord, de klare tekst met zichzelf.

- Homofone substitutie gebruikt een evenredige verdeling van letters naar getallen om bestand te zijn tegen letterfrequentie-analyse.

- Bifid is een matrix die een combinatie van substitutie met fractionering gebruikt. Elke letter wordt opgesplitst in twee getallen.

- Trifid is een drievoudige matrix welke een combinatie van substitutie met fractionering gebruikt. Elke letter wordt opgesplitst in drie getallen.

- Playfair is een substitutiecijfer waarbij een matrix is gebruikt om bigrammen te vercijferen.

- ADFGVX combineert fractionering van een Polybiusvierkant, dat een monoalfabetisch substitutie bevat, met een enkelvoudige kolomstranspositie. Het was tijdens de Eerste Wereldoorlog het veldcijfer van het Duitse leger.

- Dubbele transpositie is een tweevoudige kolomtranspositie. Dit was één van de veiligste handcijfers, gebruikt tijdens de Tweede Wereldoorlog.

- Straddling checkerboard of spreidend schaakbord is een fractionerend monoalfabetisch substitutiecijfer. Het is een matrixcijfer dat meestal gevolgd wordt door een bijkomen dubbele transpositie

(http://nl.wikipedia.org/wiki/Handcijfer)

5.1.2 Vercijferingsmethodes

Voor handcijfers zijn er drie grote indelingen in de techniek van het vercijferen:

- Substitutie: vervangen van letters door andere letters
- Transpositie: verwisselen van de positie van letters binnen een tekst
- Fractionering: breken van letters in verschillende delen waarna deze verplaatst worden

Men gebruikt ook verschillende combinaties van de verschillende methode. Zo blijkt de combinatie van transpositie en fractionering zeer effectief. Hierdoor worden de verschillende delen van één letter verspreid over de ganse tekst. Het ideale cijfer is dus een combinatie van de drie vercijferingsprincipes, en dat bovendien eenvoudig is in gebruik. Zo combineren bijvoorbeeld Bifid, Trifid, en ADFGVX transpositie en fractionering. De idee van handcijfers door middel van substitutie, transpositie en fractionering worden in de moderne crypto-algoritmes voor computer nog steeds toegepast.

5.1.3 Sleutelwoorden

Een vereiste voor een goed cijfer is dat het eenvoudig is in gebruik. Daarom gebruikt men veelal sleutelwoorden om een substitutie-alfabet of een matrix te vullen..

Een voorbeeld: men neemt het sleutelwoord, of de zin, schrapt de letters die er dubbel in voorkomen, en vult achter dit sleutelwoord de resterende letters van het alfabet aan. Hoe langer het sleutelwoord of de zin, des te minder men alfabetisch dient aan te vullen. *(http://nl.wikipedia.org/wiki/Handcijfer)*

Sleutelwoord: SLEUTELWOORD Cijferalfabet: SLEUTWORDABCFGHIJKMNPQVXYZ

5.1.4 Veiligheid

Met cryptoanalyse heeft men alle hierboven beschreven handcijfers kunnen breken. Enkele veldcijfers zijn echter nog steeds nuttig indien de tijd, nodig voor cryptoanalyse, zo lang is dat

de verkregen informatie achterhaald en nutteloos blijkt. Men moet dus een zogenaamde kost-baten analyse toepassen. De sterkste veldcijfers, hierboven beschreven, zijn dubbele transpositie en ADFGVX.

Over het algemeen geldt dat grotere sleutelwoorden een betere veiligheid geven en hoe minder tekst vercijferd is, des te moeilijker de cijfertekst te kraken is. Letterfrequentie-analyse is bijvoorbeeld onbetrouwbaar als er slechts één zin werd gecodeerd, of er verhoudingsgewijs veel zeldzame letters in de tekst zitten. Zo is het eenvoudige Vigenère onbreekbaar indien één korte zin met een lang sleutelwoord vercijferd werd, maar is het breken van het veel veiliger dubbel transpositiecijfer minder moeilijk indien er genoeg cijfertekst voorhanden is. *(http://nl.wikipedia.org/wiki/Handcijfer)*

5.2 Werking van verschillende handcijfer-encryptiemethodes

5.2.1 Rotatievercijfering van Caesar

Deze methode stamt af uit de Romeinse tijd. Ze werd gebruikt voor geheime berichten veilig te versturen tussen verschillende veldheren. De Caesarvercijfering, oftewel rotatievercijfering (afgekort ROT), is één van de klassieke handcijfers. Het is een symmetrische encryptiemethode.

Het is een substitutiecijfer dat een vast normaal alfabet gebruikt, dat met een vooraf bepaald aantal letters is verschoven. Dit cijfer wordt ook wel rotatiecijfer genoemd. Een verschuiving van 3 noemt men dan een ROT(3)-cijfer.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

De letters in de klare tekst, gevonden in het bovenste alfabet, worden eenvoudigweg vervangen door de letter eronder.

Klare tekst: **D** I T I S Z E E R G E H E I M
Cijfertekst: **A** F Q F P W B B O D B E B F J

De cijfertekst: AFQFP WBBOD BEBFJ

Hoewel dit in die tijd voor de doorsnee ongeschoolde en ongeletterde mensen ongetwijfeld een onbreekbaar cijfer was, is dit gewoon een kwestie van uitproberen welk van de 25 mogelijke verschuivingen de juiste is.

Een speciaal geval is de ROT(13) code, nog gebruikt in veel mail- en nieuwslezers. Voor het verstoppen van antwoorden op raadsels is deze code prima geschikt. Omdat 13 plaatsen vooruit of achteruit doorschuiven op hetzelfde neerkomt (13 = 26/2), is encoderen of decoderen net hetzelfde.

5.2.2 Het substitutiecijfer

Ook het substitutiecijfer is één van de klassieke handcijfers. Het eenvoudigste substitutiecijfer is de monoalfabetische substitutie. Hierbij wordt elke letter vervangen door een willekeurig andere letter.

In de oudheid heeft men gedacht dat dit cijfer onbreekbaar was vanwege de ontelbare mogelijke schikkingen van het alfabet, totdat Arabische wiskundigen in de 9e eeuw het systeem van letterfrequentie-analyse ontwikkelden. Aangezien bij substitutie elke gecodeerde letters steeds voor dezelfde klare letter staat, kan men dit cijfer gemakkelijk breken met behulp van letterfrequentie-analyse.

Elke taal heeft een typische frequentietabel van letters. Zo komen de E, N en A het meeste voor in onze taal. Als men de letterfrequenties van een cijfertekst vergelijkt met de normale waarden en ziet dat de X, P en T het meeste voorkomen, kan men besluiten dat X staat voor E, P voor N en T voor A. Hoe meer letters men zo kan vinden, hoe makkelijker de ontbrekende letters in de tekst kunnen bijeengepuzzeld worden. Hoe meer cijfertekst er ter beschikking is, hoe nauwkeuriger frequentie-analyse kan toegepast worden.

5.2.3 Het Vigenèrecijfer

Het door Giovanni Batista Belaso in 1553 uitgevonden cijfer is ook een handcijfer. Het cijfer werd echter algemeen bekend door Blaise de Vigenère waardoor het zijn naam draagt. Het werd echter lange tijd zelden gebruikt vanwege zijn complexiteit.

Deze encryptie maakt gebruik van de techniek polyalfabetische substitutie. Men vervangt letters aan de hand van verschillende alfabetische reeksen. Daarbij gebruiken we het zogenaamd Vignèretableau, een tabel waarop op iedere regel een alfabet staat waarvan elk alfabet steeds één letter verschoven is.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Men kiest eerst een geheim sleutelwoord, bijvoorbeeld `ZODIAK`. Dit schrijft men onder de klare tekst. Vervolgens zoekt men de klare letter op in het verticale alfabet en de letter van het sleutelwoord in het horizontale alfabet. De kruising van beiden is de resulterende codeletter. Zo kunnen we zien dat de kruising van `D` en `Z` in de tabel de letter `C` is.

```
Klare tekst : D I T I S Z E E R G E H E I M
Sleutelwoord: Z O D I A K Z O D I A K Z O D
              ---------------------------
Cijfertekst : C W W Q S J D S U O E R D W P
De cijfertekst: CWWQS JDSUO ERDWP
```

Om te ontcijferen schrijft men het sleutelwoord boven de cijfertekst. Vervolgens zoekt men elke sleutelletter op in het horizontale alfabet en gaat naar beneden tot men de betrokken codeletter tegenkomt. De letter, in het verticale alfabet, die zich op dezelfde rij bevindt is de klare letter.

Ook bij deze code heeft men 300 jaar lang dacht dat ze onbreekbaar was, ze kreeg zelfs de bijnaam *le chiffre indéchiffrable*. Merk op dat de letter E kan vercijferd worden als D, maar ook als Q en als E. Als het sleutelwoord 6 letters lang is kan een klare letter tot 6 verschillende coderingen hebben. Hierdoor kan de code niet gebroken worden met een eenvoudige letterfrequentie-analyse, zoals bij een enkelvoudig substitutiecijfer.

In de helft van de 19e eeuw werd er echter toch een methode gevonden om ze te breken.

Indien er voldoende cijfertekst is kan men echter de grootte van het sleutelwoord eruit afleiden door de grootst gemene deler te nemen van alle afstanden tussen veel voorkomende stukjes cijfertekst. Indien op die manier het sleutelwoord 6 letters lang blijkt, dan moet men letterfrequentie-analyse toepassen op de 6 afzonderlijke stukken van de tekst. Eén analysetekst zou dan de eerste, zevende, dertiende... letter bevatten. De tweede tekst de tweede, achtste, veertiende letter enz...

5.2.4 Het Autoclavecijfer

Een variant van het Vigenèrecijfer is het Autoclave cijfer. Hierbij maakt men gebruik van dezelfde tabel als gebruikt bij het Vigenèrecijfer.(zie supra)

Het verschil met het Vigenèrecijfer is echter dat het sleutelwoord, of in dit geval beter de sleutelzin, deze keer gevormd wordt door een kort sleutelwoord, gevolgd door volledige klare tekst. Hierdoor vercijfert men, mits een kleine verschuiving, de klare tekst met zichzelf.

In ons voorbeeld is het sleutelwoord ZODIAK. Het versleutelen gebeurd op identieke wijze als de Vigenèrevercijfering. Het sleutelwoord zodiak wordt niet meer herhaald maar gevolgd door de volledige tekst.

```
Klare tekst : D I T I S Z E E R G E H E I M . . . .
Sleutelwoord: Z O D I A K D I T I S Z E E R G E H E I M....
              ----------------------------------------
Cijfertekst : C W W Q S J H M K O W G I M D .....
De cijfertekst: CWWQS JHMKO WGIMD ..... .....
```

Om de tekst te kunnen ontcijferen dient men te beginnen met het korte sleutelwoord, om dan de ontcijferde tekst beetje bij beetje verder aan te vullen achter het sleutelwoord.

De sterkte van dit cijfer ligt erin dat niet steeds opnieuw hetzelfde sleutelwoord gebruikt is, maar de steeds variërende klare tekst. Voor de cryptoanalyse van dit cijfer zal men technieken zoals het bepalen van sleutellengte en letterfrequenties niet kunnen toepassen zoals bij de gewone Vigenèrevercijfering.

Nadeel aan deze methode is dat indien er één fout is bij het ontcijferen, de rest van de vercijfering ook fout zal zijn.

5.2.5 Het homfone substitutiecijfer

Toen de techniek van letterfrequentie-analyse op monoalfabetische substitutie algemeen bekend raakte zocht men naar een alternatief. Het homofone substitutiecijfer is een tussenoplossing die eenvoudig was, maar toch bestand tegen letterfrequentie-analyse.

Bij dit cijfer worden de letters vervangen door cijfers. Er worden 100 getallen verdeeld over de 26 letters, waarbij de meestvoorkomende letters de meeste getallen krijgen toegewezen. Als de letter E ongeveer 15 procent van de tekst vormt, geven we deze letter 15 getallen. De letter A die 7 procent voorstelt geven we dus 7 getallen. Zeldzame letters zoals de X krijgen slechts één getal. Indien we frequentie-analyse toepassen op de tekst zullen alle getallen ongeveer 1 procent vormen van de totale tekst. Merk op dat de cijfertabel dezelfde vorm heeft als de letterfrequentietabel.

Hoewel deze techniek een hele verbetering is tegenover monoalfabetische substitutie, is het breken ervan niet onmogelijk. Dit kan door anagramming toe te passen op de cijfers. Men zoekt naar typische letterparen in de taal, zoals `I` en `J` of `Q` en `U`, om de relaties met de getallen te vinden.

```
A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
-------------------------------------------------------------------------
09 42 32 10 00 56 11 34 03 04 44 12 29 05 25 72 26 01 15 06 27 28 39 61 50 17
22 68 71 31 02 94 65 43 19    64 20 45 07 36 90    14 38 16 62 51 86
67 93    41 08    81 99 53    96 35 59 13 58       24 60 48 74
70       69 18          76       95    46 63       37 87 49
78       77 21          79             52 88       47    75
83          23          85             57 98       73    89
97          30                         91          80
            33
            40
            54
            55
            66
            82
            84
            92
```

Om een tekst te vercijferen vervangen we elke letter afwisselend door één van zijn getallen.

```
Klare tekst: D  I  T  I  S  G  E  H  E  I  M
Cijfertekst: 69 19 48 03 87 65 18 43 54 19 29
De cijfertekst: 69194 80387 65184 35419 29
```

5.2.6 Het Bifid cijfer

Bifid is een handcijfer dat een combinatie van substitutie met fractionering gebruikt. Eerst wordt er een 5 X 5 matrix van letters gecreëerd, de rijen en kolommen genummerd van 1 tot 5. De matrix vullen we met het alfabet aan de hand van een sleutelwoord. In ons voorbeeld gebruiken we het sleutelwoord `NACHTBOMMENWERPER`.

```
 | 1 2 3 4 5
-+----------
1| N A C H T
2| B O M E W
3| R P D F G
4| I J K L Q
5| S U V X YZ
```

Vervolgens lezen we voor elke letter de rij en kolom af en schrijven de getallen verticaal onder de klare tekst. Zo heeft de I de waarde 41 omdat zij in rij 4 en kolom 1 staat.

```
Klare tekst: D I T I S G E H E I M
             --------------------
Rij        : 3 4 1 4 5 3 2 1 2 4 2
Kolom      : 3 1 5 1 1 5 4 4 4 1 3
```

Nu schrijven we de cijfers opnieuw, van links naar rechts en boven naar onder, in groepen van twee. Dan zetten we de nieuwe getallen terug om in letters.

```
34 14 53 21 24 23 15 11 54 44 13
F  H  V  B  E  M  T  N  X  L  C
De cijfertekst: FHVBE MTNXL C
```

Ontcijfering gebeurt door elke letter van de cijfertekst terug om te zetten in een getal aan de hand van de tabel. De getallenreeks wordt in twee verdeeld en de twee delen onder elkaar geschreven. Tenslotte zetten we elke verticale groep van twee getallen terug om in een letter met behulp van de tabel.

5.2.7 Het Trifidcijfer

Trifid is een combinatie van substitutie en fractionering gebaseerd op hetzelfde pricipe als Bifid, maar hier worden de letters gefractioneerd in drie stukken. Als voorbeeld van opvulling van het alfabet gebruiken we het sleutelwoord LEONARDO DA VINCI waarbij we de dubbele letters weglaten en aanvullen met de rest van het alfabet.

```
    1       2       3
  -----   -----   -----
1 L E O   N A R   D V I
2 C B F   G H J   K M P
3 Q S T   U W X   Y Z /
  1 2 3   1 2 3   1 2 3
```

Vervolgens lezen we voor elke letter het vierkant, de rij en kolom af en schrijven de getallen verticaal onder de klare tekst. Zo heeft de D de waarde 311, omdat zij in vierkant 3, rij 1 en kolom 1 staat. De verdere werking is identiek aan het Bifidcijfer.

5.2.8 Het Playfair-cijfer

Het **Playfair-cijfer** werd in 1854 door Sir Charles Wheatstone uitgevonden. Deze cijfermethode werd al snel overgenomen als veldcijfer door de eenvoud in gebruik en zijn veiligheid, vergeleken met substitutiecijfers en polyalfabetische substitutiecijfers.

Men stelt een vierkant op van 5 X 5. We kiezen een sleutelwoord en vullen dit in het vierkant in. De keuze van invullen speelt geen rol (spiraalgewijs, van onder naar boven, van rechts of van links), zolang beide partijen maar een invulmethode afspreken.

We gebruiken het woord `STALINGRAD`. De letters `I` en `J` worden als één letter aanzien. Duplicaten worden weggelaten.

```
S  T  A  L  I/J
N  G  R  D  B
C  E  F  H  K
M  O  P  Q  U
V  W  X  Y  Z
```

Eerst breken we de klare tekst op in bigrammen, groepen van twee letters. Indien een bigram uit twee identieke letters bestaat, voegen we een `X` tussen de tekst in. Indien er één letter overblijft, vullen we aan met een `X`. Dus voor de tekst ‘dit is een zeer geheim bericht’ krijgen we :

```
DI TI SE EN ZE ER GE HE IM BE RI CH TX
```

Nu vercijferen we per bigram. Hiervoor maken we een denkbeeldig vierkant met de letters en zoeken de letters in de tegenoverliggende hoeken. We beginnen met de tegenoverliggende letter in dezelfde rij als de eerste letter van het bigram.

```
.  .  .  L  I/J
.  .  .  D  B
.  .  .  .  .
.  .  .  .  .
.  .  .  .  .
```

Voor het vierkant `DI` is dit `BL`.

```
DI TI SE EN ZE ER GE HE IM BE RI CH TX
BL
```

Bij het volgend bigram TI liggen beide letters op dezelfde rij. We nemen dan de letters onmiddellijk rechts ervan op diezelfde rij.

```
S  T  A  .  I/J
.  .  .  .  .
.  .  .  .  .
.  .  .  .  .
.  .  .  .  .
```

Voor het trigram TI is dit dus AS.

```
DI TI SE EN ZE ER GE HE IM BE RI CH TX
BL AS TC CG WK FG
```

Bij het bigram GE liggen beide letters in dezelfde kolom. We nemen dan de letters onmiddellijk eronder op diezelfde rij.

```
.  .  .  .  .
.  G  .  .  .
.  E  .  .  .
.  O  .  .  .
.  .  .  .  .
```

Voor het trigram GE is dit dus EO.

Alle mogelijke situaties zijn nu beschreven en we kunnen alle bigrammen verder vercijferen.

```
DI TI SE EN ZE ER GE HE IM BE RI CH TX
BL AS TC CG WK FG EO KF SU GK BA EK AW
De cijfertekst: BLAST CCGWK FGEOK FSUGK BAEKA W
```

Om de cijfertekst te ontcijferen moeten we enkel het proces omkeren.

5.2.9 Het ADFGVX-cijfer

Tijdens de Eerste Wereldoorlog werd dit cijfer gebruikt door het Duitse leger. Deze 6 X 6 matrix was een uitbreiding op het ADFGX-cijfer (5 X 5 matrix), uitgevonden door kolonel Fritz Nebel. Dit cijfer combineerde fractionering van een Polybiusvierkant, dat een monoalfabetische substitutie bevat, met een enkelvoudige transpositie.

Er werd gekozen voor de letters ADFGVX omdat deze zeer duidelijk te onderscheiden zijn in morsecode.

Het ADFGVX-cijfer werd onbreekbaar geacht. Op 2 juni 1918 echter slaagde Georges Painvin, een Franse cryptoanalist, erin een eerste boodschap te ontcijferen.

Men start met het opstellen van een vierkant van 6 X 6. We kiezen een sleutelwoord en vullen dit in het vierkant in. In ons voorbeeld is het eerste sleutelwoord `NACHTBOMMENWERPER` waarbij we de dubbele letters weglaten en aanvullen met de rest van het alfabet. Om de getallen aan te vullen kunnen we deze vlak na hun letter plaatsen (1 na `A`, 2 na `B` enz...). De kolommen en rijen worden benoemd met de letters `ADFGVX`.

```
  | A D F G V X
-+------------
A| N A 1 C 3 H
D| 8 T B 2 O M
F| E 5 W R P D
G| 4 F 6 G 7 I
V| 9 J 0 K L Q
X| S U V X Y Z
```

dan zetten we de tekst om in bigrammen, bestaande uit de kop-letters van de rij en de kolom.

```
d  i  t  i  s  z  e  e  r  g  e  h  e  i  m
FX GX DD GX XA XX FA FA FG GG FA AX FA GX DX
```

Vervolgens wordt op de gefractioneerde tekst kolomstranspositie toegepast. In ons voorbeeld is het tweede sleutelwoord `PILOTEN` (in realiteit worden veel langer sleutelwoorden of zinnen gebruikt). Het sleutelwoord is genummerd volgens het alfabet. De bigrammen worden van links naar rechts en van boven naar onder ingevuld.

```
P I L O T E N
6 2 3 5 7 1 4
-------------
F X G X D D G
X X A X X F A
F A F G G G F
A A X F A G X
D X
```

Nu lezen we de tekst af volgens de nummering per kolom, en verdelen in groepen van vijf.

```
De cijfertekst: DFGGX XAAXG AFXGA FXXXG FFXFA DDXGA
```

Om de cijfertekst te ontcijferen moeten we eerst een tabel maken met het sleutelwoord en het juiste aantal kolommen. Uit het aantal letters in de cijfertekst kunnen we dan het aantal lange en korte kolommen afleiden. We vullen de tabel met de cijfertekst, kolom per kolom, in volgorde van het sleutelwoord. Vervolgens lezen we de tekst van links naar recht en boven naar onder af. De bekomen tekst splitsen we op in bigrammen. Aan de hand van het vierkant zetten we de bigrammen terug om in klare tekst.

5.2.10 Het dubbele transpositie cijfer

Het dubbele transpositie cijfer was één van de veiligste handcijfers dat door alle partijen gebruikt werd tijdens de Tweede Wereldoorlog. Belangrijk bij deze methode is dat men regelmatig van sleutelwoorden moet wisselen. De zwakke schakel bij deze cijfers is wanneer vele berichten met dezelfde sleutelwoorden vercijferd worden, deze door een ingewikkelde techniek van multiple-anagramming kunnen gebroken worden.

Het dubbele transpositie cijfer bestaat uit twee verschillende kolom-transposities. Men kan hierbij hetzelfde sleutelwoord voor beide stappen gebruiken, of twee verschillende sleutelwoorden kiezen. Men kiest best twee sleutelwoorden van verschillende lengte, het ene met even en het andere met oneven lengte. In ons voorbeeld is het eerste sleutelwoord `LEONARDO`. De letters van dit woord worden volgens alfabet genummerd, van links naar rechts. Onder dit woord schrijven we de klare tekst van links naar recht en boven naar onder.

```
L E O N A R D O
4 3 6 5 1 8 2 7
---------------
D I T I S E E N
Z E E R G E H E
I M B E R I C H
T
```

Vervolgens lezen we de tekst af per kolom, beginnende met het kleinste nummer. Kolom 1 is dus SGR, kolom 4 is DZIT. De nieuwe tekst schrijven we onder het tweede sleutelwoord DAVINCI eveneens van links naar rechts en van boven naar onder.

```
D A V I N C I
3 1 7 4 6 2 5
-------------
S G R E H C I
E M D Z I T I
R E T E B N E
H E E I
```

Tenslotte lezen we de tekst nogmaals af per kolom en volgens nummer. Daarna verdelen we in groepen van vijf.

```
De cijfertekst: GMEEC TNSER HEZEI IIEHI BRDTE
```

Normaal zullen er sleutelwoorden of zinnen gebruikt worden met een lengte van 20 of meer letters.

5.2.11 Het Straddling checkerboard cijfer

Een laatste methode die we beschrijven van de klassieke handcijfers is het straddling checkerboard cijfer. Dit cijfer is een fractionerend monoalfabetisch substitutie cijfer.

Er wordt een tabel opgesteld van 10 kolommen en 3 rijen. De eerste rij mag slechts 8 letters bevatten. Aangezien er 28 vakjes gevuld dienen te worden, kan men aanvullen met een slash (/ om begin en einde van getallen aan te geven waarbij A = 1, B = 2 enz...) en een punt.

In de bovenste rij van de tabel worden de meest voorkomende letters geplaatst. Hierdoor is het cijfer beter bestand tegen letterfrequentie-analyse door het onderdrukken van pieken in de

frequentietabel en kunnen we spreken van een homofoon cijfer. De meest voorkomende letters kan men onthouden met het woord ANTIROES(T).

We gebruiken in de eerste rij het woord ANTIROES(T) en vullen de tweede en derde rij alfabetisch aan. Vervolgens nemen we de eerste 10 letters van het sleutelwoord UBOOTJAGER en nummeren deze alfabetisch, met 0 als laatste getal.

Met de bekomen getallen nummeren we de kolommen van de tabel. De getallen die in de eerste rij geen letter hebben worden ook gebruikt om de tweede en derde rij te nummeren.

```
U B O O T J A G E R
0 2 6 7 9 5 1 4 3 8

 |0 2 6 7 9 5 1 4 3 8
-+--------------------
 |A N T I R O E S
3|B C D F G H J K L M
8|P Q U V W X Y Z . /
```

Als bijkomende veiligheid kunnen we eventueel de tweede en derde rij laten verschuiven volgens het getal van die rij. De tweede rij, met het getal 3, zou dan "K L M B C D F G H J" worden en de derde rij zouden we dan 8 plaatsen verschuiven naar "U V W X Y Z . / P Q".

De vercijfering gebeurt door omzetting van de letters naar de getallen van de rij en kolom. Voor de letters in de bovenste rij wordt echter het getal erboven genomen. Zo krijgt in ons voorbeeld de letter D de getallen 36 en krijgt de letter T enkel het getal 6.

```
Klare tekst: D  I  T  I  S  Z  E  E  R  G  E  H  E  I  M
Cijfertekst: 36 37 6  37 4  84 1  1  9  39 1  35 1  7  38
```

Aangezien onbestaande combinaties niet kunnen gevormd worden bij ontcijfering, kunnen alle getallen samengevoegd worden. Zo kan in ons voorbeeld 36376... de eerste 3 niet alleen gebruikt worden en moet dus wel aan de 6 gekoppeld worden. De volgende twee getallen, 3 en 7, zijn dus ook een paar. Het volgende getal 6 is een alleenstaand getal want er is geen rij met het nummer 6. Het is deze voor Straddling Checkerboard typische onregelmatige nummering die cryptoanalyse bemoeilijkt.

```
De cijfertekst: 36376 37484 11939 13517 38
```

Eventueel zal men het resultaat van deze vercijfering bijkomend vercijferen zoals met een dubbele transpositie, uitgevoerd op de getallenrij. Dit verhoogt de sterkte van het cijfer aanzienlijk.

Het VIC cijfer is een beroemde variant op dit cijfer. Bij dit cijfer initialiseert het sleutelwoord een LFG (Lagged Fibonacci Generator). De gegenereerde getallenreeks wordt gebruikt om eerst een gewone en daarna een onderbroken transpositie te nummeren.

5.3 Symmetrische Blok Cijfers

Dit deel schetst in het kort enkele belangrijke symmetrische blokcijfers. Zo hebben we DES (1977), IDEA (1992), RC5 (1995), RC6 (1996), en AES. Deze laatste zal snel gaan gebruikt worden in plaats van DES en RC6.

5.3.1 Data Encryption Standard (DES)

De firma IBM initieerde eind jaren ’60 het Lucifer onderzoeksproject, geleid door Horst Feistel. Dit project werd beëindigd in 1971 en LUCIFER was eerst gekend als een blok cijfer dat gebruikt maakte van 64 bits, met een sleutellengte van 128 bits. DES (Data Encryption Standard) is gebaseerd op het algoritme Lucifer van de firma IBM, en is in 1977 tot standaard verheven *(Stallings, 2000)*. DES werkt in de basisvorm met een sleutellengte van 56 bits (sleutels van 64 bits, maar elke 8e bit wordt gebruikt ter controle = pariteitbits). Dat betekent dus dat er $2^{64-8} = 2^{56} = 72057594037927936$ mogelijke sleutels zijn.

In 1995 echter is gebleken dat DES in de oorspronkelijke vorm niet meer betrouwbaar en veilig is en dat het op termijn zou vervangen worden door AES. Desalniettemin heeft DES toch 20 jaar goed overleefd en was het de wereldwijde standaard voor 18 jaar.

DES is nu een basisch veiligheidssysteem, gebruikt in bedrijven over de hele wereld. Daarom is het zeer waarschijnlijk dat DES zijn taak om netwerkcommunicatie, dataopslag en paswoord en toegangscontrole zal blijven verder zetten.

DES werkt niet met optellen of aftrekken, maar met XOR(N), de exclusieve OR functie. De XOR van twee waardes is 1 als precies 1 van beiden gelijk is aan 1. Wanneer beiden gelijk zijn aan 0 of beiden gelijk zijn aan 1 is de XOR van deze twee waarden 0. *(Rhee, 2003)*

Feistel-netwerk

DES is een algoritme dat gebruik maakt van een zogenaamd "Feistel Netwerk". DES werkt in zestien rondes waarbij in elke ronde de 64 bits gesplitst worden in een linkerhelft en rechterhelft van 32 bits. Daarna worden de rechterhelft onveranderd naar links gebracht, die komen in de volgende ronde aan de beurt. De 32 bits aan de linkerkant (L_{i-1}) worden opgeteld bij de 32 outputbits van een functie f. De eerste outputbit van L_{i-1}wordt modulo 2 opgeteld bij de eerste outputbit van f, de tweede bij de tweede outputbit van f, etc. De f-functie is een vaste functie voor alle rondes. Hiervoor wordt als invoer R_{i-1} en een gedeelte van de sleutel gebruikt. Voor decryptie wordt gewoon de volgorde omgekeerd, vermits $L_i = R_{i-1}$ en $R_i = L_i \otimes f(R_{i-1}, K_i)$

Lawine-effect

Een wenselijke eigenschap van elk encryptiealgoritme is dat een kleine verandering in de platte tekst of de sleutel een grote wijziging in de cijfertekst veroorzaakt. Dit noemt men het lawine-effect. DES vertoont een sterk lawine-effect. *(Stallings, 2000)*

Kraken

Nadeel van de basisversie van DES is, dat bij dezelfde sleutel er bij dezelfde invoer altijd dezelfde uitvoer verschijnt. En aangezien er steeds in blokken van 64 bits wordt gewerkt, kan men dus blokken van 64 bits overschrijven met een ander blok van 64 bits, zodat een deel van de boodschap wordt herhaald. DES is vanaf het begin door een grote groep deskundigen

gewantrouwd. Lucifer, waarop DES is gebaseerd, werkte met sleutels van 128 bit lengte. DES werd uiteindelijk als standaard voorzien van sleutels van slechts 56 bits lengte. De NSA (National Security Agency) heeft hierin de hand gehad, waarschijnlijk om ervoor te zorgen dat DES code voor de Amerikaanse overheid te kraken bleef. *(http://nl.wikipedia.org/wiki/-Data_Encryption_Standard)*

Kraken van standaard DES is dus lang niet onhaalbaar, zeker niet voor een overheid. Ook is het combineren van rekenkracht eenvoudig te realiseren, zeker als argeloze burgers mee willen werken om hun PC mee te laten doen. Dit type bedreiging staat wel bekend als de Chinese Loterij. Het idee is als volgt. Voor kraken met brute kracht is een hoop rekenkracht nodig, en aangezien geen gebruik wordt gemaakt van enige structuur in de te kraken sleutel is een manier om dat te doen het parallel uitproberen van random gokken. Als je dus maar heel veel parallelle rekenmachines hebt die allemaal een willekeurig pogingen wagen, dan loop je een aardige kans de sleutel te kraken, zonder dat coördinatie tussen de rekenmachines vereist is. *(http://nl.wikipedia.org/wiki/Data_Encryption_Standard)*

3DES

Om de sleutellengte en daarmee (waarschijnlijk) ook de veiligheid van DES te vergroten, heeft men een schakeling bedacht waarbij drie DES algoritmes achter elkaar zijn geschakeld. Dit wordt 3DES, of Triple DES, genoemd. Hierbij worden 3 afzonderlijke DES bewerkingen achtereenvolgens op de te vercijferen data losgelaten. Men doet dit ofwel met behulp van twee sleutels van 56 bits waarbij de eerste en derde bewerking met dezelfde sleutel worden uitgevoerd, ofwel gebruikt men drie sleutels van 56 bits. Dit brengt de totale sleutellengte voor codering op respectievelijk 112 bits of 168 bits, waarvan de laatste uiteraard de veiligste vorm is. Net als bij DES is decryptie het omgekeerde van encryptie. Men encrypteert met driemaal DES-encryptie met sleutels A, B, C en men decrypteert met driemaal DES-decryptie met sleutels C, B, A.

5.3.2 International Data Encryption Algorithm (IDEA)

In 1990 ontwikkelde Lai en Massey van het Zwitsers Federaal Instituut van de Technologie een nieuw blok cijfer. De originele naam was Proposed Encryption Standard (PES). Men is nadien nog bezig geweest om het cijfer te versterken en zo bereikt men in 1992 een sterk cijfer wat men hernoemde naar International Data Encryption Algorithm. IDEA is een blok cijfer dat gebruikt maakt van een sleutel van 128 bits om datablokken van 64 bits te encrypteren.

Pretty Good Privacy (PGP) is een dienst die authenticatie en privacy aanbied voor mail, bestandopslag en andere toepassingen. PGP is gebaseerd op IDEA voor conventionele encryptie en maakt gebruik van RSA voor public-key encryptie met MD5 voor hash codering.

Voordeel bij IDEA is dat de 128-bit sleutellengte lang genoeg is om te voorkomen dat men de volledige lijst sleutels kan generen. De 64-bit input blok grootte is algemeen erkent als sterk genoeg, zoals reeds ondervonden bij DES. Het vercijferingsproces van IDEA is redelijk complex. Er worden drie operaties gebruikt, elke operatie wordt gedaan op twee 16-bit inputs om hier een enkele 16-bit output mee te genereren. De IDEA structuur kan zowel gebruikt worden voor encryptie als voor decryptie, net zoals DES. *(Rhee, 2003)*

5.3.3 RC5

RC5, ontwikkeld door Ronald Rivest van het Massachusetts Institute of Technology (MIT), zag het daglicht in 1994. Er wordt verwacht door onder andere RSA Data Security, Inc. dat RC5 en zijn opvolger RC6 het potentieel hebben de opvolgers te zijn voor DES.

Het RC5 cijfer is een symmetrisch blok cijfer ontwikkeld voor zowel software als hardware gebruik. Het is een geparametriseerd algoritme met een variabele blok grootte, een variabel aantal iteraties en een variabele sleutellengte. Uiteraard verhogen deze kenmerken de flexibiliteit op het gebied van prestaties en mate van veiligheid van het cijfer.

De typische benaming van een RC5 algoritme is RC5-*w/r/b*:

- *w = woordlengte in bits (standaard 32 bits, mogelijk 16, 32, 64)*
- *r = aantal iteraties (0,1,…,255)*
- *b = aantal bytes in de geheime sleutel K (0,1,…,255)*
- *K = b-byte geheime sleutel (K[0], K[1], …, K[b-1])*

RC5 bestaat uit 3 componenten: een sleutel uitbreiding, een encryptie algoritme en een decryptie algoritme. Deze algoritmes gebruiken 3 primitieve operaties:

- + : Optelling van woorden modulo 2^w
- ⊕ : XOR van woorden
- <<< = Rotatie symbool : Rotaties van *x* naar links met *y* bits wordt genoteerd als *x*<<<*y*

Voorbeeld : Gegeven RC5-32/16/10. Dit algoritme heeft een woordlengte van 32 bits, 16 iteraties, een 10-byte (80-bit) geheime sleutel variabele en een uitgebreide sleutel tabel S van t = 2(r + 1) = 34 woorden. Rivest stelde voor om het RC5-32/12/16 algoritme te gebruiken (normale keuze van parameters).

Een voordeel van RC5 is zijn simpliciteit. Hierdoor is het makkelijk RC5 te implementeren. Bovendien is RC5 door het vele gebruik van data-afhankelijke rotaties tijdens de encryptie veilig tegen zowel differentiële als lineaire crypto-analyse. *(Rhee, 2003)*

5.3.4 RC6

Om tegemoet te komen aan de vereiste in prestaties en veiligheid werd RC5 verbeterd tot RC6. Ook RC6 maakt gebruik van data-afhankelijke rotaties. Een nieuwigheid bij RC6 is het gebruik van vier werk registers in plaats van slechts twee. RC6 zal dus vier 32-bit registers in de plaats van twee 64-bit registers gebruiken om de 128-bit blokken te bewerken. Het voordeel hierbij is dat er twee rotaties per iteratie kunnen worden gedaan in plaats van één bij

RC5. RC6 was één van de kandidaten waaruit NIST de nieuwe Advanced Encryption Standard (AES) zou kiezen.

Net als RC5 wordt RC6 gespecificeerd als RC6-*w/r/b*. RC6-*w/r/b* werkt op *w*-bit woorden waarbij gebruik gemaakt wordt van de volgende 6 basis operaties:

- a + b : Integere optelling modulo 2^w
- a – b : Integere aftrekking modulo 2^w
- a ⊕ b : XOR van *w*-bit woorden
- a<<<b : Roteer het w-bit woord a naar links met de minst significante lg w bits van b
- a>>>b : Roteer het w-bit woord a naar rechts met de minst significante lg w bits van b
- $lg = \log_2 w$

Door het gebruik van de 32-bit registers is RC6 veel sneller dan RC5. *(Rhee, 2003)*

5.3.5 AES (Rijndael) algoritme

De Advanced Encryption Standard (AES) is het resultaat van meerdere jaren evaluatie door het NIST (National Institute of Standards and Technology) van allerlei algoritmes inzake blokvercijfering. Verschillende grote kandidaten, zoals IBM en RSA Security stuurden hun algoritmen in. Op 2 oktober 2000 werd de winnaar bekend gemaakt: Rijndael van Daemen en Rijmen. Hun algoritme is gekozen vanwege de combinatie van veiligheid, prestatie, efficiëntie, eenvoud en flexibiliteit.

AES is een subset van het Rijndael-algoritme waarbij de sleutels altijd 128-bit zijn en de blokgrootten beperkt zijn tot 128, 192 of 256 bytes. Rijndael zelf kan alle blokgrootten en sleutels aan die een veelvoud zijn van 32-bit met een minimum van 128-bit en een maximum van 256-bit.

Verscheidene populaire softwareprogramma's zoals WinRAR, WinZip, PowerArchiver, etc. gebruiken AES voor eventuele encryptie .

Onderstaande tabel geeft een kort overzicht van de eigenschappen van drie populaire blokcijfers. Hieruit blijkt duidelijk dat AES superieur is.

Tabel 3 : Vergelijking van DES, 3DES en AES *(PANKO, 2005)*

	DES	3DES	AES
Sleutellengte (bits)	56	112 or 168	128, 192, or 256
Sterkte	Zwak	Sterk	Sterk tot zeer sterk
Verwerkingsvereisten	Gemiddeld	Hoog	Bescheiden
RAM Vereisten	Gemiddeld	Hoog	Bescheiden

5.4 Asymmetrische public-key cryptosystemen

Zoals in paragraaf 2.5.2 staat uitgelegd werkt asymmetrische encryptie met twee verschillende sleutels, een private (geheime) en een publieke (aan iedereen bekent). Public-key crytografie werd al snel populair nadat Whitefield Diffie en Martin Hellman in 1976 een innovatief concept lanceerde over een exponentieel sleuteluitwisseling schema. Sindsdien zijn er heel veel public-key algoritmes ontworpen, maar vele hiervan zijn reeds gebroken. Van de vele algoritmes die op dit moment nog als veilig worden aanzien zijn er helaas vele onpraktisch.

Slechts enkele public-key algoritmes blijken veilig en praktisch, en van deze algoritmes zijn er slechts enkele geschikt voor encryptie. Andere zijn enkel geschikt voor digitale handtekeningen. De ontwerper moet rekening houden dat de veiligheid van een encryptieschema afhankelijk is van de lengte van de sleutel en de verwerkingsvereisten om een cijfer te breken. Van de vele algoritmes zijn er slechts vier die zowel geschikt zijn voor encryptie als de digitale handtekening namelijk RSA, ElGamal, Schnorr en ECC. DSA is een algoritme dat enkel geschikt is voor digitale handtekeningen

De Diffie-Hellman exponentiele sleuteluitwisseling is oorspronkelijk bedoeld om twee partijen de mogelijkheid te bieden over een onbeveiligd kanaal een geheime encryptiesleutel te

laten uitwisselen die later kan gebruikt worden ter encryptie van het bericht. Onder andere het RSA algoritme is gebaseerd op dit systeem.

5.4.1 Sleuteldistributie Diffie-Hellman

Het sleuteldistributiesysteem van Diffie en Hellman was een antwoord op een belangrijke onderzoeksvraag binnen private-key cryptografie: de distributie van de geheime sleutel.

In private-key cryptografie moeten Alice en Bob voor ze kunnen communiceren eerst een sleutel overeenkomen, omdat deze voor codering en ontcijfering gelijk is. Een van de grote problemen bij het gebruik van een private-key cryptosysteem is de distributie van die sleutel. Om geheimhouding te garanderen moet de sleutel over een veilig kanaal worden verzonden. Je zou echter liever gebruik willen kunnen maken van een onveilig kanaal om een sleutel overeen te komen. Diffie en Hellman doen in hun artikel een voorstel voor zo'n distributiesysteem, gebaseerd op de discrete logaritme in de multiplicatieve groep F_p met p priem. Hun voorstel was een verbetering van een al bestaand distributiesysteem van Merkle. Het systeem gaat uit van de groep F_p met p priem en een voortbrenger α. Alice genereert een random getal x_A uniform gekozen uit het interval [1; p⇔1]. Ze houdt x_A geheim, maar plaatst

$$y_A = \alpha^{x_A} \bmod p$$

in het publieke domein. Bob doet hetzelfde en genereert x_B en plaatst $y_B = \alpha^{x_B} \bmod p$ in het publieke domein. Als ze nu willen communiceren fungeert

$$K_{AB} = \alpha^{x_A x_B} \bmod p$$

als hun geheime sleutel. Alice en Bob kunnen beiden deze sleutel eenvoudig construeren met behulp van hun eigen geheime sleutel en de informatie van de ander in het publieke domein. Alice berekent bijvoorbeeld

$$K_{AB} = y_B{}^{x_A} \bmod p = (\alpha^{x_B})^{x_A} \bmod p = (\alpha^{x_A})^{x_B} \bmod p$$

Eve, die alleen y_A en y_B tot haar beschikking heeft, kan K_{AB} alleen construeren door bijvoorbeeld

$$K_{AB} = y_A{}^{\log_\alpha y_B} \bmod p$$

te berekenen, waarvoor ze de discrete logaritme $\log_\alpha y_B$ op moet lossen wat praktisch niet gaat in een redelijke tijd. *(Wilschut, D.E., 2000)*

5.4.2 Het RSA algoritme

RSA is een asymmetrisch encryptiealgoritme. De RSA-methode is eind jaren zeventig uitgevonden door Rivest, Shamir en Adleman. De methode is genoemd naar de eerste letters van hun namen.

RSA is een zogeheten 'public key-methode', een methode waarbij het niet nodig is om de encryptiemethode geheim te houden en waarbij er een sleutel is die openbaar gemaakt wordt. Versleutelen gebeurt met andere woorden met een andere sleutel als ontsleutelen, vandaar asymmetrische encryptie.

De veiligheid van RSA steunt op het probleem van de ontbinding in factoren (bij heel grote getallen): op dit moment is het bijna onmogelijk de twee oorspronkelijke priemgetallen *p* en *q* te achterhalen als alleen *n= p*q* bekend is en *p* en *q* groot genoeg zijn; het zou te veel tijd in beslag nemen. Nieuwe ontwikkelingen op dit gebied zouden RSA onbruikbaar kunnen maken. *(Stinson, 2006)*

Werking RSA

Tabel 4 : Beknopt schema over werking RSA

Het RSA cryptosysteem	
Berekeningen in: $\mathbb{Z}_n$, voor samengestelde n.	Procedure voor sleutelgeneratie: 1. Kies priemgetallen p en q. 2. Bereken $n = p.q$ en $\phi(n)$. 3. Neem $e \in \mathbb{Z}^*_{\phi(n)}$. 4. Bereken $d = e^{-1}$ in $\mathbb{Z}^*_{\phi(n)}$. Publieke sleutel: (n, e) Geheime sleutel: (n, d).
Encryptie van x: $y = x^e$.	Decryptie van y: $x' = y^d$.

→ $\phi(n) = (p-1)(q-1)$

→ e geen factor gemeen met $\phi(n)$

→ d vindt men met het uitgebreide Euclidische algoritme

Het getal e noemt men de vercijferingsexponent, het getal d de ontcijferingsexponent. Encryptie gebeurt door exponentiatie met de publiek bekende e exponent en de bekende modulus n. Het inverteren van de berekening kan enkel met kennis van p en q worden gedaan, maar meestal worden de factoren alleen bij het generen van de sleutel gebruikt. Er wordt dan een speciale exponent d berekend die exponentiatie met e voor alle waarden van x ongedaan maakt. Dit omdat $e.d = 1 \bmod \phi(n)$, voor alle x:

$$(x^e)^d = x^{(e.d)} = x^1 = x$$

Op de volgende pagina leggen we de werking van RSA nogmaals uit aan de hand van een concreet getallen voorbeeld.

Voorbeeld *(http://members.home.nl/cryptonet/rsa/content.htm)*

Voorbereiding:

Stap 1:

Kies 2 verschillende priemgetallen *p* en *q*

$p = 103$ en $q = 317$

Deze moeten in het echt veel groter zijn, maar dit is een makkelijker voorbeeld.

Stap 2:

Reken getal n uit, n = p*q

In dit geval $n = 103*317 = 32651$

Stap 3:

Reken getal $\phi(n)$ uit, $\phi(n) = (p-1)(q-1)$

In dit geval $\phi(n) = 102*316 = 32232$

Stap 4:

Kies een getal *e* uit, zo dat GGD (e, $\phi(n)$) = 1 (oftewel *e* heeft geen delers gemeen met $\phi(n)$)

Van 55 zijn alleen 5 en 11 delers, 32232 is niet deelbaar door 5 of 11.

Controle met het algoritme van Euclides.

32232 = 55 * 586 + 2

55 = 27 * 2 + 1

2 = 2 * 1

$e = 55$

Stap 5:

Reken *d* uit, zo dat $e*d = 1 \pmod{\phi(n)}$

Dus $e * d = a.\phi(n) + 1$

Hiervoor gebruiken we het uitgebreide algoritme van Euclides. Bekijken we het rijtje dat we net hebben uitgeschreven. Uit de een na onderste regel blijkt dat:

$1 = 55 - (2 * 27)$

uit de bovenste dat:

$2 = 32232 - (55 * 586)$

$= -(55 * 586) \bmod 32232$

dus: $1 = 55 - (-(55 * 586) * 27) \bmod 32232$

$= 55 + (55 * 586 * 27) \bmod 32232$

$= 55 * (586 * 27 + 1) \bmod 32232$

dus: $1 = 55 * 15823 \pmod{\phi(n)}$

$\boxed{d = 15823}$

Stap 6: Maak de getallen $n = 32651$ en $e = 55$ bekend. Iemand anders kan nu berichten coderen en aan jou sturen.

Coderen:

Stap 7:

Het bericht is 'BasJan', omgezet in cijfers (volgens a = 01, z = 26) is dit x = 020119100114

Dit moet worden opgesplitst in meerdere berichten omdat onze m slechts 5 cijfers lang is.

x1 = 0201, x2 = 1910, x3 =0114

We gaan nu alleen x1 coderen.

Stap 8:

Dit coderen gaat volgens de formule:

$\boxed{y = x^e \bmod n}$

$y = 201^{55} \bmod 32651$ probleem!, 201^{55} valt al niet direct uit te rekenen met een computer, laat staan grotere getallen.

$\rightarrow$55 is binair geschreven 110111, dus $55 = 2^0 + 2^1 + 2^2 + 2^4 + 2^5$

$a^p * a^q = a^{p+q}$ dus $201^{55} = 201^1 * 201^2 * 201^4 * 201^{16} * 201^{32}$

Nu kunnen we een tabel maken, en telkens kwadrateren, en de uitkomsten modulo 32651 reduceren.

Tabel 5 : Berekening van x_1^k (mod n)

Hulptabel voor het berekenen van x_1^k *(mod n)* met x_1 *=201 ; k = 1, 2, 4, 8, 16, 32 ; n = 32651*						
k =	1	2	4	8	16	*32*
x_1^k *(mod n) =*	*201*	*7750*	*17311*	*32494*	*24649*	*3393*

Hieruit nemen we de benodigde getallen (201^8 niet omdat $201^{55} = 201^1 * 201^2 * 201^4 * 201^{16} * 201^{32}$).

201 * 7750 = 23153 (mod 32651)
23153 * 17311 = 10558 (mod 32651)
10558 * 24649 = 15672 (mod 32651)
15651 * 3393 = 19268 (mod 32651)
$201^{55} = 19268$ (mod 32651) $\rightarrow$ $y = 19268$

Decoderen:

Het gecodeerde bericht is y = 19268. Om dit bericht te decoderen moet de ontvanger in het bezit zijn van de ontcijferingexponent d. Ontcijfering gebeurt door y tot de macht d te verheffen modulo n. Dan moet er weer hetzelfde uitkomen, dit zou dus betekenen dat $y^d = (x^e)^d = x^{ed} = x$ (mod n)

Het getal 19268^{15823} valt echter moeilijk uit te rekenen. Hier gebruikt men weer dezelfde methode als bij het coderen.
Het getal 15823 wordt binair geschreven 11110111001111, dus $2^0 + 2^1 + 2^2 + 2^3 + 2^6 + 2^7 + 2^8 + 2^{10} + 2^{11} + 2^{12} + 2^{13}$
19268^{15823} is dus $19268^1 * 19268^2 * 19268^4 *$ enz. Ook nu kunnen we weer een tabel maken, telkens kwadrateren, en de uitkomsten modulo 32651 reduceren.

Tabel 6 :Berekening van y^k (mod n)

Hulptabel voor het berekenen van y^k (mod n)*met* y = 19268 ; k = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192 ; n = 32651						
k =	1	2	4	8	64	*128*
y^k *(mod n) =*	*19268*	*13954*	*16203*	*23169*	*6072*	6205
k =	256	1024	2048	4096	8192	/
y^k (mod n) =	6496	19911	32130	10233	2532	/

19268 * 13954 = 17338 (mod 32651)

17338 * 16203 = 31061 (mod 32651)

31061 * 23169 = 24269 (mod 32651)

24269 * 6072 = 7405 (mod 32651)

7405 * 6205 = 8068 (mod 32651)

8068 * 6496 = 4873 (mod 32651)

4873 * 19911 = 20182 (mod 32651)

20182 * 32130 = 31451 (mod 32651)

31451 * 10233 = 29827 (mod 32651)

29827 * 2532 = 201 (mod 32651)

$\boxed{19268^{15823} = 201 \text{ (mod } 32651)} \rightarrow \boxed{x = 201}$

Het bericht *y* is dus gedecodeerd tot het oorspronkelijke bericht x_1, namelijk 201 oftewel 0201 = 'BA' het stukje woord dat we gecodeerd hadden.

Kraken

Het kraken van RSA is erg lastig als je het geheime getal d niet weet. Dat komt omdat als iemand de y ontvangt van $x^e = y \text{ (mod } n)$ hij niet weet tot welke macht hij het moet verheffen om weer x te krijgen. De kraker kan verschillende dingen proberen:

→ Hij kan proberen om verschillende getallen voor het encoderingsgetal d in te vullen en kijken of er een zinnig bericht uitkomt. Oftewel, y^1 mod n, y^2 mod n, y^3 mod n, enz. Hiervoor moeten een heleboel getallen worden geprobeerd en telkens worden gecontroleerd of er iets

zinnigs uitkomt. Dit kost te veel tijd en er kan niet eens met zekerheid worden gezegd welk bericht het juiste is, omdat er een heleboel berichten te voorschijn komen, zo'n 10^{250}, als er gewerkt wordt met een modulogetal van 500 cijfers, waarvan er vast een redelijk aantal berichten tussen zitten die geen complete onzin zijn.

→ Hij kan proberen de bewerking terug te draaien. Hij moet hiervoor gaan worteltrekken, de e-ste machtswortel uit y. Dit wil helemaal niet want het is niet mogelijk om bijv. de $239578256723295648025608256086086^{e}$ machtswortel te trekken en al helemaal niet omdat hij niet weet hoe vaak hij m bij y moet optellen om het getal te krijgen voordat het modulo m gereduceerd was. Dit valt dus helemaal af.

→ Hij kan proberen om de bewerking na te doen. Dus net zolang zelf getallen voor x bedenken en machtsverheffen met e modulo m totdat er y uitkomt. Dit kan op zich wel, maar het duurt erg lang, zeker als het een wat groter bericht is. Er kunnen met een modulo getal van 500 cijfers zo'n 10^{499} verschillende berichten worden gecodeerd. Een bericht dat, als er 3 cijfers voor een letter of teken worden gebruikt, slechts 166 tekens bevat. Een langer bericht is opgesplitst in meerdere stukken die allemaal apart gedecodeerd moeten worden op deze manier. Om één stuk bericht te decoderen moeten al gemiddeld (10^{499}) / 2 x-en worden geprobeerd, iets wat niet te doen is. Met een miljard computers, moeten zo'n 10^{480} berekeningen per seconde worden uitgevoerd om het bericht binnen een eeuw te kraken. Deze methode valt dus ook af.

→ Hij kan proberen om d uit te rekenen met behulp van m en e. Hier heeft hij wel eerst p en q nodig, om hiermee $\phi(n)$, en daarmee d uit te rekenen. Als p en q eenmaal bekent zijn, dan is het niet zo moeilijk meer, dan kan hij dezelfde stappen volgen als degene die de sleutels heeft gemaakt. Het probleem is echter om p en q uit te rekenen. Hiervoor moet m gefactoriseerd worden in de twee priemgetallen. Dit is lastig. Bijvoorbeeld 17 * 23 = 391, het is echter wat lastiger om uit te vinden van welke twee priemgetallen 391 het product is. Behalve dat dit de enige methode is om RSA binnen enigszins normale tijd te kraken zit er nog een voordeel aan. Met het decodeergetal d, kun je alle berichten ontcijferen die aan een persoon worden gestuurd. Er zit weinig anders op dan n/2, n/3, n/5, n/7 enz. uit te rekenen totdat er een heel

(priem)getal uitkomt, maar hier zijn nog betere methodes voor te vinden. *(http://members.home.nl/cryptonet/rsa/content.htm)*

5.4.3 ElGamal

Het ElGamal algoritme dateert van 1985. Het algoritme kan zowel voor encryptie als voor digitale handtekeningen gebruikt worden. De veiligheid van het ElGamal algoritme wordt gewaarborgd door de moeilijkheid in het berekenen van discrete logaritmes over het Galois Field GF(p) waarbij p een groot priemgetal is. Deze priemfactorisatie en discrete logaritmes worden ook gebruikt bij RSA. *(Wilschut, D.E., 2000)*

ElGamal public-key systeem

ElGamal baseert zijn public-key systeem op het hierboven beschreven public-key distributiesysteem van Diffie en Hellman. Hij neemt aan dat Alice en Bob ieder een geheime en een publieke sleutel hebben ontwikkeld.

Stel Alice wil Bob een boodschap m zenden, $0 \leq m \leq p \Leftrightarrow 1$ (ElGamal neemt niet aan dat p priem is; hij eist alleen dat p-1, de orde van de groep, tenminste 1 grote priemfactor heeft). Vervolgens kiest Alice een random getal k tussen $0 < k < p \Leftrightarrow 1$. Alice berekent de sleutel

$$K = y_B^k \bmod p$$

De gecodeerde boodschap is nu het getallenpaar (c1; c2) met

$$c_1 = \alpha^k \bmod p \qquad ; \qquad c_2 = K \,.m \bmod p:$$

De vermenigvuldiging in c_2 kan worden vervangen door ieder andere inverteerbare bewerking, of een combinatie daarvan, zoals optelling modulo p.

Bob ontcijfert het bericht nu als volgt. Eerst berekent hij K uit c1. K was $y_B^k \bmod p$ dus

$$
\begin{aligned}
& c_1^{\,x_B} \bmod p \\
&= (\alpha^k)^{x_B} \bmod p \\
&= (a^{x_B})^k \bmod p \quad c_1{}^{xB} \bmod p = (\alpha^k)^{xB} \bmod p \\
&= y_B^k \bmod p \\
&= K
\end{aligned}
$$

Vervolgens deelt Bob c_2 door K en vindt hij de boodschap m. Het kraken van dit systeem is hetzelfde als het kraken van Diffie-Hellman distributie: om K uit te rekenen moet Eve k kennen en die kan alleen worden berekend uit $c1 = \alpha^k \bmod p$.

ElGamal's digitale handtekeningen-algoritme

Dit algoritme werkt in de groep F_p met voorbrenger α. De boodschap m ligt weer tussen 0 en p $\Leftrightarrow$1. In het publieke domein staan nog altijd de sleutels y_A en y_B van Alice en Bob.

Om een document te tekenen is het noodzakelijk dat Alice haar private sleutel x_A kan gebruiken om een handtekening voor m te creëren zodat alle gebruikers de authenticiteit van de handtekening kunnen controleren gebruik makend van haar publieke sleutel y_A en niemand mag haar handtekening kunnen gebruiken zonder kennis van de private sleutel x_A

Een handtekening is bij ElGamal een getallenpaar (r; s), $0 \leq r; s < p \Leftrightarrow 1$, dat voldoet aan de Vergelijking

$$\alpha^m = y^r r^s \bmod p;$$

waar y de publieke sleutel van Alice is. Als Alice nu een boodschap wil signeren kiest ze een random getal k, $0 < k \leq p \Leftrightarrow 1$, ggd(k; p $\Leftrightarrow$ 1) = 1 en berekent

$$r = \alpha^k \bmod p.$$

De eerste vergelijking kan nu als volgt worden herschreven

$$\alpha^m = \alpha^{xr}\ \alpha^{ks} \bmod p$$

met x de geheime sleutel van Alice. Deze vergelijking geeft een oplossing s via

$$m = xr + ks \bmod p \Leftrightarrow 1;$$

waar p⇔1 de orde van α is. Nota bene, dit kan alleen als k en p⇔1 inderdaad copriem zijn, zoals bij de keuze van k werd geëist.

Alice stuurt Bob nu haar boodschap m en haar handtekening (r; s). Als Bob deze handtekening wil verifiëren gaat hij als volgt te werk. Hij gebruikt de relatie

$$\alpha^m = y^r r^s \bmod p.$$

Hij berekent α^m en kijkt of dit gelijk is aan $y^r r^s$ = mod p. Alleen als deze twee gelijk zijn, accepteert Bob de handtekening.

5.4.4 Schnorr public-key cryptosysteem

In 1990 introduceerde Schnorr zijn authenticatie- en handtekeningschema. Net als bij ElGamal wordt de veiligheid van het algoritme gewaarborgd door de moeilijkheid in het berekenen van discrete logaritmes.

Het authenticatie-algoritme van Schnorr

Voorbereiding:
Kies twee priemgetallen, *p* en *q*, met *q* een priemfactor van *p-1*
Kies *a* zodat $a^q = 1 (mod\ p)$

Sleutelgeneratie:
Kies een willekeurig getal $s < q$ (private sleutel)
Bereken $\lambda = a^{-s} \pmod p$ (publieke sleutel)

Bij authenticatie van A door B:
Persoon A kiest een willekeurig getal $r < q$ en berekent $x = a^r \pmod p$. Hierna kiest persoon B een willekeurig getal t met $0 < t < 2^v - 1$ en zendt dit getal naar persoon A. Vervolgens berekent persoon A het getal $y = r + st \pmod q$ en zendt dit naar persoon B. Persoon B verifieert nu of $x = a^y \lambda^t \pmod p$.

Schnorr's digitale handtekeningen- algoritme

De voorbereiding en sleutelgeneratie gebeuren op dezelfde wijze dan daarnet. Verder 'hashed' de afzender de te ondertekenen boodschap samen met x met behulp van het Secure Hash Algorithm (SHA). De bekomen hash = h stuurt men samen met y naar de ontvanger. De ontvanger berekent op zijn beurt $z = a^y \lambda^h \pmod p$. Deze z linkt hij aan de boodschap m en het geheel 'hashed' hij met dezelfde hash-functie als de afzender. Wanneer deze hash (=h') gelijk is aan de meegezonden hash (=h) dan kan de ontvanger de handtekening als echt accepteren.

5.4.5 Digital Signature Algorithm (DSA)

In 1991 heeft NIST het DSA voorgesteld om te gebruiken bij federale toepassingen als digitale handtekening. Deze nieuwe Digital Signature Standard (DSS) maakt gebruik van een public-key handtekening schema om ervoor te zorgen dat de integriteit van de boodschap behouden wordt en de identiteit van de verzender met zekerheid is vastgelegd.

De sleutelgeneratie onder DSA is sneller dan RSA. De handtekeninggeneratie heeft dezelfde snelheid bij de twee, maar de handtekeningverificatie is veel trager dan RSA. Vele bedrijven die al een licentie hadden voor het RSA algoritme protesteerde tegen deze nieuwe standaard.

DSA is gebaseerd op de moeilijkheid in het berekenen van discrete logaritmes, en vindt zijn oorsprong in de schema's van ElGamal en Schnorr. Kies een q van een 160-bit priem getal en

kies een priemgetal p met 512 < p < 1024 bits zodat q een priemfactor is van (p–1). Kies vervolgens g > 1 van de vorm $h'^{(p-1)/q}$ (mod p) zodat h' een integer getal is tussen 1 en (p–1).

Met deze drie getallen kiest elke gebruiker een private sleutel x in het gebied 1 < x < q-1 en de publieke sleutel y is berekend van x als $y = g^x \pmod p$. Herinner dat x bepalen rekenkundig zo goed als onmogelijk is omdat men hiervoor het discrete logaritme van y $\log_g \pmod p$ dient te berekenen.

Om een bericht B te tekenen, berekent de verzender twee parameters, r en s, die functie zijn van (p, q, g en x), de message digest H(B), en een willekeurig nummer k < q. *(Rhee, 2003)*

5.4.6 Elliptische Curve Cryptosysteem (ECC)

Het Elliptisch Curve Cryptosysteem werd in 1985 geintroduceerd door Koblity en Miller. Bij ECC worden de sleutelparen ook gegenereerd door de priemgetallen-truc. Dit heeft weinig extra voordelen ten opzichte van RSA. Maar ECC heeft een ander mogelijkheid, en dat is het gebruik van discrete logaritmen in combinatie met een elliptische curve. De elliptische curve discrete logaritmes blijken veel ingewikkelder dan de bestaande logaritmes. Voordeel hiervan is dat de sleutellengte korter kan zijn dan bij normale asymmetrische systemen, terwijl de sleutel toch even sterk is. Het schijnt vrij makkelijk te zijn om de elliptische curve in te passen in al bestaande algoritmen die gebruik maken van discrete logaritmen, zoals DSA , Diffie-Hellman, ElGamal en Schnorr. Elliptische curves hebben het potentieel snellere public-key cryptosystemen te verschaffen.

Zonder al te diep in te gaan op de onderliggende wiskunde geven we een idee van hoe deze methode werkt. Voor meer details verwijzen we naar het boek "Internet security" *(Rhee, 2003)*. Onder de elliptische curve F: $y^2 = x^3 + ax + b$ gedefinieerd over Z_p, met Z_p de verzameling gehele getallen tussen 0 en p, wordt verstaan alle getallen paren (x,y) ε $Z_p \times Z_p$ die voldoen aan:

$$y^2 = x^3 + ax + b \pmod p,$$

waarbij p een priemgetal, $p > 3$ en waarbij a en b constanten zijn zodanig dat $4a^3 + 27b^2 \neq 0 \pmod{p}$.

De punten op F kunnen gevonden worden door voor iedere $x \in Zp$, $z = x^3 + ax + b \pmod{p}$ te bepalen en vervolgens op basis van de vergelijking te trachten y uit te rekenen. Dit is alleen mogelijk als z een *kwadratisch residu* is. Dat wil zeggen dat $z = y^2 \pmod{p}$ een oplossing heeft. Het criterium van Euler stelt dat z een kwadratisch residu modulo p is als en slechts als: $z^{(p-1)/2} = 1 \pmod{p}$. Door beide zijden met z te vermenigvuldigen volgt ook: $z^{(p+1)/2} = z \pmod{p}$. Hieruit volgen dan de wortels $y = \pm z^{(p+1)/4}$ mits p geschreven kan worden als $p = 3 \pmod 4$. In dat geval kunnen de punten op F gevonden worden.

Voorbeeld

Beschouw de elliptische curve $y^2 = x^3 + x + 5$ welke voor $p = 11$ is gedefinieerd over Z_{11}. Nagegaan kan worden dat de constanten $a = 1$ en $b = 5$ voldoen aan de geformuleerde voorwaarde voor a en b. Omdat $p = 11 = 3 \pmod 4$, zijn voor iedere x en daarmee corresponderende z de bijbehorende y-waarden gegeven door de vergelijking $y = \pm z^{(p+1)/4}$. In de tabel op de volgende bladzijde zijn de resultaten weergegeven.

Tabel 7 : Punten op de elliptische curve $y^2 = x^3 + x + 5$

x	$z = x^3+x+5 \pmod{11}$	kwadratisch residu	y	(x,y)
0	5	ja	4,7	(0,4) (0,7)
1	7	nee		
2	4	ja	2,9	(2,2) (2,9)
3	2	nee		
4	7	nee		
5	3	ja	5,6	(5,5) (5,6)
6	7	nee		
7	3	ja	5,6	(7,5) (7,6)
8	8	nee		
9	6	nee		
10	3	ja	5,6	(10,5) (10,6)

In dit geval worden er dus 10 punten gevonden. In het algemeen geldt dat het aantal punten in de orde van het priemgetal p ligt. Door een geschikte keuze van de operator + kunnen de punten van de elliptische curve F opgevat worden als een *Abelse (commutatieve) groep*. Dat wil zeggen de operator + zodanig is dat als $P \varepsilon F$ en $Q \varepsilon F$ dan ook $P + Q \varepsilon F$. Stel $P = (x_1,y_1) \varepsilon F$ en $Q = (x_2,y_2) \varepsilon F$, dan kiezen we de operator zo, dat als $x_2 = x_1$ en $y_2 = -y_1$, dan $P + Q = O$, waarbij O een punt is met eigenschap $P + O = P$ voor alle $P \varepsilon F$. Op basis hiervan geldt voor de inverse van P dat deze gelijk is aan $(x_1,-y_1)$.
In alle andere gevallen geldt $P + Q = (x_3,y_3)$,

waarbij $x_3 = \sigma_2 - x_1 - x_2 \pmod p$
$y_3 = \sigma(x_1 - x_3) - y_1 \pmod p$,

en $\sigma = (y_2 - y_1)/(x_2 - x_1)$, als $P \neq Q$,
$= (3x_1^2 + a)/(2y_1)$, als $P = Q$.

Door een willekeurige $P \varepsilon F$ als uitgangspunt te kiezen, kunnen met de twee bovenstaande vergelijkingen alle andere punten van de elliptische curve gegenereerd worden.

Voorbeeld

We beschouwen wederom $y^2 = x^3 + x + 5 \pmod{11}$. Zoals we in het vorige voorbeeld hebben gezien is $P = (0,7) \varepsilon F$. We berekenen nu achtereenvolgens $2P$, $3P$, ..., $10P$ met behulp van de bovenstaande vergelijkingen. We beginnen met de berekening van $2P$.

$2P = (0,7) + (0,7)$.
Hieruit volgt:
$\sigma = (3 \cdot 0^2 + 1)/(2 \cdot 7) = 1/14 = 4 \pmod{11}$, want $4 \cdot 14 = 1 \pmod{11}$

Dit levert:
$x^3 = 16 = 5 \pmod{11}$,
$y^3 = 4(0 - 5) - 7 = -27 = 6 \pmod{11}$.

Hiermee wordt gevonden (5,6), wat inderdaad een punt van de elliptische curve is. De berekening van $3P$ gaat als volgt:
$3P = P + 2P = (0,7) + (5,6)$

Dit geeft:
$\sigma = (7 - 6)/(0 - 5) = -1/5 = 2 \pmod{11}$.

Substitutie in de vergelijking levert:
$x^3 = 22 - 5 = -1 = 10 \pmod{11}$,
$y^3 = 2(0 - 10) - 7 = -27 = 6 \pmod{11}$,

waarmee het punt (10,6) wordt gevonden. Op analoge wijze kunnen $3P$, $4P$,... berekend worden. De resultaten zijn:

$P = (0,7)$	$6P = (7,6)$
$2P = (5,6)$	$7P = (2,9)$
$3P = (10,6)$	$8P = (10,5)$
$4P = (2,2)$	$9P = (5,5)$
$5P = (7,5)$	$10P = (0,4)$.

Dit zijn precies de punten uit de tabel.

Bovenstaande resultaten kunnen gebruikt worden als basis voor het ontwerp van een cijfersysteem. Het is duidelijk dat voor gegeven P het voor iedere α eenvoudig is het punt αP te berekenen. Wat echter niet gemakkelijk is, is bij gegeven punten P en αP de waarde α te vinden. In het bovenstaande voorbeeld is het eenvoudig in te zien dat als (0,7) en (2,9) gegeven zijn dat dan moet gelden $\alpha = 7$. De waarde van α kan gevonden worden door de complete lijst P, $2P$, $3P$, ... etc aan te maken. Als echter het priemgetal p zeer groot gekozen wordt, zeg in de orde van 2160, dan zal het aantal punten op de elliptische curve in dezelfde orde van grootte liggen. En aldus zal het genereren van de lijst P, $2P$, $3P$, ... ondoenbaar zijn.

6 Beveiliging

Beveiliging is tegenwoordig een belangrijk punt van aandacht in het bedrijfsleven. Er is een grote nood aan vertrouwelijkheid, en dit is in dit digitale tijdperk dikwijls niet zo eenvoudig. Computers en documenten kunnen worden aangevallen door nieuwsgierig hackers, ontevreden medewerkers en ex-medewerkers, criminele aanvallers of cyberterroristen en regeringen. Het is belangrijk dat men zich hier tegen beveiligt. In een bedrijf is er echter een brede variëteit aan middelen. Enkele van deze middelen zijn uiterst cruciaal, andere minder. Daarom zal men deze middelen moeten rangschikken naar gevoeligheid.

Een zwak punt waar hackers makkelijker kunnen toeslaan is wanneer documenten worden verstuurd. Vaak willen twee communicatiepartners op een veilige manier met elkaar communiceren, en beschermd zijn tegen meegluurders die hun berichten proberen te lezen. Ze willen authenticatie van de identiteit van de andere partij, de garantie dat er onderweg niet met de berichten gerommeld is, en met de garantie dat de berichten niet zijn toegevoegd door een aanvaller. Het is daarom noodzakelijk dat men ook bij transport beveiliging voorziet die de confidentialiteit, integriteit en authenticiteit waarborgt.

Bij toegangscontrole is de eerste stap authenticiteit, waarvoor vereist is dat iemand die van een middel gebruik wil maken, zijn of haar identiteit bewijst. De gebruiker die zijn of haar identiteit wil bewijzen noemt men de applicant. De partij die van de applicant vereist dat deze zijn of haar identiteit bewijst, is de verifier. De applicant doet dit door zijn credentials (bvb. certificaat) aan de verifier te geven. Vaak is er een derde partij, de authenticatieserver (bvb. certificaatautoriteit), die gegevens opslaat om de verifier te helpen de credentials van de applicant te controleren. *(Panko, 2005)*

6.1 Mogelijke authenticatie

Het type authenticatie dat voor elk middel gebruikt wordt moet geschikt zijn voor de gevoeligheid van het desbetreffende middel.

6.1.1 Wachtwoorden

De meest algemene authenticatiemethode is het wachtwoord. Panko definieert een wachtwoord als "*een string (reeks) van tekens die een gebruiker invoert om toegang te krijgen tot middelen die met een bepaalde gebruikersnaam op een computer geassocieerd zijn*".

Voordelen: Mensen vinden wachtwoorden relatief gemakkelijk in gebruik. Daarnaast hebben wachtwoorden geen extra kosten tot gevolg.

Nadelen: Wachtwoorden zijn vaak zwak (gemakkelijk te kraken). Men gebruikt hiervoor bijvoorbeeld een woordenboekaanval. Het is daarom belangrijk dat wachtwoorden complex zijn, door het mengen van hoofdletters en kleine letters, cijfers en andere toetsenbordtekens en bovendien is lengte ook belangrijk, elk extra teken verhoogt immers de tijd nodig om te kraken.

6.1.2 Biometrie

Een relatief nieuwe vorm van authenticatie is biometrie waarbij men bepaalde lichaamsmetingen gebruikt om een applicant te identificeren.

Mogelijkheden:

- Scannen van vingerafdrukken: Het is de goedkoopste maar tevens ook minst nauwkeurige vorm van biometrische authenticatie. Naaste de aanwezigheid van aanzienlijke error rates[1] kunnen veel vingerafdrukscanners tamelijk gemakkelijk

[1] Error rates : verwijzen naar het percentage fouten dat door een biometrisch systeem gemaakt wordt, zelfs wanneer de gebruikers niet proberen om het systeem te misleiden.

worden misleid door bedriegers. Ondanks zijn beperkingen is het wel veruit de meest gebruikte biometrische authenticatiemethode.

- Irisscanner: Veel duurder en nauwkeuriger zijn irisscanners die camera's gebruiken die het zeer complexe patroon van de iris van de applicant lezen. Irisscanners hebben echter ook kleine error rates en kunnen worden misleid.
- Gezichtsherkenning: Hierbij maakt een camera een analyse van de gezichtstructuur. Het kan ongemerkt gebeuren, zonder medeweten of toestemming van de persoon die gescand wordt. Er is een zeer hoge error rate en het is gemakkelijk te misleiden.

6.1.3 Digitaal certificaat authenticatie

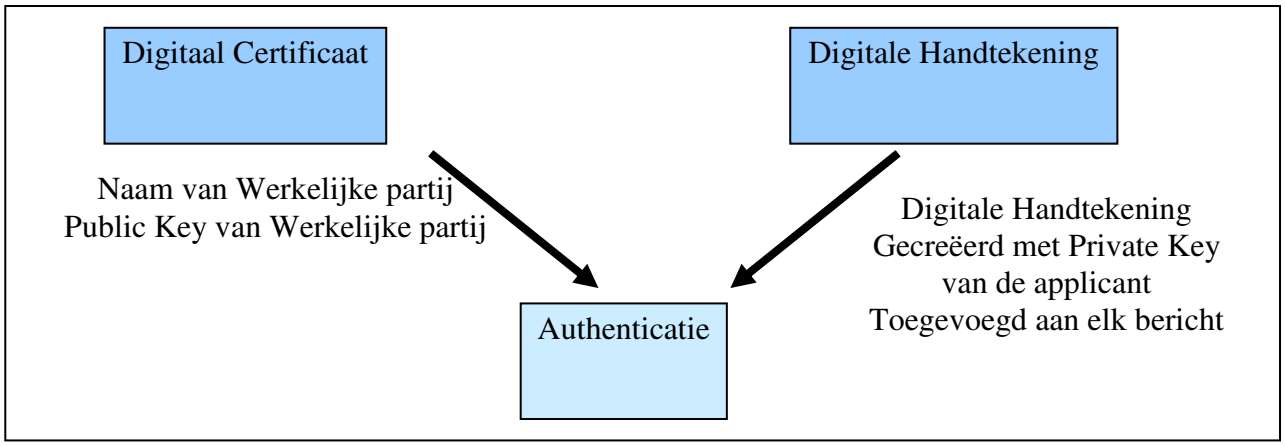
Bij digitaal certificaat authenticatie krijgt elke gebruiker een publieke sleutel (niet geheim gehouden). Deze publieke sleutel wordt gepaard aan een private sleutel die enkel aan de gebruiker bekend is. Het digitaal certificaat geeft de naam van de werkelijke partij, de publieke sleutel van de werkelijke partij, en andere informatie.

Digitaal certificaat authenticatie is een zeer krachtig middel omdat private sleutels uitermate lang zijn en perfect willekeurig. Het is zo goed als onmogelijk om aan de hand van de publieke sleutel in een digitaal certificaat de private sleutels efficiënt te berekenen.

Het nadeel is echter dat digitaal certificaat authenticatie, beter bekend als public-key authenticatie, duur en tijdrovend is om te implementeren. Op elke server en elke client-pc moet digitaal certificaat authenticatiesoftware en een private sleutel worden geïnstalleerd. Hiervoor is veel werk nodig. Ondanks de kracht van digitaal certificaat authenticatie zijn veel bedrijven terughoudend om hier zoveel geld in te investeren.

Belangrijk te begrijpen is dat het certificaat op zichzelf geen afzender authenticeert! Zoals duidelijk wordt uit figuur 7 biedt het digitale certificaat de publieke sleutel (en naam) van de werkelijke partij, maar meer ook niet. De digitale handtekening op zijn beurt krijgt pas betekenis als deze getest is met de publieke sleutel van de werkelijke partij, die alleen via een

certificaat op een betrouwbare manier kan worden verkregen. Bij public-key authenticatie moeten digitale certificaten en public-key authenticatie samen gebruikt worden. Geen van beide is voldoende voor authenticatie. *(Panko, 2005)*



Figuur 7 : Een certificaat autheticeert op zichzelf geen afzender *(Panko, 2005)*

7 De digitale handtekening

In dit hoofdstuk behandelen we eerst wat een handtekening is en welke functie zij vervult. Vervolgens gaan we dieper in op de digitale handtekening. We leggen abstract het werkingsprincipe uit, zowel voor wanneer er geen confidentialiteit verreist is als voor wanneer dit wel het geval is. Nadien wordt in het volgende hoofdstuk uitleg gegeven over de codetheorie.

7.1 Wat is een handtekening?

Van Dale: eigenhandige ondertekening

Een handtekening is een manier om een identiteit met informatie te verbinden. Het drukt goedkeuring, bijvoorbeeld bij een koopcontract, of auteurschap, bijvoorbeeld bij een schilderij, van de ondertekenaar uit. Omdat een handtekening een verbinding is tussen informatie en een persoon heeft hij alleen betekenis in combinatie met de plaats waar hij zich bevindt, bijvoorbeeld onderaan een contract; een handtekening op een leeg vel papier betekent niets. *(Wilschut, D.E., 2000)*

De handtekening wordt in het dagelijkse leven veel gebruikt. Dit is het gevolg van het juridische kader dat samenhangt met de handtekening. Aan een handtekening worden juridisch de volgende eigenschappen verbonden:

- Een handtekening is authentiek. De handtekening overtuigt de ontvanger dat de ondertekenaar de informatie willens en wetens heeft gesigneerd.

- Een handtekening zou niet te vervalsen zijn. De handtekening bewijst dat de ondertekenaar, en niemand anders, de informatie heeft gesigneerd.

- De gesigneerde informatie kan niet worden veranderd. De handtekening is een bewijs dat de informatie nog dezelfde vorm heeft als toen het werd ondertekend.

- De handtekening kan niet worden ontkend. Immers, alleen de rechtmatige 'eigenaar' van de handtekening kan deze hebben geplaatst.

Het spreekt voor zich dat in de praktijk een geschreven handtekeningen niet voldoet aan deze eisen: men kan handtekeningen vervalsen, een boodschap kan na het signeren gemakkelijk gewijzigd worden en met een beetje handigheid kan een handtekening van het ene document naar het andere worden gekopieerd.

7.2 Wat is een elektronische handtekening?

“Het concept elektronische handtekening is een soortnaam voor alle technische mechanismen (geheime code, technieken gebaseerd op symmetrisch of asymmetrisch cijferschrift, biometrische handtekening, enz.) die onder de noemer ‘elektronische handtekening’ vallen, voor zover ze via elektronische weg dezelfde functies hebben als de klassieke handtekening, namelijk: identificatie van de ondertekenaar en uitdrukking van zijn instemming met het ondertekende bericht. Deze mechanismen van elektronische handtekening omvat ook de digitale handtekening, gebaseerd op een specifieke codetaal: de asymmetrische codetaal.”
(http://mineco.fgov.be/information_society/enterprises/designers_internetguide/designers_nl-05.htm#P889_77652)

7.3 Wat is een digitale handtekening?

Encryptie wordt hoofdzakelijk gebruikt als een manier om vertrouwelijkheid te creëren. Cryptografie kan echter ook worden gebruikt op het gebied van authenticatie, dat wil zeggen, het verifiëren van de identiteit van de andere partij. *(Panko, 2005)*

Net zoals de handgeschreven handtekening gebruikt wordt op documenten vandaag, worden digitale handtekeningen gebruikt om de identiteit van auteurs/medeondertekenaars van e-mail of elektronische informatie te garanderen. *(http://www.digitalehandtekening.be/what.cfm)*

De vraag is nu hoe men een digitale handtekening met digitale informatie verbindt. Bij de geschreven handtekening merk je aan de plaats, meestal onderaan een document, waarop deze van toepassing is. Bij een digitale handtekening is dat echter minder duidelijk. Er moeten dus twee bitstrings met elkaar verbonden worden zodat het niet eenvoudig is ze los te koppelen en ze afzonderlijk te kopiëren of te veranderen. Daarom is het niet voldoende een geschreven handtekening om te zetten naar een digitale vorm en deze gewoon onder een document te plakken. Ze kan immers los geknipt worden en aan andere documenten worden geplakt, of men kan ze eenvoudigweg kopiëren. Het blijft ook mogelijk een document na de ondertekening nog te veranderen zonder sporen achter te laten.

Daarom gaat men bij de digitale handtekening op zoek naar het equivalent van de fysieke verbinding die een geschreven handtekening heeft met de gesigneerde informatie; de handtekening moet onlosmakelijk met de informatie worden verbonden. Omdat in digitale vorm alles uiteindelijk als bitstring wordt gerepresenteerd wordt aangenomen dat de te signeren informatie zowel als de handtekening een rij nullen en enen is. Zo bezien zijn het dus twee getallen en dringt de volgende oplossing zich op. De handtekening wordt rekenkundig op de boodschap geplaatst, door een wiskundige bewerking uit te voeren met beide strings als invoer. De digitale handtekening hoort daardoor specifiek bij de ondertekende, onaangepaste boodschap. *(Wilschut, D.E., 2000)*

Achter de digitale handtekening zit heel wat wiskunde. Om digitaal te kunnen signeren moet gebruik worden gemaakt van een zogenaamd digitaal handtekeningenalgoritme. Vooral de one-way functies van public-key cryptosystemen lijken hiervoor het meest bruikbaar. De eisen die aan een digitale signeermethode worden gesteld komen overeen met de vereisten van een cryptosysteem.

De digitale handtekening is gebaseerd op asymmetrische cryptografie met een zogenaamde «publieke sleutel». Om iemand te identificeren door middel van een publieke sleutel moet men over twee elkaar aanvullende mathematische sleutels beschikken: één privé-sleutel die de gebruiker strikt geheim moet houden en een publieke sleutel die vrij mag doorgegeven worden. Deze twee sleutels worden gegenereerd door een functie die ervoor zorgt dat de privé-sleutel niet kan worden afgeleid uit de bijbehorende publieke sleutel. De publieke sleutel moet dus een onomkeerbare functie (one-way functie) zijn van de privé-sleutel. De privé-sleutel maakt het mogelijk het bericht te «ondertekenen». De ontsleuteling gebeurt volgens het principe van de complementariteit van de sleutels: een bericht beveiligd met een privé-sleutel kan enkel ontsleuteld worden met zijn complementaire publieke sleutel.

Digitaal signeren bestaat uit drie stappen:

- Handtekening creëren: Alice moet eerst een handtekening maken.

- Signeren: Alice moet de informatie kunnen ondertekenen. Ze moet dus haar handtekening aan de informatie kunnen koppelen.

- Verifiëren: Bob moet liefst eenvoudig en snel kunnen controleren dat de boodschap inderdaad door Alice is ondertekend.

7.3.1 Eigenschappen

Digitale handtekeningen hebben enkele belangrijke eigenschappen, vereisten zoals: authenticatie, integriteit en onweerlegbaarheid. Op de website van Globalsign vonden we een verduidelijking van deze begrippen. (*http://www.digitalehandtekening.be/what.cfm)*

Authenticatie is de verificatie van de identiteit van een persoon (server, stukje software...). Het garandeert de identiteit van diegene die de informatie ondertekende, zo weet u wie deelnam aan de transactie en dat het niet werd vervalst door anderen. Het laat eveneens toe de ware identiteit te achterhalen van een gebruiker die toegang probeert te verkrijgen tot een systeem.

Een digitale handtekening beschermt de **integriteit** van de informatie, dus u weet wanneer deze werd gewijzigd, zowel toevallig als kwaadwillig. Technisch: een digitale handtekening bevat een verkapte vorm (de hash) van de informatie die gehandtekend wordt. Elke wijziging aan die informatie nadat het gehandtekend is, zou bij authenticatie een totaal andere verkapte vorm vertonen en de authenticatie dus ongeldig maken. Hierover volgt nog meer bij het werkingsprincipe.

Authenticiteit van een digitale handtekening zorgt ervoor dat de auteur van een bericht zijn identiteit kan bewijzen. **Onweerlegbaarheid** laat u echter ook toe om later te bewijzen wie in een transactie participeerde. Iemand die een bericht in een transactie verzond kan niet meer ontkennen dat hij dit deed.

De digitale handtekening zorgt er echter niet voor dat de boodschap geheim blijft. Meestal echter, wordt confidentialiteit van de data vereist. Hiervoor zorgt in wezen de digitale handtekening niet. Daarom zal men de hulp inroepen van de cryptografie en de boodschap + de digitale handtekening encrypteren aan de hand van de 'publieke' sleutel van de ontvanger. Enkel de ontvanger kan dan het berichtje lezen. Voor lange berichten is het eenvoudiger en sneller om de berichten via symmetrische encryptie te versleutelen.

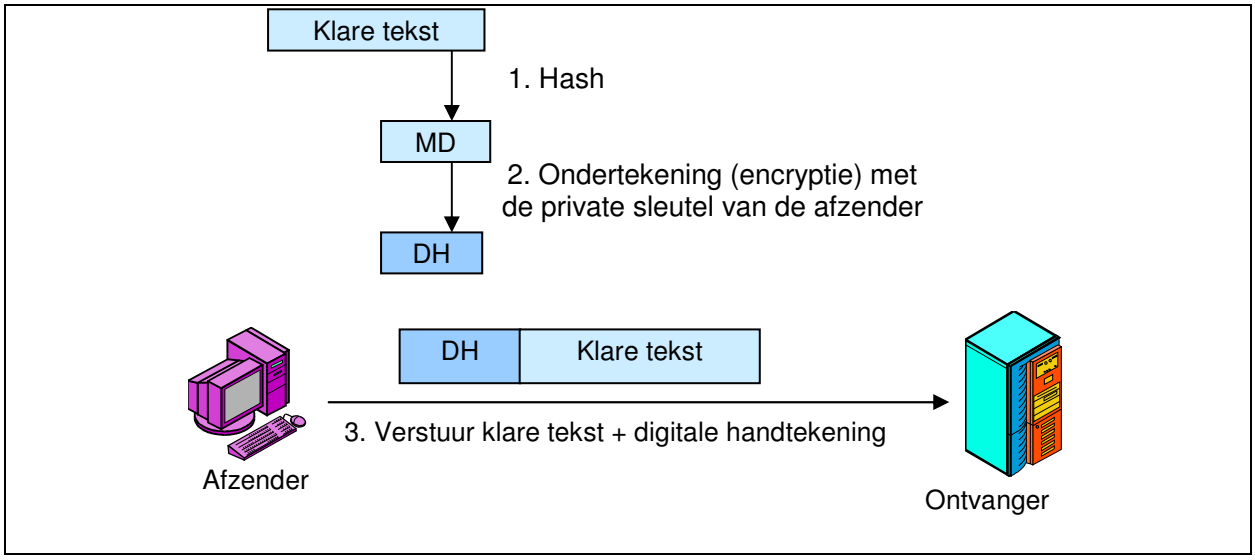
7.3.2 Korte herhaling hash-functie

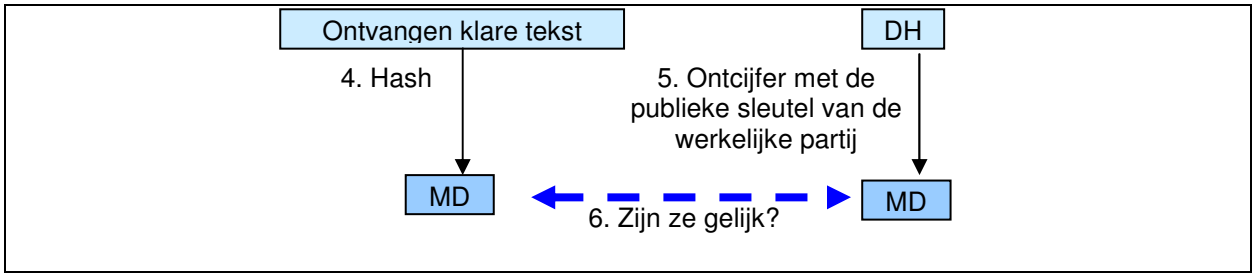
Aangezien we dadelijk toekomen aan het werkingsprincipe van de digitale handtekening vermelden we nog even kort de hash-operatie bij de digitale handtekening. Zoals eerder uitgelegd dient de hash-functie om een bitstring van willekeurige lengte (in het geval van de digitale handtekening: de boodschap), om te zetten in een zogenaamde hashwaarde van vaste, kleine bitlengte (de message digest). De boodschap wordt dus 'gekapt'.

De vraag die zich nu stelt is waarom we eigenlijk hashen. Zoals in één van de vorige paragrafen is beschreven wordt de digitale handtekening op de boodschap geplaatst. In de praktijk is die boodschap echter vaak heel groot. Wanneer met deze volledige boodschap gerekend moet worden kost dat veel tijd. In plaats daarvan wordt daarom een bitstring kenmerkend voor de boodschap, de hashwaarde, die veel kleiner en van vaste grootte is, ondertekend. Hierdoor kan het proces van ondertekenen veel sneller gebeuren.

7.3.3 Werkingsprincipe – Confidentialiteit niet vereist

MD = message digest
DH = digitale handtekening
Uitleg onder figuur





Figuur 8 : Werkingsprincipe, confidentialiteit niet vereist *(Panko, 2005)*

Figuur 8 laat zien hoe je een digitale handtekening creëert, die elk bericht authenticeert analoog aan de manier waarop een menselijke handtekening documenten authenticeert.

Het werkingsprincipe wordt uitgelegd aan de hand van de figuur:

1. Om de digitale handtekening te creëren, maakt de afzender (de applicant) een hash[2] (of message digest) van het bericht (de klare tekst) dat de afzender wil verzenden. Door de toepassing van de hashfunctie op het bericht wordt dus een message digest (MD) gegenereerd. *De message digest wordt gegenereerd omdat digitale handtekeningen gebruik maken van public key encryption, een methode die alleen kan worden toegepast op het versleutelen van korte berichten, zoals hashes die kenmerkend uit een vast bepaald, klein aantal bits bestaan.*
2. Vervolgens versleutelt[3] de afzender de message digest met zijn eigen private sleutel. Hierdoor wordt de digitale handtekening gecreëerd. *Merk op dat de message digest niet hetzelfde is als de digitale handtekening, maar alleen gebruikt wordt om de digitale handtekening te produceren.*
3. Het bericht dat de afzender verstuurt bestaat dus uit het oorspronkelijke klare tekstbericht, gecombineerd met de digitale handtekening. Als vertrouwelijkheid niet belangrijk is, kan de afzender het gecombineerde bericht gewoon versturen. *Vertrouwelijkheid is echter meestal wel belangrijk, dus versleutelt de afzender normaal gesproken het gecombineerde bericht en de digitale handtekening voor*

[2] Voor de werking van 'hashing' verwijzen we naar de paragraaf over de hashfunctie
[3] Voor methodes van versleuteling zie het deel asymmetrische encryptiemethodes in paragraaf 5.4

vertrouwelijkheid. Zie hiervoor de paragraaf: Werkingsprincipe –Confidentialiteit vereist

4. Wanneer de ontvanger het gecombineerde bericht heeft aangekregen hashed hij het ontvangen klare tekstbericht met hetzelfde hashing-algoritme dat de applicant heeft toegepast, zodat men een message digest creëert.
5. Vervolgens ontcijfert de ontvanger de digitale handtekening met de publieke sleutel van de afzender. Hierbij bekomt men ook een message digest.
6. De twee message digests worden met elkaar vergeleken, wanneer ze identiek zijn betekent dit dat de afzender in het bezit is van de private sleutel van de werkelijke partij, die alleen aan de werkelijke partij bekend is. Het bericht wordt geauthenticeerd als afkomstig van de werkelijke partij. De digitale handtekening is hierdoor een stuk veiliger dan de gewone handtekening. *Merk op dat de kleinste verandering zorgt voor een totaal verschillende hash.*

De digitale handtekening zorgt niet enkel als bewijs van identiteit van de afzender maar ook voor data-integriteit en onweerlegbaarheid (zoals gezien bij eigenschappen van de digitale handtekening supra).

Vanuit het werkingsprinicipe is gemakkelijk te begrijpen dat wanneer er onderweg iemand het bericht verandert, of als er transmissiefouten optreden, de twee message digests niet overeen zullen komen. Om die reden bieden digitale handtekeningen bericht-integriteit: het vermogen om aan te geven of een bericht onderweg gewijzigd is. Een bericht dat gewijzigd is, komt niet door de authenticatietest (stap 6) en zal worden verwijderd.

Er wordt onderzoek verricht om berichten waarin transmissiefouten optreden te herkennen en zelfs foutcorrigerend op te treden. Dit is zeer essentieel omdat er anders juiste berichten niet door de authenticatietest zouden komen. Meer informatie hierover vind u in hoofdstuk 8 betreffende codetheorie met de Hamming-code als belangrijkste algoritme van het moment.

7.3.4 Werkingsprincipe – Confidentialiteit vereist

Een misverstand is dat de digitale handtekening zorgt voor geheimhouding, dit is niet correct. De digitale handtekening zorgt er niet voor dat niemand het bericht kan onderscheppen of lezen. Deze beveiliging is echter dikwijls een vereiste. Men gaat daarom na de creatie van de digitale handtekening, het **bericht + de digitale handtekening versleutelen** zodat enkel de ontvanger ze kan ontcijferen.

De verschillende methodes van versleutelen werden al behandeld in het hoofdstuk over cryptografie, we vermelden hier daarom slechts beknopt hoe ze kunnen bijdrage tot de confidentialiteit in combinatie met de digitale handtekening.

Er zijn twee soorten versleutelmethodes namelijk symmetrische encryptie en asymmetrische encryptie. Het voordeel van het gebruik van symmetrische encryptie ligt in het feit dat het versleuteling van lange berichten mogelijk maakt, dit in tegenstelling tot asymmetrische encryptie. Nadeel is dat men nog altijd niet heel zeker kan zijn dat het bericht enkel door de bedoelde ontvanger zal gelezen worden vermits er eventueel meerdere gebruikers dezelfde sleutel hanteren.

Doorgaans wordt er voor asymmetrische encryptie geopteerd. Hierbij is men zeker dat het verzonden bericht enkel zal kunnen ontsleuteld worden door de persoon voor wie het bericht bedoeld was. Het probleem dat enkel korte berichten kunnen versleuteld worden met asymmetrische encryptie wordt opgelost door het lange bericht eerst op te delen in verschillende blokken. Elk blok wordt afzonderlijk vercijferd. Een andere mogelijkheid is werken volgens het systeem van ‘Public-key distrbutie van symmetrische sleutels’ zoals besproken in paragraaf 2.6.

We hebben hierboven het werkingsprincipe besproken voor het verzenden van een bericht met een digitale handtekening. Het enige verschil is dat nu zowel het bericht als de digitale handtekening vercijferd worden met de publieke sleutel van de ontvanger alvorens het bericht te versturen. Wiskundig wordt dus het volgende toegepast:

Afzender (A) wil een confidentieel bericht naar ontvanger (B) versturen:

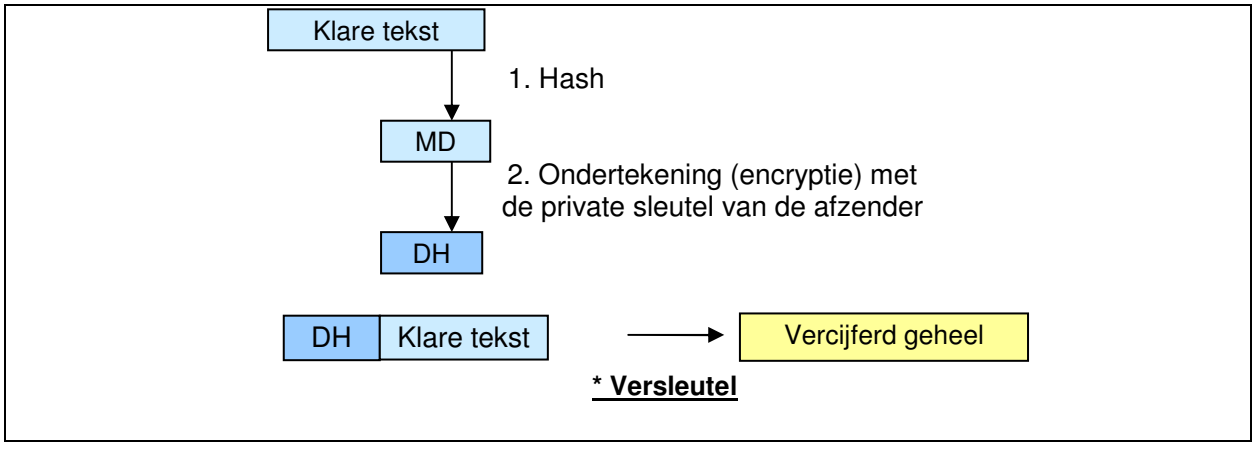
Bericht = x; hashfunctie = h; publiek sleutel A resp. B = f_A , f_B; private sleutel A resp. B : f^1_A , f^1_B

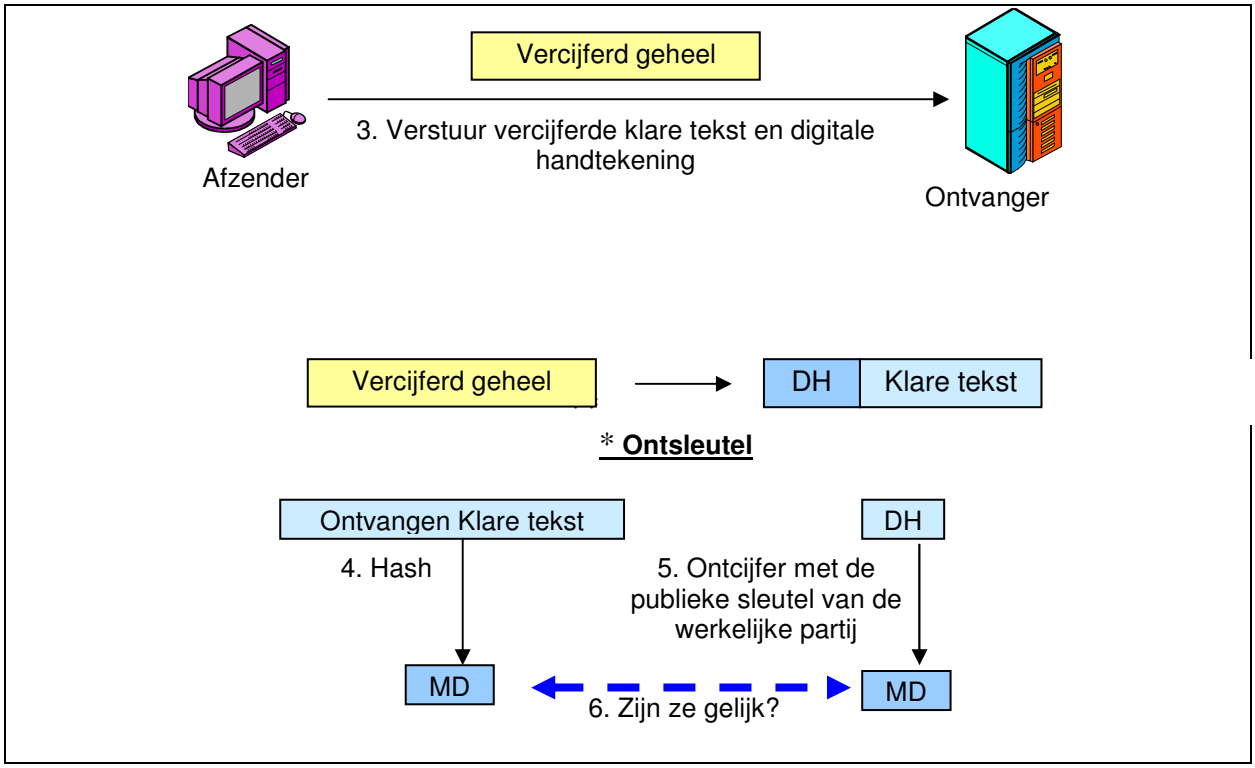
- Hash het bericht: h(x) = y
- Handtekening met eigen private sleutel A: $f^{-1}_A(y) = z$
- Versleutel het bericht + de handtekening met publieke sleutel van ontvanger B : $f_B(x+z) =$ C

  $\rightarrow$ Verstuur C naar ontvanger (B)
- Ontsleutel C met private sleutel B : $f^{-1}_B(C) = x+z$
- Authenticeer: als $h(x) = f_A(z)$ dan OK

In de praktijk wordt wanneer het bericht (x) te lang is dit opgesplitst in blokken en afzonderlijk verstuurt. Men verstuurt dus nu $C = f_B(x_1) + f_B(x_1) + f_B(x_2) + f_B(x_3) + \ldots + f_B(x_n) + f_B(z)$
Door het opsplitsen in blokken wordt het breken wel eenvoudiger, de nodige tijd wordt korter.

De figuur op de volgende pagina geeft het werkingsprincipe weer met de aanpassing voor confidentialiteit.





Figuur 9 : Werkingsprincipe, confidentialiteit vereist

7.4 Public key en certificaat autoriteiten

Het gebruik van de digitale handtekening is ondenkbaar zonder certificerende autoriteiten (verder CA's genoemd). Deze spelen een fundamentele rol bij de identificatie van de verschillende gebruikers van open netwerken .

Bij op publieke sleutels gebaseerde authenticatie moet de verifier de publieke sleutel van de werkelijke partij weten. De verifier moet de applicant niet gaan vragen om de publieke sleutel van de werkelijke partij, omdat wanneer de applicant een bedrieger is, de bedrieger zijn of haar eigen publieke sleutel zal versturen en beweren dat dit de publieke sleutel van de werkelijke partij is. Als de verifier naïef genoeg is om de publieke sleutel van de bedrieger als de publieke sleutel van de werkelijke partij te accepteren, zal de bedrieger digitale handtekeningen met zijn of haar eigen private sleutel zetten, en zal de verifier de publieke

sleutel van de bedrieger gebruiken om de bedrieger als de werkelijke partij te verifiëren. *(Panko, 2005)*

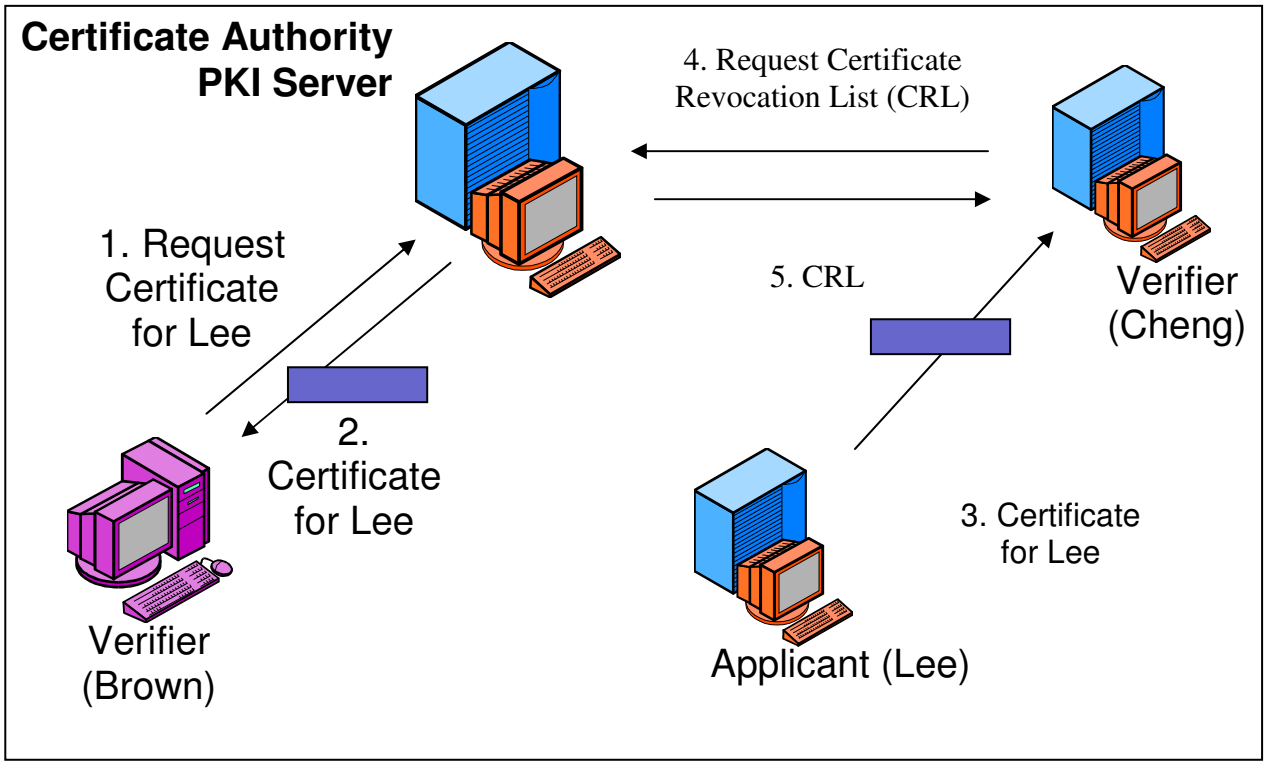
Daarom zal de verifier contact moeten opnemen met een certificaat autoriteit (of Trusted Authority). Deze autoriteit is (of zou moeten zijn) een onafhankelijke en betrouwbare bron van informatie over de publieke sleutels van de werkelijke partijen.

Een certificaat zorgt ervoor dat een publieke sleutel verbonden wordt met een reeks gegevens die een persoon identificeren. Er worden verschillende soorten certificaten uitgegeven voor diverse gebruiken en procedures afhankelijk van de toepassing. De standaard voor digitale certificaten is X.509 versie 3, een klasse 3 certificaat.

In België is de derde klasse verplicht voor elke elektronische mededeling waar delicate, vertrouwelijke en financiële gegevens tussen ondernemingen, overheid, bank- en bijzondere instellingen worden geruild. Eens de mededelingen ondertekend zijn, moet elke partij bovendien zeker zijn van de integriteit van de geruilde gegevens. Eens de gebruiker zijn digitale handtekening heeft aangebracht, houdt dit ook in dat de transactie niet meer geweigerd of weerlegd kan worden.

In België is Isabel de grootste Certification Authority met 85.000 houders van een elektronische handtekening. De Public Key Infrastructure van Isabel wordt door de Amerikaanse specialist op dit gebied TruSecure gewaarborgd. Het bedrijf reikt certificaten van de klasse 3 uit. Sinds de heropleving van de E-Trust activiteiten van Belgacom, is Certipost eveneens een instantie van certificatie. Dit zijn zeker niet de enige Certification Authorities en men kan zich evengoed inschrijven bij bijvoorbeeld Globalsign. Het hangt er gewoon vanaf met welke reden men zich met een certificaat en een elektronische handtekening wil uitrusten. De Belgische operators willen vooral lokale meerwaarde brengen om hun klanten te binden. *(De Financieel Economische Tijd, 2004)*

Een certificaat autoriteit kan een digitaal certificaat van een partij intrekken voordat de datum die in het certificaat genoemd staat, verstreken is. Als de verifier dus het digitaal certificaat ontvangt van een andere partij dan de certificaat autoriteit, zou de verifier de certificaat revocation list (CRL) moeten controleren om er zeker van te zijn, dat het digitale certificaat nog steeds geldig is. Hiertoe download de verifier de CRL en kijkt of het serienummer van het digitale certificaat op de lijst voorkomt. *(Panko, 2005)*



Figuur 10 : Controle geldigheid van certificaat *(Panko, 2005)*

Uitleg figuur

We veronderstellen dat de applicant (Lee) een private sleutel heeft ontvangen van de certificaat autoriteit. Deze laatste is in het bezit van Lee's publieke sleutel.

Wanneer een verifier (ontvanger) de digitale handtekening die bij een document is gevoegd wil controleren om zeker te zijn dat het document van de applicant (Lee) afkomstig is, gaat hij

de digitale handtekening ontsleutelen met de publieke sleutel en vergelijken met de message digest zoals hierboven bij werkingsprincipe staat uitgelegd.

Om er zeker van te zijn dat de publieke sleutel werkelijk van Lee is zal men deze sleutel opvragen bij de certificaat autoriteit, zoals te zien in stappen 1 en 2 op de figuur.

Er is nog een andere mogelijkheid. Lee kan de ontvanger (Cheng) zelf de publieke sleutel met bijhorend certificaat opsturen. De ontvanger gaat nu controleren of het certificaat wat Lee heeft doorgestuurd nog geldig is door bij de certificaat autoriteit de Certificate Revocation List op te vragen, zoals te zien in stappen 3, 4 en 5 op de figuur.

7.5 Wetgeving

7.5.1 Waarom nood aan nieuwe wetgeving?

In de nieuwe virtuele wereld die we vandaag kennen is er een grote vrees voor onzekerheid, vooral wat betreft in allerhande betalingsomgevingen. Er is nood aan identificatie (naam waardoor iemand herkend wordt), authentificatie (zelf geplaatst), autorisatie (toegestaan), integriteit (ongewijzigd), onweerlegbaarheid en vertrouwelijkheid. Wanneer deze criteria veilig zijn gesteld zal de onzekerheid plaatsmaken voor zekerheid.

De zoektocht om deze criteria te verwezenlijken bracht ons tot twee technieken : (1) de elektronische handtekening om ervoor te zorgen dat de boodschappen beschermd zijn, zodat men zeker weet door wie de boodschap is verzonden en dat deze ongewijzigd is ; (2) encryptie om ervoor te zorgen dat de boodschappen afgeschermd zijn, zodat de boodschap onleesbaar is voor iedereen behalve voor de bestemmeling. Deze beide technieken kunnen gerealiseerd worden door asymmetrische encryptie (PKI).

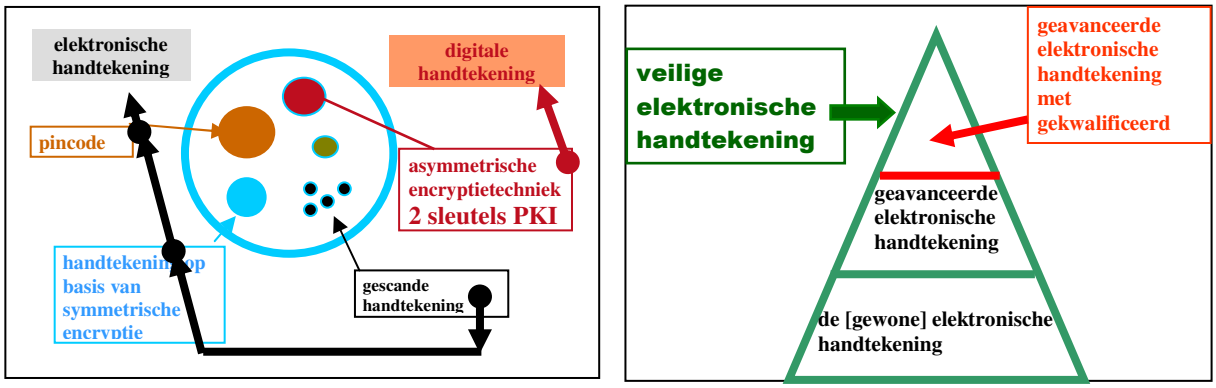
De wet van 9 juli 2001 zet de bepalingen om van de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen. In deze wet legt men bepaalde regels vast in verband met het juridisch kader voor elektronische handtekeningen en bepaalt men het juridisch stelsel en de na te leven regels voor de certificatiedienstverleners.

7.5.2 Verschil in begrippen: elektronische en digitale handtekening

Kort:

- Elektronische handtekening: alle elektronische handtekeningen die niet op basis van PKI werden gemaakt → *niet veilig*
- Digitale handtekening: elektronische handtekening op basis van PKI → *veilig*

In de wet onderscheidt men drie soorten elektronische handtekeningen: de gewone elektronische handtekening, de geavanceerde elektronische handtekening, en de geavanceerde elektronische handtekening met gekwalificeerd certificaat. Enkel deze laatste wordt als een veilige elektronische handtekening aanzien. *(De Corte, 2003)*



Figuur 11 : Veiligheid van de drie soorten elektronsche handtekeningen

De gewone elektronische handtekening

art. 2, 1° *«elektronische handtekening»: gegevens in elektronische vorm, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie*

Voorbeelden van zulke handtekeningen zijn onder andere gescande handtekeningen op een elektronisch document, een pincode, of handtekeningen op basis van biometrische gegevens. Het zijn dus elektronische gegevens, geassocieerd met andere elektronische gegevens met de bedoeling een handtekening te plaatsen die dan moet zorgen voor authentificatie. Vraag is nu hoe men met zulke handtekeningen identificeert en hoe men de integriteit van de ondertekende boodschap ermee bewaart.

De geavanceerde elektronische handtekening

Art. 2, 2° «geavanceerde elektronische handtekening»: elektronische gegevens vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie en aan de volgende eisen voldoen:
1)zij is op unieke wijze aan de ondertekenaar verbonden;
2) zij maakt het mogelijk de ondertekenaar te identificeren;
3) zij wordt aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
4) zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke latere wijziging van de gegevens kan worden opgespoord.

Deze vorm van elektonische handtekeningen voldoet aan de vereisten van identificatie van de houder + authentificatie (mbv. certificaatautoriteit) en aan de kwaliteitsvereisten van veiligheid (mbv. PKI) en integriteit (mbv. hashing) .

7.5.3 Wettelijke regeling

De wet voorziet wat betreft de elektronische handtekening de volgende regelingen:

Assimilatie

Hierbij wordt de elektronische handtekening volledig gelijkgesteld of geassimileerd met een handgeschreven handtekening onder de volgende 3 cumulatieve voorwaarden:

- een geavanceerde elektronische handtekening
  - → gerealiseerd door gebruik van PKI
- op basis van een gekwalificeerd certificaat
  - → eisen gesteld aan certificaat en certificatiedienst
- aangemaakt met veilige middelen
  - → private key mag slechts eenmaal aangemaakt kunnen worden
  - → public niet af te leiden uit private key
  - → wijzigingen private key opspoorbaar
  - → aanmaakmiddelen beschermd
  - → aanmaakprocedure los van te ondertekenen document

Art. 4. § 4 wet elektronische handtekening
Onverminderd de artikelen 1323 en volg. B.W. wordt een geavanceerde elektronische handtekening, gerealiseerd op basis van een gekwalificeerd certificaat en aangemaakt door een veilig middel voor het aanmaken van een handtekening, geassimileerd met een handgeschreven handtekening ongeacht of deze handtekening gerealiseerd wordt door een natuurlijke dan wel door een rechtspersoon.

Een veilige elektronische handtekening wordt geacht te zijn aangebracht door de titularis van het certificaat, behoudens tegenbewijs. Zo staat het in de oorspronkelijke wetgeving.

Non-discriminatie

Hierbij stelt de wet dat men een elektronische handtekening niet mag verwerpen enkel op grond van het feit dat het (1) elektronisch is en (2) niet veilig is.

Art. 4 § 5 Wet elektronische handtekening
§ 5. Een elektronische handtekening kan geen rechtsgeldigheid worden ontzegd en niet als bewijsmiddel in gerechtelijke procedures worden geweigerd louter op grond van het feit dat:
— de handtekening in elektronische vorm is gesteld, of
— niet is gebaseerd op een gekwalificeerd certificaat, of
— niet is gebaseerd op een door een geaccrediteerd certificatiedienstverlener afgegeven certificaat, of
— zij niet met een veilig middel is aangemaakt.

Overheid

Er kunnen nog aanvullende eisen gesteld worden voor het gebruik van elektronische handtekening in de openbare sector.

Art. 4 § 3 Wet elektronische handtekening
De Koning kan, bij een besluit vastgesteld na overleg in ministerraad, voor het gebruik van elektronische handtekeningen in de openbare sector eventuele aanvullende eisen stellen. Deze eisen moeten objectief, transparant, evenredig en niet discriminerend zijn en mogen slechts op de specifieke kenmerken van de betrokken toepassing betrekking hebben. Zij mogen geen belemmering vormen voor grensoverschrijdende diensten voor de burgers.

7.6 Voor- en nadelen bij het gebruik van de digitale handtekening

De digitale handtekening is een onderdeel van de informatisering van onze maatschappij. Men zou dus kunnen stellen dat de digitale handtekening de geschreven handtekening zal vervangen zoals de computer de typemachine heeft vervangen. Door de elektronica die we voorhanden hebben, verhogen we de gebruiksvriendelijkheid en veelzijdigheid in verschillende producten van onze maatschappij. De digitale handtekening is hier geen uitzondering op. De voordelen van de digitale handtekening hangen dus ook eerder samen met de voordelen van elektronica en technologie. De communicatietechnologie is echter vatbaar voor aanvallen en daarom niet altijd even veilig. Het is de digitale handtekening die het beveiligde kader verschaft.

De bedrijven zullen door toepassing van de digitale handtekening de volledige mogelijkheden van hun elektronische processen kunnen gebruiken. Hierdoor zal men tijd besparen doordat de verwerkingstijd van deze processen sneller zijn dan zijn manuele voorgangers. Uit deze tijdsbesparing volgt dan een kostenbesparing vermits de kortere verwerkingstijd zorgt voor lagere verwerkingskosten en omdat er meer tijd kan worden besteed aan de kerntaken. Algemeen zorgt dit voor een verhoging in productiviteit en efficiëntie. Tot slot is er naast deze operationele voordelen ook een verbetering van de dienstverlening naar de klanten toe. Door de elektronische toepassingen zal het niet altijd nodig zijn om mankracht in te zetten en zullen de systemen dag en nacht beschikbaar kunnen blijven

Vooraleer bedrijven zullen overstappen naar zulke elektronische processen zullen ze eerst onderzoeken of de baten van het systeem zullen opwegen tegen de implementatiekost van de noodzakelijke IT infrastructuur. De kost zal hoger zijn naarmate men een hoger niveau van veiligheid wenst. De onderneming zal moeten beslissen wat voor hun als voldoende wordt geacht. Naast de implementatiekost moet er ook rekening gehouden worden met systeemonderhoudskosten, training, updates, etc…

Verder zijn er risico's verbonden aan het gebruiken van publieke sleutel technologie voor een digitale handtekening, namelijk fraude, het niet kunnen voldoen van deze technologie aan zijn doel en de verantwoordelijkheid. Ondernemingen zouden deze risico's moeten evalueren op twee verschillende vlakken. Ten eerste moet men zich afvragen of het gebruik van PKI technologie zorgt voor nieuwe risico's. Als dat zo is moeten de grootst mogelijk monetaire en ontastbare verliezen geschat worden. Ten tweede is het belangrijk het relatieve risico te kennen; dit wil zeggen het risicoverschil met de huidige systemen die dezelfde diensten aanbieden. *(Simons, 2005)*

Wat betreft fraude is het zeer moeilijk identiteit-fraude te plegen bij het correcte gebruik van een digitaal certificaat door de efficiëntie van PKI. Maar stel nu dat iemand in het bezit raakt van een ander zijn private sleutel, dan kan deze persoon frauduleuze documenten ondertekenen.. Ook kan het gebeuren dat de eigenaar van het certificaat zelf een fout maakt

doordat het gehele document niet zichtbaar was of omdat de handtekening ‘per ongeluk’ wordt gezet. Doordat dit ondertekenen elektronisch gebeurt is het moeilijker personen te vervolgen wegens fraude Er zijn immers geen biometrische of forensische elementen zoals bij de geschreven handtekening waaruit blijkt dat de handtekening gezet is door de persoon die fraude pleegt.

Om dit soort fraude tegen te gaan is het uiteraard bijzonder belangrijk dat een individu kan gelinkt worden aan een bepaalde transactie. Ook moet kunnen bewezen worden dat de betreffende persoon wel werkelijk de bedoeling had het document te handtekenen en bijvoorbeeld niet zomaar op een knopje duwde om iets uit te proberen. Tenslotte zou er een digitaal getekend attest verzonden moeten worden na de transactie waarin precies vermeld wordt wat is overeengekomen. *(Simons, 2005)*

Een ander risico van het gebruik van de digitale handtekening is het risico van het niet kunnen verschaffen van de nodige diensten. Vermits er gewerkt wordt met elektronische processen is er altijd een risico op technische panne. Het is dus belangrijk voor een onderneming om methodes te ontwikkelen om met de mogelijke tekortkomingen van zulke systemen om te gaan.

Het is dus duidelijk dat bedrijven de baten van een digitale onderneming moeten afwegen tegenover de kosten en de risico’s ervan. Ook moet men rekening houden dat zelfs wanneer de digitale handtekening soms niet rendabel lijkt in eerste instantie, dit op lange termijn wel eens zou kunnen veranderen.

8 Codetheorie

Codetheorie, niet te verwarren met cryptografie, is een onderdeel van de informatietheorie dat zich richt op het toevoegen van redundantie aan gecodeerde informatie, waardoor het beter beschermd is tegen transport over een kanaal met een zekere kans op fouten. *(http://nl.wikipedia.org/wiki/Coderingstheorie)*

Er bestaan twee vormen van codering, namelijk broncodering en kanaalcodering. Voor de digitale handtekening wordt gebruikt gemaakt van kanaalcodering. Bij kanaalcodering worden symbolen toegevoegd aan de gecodeerde informatie, ter bescherming van het transport over het kanaal.

Er bestaan twee vormen van bescherming tegen fouten op een kanaal: foutdetectie en foutcorrectie. Foutdetectie geeft aan de ontvangstzijde een indicatie dat er fouten zijn opgetreden. De ontvanger kan in dat geval aan de zender vragen om hertransmissie van de foutief ontvangen informatie. Bij foutcorrectie is de ontvanger in staat om uit de foutief ontvangen informatie te herleiden wat de meest waarschijnlijk verzonden informatie was; hierbij wordt gebruik gemaakt van een zogenaamde 'foutcorrigerende code'. De foutkans kan hierdoor worden verkleind, maar wordt nooit helemaal nul. Wetenschappers die een belangrijke rol hebben gespeeld in de codetheorie zijn onder andere Richard Hamming, Andrew Viterbi, Claude Shannon, Neil Sloane en Robert Gallager.

De codetheorie heeft twee toepassingen: 1) het verschaffen van een grote zekerheid van juistheid van de verzonden boodschap, 2) om bij kanalen waar zeer hoge foutpropagaties voorkomen toch nog een beeld te krijgen van de verstuurde boodschap (bijvoorbeeld in de ruimtevaart).

8.1 Verschillende types codes

Een aantal eenvoudige foutdetecterende codes, waarvan we er enkele hier kort beschrijven, waren reeds eerder in gebruik, maar een echte doorbraak kwam er pas bij de Hamming-code. Deze is bij een zelfde percentage redundantie veel meer effectief.

8.1.1 Pariteitsbit

Bij de pariteitsbit wordt er een enkele bit toegevoegd aan een codewoord. Deze bit geeft aan of het codewoord al dan niet even of oneven is in bitaantal. Wanneer er een enkelvoudige bitfout optreedt door de transmissie zal de pariteit veranderen en wordt zo de fout gedetecteerd. Probleem is er echter wanneer we te maken hebben met een even aantal bitfouten. Deze worden niet opgemerkt door deze methode. Bovendien kan men bij detectie van een fout geen uitsluitsel geven over welke bit fout ontvangen is. De enige correctiemethode die bijgevolg mogelijk is, is het uitvoeren van een hertransmissie.

8.1.2 Constant gewicht code

Deze code, ook wel de ‘two-of-five’-code genoemd door Bell, houdt in dat elk 5-bits codewoord exact twee enen bevat. Als men dus een woord ontvangt met niet exact twee enen, dan vindt er foutdetectie plaats. Bij deze code kan het echter ook voorkomen dat er 2 bitfouten in 1 woord niet worden gededecteerd.

8.1.3 Repetitie code

De repetitiecode is een code die ieder bit een aantal malen herhaalt. Als er bijvoorbeeld een bit met waarde 1 moet worden verzonden, dan zal bij een repetitiecode 3 het woord “111” worden verzonden. Als de drie bits die ontvangen worden niet identiek zijn is er foutdetectie. Bij de repetitie code is er ook een foutcorrigerende toepassing, immers, bij ontvangst van 000, 001, 010 of 100 wordt de gedecodeerde databit een 0 (meer nullen als enen), terwijl bij ontvangst van 111, 110, 101 of 011 resulteert in decodering tot 1. Deze code kan echter niet alle codes op correcte wijze corrigeren. Bovendien is de repetitiecode zeer inefficiënt.

8.2 De Hamming-code

Een Hamming-code is een foutcorrigerende code die men gebruikt in de telecommunicatie. De code is genaamd naar zijn uitvinder, Richard Hamming. Hamming-codes zijn lineaire codes, die 1 of 2 bitfouten kunnen detecteren en bovendien 1 bitfout corrigeren. Dit in tegenstelling tot andere pariteitscontroles zoals de enkelvoudige pariteitscontrole (met 1 pariteitsbit) die een even aantal bitfouten niet detecteert en die geen hulp kan bieden voor het corrigeren van gevonden bitfouten.

8.2.1 Historiek

Hamming werkte bij Bell Labs aan de Bell Model V computer. De invoer van gegevens vond plaats via ponskaarten, waar altijd leesfouten bij optraden. Tijdens weekdagen zorgde een speciale code ervoor dat fouten werden gedetecteerd en via lichtsignalen de operators werden gewaarschuwd, zodat die het probleem konden verhelpen. Buiten kantooruren en tijdens weekends, wanneer er geen operators aanwezig waren, ging de machine eenvoudigweg door met de volgende taak. Hamming werkte tijdens weekends, en werd steeds gefrustreerder over het opnieuw moeten starten van zijn programma's vanwege de onbetrouwbaarheid van de kaartlezer. Gedurende een aantal jaren werkte hij aan het vraagstuk van foutcorrectie, waarbij hij een set krachtige algoritmes ontwikkelde. In 1950 publiceerde hij wat nu bekend staat als de Hamming-code, die momenteel nog steeds toegepast wordt. (*http://nl.wikipedia.org/wiki-/Hamming-code*)

8.2.2 Werkingsprincipe

Hoe zit deze Hamming-code nu in elkaar. Wanneer er foutcorrigerende bits worden toegevoegd aan een boodschap, en als deze bits zo gerangschikt worden dat eventuele foutieve bits verschillende effecten (altijd verschillende codes) opleveren, dan worden de foutieve bits identificeerbaar. Dit is het sterke punt van de Hamming-code. Stel bijvoorbeeld een boodschap van 7 bits. Zo een boodschap impliceert dat er 7 enkelvoudige bitfouten mogelijk zijn. Wanneer men 4 extra bits toevoegt, is dit voldoende om aan te geven of er al dan niet een fout

is opgetreden, en bovendien kan men weten welke bit foutief is. Hoe dit werkt wordt dadelijk uitgelegd.

Door het bestuderen van de bestaande codes zocht Hamming generalisaties. Hij ging op zoek naar de information rate, waarmee hij het aantal bits nodig voor transactie deelde door het eigelijk aantal bits van de code. Dus bijvoorbeeld bij de pariteitscode van een 5 bit boodschap is de information rate 5/(5+1)= 5/6. Om nog een ander voorbeeld te geven, bij de repetitiecode is de information rate van een 1 bit code woord = 1/3.

Een tweede punt waar Hamming aandacht aan besteedde was in verband met problemen die ontstonden wanneer er twee of meerdere bitfouten optraden. Hiervoor ontwikkelde hij het concept de Hamming-afstand. Bij de Hamming-afstand wordt er gekeken hoeveel bitfouten er nodig zijn vooraleer deze fouten niet meer opgemerkt worden. Dus ter illustratie: de pariteitscode heeft een Hamming-afstand 2, want iedere tweevoudige bitfout wordt niet meer opgemerkt. De repetitiecode van een 1 bit boodschap heeft een afstand 3, want van een correct codewoord (000 of 111) moeten er drie bits gewijzigd worden om een ander correct codewoord te vormen.

Het uiteindelijke doel van Hamming was nu een code te ontwikkelen die zowel de afstand zo groot mogelijk maakte (en dus het foutcorrigerende vermogen verhoogde), en de information rate zo groot mogelijk trachtte te krijgen (dus de gemiddelde informatie-inhoud zo hoog mogelijk). Hij ontwikkelde uiteindelijk een code waarvan de pariteitsbits zowel elkaar controleerde als de databits.

Het gegeneraliseerde algoritme van de Hamming-code is simpel:
(*http://nl.wikipedia.org/wiki/Hamming-code)*

- Alle bitposities die een macht van twee zijn worden gebruikt als pariteitsbits (bitposities 1, 2, 4, 8, 16, 32, 64, etc.)

- Alle overige bitposities worden gebruikt voor de te coderen data (bitposities 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, etc.)

- Ieder pariteitsbit berekent de pariteit voor een aantal bits uit het codewoord. De positie van het pariteitsbit bepaalt de rij van de bits die wel resp. niet worden meegenomen in het berekenen van het pariteitsbit :
  pos. 1: skip 1 bit, check 1 bit, skip 1 bit, check 1 bit, etc.
  pos. 2: check 1 bit, skip 2 bits, check 2 bits, skip 2 bits, check 2 bits, etc.
  pos. 4: check 3 bits, skip 4 bits, check 4 bits, skip 4 bits, check 4 bits, etc.
  pos. 8: check 7 bits, skip 8 bits, check 8 bits, skip 8 bits, check 8 bits, etc.
  pos. 16: check 15 bits, skip 16 bits, check 16 bits, skip 16 bits, check 16 bits, etc.
  pos. 32: check 31 bits, skip 32 bits, check 32 bits, skip 32 bits, check 32 bits, etc.
  enzovoorts

8.2.3 Voorbeeld

Beschouw het 7-bit datawoord "0110101". Zie de tabellen ter illustratie van hoe Hamming-codes worden ontworpen en gebruikt om een fout te detecteren. Met **d** wordt een databit aangegeven, en met **p** een pariteitsbit.

Eerst worden de databits in de correcte bitpositie geplaatst en vervolgens worden de pariteitsbits berekend, steeds uitgaande van *even* pariteit. Dit wil zeggen dat de pariteitbit een waarde 1 krijgt wanneer de som van de rij oneven is een waarde 0 wanneer de som van de rij even is.

De rijen worden als volgt bepaald : bij pariteitsbit p_1 begint men bij de eerste bit (in dit geval p_1 die voorlopig nog geen waarde heeft) en laat vervolgens telkens één positie open (omdat p_1 overeenkomt met bitpositie 1) ; bij pariteitsbit p_2 begint men bij de tweede bit (in dit geval p_2 die voorlopig nog geen waarde heeft) en de derde bit (dus in paren van twee) en laat vervolgens twee posities open (omdat p_2 overeenkomt met bitpositie 2); zo gaat men verder,

bij p_3 zal men dus starten bij de derde, vierde en vijfde bit (groep van 3) en vervolgens 3 plaatsen tussen laten, enz.

Tabel 8 : Berekening van Hamming-code pariteitsbits

	p_1	p_2	d_1	p_3	d_2	d_3	d_4	p_4	d_5	d_6	d_7
datawoord (zonder pariteit):			**0**		**1**	**1**	**0**		**1**	**0**	**1**
p_1	**1**		0		1		0		1		1
p_2		**0**	0			1	0			0	1
p_3				**0**	1	1	0				
p_4								**0**	1	0	1
codewoord (met pariteit):	**1**	**0**	0	**0**	1	1	0	**0**	1	0	1

Het codewoord (met pariteitsbits) is "10001100101".

Neem nu aan dat het laatste bit foutief wordt ontvangen. Ons ontvangen woord is "10001100100"; en nu zetten we ieder pariteitsbit op 1 indien de pariteitscontrole een foutdetectie oplevert (dus wanneer de som van de rij oneven is).

Tabel 9 : Controle van pariteitsbits (gewijzigde bit gemarkeerd)

	p_1	p_2	d_1	p_3	d_2	d_3	d_4	p_4	d_5	d_6	d_7	**Pariteitscheck**	**Pariteitsbit**
Ontvangen woord:	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	
p_1	**1**		0		1		0		1		0	**Detectie**	**1**
p_2		**0**	0			1	0			0	0	**Detectie**	**1**
p_3				**0**	1	1	0					Correct	0
p_4								**0**	1	0	0	**Detectie**	**1**

De laatste stap is het bepalen van de waarde van de pariteitsbits (het bit met de laagste waarde gaat het verste naar rechts). De decimale waarde van de pariteitsbits is 11, waaruit volgt dat het elfde bit in het ontvangen woord (incl. pariteitsbits) foutief is, en dus dient te worden geïnverteerd.

	p_4	p_3	p_2	p_1	
binair	1	0	1	1	
decimaal	**8**		**2**	**1**	**Σ = 11**

Inverteren van het elfde bit verandert 10001100100 terug naar 10001100101. Verwijderen van de Hamming pariteitsbits levert het oorspronkelijke datawoord 0110101 op.

De dag van vandaag wordt met de Hamming-code een specifieke (7,4) code aangeduid. Deze code kan iedere enkelvoudige bitfout corrigeren, en alle dubbele bitfouten detecteren. Hierdoor is men met de Hamming-code verzekerd van foutvrij dataverkeer.

Men kan de Hamming-code ook definiëren als een lineaire code waarvoor de kolommen van de pariteitstestmatrix gelijk zijn aan de binaire voorstelling voor de getallen van 1 tot n. Voor meer informatie hieromtrent verwijzen we naar de boeken “Error correcting coding and security for data networks” van Kabatiansky e.a.(2005) en “Opgaven over moderne algebra – Kode theorie” van Lemeire (1992).

9 Elektronische facturatie

Noot: De begrippen elektronische facturatie, digitale facturatie en e-invoicing worden door elkaar gebruikt en als gelijk beschouwd.

In dit hoofdstuk behandelen we een elektronische toepassing waar veel bedrijven momenteel, of toch zeker in de toekomst mee zullen geconfronteerd worden, namelijk elektronische facturatie. Het versturen van elektronische facturen is elektronische informatie-uitwisseling en er zal dus nood zijn aan cryptologie en de digitale handtekening om deze communicatie veilig te laten verlopen.

'De factuur is wellicht het belangrijkste document in het handelsverkeer, en elektronisch factureren een van de hoekstenen van digitaal Europa', aldus Ine Lejeune, vennoot van Pricewaterhouse Coopers Belastingadviseurs.

In 2000 werd reeds gesteld dat een harmonisering van de regels inzake facturatie aan de hand van elektronische factureren bedrijven vele miljarden euro's zou besparen. Dagelijks versturen Belgische bedrijven zo'n 800.000 tot 900.000 facturen. Daarbij hoort uiteraard een gigantische papierberg en administratiekosten. Een groot Belgisch nutsbedrijf zit maandelijks aan twee kartonnen dozen met factureren van zijn mobilofoonleverancier. Het is dan ook niet meer dan logische dat de bedrijven druk uit begonnen te oefenen op de operatoren en zelf gaan investeren in elektronische facturatie. *(De financieel economische tijd, 2005)*

Elektronische facturatie zou een einde moeten maken aan deze gigantische papierberg van facturen. Maar zoals altijd met nieuwigheden vergt deze omschakeling tijd.

Van in het begin werden er platformen opgericht, zoals het digitaliseringplatform dat past in het project 'The Digital Company' van PwC en Landwell, die er voor trachten te zorgen dat bij de omzetting van de richtlijn inzake elektronische facturatie in de Belgische wetgeving er

geen discrepanties ontstaan met andere wetgevingen. Ook zou de Belgische oplossing internationaal competitief en goedkoop moeten zijn. De baten van elektronische facturatie staan vast mits de kosten laag blijven. *(De financieel economische tijd, 2005)*

In het begin was het toegestaan een elektronisch factuur te verzenden, maar daarnaast was er ook nog een papieren exemplaar vereist. Begin 2002 werd deze wettelijke beperking verholpen aanvankelijk door een nieuwe Europese richtlijn en later vertaald in de Belgische wetgeving, zie hiervoor de paragraaf 'wetgeving'. Eens deze wettelijke beperkingen van de baan zijn, is er nog een hindernis: de huidige manier van werken. Bepaalde gewoontes, zoals het afstempelen of fotokopiëren bij ontvangst is niet meer mogelijk bij de elektronische factuur. De elektronische factuur zal een aanpassing vergen van de bedrijfsprocessen.

Een van de verschaffers, Isabel, besloot in 2004 zelf over te stappen naar het uitsluitend elektronisch facturen. Door deze invoering bespaart Isabel op jaarbasis 330.000 euro. Dit eigen overstappen moet klanten overtuigen van het systeem. Het werkte blijkbaar want drie belangrijke klanten van Isabel, Fortis Lease, Randstad en Partena volgden in het gefaseerde overstapplan van Isabel. Deze drie maken samen twee miljoen facturen per jaar. Hierna in 2005 volgen ook de andere grootste uitzendkantoren van België voor de facturen van de uitzendkrachten. Adecco, Crey's, Manpower, Randstad en Vedior tellen samen 25.000 klanten en versturen jaarlijks een miljoen facturen. De omzetting naar elektronische facturatie levert hun op termijn een miljoenenbesparing op. De vijf beseffen dat de factuur geen concurrentiemiddel is maar een standaarddocument en besloten daarom een standaardfactuur te ontwerpen dat door bedrijven makkelijk kan worden verwerkt in de elektronische boekhouding. Er wordt gehoopt dat de andere sectoren het voorbeeld van de uitzendsector volgen. *(De financieel economische tijd, 2005)*

Eind 2005 publiceert PwC een onderzoek verricht in tien Europese lidstaten. Voorspeld wordt dat de elektronische facturatie fors zal toenemen in de komende twaalf maanden. Slechts 27 procent van de grootfactureerders (minstens 100 miljoen euro omzet) verzendt elektronische facturen naar zijn klanten en een even grote groep van 27 procent ontvangt elektronische

facturen van zijn leveranciers. Samen levert dat een groep van 36 procent van bedrijven die vrij intensief gebruik maken van elektronische facturatie. Een groep van 48 procent is bezig met de invoering (20%) of plant de invoering (28%) in de komende twaalf maanden. Ruim een kwart van deze bedrijven versturen jaarlijks meer dan 500.000 facturen. Het probleem is dat veel bedrijven ten onrechte denken dat elektronisch factureren nog veel vergunning vergt en technisch ingewikkeld is. Zij lopen daardoor veel concurrentie voordelen mis. Kostenbesparingen, snellere betaling en hogere efficiëntie zijn de drie belangrijkste voordelen die de ondernemingen aanstippen. Het gebrek aan voorbereiding bij de klanten en de niet-aangepaste eigen informatiesystemen worden samen met de hoge investeringskosten als belangrijkste hinderpalen aangeduid. *'Het gebrek aan informatie over de juridisch, fiscale en technologische aspecten wekt bij vele bedrijven de valse indruk dat nog veel problemen opgelost moeten worden vooraleer ze vlot kunnen elektronisch factureren'*, aldus Danieël Evrard, accountant PricewaterhouseCoopers. *(De financieel economische tijd, 2005)*

Met deze inleiding willen we aanhalen dat de tijd voor de overstap naar elektronische facturatie rijp lijkt. We starten dit hoofdstuk met de algemene definities van de factuur en de elektronische factuur, waarna we vervolgens de wetgeving, werking en voor- en nadelen behandelen. Tot slot halen we kort de reacties van de bevoorrechte getuigen en de antwoorden uit de korte bevraging aan en proberen we met de kennis uit zowel de praktijk en de literatuurstudie een conclusie te vormen omtrent het elektronisch factureren.

9.1 Wat is een factuur?

Van Dale: lijst van geleverde goederen met vermelding van de prijzen en de datum van levering

Een factuur is dus een document, dat een betalingsverplichting van een klant aan een leverancier weergeeft. De factuur omvat doorgans de volgende informatie *(www.ey.be)*:

Vanboven bij de factuur (de factuurkop) vind men algemene gegevens betreffende de gehele factuur, zoals:

- Leveranciersnaam
- Adresinformatie
- Gegevens over inschrijving bij de kamer van koophandel
- BTW-nummer
- De klant
- De identificatie van de factuur (het factuurnummer)
- Factuurdatum
- Het ordernummer van de klant

In het midden van de factuur vindt men de verschillende regels van producten te betalen. Een factuur kan betrekking hebben op meerdere goederen en diensten die zijn geleverd, inclusief de aantallen en de prijzen die hiervoor gelden.

Tenslotte is er naast de kop met algemene gegevens ook meestal nog een voet of totaal met informatie, zoals:

- Nettobedrag
- BTW bedrag
- Het te betalen bedrag, inclusief BTW, het brutobedrag
- Betalingsvoorwaarden
- Betaalmogelijkheden
- Algemene leveringsvoorwaarden

9.2 Wat is elektronisch factureren?

Electronisch factureren wordt gedefinieerd als *"de uitwisseling van facturen in een electronisch formaat via een beveiligd computernetwerk"*. Elektronische facturatie

automatiseert het facturatie-proces van A tot Z. Alle papieren facturen zijn vanaf nu verleden tijd. De facturatie gebeurt volledig in een virtuele infrastructuur. Het is mogelijk facturen digitaal te verzenden, digitaal te ontvangen en digitaal wettelijk te ondertekenen. Voorts worden de facturen op eenvoudige wijze gearchiveerd. Het is ondermeer door de ondertekening op basis van de digitale handtekening dat de elektronische factuur een wettelijke status verwerft. Hierdoor is het bijvoorbeeld niet meer nodig om een kopie te bezitten van elk factuur voor de BTW-administratie. Het gevolg zal een dematerialisatie van de factuur zijn. *(Certipost, 2006)*

Microsoft verdeelt elektronische facturatie in de volgende twee soorten:

- **electronic bill presentment & payment (EBPP)**: het aanbieden en betalen van facturen via internet in een business to consumer-context (B2C). Dit is meestal een vrij eenvoudig proces dat vooral populair is bij bedrijven met veel klanten, zoals nutsbedrijven.
- **electronic invoice presentment & payment (EIPP)**: het aanbieden en betalen van facturen via Internet in een business to business-context (B2B). Hiervoor bestaat veel interesse, maar het is meestal een vrij complex proces, vooral vanwege de BTW-regelmentering. In de praktijk wordt het dan ook nog maar mondjesmaat toegepast, hoewel de return on investment aanzienlijk kan zijn.

Verder onderscheidt Microsoft drie modellen van elektronische facturatie:

- **seller direct:**

  De verkoper is de dominante partij en stelt een elektronische factuur op voor zijn klanten. Hij draagt het merendeel van de kosten voor de oplossing en haalt er ook de meeste voordelen uit, bijvoorbeeld door de oplossing te gebruiken voor marketingdoeleinden. De koper maakt weinig of geen kosten maar moet wel met verschillende systemen kunnen werken. Dit is een courant model in B2C-sectoren met veel uitgaande facturen, zoals productie, nutsvoorzieningen, gezondheidszorg en financiële diensten.

- **buyer direct:**
  De koper is de dominante partij en legt elektronische facturatie op aan zijn leveranciers. Dit model vindt stilaan ingang bij grote inkopers die veel facturen binnenkrijgen. De koper draagt de meeste kosten maar heeft ook het grootste voordeel. De verkoper kan elektronische facturatie aangrijpen om de relatie met zijn koper te verstevigen. Hij maakt minder kosten maar moet wel met verschillende systemen kunnen werken.
- **consolidator:**
  Koper en verkoper werken via een tussenliggend platform zoals dat van Certipost en Isabel. Deze aanpak wint aan populariteit vanwege de complexiteit van de twee voorgaande modellen. Hij is bovendien geschikt voor elk soort koper of verkoper. Het systeem biedt verkopers en kopers minder extra voordelen, maar iedereen hoeft wel maar één keer te integreren met een extern platform.

In dit hoofdstuk leggen we de klemtoon op deze laatste variant, namelijk het elektronisch factureren tussen de bedrijven met een tussenliggend platform.

9.3 Wetgeving

Het startschot voor de digitale factuur werd gegeven door de op 1 januari 2004 gepubliceerde Europese richtlijn over elektronische facturatie. Deze richtlijn, geldend voor alle lidstaten, heeft tot doel de voorschriften op het gebied van elektronische facturatie te vereenvoudigen en te synchroniseren met de bestaande wetgeving waardoor er een deel voorwaarden en beperkingen verleden tijd worden.

Deze Europese richtlijn 2001/115/EG die ‘met het oog op de vereenvoudiging, modernisering en harmonisering van de ter zake van de facturering geldende voorwaarden op het gebied van de belasting over de toegevoegde waarde’ de tot dan geldende Richtlijn 77/388/EEG wijzigde, werd wat later vertaald in de Belgische wetgeving. Hoewel de datum op 1 januari was

vastgelegd, dateert de eigenlijke wet van 28 januari 2004. Dankzij de publicatie van de wet in Bulletin of Acts op 10 februari is elektronische facturatie dus sinds februari 2004 wettelijk ondersteund in België en de Europese Unie. Door deze goedkeuring staat België ongeveer even ver als de andere landen van de EU, waar meestal wel reeds een wet was gestemd vóór het einde van 2003, maar waar het nog wachten was op uitvoeringsbesluiten. De krachtlijnen in het ingediende wetsontwerp, zoals voorzien in de Europese Richtlijn zijn: een geharmoniseerde lijst van verplichte vermeldingen die een factuur moet bevatten (de in de Belgische regelgeving voorgeschreven vermeldingen worden niet uitgebreid, zie paragraaf 'Wat is een factuur'); een aantal gemeenschappelijke voorwaarden voor elektronische facturering, elektronische opslag van facturen, eigenhandige facturering (selfbilling) en uitbesteding van factureringswerkzaamheden. Ook wordt nog verduidelijkt dat, waar nodig, de voorkeur zal worden gegeven aan de eenvoudigste bestaande (technische) oplossing.

Er rijst ook de vraag of er op termijn een verdere stap voor de e-factuur zou kunnen genomen worden. Men denkt aan een Europese harmonisatie zodat alle lidstaten tot één enkele 'Europese factuur' zouden komen. Een Europese factuur-werkgroep houdt zich op dit moment bezig met het inventariseren en interpreteren van de huidige factuurgegevens voor alle deelnemende landen. Uit de eerste werkzaamheden van deze werkgroep, die uiteraard geen wetgevende bevoegdheden heeft, is echter al gebleken dat het water tussen de verschillende lidstaten erg diep is. Het blijkt zelfs moeilijker dan verwacht om vast te stellen of begrippen met eenzelfde naam wel dezelfde lading dekken, en omgekeerd, om na te gaan of begrippen met op het eerste gezicht eenzelfde invulling, inderdaad volledig identiek zijn. Voorlopig zal er echter voldoende uitdaging liggen in het implementeren van de elektronische factuur in België.

9.3.1 Belangrijke voorwaarden

Authenticiteit en integriteit

Een wettelijke elektronische factuur moet de authenticiteit van de herkomst en de integriteit van de inhoud ondubbelzinnig waarborgen. Het moet duidelijk zijn wie de factuur heeft

opgesteld en er moet worden gegarandeerd dat de inhoud ervan niet is gewijzigd tussen het ogenblik van versturen en de aankomst ervan bij de klant. De Richtlijn zelf voorziet in twee mogelijkheden namelijk het gebruik van een digitale handtekening enerzijds en het klassieke EDI anderzijds. Het zijn opt-out opties wat betekent dat deze technieken standaard zijn en dat alle lidstaten ze moeten aanvaarden. Anderzijds voorziet de Richtlijn in één opt-in mogelijkheid, d.w.z. dat de lidstaten zelf mogen beslissen of ze die al dan niet aanvaarden. Het betreft hier alle andere methoden die in de praktijk ook voldoende garanties voor authenticiteit van de herkomst en integriteit van de inhoud bieden waarbij het hier niet gaat om een expliciet technisch omschreven oplossing, de garantie kan evengoed in de gevolgde procedure ingebed zitten.

Archivering

Een ander veel besproken aspect is de elektronische archivering van de factureren. Veel (grote) bedrijven maakten voor hun debiteurenadministratie immers reeds gebruik van EDI. Dit zorgde reeds voor een verregaande vereenvoudiging van de factuuropvolging maar de wet erkende deze elektronische documenten niet als wettelijk, zodat de papieren versie onontbeerlijk bleef. Die ‘klassieke’ factuur moet bovendien gedurende lange tijd worden bewaard (tien jaar in België). Voor grote bedrijven betekent dit al gauw over een papierberg van ettelijke kubieke meter, die gemakkelijk een hele verdieping vult.

De nieuwe Richtlijn maakt het nu wel mogelijk om de factuur elektronisch te archiveren, zolang de leesbaarheid, de authenticiteit van de oorsprong en de integriteit van de inhoud van de facturen maar wordt gewaarborgd. Tevens mag het archief in een andere lidstaat van de Europese Unie bevinden, op voorwaarde dat de administratie er online toegang toe heeft.

Sommige dienstverleners inzake certificaten en elektronische facturatie bieden een bijkomende waarborg aan, namelijk notarisatie. Zij achten het noodzakelijk om bijkomende maatregelen te nemen om een 100% afdoende garantie te waarborgen op lange termijn. Zij notariseren de facturen en garanderen zo zowel de authenticiteit van herkomst als de integriteit van de inhoud van uw factuur gedurende de volledige archivagecyclus. Deze methode biedt

eveneens een extra veiligheid inzake onweerlegbaarheid : ook de zender kan zijn transactie bewijzen dankzij de notarisatielijsten.

Outsourcing

Verder regelt de Richtlijn tenslotte ook het uitbesteden (outsourcen) van het factureringsproces aan derden. De Richtlijn erkent het principe, waarbij het voor de lidstaten onmogelijk is de richtlijn te beperken, met uitzondering voor het uitbesteden aan een bedrijf buiten de Europese Unie, want in dat geval mogen de lidstaten wél beperkende maatregelen invoeren. Ook voor eigenhandige facturering (selfbilling), waarbij de klant zelf zijn facturen opmaakt, kunnen de lidstaten zélf beperkingen invoeren. Beide partijen moeten daar voorafgaandelijk een akkoord over hebben. Verder moet elke self bill worden goedgekeurd door de leverancier: de lidstaten beslissen zelf welke procedure daarbij wordt gevolgd. De selfbilling-techniek is echter niet gekoppeld aan het elektronisch factureren.

9.4 Hoe werkt het?

Elektronische facturen worden gemaakt met behulp van een financiële applicatie, zoals boekhoudsoftware. Ze kunnen verstuurd worden van de ene computer naar de andere, en automatisch geïntegreerd worden in een applicatie of database. Voorts kan men deze facturen versturen langs een publiek netwerk zoals het Internet, of via private netwerken. Hierbij gebruikt men verschillende communicatie protocollen. De factuur kan in verschillende document standaarden worden opgesteld zoals XML, EDI, ASCII of ERP.

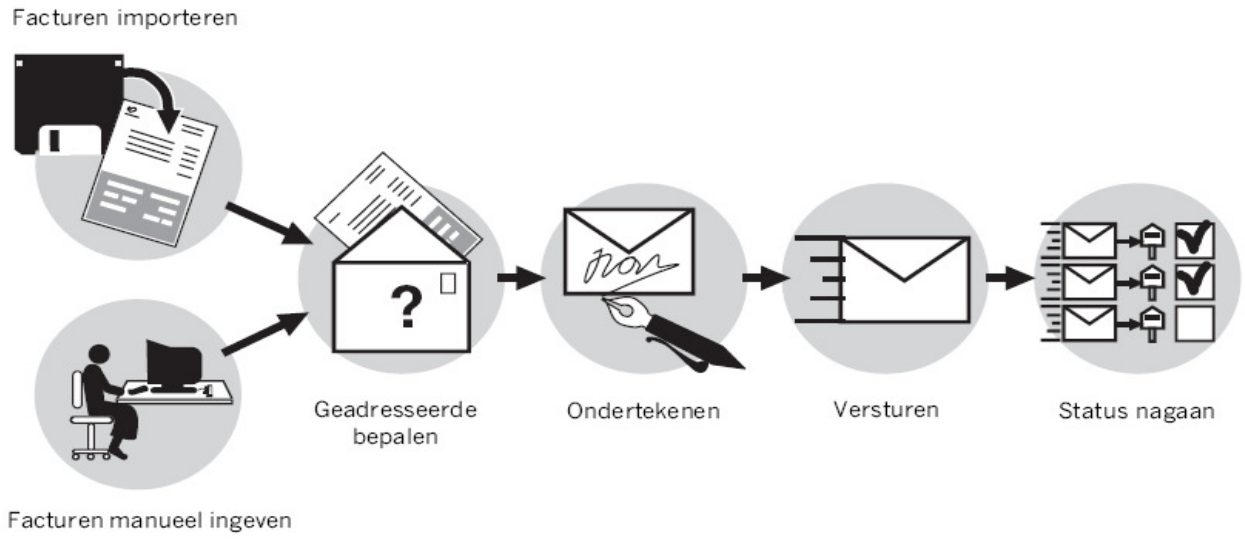
9.4.1 Versturen

Bij de meeste platformen die elektronische facturatie aanbieden moet men verschillende stappen doorlopen om een elektronische factuur te versturen. Eerst moet er natuurlijk voor gezorgd worden dat de inhoud van de factuur beschikbaar is in het programma. Hier zijn er twee mogelijkheden: u kunt de factuur importeren uit een boekhoudpakket of u kunt de factuur manueel ingeven.

Bij het versturen van elektronische facturen is het belangrijk dat de geadresseerde eenduidig vastgelegd wordt. Om een factuur te kunnen verzenden, moet het adres van de klant ingevuld zijn. Het programma heeft voldoende aan een eenmalige toewijzing van het adres van een bepaalde klant, zodat er voor volgende facturen die naar deze klant worden verstuurd het adres niet meer hoeft toegewezen te worden.

Vooraleer een factuur verstuurt wordt, moet deze zijn voorzien van de digitale handtekening van het bedrijf zodat de ontvanger ondubbelzinnig kan vaststellen dat de factuur van het juiste bedrijf afkomstig is.

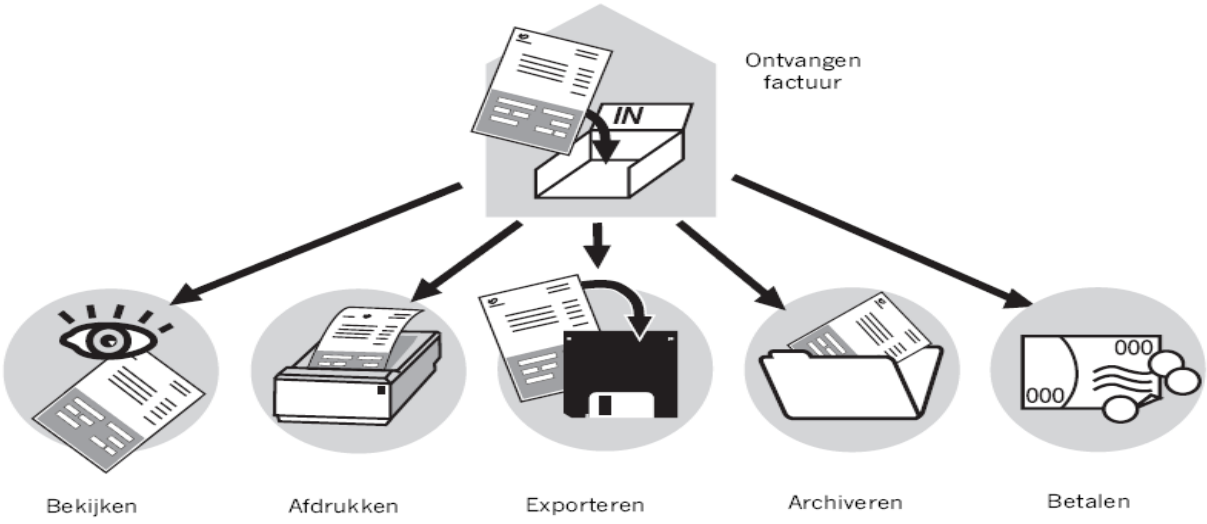
Wanneer de factuur ondertekend is, is ze klaar voor verzending. Na de verzending is het mogelijk om de factuur op te volgen door de status van de ontvangstbevestiging te bekijken. Let wel dat een ontvangstbevestiging enkel garandeert dat een factuur technisch leesbaar is (volgens de Edifact-norm). Het betekent niet dat de ontvanger akkoord gaat met de inhoud en de betaling van de factuur.



Figuur 12 : Het versturen van een elektronische factuur

9.4.2 Ontvangen

Bij elke factuur die er ontvangen wordt, wordt er automatisch een ontvangstbevestiging aangemaakt en klaargezet voor verzending. Bij ontvangst van een elektronische factuur kan men de volgende acties doorvoeren:



Figuur 13 : Mogelijkheden na ontvangst van een elektronische factuur

- De factuur bekijken
- De factuur afdrukken. Meestal zijn de afdrukken genormaliseerd: alle facturen worden afgedrukt in dezelfde vorm.
- Met de exportfunctie is het mogelijk facturen die men van klanten ontvangt, te exporteren naar een folder op de harde schijf voor verwerking door het boekhoudpakket. Dit kan manueel of automatisch gebeuren.
- De factuur archiveren. Het is wettelijk verplicht alle uitgaande en inkomende facturen in een archief te bewaren. Alle facturen zelf worden verzonden worden automatisch lokaal (op de pc) gearchiveerd. Ontvangen facturen moeten echter manueel gearchiveerd worden.
- De factuur betalen. Er zijn verschillende mogelijkheden voor elektronische betaling van de factuur. U kunt de betalingsbestanden in uw boekhoud- of ERP-pakket aanmaken en dan exporteren naar het facturatieprogramma voor verdere verwerking

door uw bank of er kan gebruik gemaakt worden van een automatische procedure voor het aanmaken van een overschrijvingsformulier waarop de gegevens van de factuur al ingevuld zijn.

9.5 Voordelen

- **Tijdsbesparing:** Dankzij de digitale facturatie zal men meer tijd hebben voor de kerntaken. De manuele, tijdrovende financiële handelingen worden vervangen door geautomatiseerde en snelle, elektronische documentenstromen. Hierdoor zal men ook sneller zaken kunnen opzoeken met behulp van een elektronisch archief. De dienstverlening (het call center) van het bedrijf zal minder oproepen moeten behandelen omdat de klant de mogelijkheid heeft van online toegang. Door de orde van de elektronische facturen zal er ook een snelle en makkelijke analyse van deze facturen mogelijk zijn.

- **Kostenbesparing:** De integratie van facturen in financiële toepassingen waardoor de tijdsinvestering van het personeel aanzienlijk slinkt, zal zorgen voor een verlaging van de operationele onkosten (zoals papier, postzegels, inkt, personeel, ...)van tot soms wel 70 procent. Bovendien zal men minder fouten maken door het uitschakelen van manuele processen. Uit onderzoek blijkt dat een papieren factuur de ondernemer gemiddeld € 1,65 kost (zonder rekening te houden met loonkost etc.). De kosten van een digitale factuur liggen aanzienlijk lager, ongeveer tussen € 0,30 en € 0,50. *(www.syntens.nl)*

- **Hogere ROI op uw financiële software en netwerkinfrastructuur:** Implementatie van elektronische facturatie zijn slecht minimale IT-investeringen door bestaande applicaties aan elkaar te koppelen via het Internet. Hierdoor verhoogt men het rendement op de bestaande informaticastructuur. Dus met een minimale investering meer besparen.

- **Gebruiksvriendelijk :** Op eender welk tijdstip is het mogelijk digitaal te factureren. Alles is te controleren zoals het tijdstip van verzending en het moment van ontvangst van de factuur door uw relatie.

- **Betere customer service :** Doordat de applicaties van het bedrijf worden gekoppeld aan die van uw klanten zal de administratie volledig automatisch en gestroomlijnd verlopen. Dit zal zorgen voor een grotere binding van de klant ten opzichte van de leverancier. Gevolg is dus een hogere omzet tegen lagere kosten.

- **Garanties inzake veiligheid :** Door het gebruik van de digitale handtekening en gekwalificeerde certificaten wordt er gezorgd voor de authenticiteit, de vertrouwelijkheid, de integriteit en de onweerlegbaarheid van de factuur.

9.6 Nadelen

Een aantal voordelen van de digitale factuur liggen voor de hand. Maar zijn er ook nadelen?

- **Kostenbesparing mogelijk?** Het gebruik van de digitale factuur wordt maar interessant wanneer een aanzienlijke kostenbesparing mogelijk wordt. Dat zal in grote mate afhankelijk zijn van de aantallen en de complexiteit van het factuurbeheer. Daarom is het noodzakelijk dat men de proef doet wat het factuurbeheer vandaag kost, maar ook om in detail te bekijken wat elektronische facturatie gaat kosten. Want zelfs als de variabele kost per factuur gevoelig daalt (eventueel ook door (efficiëntieverbetering), de opstartkost (software-ontwikkeling) en vaste kosten als verbindingen, back-up en opslagruimte gaan waarschijnlijk extra kosten.

- **Hoe gestructureerd zijn de bedrijfsprocessen?** Wanneer de administratie van het bedrijf al zwaar geautomatiseerd is zal de elektronische factuur waarschijnlijk niet veel

problemen scheppen. Al moet er toch rekening worden gehouden met de kosten om de applicaties een elektronische factuur te laten herkennen. Als het bedrijf standaardsoftware gebruikt, dan heeft de leverancier waarschijnlijk al eerder elektronische facturatie geïmplementeerd en zouden de kosten moeten meevallen. Wanneer het bedrijf echter helemaal niet geautomatiseerd is, dan kan het bedrijf dat waarschijnlijk beter eerst doen voor het zich aan elektronische facturen waagt. Digitale communicatie vereist immers structuur en die kan maar beter meteen aan de bron worden vastgelegd.

- **Zijn de correspondenten er klaar voor?** Het belangrijkste nadeel is echter dat het gebruik van de digitale factuur maar relevant wordt voor zover ook de correspondenten van het bedrijf van het medium gebruik maken. Denk maar aan de fax of e-mail. Met elektronische facturen geldt hetzelfde. Pas als de correspondenten er ook klaar voor zijn en ermee akkoord gaan, kan het bedrijf hen elektronische facturen toesturen. Er is echter wel de mogelijkheid om als pionier op te treden en andere bedrijven proberen te overtuigen of zelfs dwingen. Of bedrijven zouden promotieacties kunnen inbouwen voor diegenen die akkoord gaan met het uitwisselen van elektronische facturen.

9.7 Bedenkingen voordat men elektronische facturatie implementeert

Er zijn twee basiselementen die de aanpak bepalen, namelijk het klantenbestand en de geografische markt. Doet men aan business-to-business (B2B), of juist aan business-to-consumer (B2C)? Dit is belangrijk bij de keuze van een oplossing. Dit verschil heeft ook impact op de bereidheid van uw klanten om e-invoicing te aanvaarden, een cruciaal aspect voor het rendement van uw investering. Het tweede basiselement is de geografische markt. Werkt men nationaal, Europees of is men wereldwijd actief? Dit bepaalt sterk de complexiteit (wetgeving) van de oplossing.

Naast deze basiselementen zijn er nog andere factoren waarmee men rekening dient te houden. Het is noodzakelijk dat men de economische haalbaarheid van elektronisch factureren analyseert voor het bedrijf. Bedrijven zouden op zoek moeten gaan naar mogelijke flessenhalzen en andere problemen. Wanneer de organisatie te klein is voor een rendabele oplossing, dan kan men trachten de krachten te bundelen met zusterbedrijven of ondernemingen uit de sector. Een andere optie is te werken met outsourcing waarbij men nou samenwerkt met de klanten en leveranciers.

Het is belangrijk voor een goede return on investment (ROI) dat de oplossing snel aanslaat. Werken via een extern platform kan voordelen bieden wat betreft de snelheid.. Daarnaast is het geen slecht idee dat bedrijven een programma opstellen om de introductie bij klanten of leveranciers in goede banen te leiden. Voor een bedrijf met elektronische facturatie begint is het nodig dat men zich informeert bij de grootste klanten en leveranciers of zij plannen hebben of al een e-invoicing oplossing gebruiken. Het is belangrijk dat elk bedrijf zorgt dat zijn oplossing aan de behoeften van zijn cliënteel beantwoordt.

Een pluspunt voor de instap naar elektronische facturatie is wanneer men reeds vertrouwd is met technologie. Vele bedrijven hebben reeds een ERP-systeem in huis. Zij kunnen dit systeem onderzoeken naar de mogelijkheden voor elektronische facturering en archivering.

De uiteindelijke economische haalbaarheid van elektronische facturatie voor een bedrijf kan onderzocht worden via een klassieke break-even analyse die het minimum aantal elektronische facturen voor een rendabel project bepaalt. Meestal is een positieve return-on-investment al mogelijk als 12 tot 15 procent van de klanten of leveranciers de oplossing aanvaardt. Om de investering te laten renderen, moet de oplossing in elk geval snel ingang vinden. In de B2C-sector slorpt het overtuigen van klanten het grootste aandeel van de investering op, in de B2B-sector gaat dat naar de implementatie van de juiste software en de integratie met de bestaande systemen.

9.8 Praktijkonderzoek

In dit deel van het eindwerk gaan we de voordelen van elektronische facturatie, die vooropgesteld worden door de leveranciers van deze technologie, trachten te toetsen aan de realiteit.

In een bovenstaande paragraaf staan de voordelen beschreven die elektronische facturatie met zich mee zou brengen. Deze lijken op het eerste zicht logisch, maar toch zijn we benieuwd of de mogelijkheden van deze techniek niet zijn opgesmukt uit commerciële overwegingen.

9.8.1 Werkwijze

Een eerste stap was het interviewen van de heer Christian Luyten, de Sales Manager van Isabel, het toonaangevende bedrijf voor het verschaffen van de digitale handtekening. Het doel van dit interview was wat meer te weten te komen over de gebruikte algoritmes en technieken, maar vooral naar de mening van Isabel als leverancier omtrent de voordelen, gebruikvriendelijkheid en interesse in elektronische facturatie.

Met behulp van deze informatie en de informatie reeds bekomen uit de literatuurstudie hebben we twee korte online vragenlijsten opgesteld met behulp van de website “Student & Onderzoek”. U vindt deze in bijlage. Eén vragenlijst is gericht tot bedrijven die reeds gebruik maken van elektronisch facturatie, de andere vragenlijst is gericht tot bedrijven die deze technologie nog niet toepassen. Deze vragenlijsten werden verstuurd naar ongeveer 150 (voornamelijk Limburgse) ondernemingen met een bedrijfsgrote van minimaal 100 werknemers gaande tot bedrijven met een bedrijfsgrote van meer dan 1000 werknemers. Het leverde een dertigtal ingevulde exemplaren op.

De bedoeling van de vragenlijsten zijn:

1. Toetsen of de voordelen vernoemd in de literatuur en de voordelen gesteld door de leveranciers van elektronische facturatie inderdaad naar waarheid met de praktijk zijn

1. Polsen naar nadelen en punten waar verbetering mogelijk is
2. Polsen naar het vertrouwen in het systeem
3. Polsen naar wie de meest populaire leverancier is
4. Ontdekken of de techniek bij de bedrijven bekend is
5. Ontdekken waarom het systeem nog niet gebruikt wordt
6. Ontdekken welke voor- en nadelen niet gebruikers verwachten van het systeem

Het is echter niet de bedoeling met deze vragenlijsten een statistisch representatieve studie te verwezenlijken. De basisdoelstelling is meer informatie uit de praktijk te vergaren om zo het begrip elektronische facturatie beter te begrijpen.

Naast deze korte vragenlijsten deed de kans zich voor om Jean-Francois Renson, Manager van CF IT Projects & Business transformation Europe, te interviewen van het internationale bedrijf IBM. Aanvullend kregen we ook informatie van Didier Boullery en Werner Hanke, respectievelijk manager Client Process France en van de dienst Customer Fulfillment Systems & Applications Germany. Deze contactpersonen werden me aangereikt door de heer Jan Hulsbosch waarvoor dank.

9.8.2 Hypotheses en reactie

Hypothese 1 : Elektronische facturatie zorgt voor tijdsbesparing

Door de band genomen vinden gebruikers dat elektronische facturatie leidt tot tijdsbesparing. Bij enkele bedrijven is dit echter wel minder dan verwacht. Vooral de verwerking (‘handling’), postbehandeling en transmissietijd worden gereduceerd. Ook het niet hoeven ingeven aan de ontvangstzijde van de factuur zorgt voor tijdsbesparing. Verder kan men veel vlugger beschikken over de facturen en gaan er geen verloren via post, dus opnieuw tijdswinst. Tenslotte wezen enkele bedrijven erop dat elektronische facturatie ook leidt tot een positieve impact op de snelheid van geldontvangst.

Ook de niet-gebruikers verwachten dat het systeem zal leiden tot een aanzienlijke tijdsbesparing en vernoemen dezelfde oorzaken. Nochtans is er ook een bedrijf dat zich zorgen maakt omtrent elektronische facturatie in een internationale omgeving. Het bedrijf vreest voor een onduidelijk en ongelijk wettelijke opzet wat al dan niet toegelaten zal zijn met betrekking tot het digitaliseren van facturen. Ze verwijzen naar de BTW-wetgeving, die vaak extra administratie vereist, en stelt zich de vraag of elektronische facturatie in internationale context ook extra administratie vereist en bijgevolg niet tijdrovend is.

Hypothese 2 : Elektronische facturatie zorgt voor kostenbesparing

Allereerst stellen de bedrijven dat er kritisch moet gekeken worden naar de mogelijke besparingskosten in vergelijking tot de implementatiekosten. Voorlopig blijken enkel de grootfactureerders baat te hebben met een systeem van elektronische facturatie. Zo stelt ook Christian Luyten van Isabel vast : "*Wij werken vooral op grotere verzenders met 5000 facturen per maand. Rendement verzekerd!"*. Op de vraag hoeveel facturen men dient te verzenden alvorens het systeem rendeert, zijn de antwoorden verdeeld. De ene respondent stelt dat dit business case per business case te evalueren valt terwijl volgens andere 1000 facturen per maand nodig zijn om rendabel te zijn, en weer andere stellen dat er slechts 300 facturen per jaar nodig zijn.
Nochtans vindt 59% van de ondervraagde niet-gebruikers de implementatiekost geen drempel. De meeste bedrijven zijn vandaag de dag voldoende geïnformatiseerd zodat de basis-IT infrastructuur reeds aanwezig is (en dus de grootste kost al gemaakt is). Er zijn andere redenen voor het uitblijven van de installatie van elektronische facturatie waarover later meer.

De gebruikers van elektronische facturatie beoordelen de kosten van het nieuwe systeem momenteel als 'gelijk' tot 'licht dalend' met hun vorige kosten. De lichte daling van de kosten zou momenteel gerealiseerd worden door de versnelling van de dataverwerking. Vele bedrijven die momenteel elektronisch factureren, printen nog steeds papieren facturen. Ook wordt de participatie laag bevonden. Hierdoor is het systeem nog niet rendabel. Toch stellen de verschillende bedrijven dat ze in de toekomst een aanzienlijke kostenbesparing verwachten

inzake papier- en frankeringkosten wanneer ze niet meer printen en wanneer de participatiegraad stijgt. Dit strookt dus met de bevindingen in de literatuur.

Hypothese 3 : Elektronische facturatie is gebruiksvriendelijk

Volgens dhr. Luyten van Isabel is het systeem zeer gebruiksvriendelijk en vergt het geen extra scholing van de gebruikers: *"Wie eBanking kan, kan eInvoice"*. Ook wat betreft de integratie van het nieuwe boekhoudingssysteem in het oude zou zeer vlot verlopen en bij een aantal boekhoudingpakketten zou dit al gestandaardiseerd verlopen. Het ontvangen van een e-factuur zou net zo eenvoudig zijn als het ontvangen van e-mail, het versturen zou enige aandacht vereisen.

Deze beweringen van de leverancier worden doorgaans door de gebruikers beaamd. Eens de integratie van het nieuwe programma achter de rug is, is het systeem zeker gebruiksvriendelijk en vanzelfsprekend. Het personeel heeft geen extra training nodig indien ze reeds gewend zijn te werken met B2B toepassingen.

Bij navraag of er al problemen zijn voorgevallen met elektronische facturatie bleek dat er hier en daar wel al wat was voorgevallen maar dat problemen met het systeem al bij al zeer beperkt bleven. De vernoemde problemen zijn: problemen wanneer men grote volumes van uitgaande facturen wil versturen, een systeemcrash en inconsistentie in de gebruikte codes.

Als punten die voor verbetering vatbaar zijn werden de volgende vernoemd:

- Compatibiliteit. Koppelingen tussen andere providers zoals nu met Isabel en Certipost
- Facturatie linken met archivering, momenteel wordt er gewerkt met twee archieven: 1 met papieren facturen en 1 met elektronische facturen
- Flexibiliteit. Via het klassieke BMF-100 formaat zijn er weinig extra mogelijkheden. Er is één standaardversie en daarmee moet het gebeuren. Sommige klanten zijn echt veeleisend. Zo moet er bijvoorbeeld een vermelding zijn van subtotalen per kostcenter,

product, etc.. Ofwel moet de klant zijn werkwijze/behandeling gaan aanpassen ofwel het systeem. De toekomst zal dit uitmaken.

Als conclusie mogen we stellen dat elektronische facturatie gebruiksvriendelijk is, zeker in onze tijd waarin personeelsleden dagelijks geconfronteerd worden, en dus gewend zijn te werken, met informatica. Wel mag er gewerkt worden aan de flexibiliteit van de huidige systemen.

Hypothese 4 : Elektronische facturatie implementeren is nodig om concurrentiepositie te behouden

Uit de gesprek met een medewerker van Isabel en uit de reacties van verschillende bedrijven kunnen we afleiden dat er een absoluut stijgende trend merkbaar is wat betreft gebruikers van elektronische facturatie. Exacte cijfers of percentages konden ons echter niet worden meegeven. Ook bij de kleinere bedrijven is er interesse, maar door de band genomen starten ze als ontvangers. Uit de antwoorden van de ondervraging blijkt echter dat het voorlopig nog niet zo is dat wanneer men geen gebruik maakt van elektronische facturatie, de concurrentiepositie in het gedrang komt. Het gesprek met een medewerker van IBM doet nochtans het tegengestelde vermoeden. Hij stelt dat B2B en de mogelijkheid tot elektronische facturatie wel zeker door de partners gevraagd wordt, zelfs in die mate dat men stelt dat: ‘If you do not do B2B orders and B2B invoice, we don’t do business together’. Onze mening is dat dit het verschil duidelijk maakt tussen internationale bedrijven en de meer lokale bedrijven. Volgens ons is het niet meer dan de normale gang van zaken dat de ‘grote’ bedrijven een pioniersrol spelen en dat de ‘kleinere’ de beproefde techniek later implementeren. Maar het is meer dan waarschijnlijk dat, in de toekomst, zoals de heer Luyten van Isabel ook stelde, niemand nog een papieren factuur zal verzenden.

We kunnen dus concluderen dat, wat betreft de concurrentiepositie, het momenteel niet uiterst noodzakelijk is voor de kleine onderneming om onmiddellijk over te stappen naar elektronische facturatie. Uit de reacties van gebruikende bedrijven blijkt wel dat een overstap

op appreciatie zou kunnen rekenen en een stijgende klanttevredenheid in de hand zou werken. De grote ondernemingen die momenteel nog geen gebruik maken van het nieuwe systeem van factureren zouden echter wel eens mogen beginnen nadenken om de techniek te implementeren. Zo zou volgens dhr. Renson het te laat op de trein springen, in dit geval wel eens nadelig kunnen zijn voor de concurrentiepositie. Ook wordt er gesteld door een bedrijf dat hoe sneller er kan gefactureerd worden, hoe sneller er kan betaald worden. Deze verbetering van de liquiditeit zou de concurrentiepositie ook kunnen beïnvloeden.

Hypothese 5 : Elektronische facturatie is veilig

Nagenoeg elke respondent zegt het systeem voldoende tot zeer veilig te vinden. Er is veel vertrouwen in de nieuwe technologie. Ook denken de meeste dat een elektronisch archief voldoende en veel efficiënter is. Eén respondent is blijkbaar radicaal tegen enkel elektronische archivering, maar de reden waarom geeft hij niet.

Ook in de digitale handtekening is veel vertrouwen, hoewel er gesteld wordt dat de digitale handtekening nog niet vaak gebruikt wordt in combinatie met elektronische facturatie. In de toekomst zijn er bij de meeste bedrijven wel plannen om de digitale handtekening en het elektronische factuur te koppelen.

Het algoritme gebruikt door de populairste provider Isabel is het RSA algoritme. Isabel gebruikt hierbij een sleutelgrootte van 1024 bits. Om de 4 maanden worden de publieke en private sleutels automatisch veranderd.

10 Conclusies en mogelijkheden tot verder onderzoek

Dit slotdeel heeft tot doel na te gaan in welke mate de vooropgestelde onderzoeksdoelen in de eindverhandeling aan bod zijn gekomen. Ten slotte zouden we willen eindigen met een woordje over de mogelijkheden voor verder onderzoek van het onderwerp.

10.1 Conclusies

Onze samenleving wordt geïnformatiseerd. De typmachines zijn vervangen door computers, de fototoestellen door hun digitale variant en zelfs de hedendaagse muziek wordt gemaakt met computerprogramma's. Langzaam maar zeker lijkt alles te gaan draaien rond informatica. De bedrijfswereld kan natuurlijk niet achterblijven, de voordelen van de nieuwe technologieën zijn immers overduidelijk: sneller, efficiënter, productiever en dikwijls veel goedkoper. Maar uit deze nieuwe technologieën vloeien ook nieuwe gevaren en zorgpunten voort. Zo is men onder andere bezorgd over de gebruiksvriendelijkheid, kostprijs en stabiliteit van de nieuwe systemen maar bovenal stelt men zich vragen over het al dan niet veilig zijn van elektronische acties. Deze eindverhandeling heeft getracht te onderzoeken of cryptologie en de digitale handtekening mogelijke middelen zijn om dit veiligheidsgevoel te verhogen bij elektronische informatie-uitwisseling.

De mens van vandaag heeft de wens sommige zaken confidentieel te houden. Een methode die we besproken hebben voor het waarborgen van deze confidentialiteit is cryptologie, de leer van het geheimschrift. Belangrijk hierbij is de cryptografie die zich bezighoudt met het ontwikkelen van systemen voor het versleutelen en ontcijferen van informatie. De crypto-analyse houdt zich op zijn beurt bezig met het onderzoeken van zwakheden en het trachten kraken van cryptosystemen. Cryptoanalysten worden steeds slimmer en inventiever. Daarom is het belangrijk dat men voortdurend zoekt naar nieuwe, betere cryptosystemen om zo de confidentialiteit te waarborgen. In deze eindverhandeling hebben we getracht enkele

belangrijke cryptosystemen te bespreken. Het is moeilijk te zeggen welk systeem nu eigenlijk het beste is, elk systeem heeft zijn voor en nadelen en eigen specifieke kenmerken.

Veel van de veiligheid hangt af van de gebruikte sleutelgrootte. Hoe groter de sleutel, hoe veiliger, maar hoe meer tijd het encrypteren en decrypteren in beslag neemt. Men moet dus afwegen welk gewenst niveau van veiligheid men wil. Ook belangrijk voor de keuze van het cryptosysteem is het gewenste doel. Cryptografie kan immers voor meerdere doelen worden aangewend dan louter voor confidentialiteit.

Gebruikt men cryptografie met het oog op het onleesbaar maken van boodschappen om zo de confidentialiteit te waarborgen, dan zal men eerder symmetrische cryptografie gaan toepassen. Bij symmetrische cryptografie gebruikt men dezelfde sleutel voor het versleutelen en ontsleutelen. Het voordeel van symmetrische cryptosystemen is dat ze minder rekenintensief en sneller zijn dan zijn asymmetrische tegenhanger waardoor het de voorkeur heeft voor het versleutelen en ontsleutelen van grote bestanden en hoge datasnelheden.

Stelt men echter authenticatie, berichtintegriteit en onweerlegbaarheid voorop als doel, dan kiest men voor asymmetrische cryptografie. Bij asymmetrische cryptografie gebruikt men twee sleutels: één sleutel voor het versleutelen van de boodschap, en een andere sleutel voor de ontsleuteling. Doordat men gebruikt maakt van twee sleutels (één publieke en één private), noemt men deze techniek ook vaak PKI, voluit Public Key Infrastructure. De asymmetrische cryptosystemen zijn gebaseerd op trapdoor-functies. Bij deze varianten van de one-way functie is het gemakkelijk de inverse richting te vinden wanneer men beschikt over bepaalde informatie. Het is echter zo goed als onmogelijk de inverse richting te vinden wanneer men niet over deze informatie beschikt. Een nadeel van PKI cryptografie is zijn grote complexiteit. Doordat de computer zeer veel verwerkingscycli voor de versleuteling nodig heeft, ongeveer 100 keer zoveel cycli als bij symmetrische encryptie, kan men deze systemen in feite enkel efficiënt gebruiken voor het versleutelen van kleine berichten.

De (geavanceerde) digitale handtekening vond hiervoor een oplossing. Alvorens men gaat versleutelen, zal men de boodschap 'hashen'. De hash-functie zorgt ervoor dat de boodschap van willekeurige lengte wordt 'verkapt' tot een korte, unieke 'message digest' met vaste lengte. Men kan deze message digest zien als een soort vingerafdruk van de oorspronkelijke boodschap. Op deze message digest zal men nu een asymmetrisch cryptosysteem toepassen, de afzender versleutelt zijn message digest met zijn private sleutel, waardoor men uiteindelijk de digitale handtekening bekomt. Deze digitale handtekening is onlosmakelijk verbonden en uniek bij de boodschap. De ontvanger van het ondertekende bericht zal de boodschap verifiëren door de volgende stappen te ondernemen: eerst zal hij van de ontvangen boodschap een message digest creëren door toepassing van dezelfde hash-functie, vervolgens gebruikt hij de publieke sleutel van de afzender om de digitale handtekening te converteren naar de message digest die gecreëerd was door de afzender. Zijn deze twee message digests gelijk dan kan de ontvanger er zeker van zijn dat het bericht onderweg niet gewijzigd is, en dat het afkomstig is van de afzender. Verder zal de afzender niet meer kunnen ontkennen dat hij het bericht verstuurde.

De digitale handtekening is dus een unieke methode om relatief snel en zeer veilig een boodschap authenticiteit, integriteit en onweerlegbaarheid te verschaffen. We stellen dat de digitale handtekening veilig is omdat men momenteel sleutels implementeert die onkraakbaar zijn in een redelijke termijn. Zo gebruikt het populaire Isabel een RSA-algoritme op basis van sleutels met een grote van 1024 bits. In vergelijking met andere technieken zoals EDI is de digitale handtekening een superieure methode op het gebied van authenticiteit en integriteit bij elektronische boodschappen. Zo stelt ook de heer Luyten van Isabel : "*Vanuit een technisch-wetenschappelijke hoek is de digitale handtekening de enige juiste oplossing*". Verscheidende elektronische toepassingen met betrekking tot informatie-uitwisseling gebruiken meer en meer de digitale handtekening voor verificatie. Volgens de heer Luyten zal de digitale handtekening in de toekomst standaard gebruikt worden bij informatie-uitwisseling.

De digitale handtekening is alleen veilig wanneer men werkt met certificaten. Deze worden uitgekeerd door certificaatautoriteiten (zoals Certipost, Isabel, etc.). De certificaten zorgen

voor de identificatie van de verschillende gebruikers van open netwerken. Bij op publieke sleutels gebaseerde authenticatie moet de ontvanger van een ondertekend bericht de publieke sleutel van de werkelijke partij weten. De ontvanger moet de verzender niet gaan vragen om de publieke sleutel van de werkelijke partij, want deze kan een bedrieger zijn. Daarom zal de ontvanger contact moeten opnemen met een certificaatautoriteit (of Trusted Authority). Deze autoriteit is een onafhankelijke en betrouwbare bron van informatie over de publieke sleutels van de werkelijke partijen. Hun rol mag zeker niet onderschat worden.

Als concrete toepassing van elektronische informatie-uitwisseling hebben we de elektronische facturatie tussen bedrijven besproken. Elektronische facturatie is een sterk opkomend fenomeen en kent verscheidende voordelen ten opzichte van de klassieke facturatie. Zo kan elektronische facturatie zorgen voor tijdsbesparing, kostenbesparing, hogere return-on-investements, gebruiksvriendelijkheid, betere klantenservice en bovenal biedt elektronische facturatie garanties betreffende veiligheid mede dankzij het gebruik van de digitale handtekening en gekwalificeerde certificaten. De vraag die zich hierbij opdringt is of de kosten van implementatie de baten ervan niet te boven gaan. Dit is onder andere in sterke mate afhankelijk van de huidige infrastructuur van het bedrijf. Verder stellen sommige auteurs zich de vraag of de bedrijfswereld wel al klaar is voor elektronische facturatie.

Deze bedenkingen uit de literatuur hebben we onderzocht aan de hand van een bevraging van bevoorrechte getuigen en een online enquête gericht aan bedrijven van variërende grootte. We hebben telkens een onderscheid gemaakt tussen bedrijven die het systeem van elektronische facturatie al geïmplementeerd hadden, en bedrijven die dit nog niet deden. Men kan wel stellen dat iedereen het nut van elektronische facturatie inziet. Pluspunten die de gebruikers geven zijn ondermeer een grotere aandacht aan de kernactiviteiten doordat men tijd bespaart op het gebied van factuurverwerking en de positieve impact op de snelheid van geldontvangst. Verder is er bij de grootfactureerders al een lichte daling van de kosten waar te nemen en verwacht men in de toekomst een nog grotere kostendaling. Op het gebied van de gebruiksvriendelijkheid van de systemen hebben weinig respondenten iets aan te merken, al werd er af en toe opgemerkt dat de systemen wel wat meer flexibiliteit mochten bieden (keuze

vorm en elementen op factuur etc.). Ook wat betreft de BTW-administratie waren er wat opmerkingen. Verder merkt men op dat het voor kleine bedrijven voorlopig nog niet rendabel is om het systeem te implementeren vermits de participatie van hun partners momenteel nog vrij laag ligt. Men verwacht wel dat dit gaat veranderen omdat de bedrijven uiteindelijk wel elektronisch zullen moeten factureren om competitief te blijven ten opzichte van de concurrentie, dit geldt zeker voor de grote bedrijven. Tenslotte stellen nagenoeg alle respondenten het systeem voldoende tot zeer veilig te vinden. Hoewel de kennis over de verschillende beveiligingstechnieken zeer beperkt zijn is er veel vertrouwen in de veiligheid.

10.2 Mogelijkheden tot verder onderzoek

Elektronische informatie-uitwisseling is een thema waarin vele aspecten behandeld kunnen worden. In dit eindwerk zijn we opzoek gegaan naar enkele mogelijke technieken voor het beveiligen van informatie-uitwisseling. Hierbij hebben we onderzocht of cryptologie en de digitale handtekening een mogelijke oplossing kan zijn. Uiteraard bestaan er ook andere methodes en zijn er ongetwijfeld veel meer onderwerpen betreffende de elektronische informatie-uitwisseling geschikt om onderzoek naar te verrichten.

Een mogelijkheid tot verder onderzoek zou kunnen bestaan uit het opsporen en bespreken van andere technieken dan cryptologie en de digitale handtekening voor het beveiligen van informatie-uitwisseling.

Men zou ook onderzoek kunnen verrichten naar de verschillende soorten aanvallen op het elektronische dataverkeer. Heeft men voor alle soorten al verdedigingsmechanismen?

Ook zou men kunnen behandelen in welke mate draadloze communicatie een weerslag zal hebben op de elektronische informatie-uitwisseling. Bij draadloze communicatie zal informatie immers veel vlotter te onderscheppen zijn. Ook zal men meer te kampen hebben met fouten tijdens de verzending. Hoe kan men hier een oplossing aan bieden?

Verder kan men onderzoeken of een groter inzicht in de achterliggende principes van de cryptologie en de digitale handtekening, leidt tot een toename in het vertrouwen van nieuwe technologieën. Hierbij kan men zich de vraag stellen of er nood is aan een aanpassing van het huidige onderwijsprogramma in het secundair en hoger onderwijs, een programma waar meer aandacht besteed wordt aan de achterliggende wiskunde van de nieuwe technologieën.

Tenslotte zijn er een heel aantal nieuwe toepassingen waarop men zich kan toespitsen. Zo zou men zich kunnen verdiepen in elektronische notariële akten, elektronische testamenten of in de beveiliging van medische patiënten dossiers. Welke technieken gebruikt men bij deze toepassingen voor het waarborgen van de veiligheid en in welke mate is dit te verbeteren door het gebruiken van de digitale handtekening en cryptologie?

Lijst van geraadpleegde werken

Boeken en syllabi

Broekmans, J., *Methoden van onderzoek en rapportering*, Diepenbeek, Limburgs Universitair Centrum, 2002

Hill, R., *A first course in coding theory,* Clarendon Press, Oxford, 1986, 160p.

Kabatiansky, G., Krouk, E., Semenov, S., *Error correcting coding and security for data networks,* John Wiley & Sons Ltd., Chichester, 2005, 288p.

Lefebvre, E.R.J., *Tekst en organisatie : Ideeën en beschouwingen voor het management van academisch denken en schrijven*, Acco, Leuven, 1997, 135p.

Menezes, A.J., Oorschot, P.C. van, Vanstone, S.A., *Handbook of applied cryptography*, CRC Press LLC, Florida, 1997, 780p.

O'Brien, J.A., *Introduction to information systems : essentials for the E-Business*, McGraw-Hill Higher Education, United States, 2003, 450p.

Panko, R., *Datanetwerken en telecommunicatie*, Pearson Education Benelux, Amsterdam, 2005, 577p.

Rhee, M.Y., *Internet Security : Cryptographic principles, algorithms and protocols*, John Wiley & Sons Ltd, West Sussex, 2003, 405p.

Silberschatz, A., Galvin, P.B., Gagne, G., *Operating systems met java*, Academic Service, Den haag, 2004, 767p.

Stallings, W., *Netwerkbeveiliging en Cryptografie : Beginselen en praktijk*, Academic Service, Schoonhoven, 2000, 644p.

Stinson, D.R., *Cryptography : Theory and practice,* Chapman & Hall/CRC, London, 2006, 616p.

Van Dale, *Handwoordenboek van hedendaags Nederlands*, Utrecht, 1994,

Geraadpleegde artikels en websites

Bulletin 2004/1, *Laatste rechte lijn voor de wettelijke e-factuur?*, 2004, geraadpleegd via http://www.gs1belu.org/publicaties/2004_1_e-invoicing_n.pdf

Certipost, *CertiONE e-billing : Secure and legal electronic invoicing*, 2005

Certipost, *CertiONE e-billing : Invoice Management*, 2005

Certipost, *Open Up nummer 1*, 2006

Certipost, *Open Up nummer 2*, 2006

Certipost, *Open Up nummer 3*, 2006

Certipost, *Open Up nummer 4*, 2006

Certipost, *Open Up nummer 5*, 2006

Certipost, *White paper e-Invoicing with CertiBusiness.Net Version 1.0.*, 2003

Cryptonet, *RSA*, geraadpleegd via http://members.home.nl/cryptonet/rsa/content.htm

Cryptotel, *Getallen en Public key cryptografie*, cryptoTel.pdf, bron onbekend

De Corte, R., *Elektronisch geschrift, elektronische handtekening*, *2003* geraadpleegd via users.ugent.be/~rdecorte/slides/ri_de_corte_e-signature_2003.ppt

Decruyenaere, F., *Algebra en Getaltheorie@Work:van cryptosysteem tot digitale handtekening,* 2004, geraadpleegd via www.kuleuven.be/wet/leerkrachten/lessenpakket2005/-wiskunde/algebra_at_work.pdf

De Financieel Economische Tijd, *De elektronische handtekening*, 2004

De Financieel Economische Tijd, *Belgacom lanceert in juli elektronische facturatie*, 2004, geraadpleegd via http://www.tijd.be/mijn_onderneming/technologie/t-zine/artikel.asp?iD=-1538282&eD=01/30/2004

De Financieel Economische Tijd, *Elektronische facturatie*, 2005 geraadpleegd via http://www.tijd.be/ondernemen/elektronische_facturatie/artikel.asp?Id=1223590

De Standaard, *Leven in 2025. De digitale uitdaging*, 2005, geraadpleegd via http://www.standaard.be/Artikel/Detail.aspx?artikelId=GEKGRG4C

Dumortier, J., *De omzetting van de richtlijn e-handtekening in België*, 2000, geraadpleegd via www.law.kuleuven.ac.be/icri/documents/49dumortier2.ppt

Ernst&Young, *De nieuwe facturatiewetgeving is op komst – zijn de ondernemingen klaar om van de opportuniteiten te profiteren?*, 2004, geraadpleegd via www.ey.be

Hogeschool van Amsterdam, onbekend auteur, *Cryptografie*, 2002, geraadpleegd via http://home.bl.hva.nl/Archief/2002-2003/BWK/Jaar3/COD3.2/CRYPTOGRAFIEversie2.pdf

Lejeune, I., Cambien, J., Stessens, E*., Elektronisch factureren: de digitale onderneming vanaf 1 januari een stap dichter,* 2003, geraadpleegd via http://www.tijd.be/mijn_onderneming/technologie/e-business/artikel.asp?Id=737348

Loidreau, P., *Introductie in cryptografie, 2002*, geraadpleegd via http://linux.atlink.it/linuxfocus/Nederlands/May2002/article243.shtml

Lubbe, J.C.A. van der, *Basismethoden cryptografie*, 1997, geraadpleegd via http://mail.vssd.nl/hlf/e012.pdf

Noorden, D, *Public Key Infrastructure*, 2000, geraadpleegd via http://infolab.uvt.nl/~remijn/telematica/scripties01/groep19

Reinehr, C., *Encryptie : RSA*, 2003, geraadpleegd via http://users.pandora.be/reinehr/data-rsa.pdf

Robben, F., *Elektronische identiteitskaart : Stand van zaken* , 2001, geraadpleegd via www.law.kuleuven.be/icri/frobben/presentations/20010619.ppt

Silverback, *Wat levert digitaal factureren mij op?*, 2005, geraadpleegd via http://www.silver-back.nl/index.php/id_pagina/5360/naam/wat_levert_digitaal_factureren_mij_op.htm

Storme,M.E., *De invoering van de elektronische handtekening in ons bewijsrecht - een inkadering van en commentaar bij de nieuwe wetsbepalingen,* geraadpleegd via http://www.storme.be/elektronischehandtekening.pdf

Syntens, *Succesvol innoveren*, geraadpleegd via www.syntens.nl

Tieleman,O., Vernooij, J., *Cryptografie*, 2002, geraadpleegd via http://jelmer.vernstok.nl/publications/cryptografie.pdf

Uw digitale informatiecentrum, *Wat?*, geraadpleegd via http://www.digitalehandtekening.be/what.cfm

Weger, B. de**,** *Internet-beveiliging***,** 2004, geraadpleegd via www.apeldoorn-it.nl/download/ppt/Apeldoorn-IT-Benne_de_Weger-websiteversie.ppt

Wetten, decreten, ordonnanties en verordeningen, *Wet van 9 juli 2001*, 2001, geraadpleegd via mineco.fgov.be/information_society/e-signatures/law_e_signature_002.pdf

Wikipedia, *Cryptografie*, 2006, geraadpleegd via http://nl.wikipedia.org/wiki/cryptografie

Wikipedia, *Handcijfer*, 2006, geraadpleegd via http://nl.wikipedia.org/wiki/handcijfer

Wikipedia, *Data Ecryption Standard*, 2006, geraadpleegd via http://nl.wikipedia.org/wiki/data_encryption_standard

Wikipedia, *RSA* (*Cryptografie)*, 2006, geraadpleegd via http://nl.wikipedia.org/wiki/RSA_%28cryptografie%29

Wikipedia, *Coderingstheorie*, 2006, geraadpleegd via http://nl.wikipedia.org/wiki/coderingstheorie

Wikipedia, *Hamming-code*, 2006, geraadpleegd via http://nl.wikipedia.org/wiki/Hamming-code

Wilschut, D.E., *Digitale Handtekeningen: een experimentele vergelijking*, 2000, geraadpleegd via http://ftp.cwi.nl/CWIreports/MAS/MAS-N0001.pdf

WISH-e, *Gilbert Vernam : One-time-pad, een onbreekbare methode,* geraadpleegd via http://proto.thinkquest.nl/~klb024/vernanhistorie.htm

WISH-e, *Hellman en de sleuteldistributie,*geraadpleegd via http://proto.thinkquest.nl/~klb024/whellman.htm

X5, Cryptography : frequently asked questions, geraadpleegd via http://www.x5.net/faqs/crypto/index.html

Geraadpleegde eindverhandelingen

Deckers, M., *De digitale handtekening als stimulans voor e-commerce en economische vooruitgang*, LUC, Diepenbeek, 2004, 106p.

Hermans, I., *De digitale handtekening en de elektronische bedrijfsvoering*, LUC, Diepenbeek, 2001, 81p.

Simons, A., *De digitale handtekening : betekenis en belang ervan bij de elektronische communicatie*, LUC, Diepenbeek, 2004, 122p.

Smets, E., *De digitale handtekening : principe en mogelijke toepassingen met de elektronische identiteitskaart*, LUC, Diepenbeek, 2004, 96p.

Lijst van figuren

Lijst van tabellen

Lijst van bijlagen

Bijlage 1 : Outprint online vragenlijst voor gebruikers van elektronische facturatie

1. Welke software gebruikt u ? : Isabel, Certipost, ...

Waarom deze keuze?

2. Is het systeem gebruiksvriendelijk?

Is er nood aan extra scholing?

zeer weinig O O O O O zeer veel O geen mening

Is er een verschil in de behandeling van in- en uitgaande facturatie?
zeer weinig O O O O O zeer veel O geen mening

Heeft u al ooit problemen gehad met het systeem?
zeer weinig O O O O O zeer veel O geen mening

3. Zo ja, welke problemen hebben zich zo al voorgedaan?

4. Heeft het systeem van digitaal factureren voor tijdsbesparing gezorgd?

Meer of minder dan u aanvankelijk dacht te realiseren?
veel minder O O O O O veel meer

5. Volgende op vraag 6 : Op welke manier wel/niet?

6. Heeft het systeem van digitaal factureren voor kostenbesparing gezorgd?

positie 1 : stijging kosten

middenpositie : gelijke kosten

positie 5 : daling in kosten

stijging O O O O O daling

7. Volgend op vraag 8 : Op wat bespaart u? Factuurpapier, archivering, hogere ROI op netwerkinfrastructuur etc.

8. Weegt deze kostenbesparing op tegen de implementatiekost?

9. Vanaf hoeveel facturen (per maand, jaar) denkt u dat het systeem rendeert?

10. Heeft u het gevoel dat u nu een betere service aan u klanten biedt?

Wordt de mogelijkheid tot digitaal factureren door de klanten geappreciëerd of is er weinig interesse

geen interesse O O O O O veel appreciatie O geen mening

11. Maken vele klanten gebruik van deze mogelijkheid? Is er een stijgende trend merkbaar?

12. Wat denkt u over het vertrouwen?

Denkt u dat het systeem veilig is of bent u eerder wantrouwig?

zeer onveilig O O O O O zeer veilig O geen mening

Is enkel elektronische archivering volgens u voldoende?

zeer onveilig O O O O O zeer veilig O geen mening

13. Zijn er punten die voor verbetering vatbaar zijn? Wat zou u wijzigen?

14.

Zou u andere bedrijven aanraden over te stappen naar digitaal factureren?
eerder niet O O O O O eerder wel O geen mening

15. Opmerkingen :

Bijlage 2 : Outprint online vragenlijst voor niet-gebruikers van elektronische facturatie

1. Heeft u al ooit van het concept 'digitale facturatie' gehoord?

- ○ Ja, ik weet wat het is
- ○ Van gehoord, maar ik weet niet juist wat het is
- ○ Nee, nooit van gehoord

---

2. Waarom heeft u het systeem van digitaal factureren nog niet in gebruik?

De implementatiekost is te hoog
zeer mee oneens O O O O O zeer mee eens O geen mening

Het bedrijf is nog niet voldoende geïnformatiseerd, de netwerkinfrastructuur is hiervoor nog niet klaar
zeer mee oneens O O O O O zeer mee eens O geen mening

Er is gewoonweg geen interesse
zeer mee oneens O O O O O zeer mee eens O geen mening

Er is nog geen vraag naar door de klanten of leveranciers
zeer mee oneens O O O O O zeer mee eens O geen mening

Het systeem is niet veilig, betrouwbaar genoeg
zeer mee oneens O O O O O zeer mee eens O geen mening

---

3. Zijn er nog andere redenen, die niet vermeldt staan in bovenstaande lijst, waarom u niet overgaat tot een systeem van digitale facturatie?

---

4. Welke voordelen verwacht u van het systeem?

5. Welke nadelen verwacht u van het syteem?

6. Welke certificaatautoriteiten (oftewel verschaffers van de digitale handtekening voor toepassing bij het digitaal factureren) zijn u bekend?

7. Opmerkingen?

Bijlage 3: Vragenlijst t.a.v. de heer Renson (IBM)

Questionnaire for the attention of Jean-Francois Renson of IBM

1. In which ways is IBM already a user of electronic communication?

2. Which software do you use for e-invoicing? Isabel, Certipost, … Why this choice?

3. Can you tell me more about the technical background? Algorithms used, etc.?

4. How went the integration of your original accounting software into the system of digital invoicing?

5. Is the system user friendly?

    a. Does it require extra training?
    b. Is there a difference between in- and outgoing invoicing
    c. Did you ever have any problems with the system? If so, in what manner?

6. Does e-invoicing leads to time-saving?
    a. How/how not?
    b. More of less then you initially thought you would realize?

7. Does e-invoicing leads to cost-saving?
    a. On what items do you save money? Paper, archive, higher ROI of the network infrastructure etc.
    b. Does this cost saving counterbalance the implementation costs?
    c. How many invoices (per month, per year) are needed to profit from the system?

8. Do you have the feeling that your customer service has improved?

a. Is the possibility of electronic invoicing appreciated by the customer or is there little interest?
b. Are there many customers who are making use of this possibility? Is there a up going trend noticeable?

9. Do you feel that the system is save or are you rather skeptical?

a. Do you trust the system of the digital signature for authentication?
b. Do you think that an electronic archive will be sufficient?

10. Which points of the system would you improve?

11. Would you recommend electronic invoicing to other company's?

12. Further comment?

Bijlage 4 : Vragenlijst t.a.v. de heer Luyten (Isabel)

Vragenlijst t.a.v. de heer Luyten van Isabel

1. Hoe verloopt de integratie van het oorspronkelijke boekhoudingsysteem in het systeem van digitale facturatie? Duurt dit lang?

2. Is het systeem gebruiksvriendelijk?

a) Nood aan extra scholing van gebruikers?

b) Is er een verschil in de behandeling van in- en uitgaande facturatie?

c) Met welke problemen wordt u helpdesk het meest geconfronteerd?

d) Zijn er punten voor verbetering vatbaar? Waar werkt u momenteel aan?

3. Betreft kostenbesparing

Vanaf hoeveel factureren per maand rendeert het systeem? Vergelijking kostenbesparing op papier, archivering, hogere ROI op netwerkinfrastructuur ten opzichte van de implementatiekost.

4. Betreft interesse

a) Hoeveel procent van de grootfactureerders maakt gebruik van elektronische facturatie? Wat is het marktaandeel van Isabel hierbij?

b) Is er interesse bij de kleinere bedrijven?

c) Is er een stijgende trend, of stagneert het gebeuren?

5. Betreft de digitale handtekening & veiligheid

a) Welk algoritme wordt gebruikt voor de digitale handtekening?

b) Uit hoeveel bits bestaat de sleutel?

c) Wordt er altijd van de zelfde publieke en private sleutel gebruik gemaakt of is deze veranderlijk?

d) Is elektronische facturatie altijd confidentieel? Met welke methode wordt deze informatie dan versleuteld?

e) Is enkel elektronische archivering van facturen volgens u voldoende?

f) "Vooraleer een factuur verstuurt wordt, moet deze zijn voorzien van de digitale handtekening van het bedrijf zodat de ontvanger ondubbelzinnig kan vaststellen dat de factuur van het juiste bedrijf afkomstig is." Hieruit maak ik op dat wanneer men Isabel gebruikt om elektronisch te factureren er zowiezo altijd een digitale handtekening aan verbonden is. Klopt dit? Want een paar bedrijven die ik mailde stelde dat ze wel elektronisch facturen, maar dat ze de factuur niet digitaal handtekenen, dat ze dit niet nodig achten. Is dit een misverstand bij deze bedrijven? Kan het zijn dat deze bedrijven niet digitaal handtekenen omdat ze werken met een systeem van EDI (ook in de wet aanvaard om authenticiteit te garanderen)? Indien dit zo is, wat maakt EDI evenwaardig qua veiligheid ten opzichte van de digitale handtekening?

Auteursrechterlijke overeenkomst

Opdat de Universiteit Hasselt uw eindverhandeling wereldwijd kan reproduceren, vertalen en distribueren is uw akkoord voor deze overeenkomst noodzakelijk. Gelieve de tijd te nemen om deze overeenkomst door te nemen en uw akkoord te verlenen.

Ik/wij verlenen het wereldwijde auteursrecht voor de ingediende eindverhandeling:
De rol van de cryptologie en de digitale handtekening inzake de veiligheid van elektronische informatie-uitwisseling
Richting: **Handelsingenieur** Jaar: **2006**
in alle mogelijke mediaformaten, - bestaande en in de toekomst te ontwikkelen - , aan de Universiteit Hasselt.

Deze toekenning van het auteursrecht aan de Universiteit Hasselt houdt in dat ik/wij als auteur de eindverhandeling, - in zijn geheel of gedeeltelijk -, vrij kan reproduceren, (her)publiceren of distribueren zonder de toelating te moeten verkrijgen van de Universiteit Hasselt.

U bevestigt dat de eindverhandeling uw origineel werk is, en dat u het recht heeft om de rechten te verlenen die in deze overeenkomst worden beschreven. U verklaart tevens dat de eindverhandeling, naar uw weten, het auteursrecht van anderen niet overtreedt.

U verklaart tevens dat u voor het materiaal in de eindverhandeling dat beschermd wordt door het auteursrecht, de nodige toelatingen hebt verkregen zodat u deze ook aan de Universiteit Hasselt kan overdragen en dat dit duidelijk in de tekst en inhoud van de eindverhandeling werd genotificeerd.

Universiteit Hasselt zal u als auteur(s) van de eindverhandeling identificeren en zal geen wijzigingen aanbrengen aan de eindverhandeling, uitgezonderd deze toegelaten door deze licentie

Ik ga akkoord,

Philippe SCHRAEPEN

Datum: