De toekomst der kwantum-cryptografie is nabij

Of wint toch de kwantum-computer eerder terrein?

Lilian Roos

[BWI-Werkstuk, najaar 2005]

De toekomst der kwantumcryptografie is nabij

Of wint toch de kwantumcomputer eerder terrein?

Lilian Roos

BWI-werkstuk, najaar 2005

vrije Universiteit
Faculteit der Exacte Wetenschappen
Studierichting Bedrijfswiskunde en Informatica
De Boelelaan 1081_a
1081 HV Amsterdam

Werkstukbegeleider: Evert Wattel
Extern werkstukbegeleider: Said El Aoufi

Voorwoord

Welke toekomst is nabij? Het einde der cryptografie? Zodra de kwantumcomputer er is, is ons huidige cryptografische systeem in één tel gekraakt. Of... worden we gered door dat ene briljante idee, dat misschien helemaal niet zo complex is, als dat het aanvankelijk maar lijkt: een over onmeetbare afstanden werkend kwantumcryptografisch systeem.

Vanaf hier begint mijn zoektocht naar beschikbare, maar nog voor mij onbekende, informatie. Deze informatie wekt bij mij zeer veel interesse, zodat ik kan beginnen met het verplichte BWI-werkstuk. Maar... eerlijk is eerlijk, zonder het gesprek met Said El Aoufi, afgestudeerd BWI'er in 1996, ben ik niet eens op het idee gekomen om kwantumcryptografie verder uit te lichten. Hoewel ik wel naar een onderwerp heb gezocht in de cryptografie.

Eén enkele vermelding van de kwantumtheorie vanaf dat gesprek, verandert eensklaps mijn hele kijk op de rest van dit werkstuk. Van het Internationale Jaar van de Natuurkunde (2005), omdat Albert Einstein (1879-1955) 100 jaar geleden tot drie wereldveranderde ontdekkingen komt, waaronder de kwantumtheorie. Tot derde Zomergast[1] Robbert Dijkgraaf (1960), die meerdere malen de kwantumtheorie naar voren haalt als invulling in dit aardse leven.

Daarom begin ik met het bedanken bij Evert Wattel, mijn begeleider vanuit de VU. Uiteraard volg ik direct met Said El Aoufi, mijn extern praktijk 'begeleider'. Dit werkstuk draag ik op aan Alice, Bob en... oké, ook aan Eve, de hoofdrolspelers in mijn verhaal, die hun geluk nog altijd niet lijken te hebben gevonden...

Lilian Roos
⁂, najaar 2005

Samenvatting

In dit BWI-werkstuk staan de rollen van de natuurwetenschappen en informatica in de cryptografie centraal voor de literatuurstudie naar de kwantumcryptografie. En wat de rol van het bedrijfsleven hierin is.

Het begint in 1976, wanneer Alice en Bob een geheim kunnen afspreken in een publiekelijk toegankelijk gesprek, dankzij de éénwegfunctie $Y^x (mod\ P)$ van Martin Hellman (1945). Alleen het al tweeduizend jarige sleuteldistributie is nog een probleem. De éénwegfunctie van Hellman brengt zijn vriend Whitfield Diffie (1944) op een miraculeus idee: een asymmetrische sleutelsysteem met één publieke sleutel om te vercijferen en één privé-sleutel om te ontcijferen.

Ron Rivest (1947), Leonard Adleman (1945) en Adi Shamir (1952) vragen in 1977 patent op de éénwegfunctie, die nodig is om het asymmetrische sleutelsysteem functioneel te maken: het RSA-cijfer. Vanaf dit moment staat het RSA-cijfer in het midden van de belangstelling.

In 1991 ontwikkelt Phil Zimmermann (1954) het programma PGP om iedereen de gelegenheid te bieden het veiligste, onder bepaalde voorwaarden, encryptiesysteem te gebruiken voor beveiliging van informatie en waarborging van de authenticiteit.

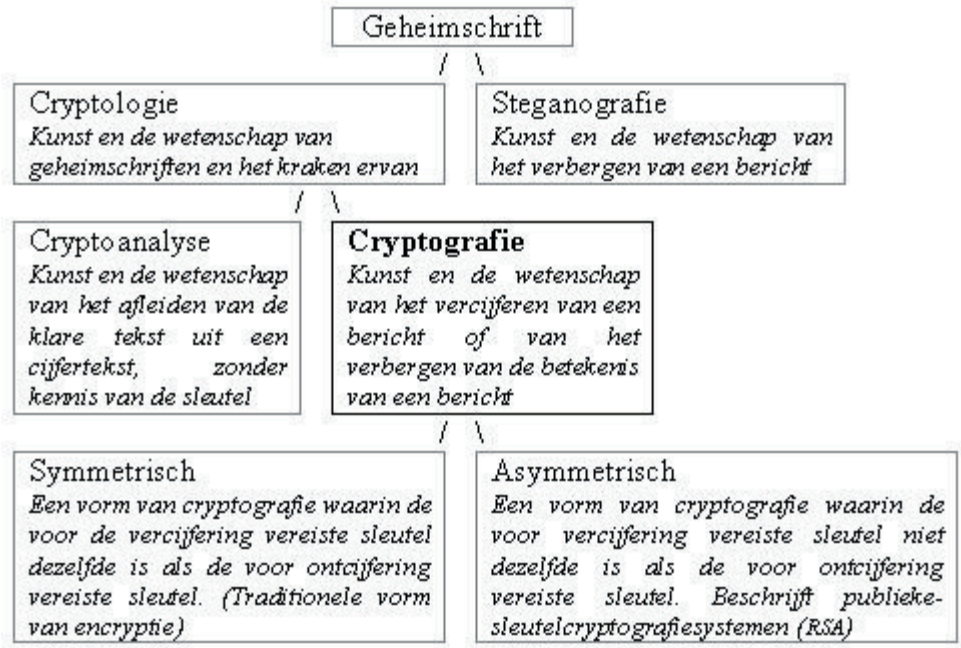
Het RSA-cijfer is nauwelijks te kraken. Door de enorm grote getallen, van meer dan 130 cijfers lang die gebruikt worden voor de sleutels, is het voor traditionele computers haast ondoenlijk om deze te factoriseren. Factorisatie is namelijk de 'sleutel' naar de geheimhouding. Cryptoanalisten breken hun nek over dit probleem. In samenwerking met de fysische wereld zoekt men naar oplossingen. Deze lijkt men gevonden te hebben in de kwantumtheorie.

De theorie die pas sinds enkele decennia erkend wordt, geeft nieuwe positieve inzichten. De waarschijnlijkheidsberekening legt de 'magie' van de kwantummechanica, van waaruit de kwantumtheorie is geformuleerd, bloot. Zo kan de traditionele bit worden gevormd naar een kwantumbit, de qubit, die de prachtige eigenschap heeft dat het tegelijkertijd 0 én 1 kan zijn. De kwantumcomputer gebruikt deze qubits, om in enkele tijdseenheden, een factorisatieprobleem op te lossen. Als dit probleem oplosbaar is, is het RSA-cijfer gekraakt. Een moment waar vele codebrekers op wachten, maar ook een moment zal worden, dat het huidige encryptiesysteem in duigen valt. Terwijl de codemaker niet stilzit en ondertussen al voorbij het eventuele kraaksysteem van het RSA-cijfer is gekomen: de kwantumcryptografie. De kwantumcryptografie is een onbreekbare vorm van de cryptografie die tevens gebaseerd is op de kwantumtheorie en de veilige uitwisseling van een willekeurige reeks bits garandeert, die dan wordt gebruikt als de basis voor een eenmalig blokcijfer. Hiermee komt het einde van de wereld van de cryptografie misschien toch in zicht.

Inhoudsopgave

1 Inleiding

Alvorens een enkel woord over cryptografie te schrijven, moeten belangrijke verschillen worden onderscheiden:



Afbeelding 1. De belangrijkste vertakkingen van het geheimschrift in dit werkstuk.
(*Code*, Singh, S., pagina 49)

Cryptografie lijkt al zo oud als de weg naar Rome. De mensen hebben altijd onderling geheimen gehad die onder geen geval mochten uitlekken. Directe mond-op-mond-overbrenging is dan wel het allerveiligste, maar toch ook wel het alleronhandigste. Al eeuwen lang wordt de sport van het geheimschrift uitgeoefend door codemakers en codebrekers. Ook in deze moderne tijd, zijn regeringen, krijgsmachten, de bedrijfswereld en het publiek, zeer geïnteresseerd in de wondere wereld van de cryptografie in positieve en negatieve zin.

Er is gezegd dat de Eerste Wereldoorlog de oorlog der chemici was, omdat voor het eerst mosterdgas en chlorine worden gebruikt, en de Tweede Wereldoorlog die van de fysici, omdat de atoombom tot ontploffing wordt gebracht. Zo is wel eens gezegd dat de Derde Wereldoorlog die van de wiskundigen zal zijn, omdat zij controle zullen hebben over het volgende wapen: de informatie[2].

In dit werkstuk wordt aan de hand van een tijdbalk de ontwikkelingen tot de kwantumcryptografie, kwantumtheorie en kwantumcomputer gegeven. Met het (liefdes)verhaal van Alice en Bob en Alice' rivaal Eve wordt de communicatie tussen hen in de praktijk verduidelijkt. Alice en Bob kennen elkaar alleen als penvrienden. Bob heeft dus geen weet van Eve en zou Eve voor Alice kun-

nen ‘aanzien’, dankzij Eve’s smerige praktijken. Met het in de mond nemen van de hedendaagse encryptiemethode en de voortdurende ontwikkelingen hierin, sluiten we het werkstuk af met waar de praktijk van de kwantumcryptografie ophoudt en er slechts nog theorie rest. Uiteraard ontbreekt de *onmisbare* begrippenlijst niet.

In dit werkstuk wordt niet uitgebreid ingegaan op allerlei zaken rondom de encryptiemethoden, de natuurwetenschappelijk ontdekkingen en de digitale vooruitgang. Hiervoor zijn genoeg bronnen en literatuur om in te verdiepen. Mijn blik in dit werkstuk is gericht op de kwantumtheorie, de kwantumcryptografie en de kwantumcomputer. Echter de Onmisbare introductie en Alice, Bob en Eve doen hun verhaal kunnen hierin niet ontbreken.

Dit werkstuk zal geen bwi-werkstuk zijn als er geen link is naar het bedrijfskundige, wiskundige en informaticavlak. Mijn hoofdvraag en subvraag luiden dan ook als volgt:

Hoe brengen de rollen van natuurwetenschappen en informatica in de cryptografie, ons naar de toekomst: de kwantumcryptografie?

Wat kan het bedrijfsleven met deze ‘toekomst’ ondernemen?

2 Onmisbare introductie

De Onmisbare Introductie is als bijlage (*B Onmisbare introductie*) opgenomen. Slechts de laatste drie decennia zijn hier te lezen.

Tijdbalk, slechts ten ingeleide tot de ...

Kwantumcryptografie	Kwantumtheorie	Kwantumcomputer
(...)	(...)	(...)
1977 RSA is het eerste systeem dat voldoet aan de eisen van de publieke-sleutelcryptografie en wordt uitgevonden door Ron Rivest (1947), Adi Shamir (1945) en Leonard Adleman (1952).		**1977** Verschillende 'hobby'-computers komen op de markt waaronder de PET-computer voor $600 en de Apple II.
Honderd miljoen computers zouden meer dan duizend jaar nodig hebben om een RSA-cijfer te kraken, met voldoende grote waarden van *p* en *q* (de priemdelers) is RSA onaantastbaar.		
Whitfield Diffie (1944), Martin Hellman (1945) en Ralph Merkle (1952) krijgen wereldwijde erkenning voor hun concept van de publieke-sleutelcryptografie. Rivest, Shamir en Adleman krijgen de eer van het ontwikkelen van RSA.		**1979** Eerste relationeel database management systeem (dbms) gebruikmakend van SQL wordt door Oracle Corporation op de markt gebracht.
	1980 Het experiment dat in Bell's artikel (1965) wordt beschreven, wordt in Parijs uitgevoerd. Bell's voorspellingen komen uit.	**1980** Wereldwijd zijn er 700.000 'huis-, tuin- en keuken' computers. Ashton-Tate zijn de bouwers van het populaire databasepakket voor pc's dBase.

[14] Kwantumverstrengeling is vanaf nu een hot item, het test niet alleen de grondslagen van de natuurwetenschappen, maar blijkt ook interessant te zijn voor geheime informatieoverdracht: het zogenoemde kwantumgeheimschrift.
Men was op dreef en deed niet lang hierna voorspellingen van de kwantumteleportatie.

1981 Richard Feynman (1918-1988) stelt in zijn lezing *Simulating physics with computers* voor om een kwantumsysteem te simuleren met een kwantumsysteem. Ook Charles Bennett (1943) van IBM en Paul Benioff van Argonne National Laboratory speelden een vooraanstaande rol bij de allereerste verkenningen.

IBM komt met de IBM-PC, een veel goedkopere pc gebaseerd op de Intel 8086-processor Microsoft MS-DOS.

1982 De enorme groei van ARPA brengt het Internet voort.

Fundamenten voor Sun Microsystems worden gecreëerd door Scott McNealy, gebaseerd op Unix- en risc-technologie.

1984 Introductie van:
1. IBM met 80286 16-bit PC AT;
2. Apple met Macintosh;
3. Hewlett-Packard met laserjet printer voor pc's.

Ontwikkeling van een apparaatje waarmee Sandy Lerner en Len Bosack elkaar email kunnen versturen: de tegenwoordige router.

1985 David Deutsch van Oxford University beschrijft als eerste een universele kwantumcomputer, zij het als een abstract idee. Deutsch bedenkt ook de kwantumequivalenten voor de klassieke logische poorten AND, OR en NOT. Anders dan bij een klassieke computer moeten deze bij een kwantumcomputer evenveel ingaande bits hebben als uitgaande.

		1986 Sleuteldistributie is een probleem. De VS-regeringssleutels worden beheerd door Communication Security (COMSEC).
		1988 Toshiba, Tandy en NEC komen met een nieuwe generatie compacte computers: de laptops.
	1989 In CERN, het Europese centrum voor deeltjesonderzoek in Genéve, schrijft Time Berners Lee een projectvoorstel, geheten *World Wide Web*, voor een hypertext-achtige systeem waarbij gegevens opgeslagen kunnen worden op geografisch verspreid staande computers. Men vindt het niks.	
		1990 Het projectvoorstel *World Wide Web* wordt toch onveranderd aangenomen.
		Populariteit van geautomatiseerde hulpmiddelen voor de ontwikkeling van software (zogenoemde CASE-tools: computer aided software engineering) groeit.
1991 Phil Zimmermann (1954) ontwikkelt een RSA-encryptieproduct voor het versleutelen van het digitale dataverkeer en noemt het *Pretty Good Privacy* (PGP).		
1992 Toepassing van de symmetrische IDEA-sleutel (lijkt op DES), dat binnen PGP gebruikt wordt om RSA-sleutels te vercijferen.		**1992** Het International Data Encryption Algorithm (IDEA) wordt ontwikkeld door het Swiss Federal Institute of Technology ETH in Zurich.
		Intel presenteert de Pentium als opvolger van de 486-processor. DEC komt met de alpha-familie van risc-systemen.

[16]

1994 Terwijl de pro-encryptie-lobby pleit voor cryptografische vrijheid en de anti-encryptie-lobby pleit voor cryptografishe beperkingen, is er een derde optie die een compromis zou kunnen bieden: cryptografische sleutelbewaring.

1994 Wiskundige Peter Shor van AT&T Bell Labs ontdekt een zeer bijzonder algoritme om grote getallen snel te factoriseren met een kwantumcomputer. Deze ontdekking stimuleert het onderzoek naar kwantumcomputers enorm.

Er zijn zo'n 26 miljoen personal computers op de wereld.

1995 Shor doet een voorstel voor methoden van kwantumcorrectie om de fouten te repareren die de omgeving veroorzaakt in een systeem van vele kwantumbits.

Sun Microsystems zet de eerste versie van Java op internet in samenwerking met Arthur van Hoff.

De president van Oracle denkt dat het nieuwe tijdperk *Netwerk Computer* de pc snel gaat verdringen.

1996 Louis J. Freeh, directeur van de FBI, zegt: 'De gemeenschap van wetshandhavers steunt volledig een evenwichtig encryptiebeleid. [...] Sleutelbewaring is niet zomaar de enige oplossing, het is zelfs een uitstekende oplossing, omdat zij daadwerkelijk een evenwicht aanbrengt tussen fundamentele maatschappelijke aangelegenheden als privacy, informatiebeveiliging, elektronische handel en nationale veiligheid.'

Half miljoen Nederlanders is aangesloten op Internet.

RSA Data Security Inc., het voor RSA-producten verantwoordelijke bedrijf, wordt voor 200 miljoen dollar verkocht.

Lov Grover ontwikkelt bij Bell Labs (inmiddels overgedaan aan Lucent Technologies) het Grover-algoritme. Hiermee kan een kwantumcomputer bepaalde zoekproblemen in grote databestanden kwadratisch sneller oplossen dan een klassieke computer.

Deep Blue, schaakcomputer van IBM, verliest van de wereldschaakmeester Garry Kasparov.

1997 Ellis, Cocks en Williamsen krijgen de erkenning die hun toekomt, na bijna dertig jaar geheimhouding.	**1997** MIT-onderzoekers publiceren meetresultaten van een enkel kwantumbit: een vloeistof met een miljard maal een miljard identieke moleculen, die gezamenlijk het signaal van een enkele kwantumbit representeren. Met kernspinresonantie (NMR) manipuleren ze het enkele kwantumbit.	
Deep Blue verslaat de wereldschaakmeester Garry Kasparov.		
		Het DES-systeem wordt gekraakt in 96 dagen.
		Het Amerikaanse National Institute of Standards (NIST) zoekt naar een vervanger van DES middels een wedstrijd.
	1998 Het eerste twee-kwantumbitsysteem, gerealiseerd met vloeistof- NMR (University of California, Berkely, VS).	
	1999 Het eerste drie-kwantumbitsysteem, gerealiseerd met vloeistof- NMR (IBM Almaden Research Center, VS). Dit systeem toont als eerste aan dat het zoekalgoritme van Grover op een kwantumcomputer werkt.	
	2000 Het eerste vijf-kwantumbitsysteem, gerealiseerd met vloeistof- NMR (IBM). Dit systeem voert een deel van het factorisatie-algoritme van Shor uit. In hetzelfde jaar maken onderzoekers van het NIST in Boulder (VS) een simpele kwantumcomputer van vier ionen in een ionenval.	
	Hendrik Casimir (1909-2000) omschreef natuurkunde als een *benaderende* beschrijving van een *beperkt* gedeelte der fysische verschijnselen, die op hun beurt slechts een beperkt gedeelte van onze menselijke ervaringen uitmaken.	Het algoritme "Rijndael" van de Belgische cryptografen Joan Daemen (1965) en Vincent Rijmen (1970) wordt door de NIST verkozen tot veiligste voor het nieuwe AES.
	2001 Het eerste zeven-kwantumbitssysteem, gerealiseerd met vloeistof- NMR (IBM). Voor het eerst wordt het algoritme van Shor helemaal uitgevoerd. De zeven kwantumbits factoriseren het getal 15 in zijn priemdelers 3 en 5.	

[18]

2002 Zwitserse onderzoekers hebben een kwantumsysteem ontwikkeld om kwantumsleutels te distribueren via een optische vezel over een afstand van 67 km.
Het Japanse Mitshubishi Electric lukte het over een afstand van 87 km.

2003 De onderzoekers van Toshiba is het gelukt een afstand van 100 km te overbruggen met behulp van kwantumencryptie.

2004 Bijna alle tot nu toe werkende kwantumrekenaars zijn gebaseerd op vloeistof- NMR. Deze techniek laat zich net als ionenvallen echter niet opschalen naar duizenden kwantumbits. Wereldwijd gebeurt onderzoek naar betere kandidaten als nieuwe ionenvallen, vaste-stof- NMR, supergeleidende lusjes en kwantumdots.

2004 Er zijn zo'n 575 miljoen pc's ter wereld.

2005 De Japanse Groep NEC heeft de industrialisatie van een zender en een ontvanger van verdeelde sleutels via kwantumcryptografie aangekondigd.

2005 Internationaal Jaar van de Natuurkunde. Dit jaar is het precies 100 jaar geleden dat Albert Einstein (1879-1955) zijn 'wonderjaar' had .

2005 Bijna elk huishouden in de westerse wereld heeft al meer dan één computer.

3 Van hedendaags cijfer tot kwantumcryptografie

Cryptografie heeft zich zo door de eeuwen heen enorm ontwikkeld. Hedendaagse cijfers zijn bijvoorbeeld het asymmetrische RSA-cijfer en het symmetrische 3DES en AES voor het vercijferen van berichten. In de praktijk wordt het RSA-cijfer voornamelijk toegepast voor het zetten van digitale handtekeningen en het transporteren van de sessiesleutel[3]. 3DES of AES zijn voor het vercijferen van grote of veel data.

De evolutie van de cryptografie vóór deze cijfers kan worden nagelezen in de tijdbalk en de bijbehorende begrippenlijst, zie bijlage A en B.

Het hoofdstuk *Alice, Bob en Eve doen hun verhaal* is er voor de 'visuele' ondersteuning, het is raadzaam de volgende subhoofdstukjes eerst te lezen, alvorens met dit hoofdstuk verder te gaan:

4.1 Het probleem van sleuteldistributie

4.2 Het hulpstuk éénwegfunctie

4.3 Het briljante asymmetrische sleutelsysteem

In dit hoofdstuk wordt het RSA-cijfer slechts uitgelegd als inleiding op de kwantumcryptografie. Via kort uitgelegde begrippen komen we uit bij de kwantumwereld. Voor meer theorie en informatie rondom het RSA-cijfer, 3DES en AES zijn er tal van boeken en artikelen geschreven, waarover ik verder in dit werkstuk niet uitweid.

3.1 RSA

RSA staat voor de bedenkers van dit cijfer: de computerwetenschappers Ron Rivest (1947) en Adi Shamir (1952) en wiskundige Leonard Adleman (1945). Zij hebben in 1977 een onbreekbaar algoritme bedacht voor het maken van publieke- en privé-sleutels; voor de uiteindelijke methode voor encryptie en decryptie. Voornamelijk kan deze methode worden gebruikt voor de digitale handtekening.

RSA is het meest gebruikte coderingsysteem voor het ondertekenen van berichten tot nu toe. In de praktijk, zoals bij banken, wordt voor het vercijferen van data 3DES en AES, opvolger van des en straks ook van 3des, gebruikt. Deze cijfers zijn namelijk heel goed te gebruiken voor de beveiliging van informatie, maar zij is ook te gebruiken om de authenticiteit van een bericht te waarborgen. Het rsa-algoritme is een systeem voor codering én validering op het Internet en wordt automatisch meegeleverd met de browsers Netscape en Microsoft. Maar dit laatste terzijde.

[20] Alvorens het recept te geven voor het RSA-cijfer, volgt hieronder eerst een lijst van veelkomende afkortingen en relaties in voorbeelden binnen de moderne cryptografie:

M	Message	Het originele bericht, ook wel klare tekst of plaintext genoemd
K	Key	Sleutel om M te transformeren door een functie met parameter K
C	Ciphertext	Uitvoer van het vercijferingsproces
E_K	Encryption	Bericht wordt vercijferd met behulp van een sleutel K
$D_{K'}$	Decryption	Bericht wordt ontcijferd met behulp van een sleutel K'

$C = E_K (M)$	Versleuteling van klaretekst M tot cijfertekst C
$M = D_{K'} (C)$	Ontcijfering van cijfertekst C tot klaretekst M

Het recept voor het aanmaken van de sleutels is als volgt:

1 Constructie van de modulussen

- Kies twee grote priemgetallen p en q, van minstens 100 cijfers lang.
- Bepaal het product, het zogeheten sleutelgetal, $n = p^*q$. Deze n wordt de modulus, die wordt gebruikt bij het vercijferen en het ontcijferen van het bericht.
- Bepaal tevens het product[4] $\varphi(n) = (p-1)(q-1)$. Deze modulus wordt gebuikt bij de publieke sleutel
- Elk bericht wordt eerst omgezet in een groot openbaar getal. Wanneer het bericht langer wordt dan n, dan splits je dit in blokken op, die op hun beurt apart worden vercijferd en ontcijferd.

2 Constructie van de vercijferexponent d, onderdeel van de privé sleutel

- Kies d, een willekeurig groot getal, relatief priem ten opzichte van $(p-1)(q-1)$ dus dat wil zeggen de grootste gemeenschappelijke deler is $GGD(d, \varphi(n)) = 1$
- De privé-sleutel is het getallenpaar $\{d, n\}$

3 Constructie van de ontcijferexponent e, onderdeel van de publieke sleutel

- Bereken het getal e, zódanig dat $e^*d = 1 (mod\ \varphi(n))$
- De publieke sleutel is het getallenpaar $\{e, n\}$
  Hieruit volgt tevens de geheimhouding van alle andere grootheden $(p, q, \varphi(n))$

Het recept voor vercijferen gaat als volgt:

- Het symbool M krijgt een unieke getalwaarde
- Het te vercijferen bericht wordt opgedeeld in blokken M met een getalwaarde kleiner dan n.
- Het vercijferde blok C ontstaat door in de vercijferoperatie het blok M te verheffen tot de macht $e (mod\ n)$: $C = M^e (mod\ n)$
- Het ontcijferde blok M gaat op dezelfde manier: $M = C^d (mod\ n)$

Het is nu praktisch onmogelijk om de grootheid d te berekenen als alleen het publieke sleutelpaar $\{e, n\}$ bekend is; naast d zullen namelijk ook de priemgetallen p en q bekend moeten zijn,

dat maakt het RSA-cijfer onbreekbaar. Zolang de priemgetallen p en q uit minstens honderd cijfers bestaat, beslaat het product $n = p*q$ ongeveer tweehonderd cijfers. Het kost nu al zeshonderd traditionele computers enkele maanden om een getal n van 129 cijfers te ontbinden in factoren, laat staan een getal van tweehonderd cijfers.

Voor een voorbeeld lees **4.4 Het verlossende asymmetrische RSA-cijfer** *in "Alice, Bob en Eve doen hun verhaal".*

3.2 (A)symmetrische encryptie

Het RSA-cijfer is een vorm van een éénrichtingsalgoritme. De encryptie is gemakkelijk uit te rekenen, maar de inverse, dus de decryptie ervan is een stuk moeilijker. Een éénrichtingsalgoritme of éénwegfunctie bezit de eigenschap asymmetrische encryptie. In tegenstelling tot symmetrische encryptie, ook wel privé-sleutel encryptie waarbij er maar één sleutel om te coderen en te decoderen is, met als voordeel de snelheid en de eenvoudigheid. Echter asymmetrische encryptie bevat twee sleutels: één publieke sleutel om te coderen en één privé sleutel om te decoderen. Hiervan is het grote voordeel dat het zeer lastig te kraken is.

3.3 Hybride encryptie

Een combinatie van beide heeft het symmetrische voordeel van de snelheid van de encryptie en het asymmetrische voordeel van de veiligheid, dit heet hybride encryptie. Zo wordt RSA vaak gekoppeld met DES . Het te verzenden bericht wordt gecodeerd met een willekeurige DES-sleutel (de zogenoemde sessiesleutel). De DES-sleutel wordt dan gecodeerd met een RSA publieke sleutel, samen worden ze dan met het DES versleutelde bericht, verstuurd.

3.4 DES

Des staat voor Data Encryption Standard, een IBM-product uit 1972 dat in 1977 door de Amerikaanse Nationale Standaardisatie Instituut (ANSI) tot bron is gemaakt. Deze Amerikaanse encryptie standaard is een eenvoudige maar doeltreffende versleutelmethode voor encryptie van berichten. Des maakt gebruik van een 64-bit blokvercijfering en een 56-bit sleutel. Sinds 1991 wordt er gewerkt met een drievoudig DES-algoritme, zoals Blowfish en IDEA. Het coderingsprogramma Pretty Good Privacy (PGP) heeft IDEA wereldwijd bekend gemaakt. In 1997 is het DES-systeem gekraakt in 96 dagen. Des is geen zwak algoritme, maar de sleutels zijn wat kort, namelijk 56-bits. Het aantal mogelijke sleutels van 2^{56} is dusdanig klein dat het doorzoeken van alle mogelijke sleutels praktisch haalbaar is, dat hangt er ook maar net van af hoeveel geld men in de computers en rekentijd wil pompen.

3.5 3DES

Een verbeterde versie van DES is 3DES. Triple Data Encryption Standard is een encryptiealgoritme dat gebruik maakt van DES, maar op een zodanige wijze dat het veel moeilijker te kraken is. Des is kraakbaar omdat de sleutels 56-bits zijn, dat wil niet zeggen dat het algoritme te kraken is, daarom is 3DES ontwikkeld. In 3Des worden drie afzonderlijke DES bewerkingen achterelkaar losgelaten op de te versleutelen data.

[22] Dit kan op twee manieren. Of met twee sleutels van 56-bits (waarbij de eerste en derde bewerking met dezelfde sleutel worden uitgevoerd), of met drie onafhankelijke sleutels van 56-bits. De totale sleutellengte waarmee gecodeerd wordt is dus respectievelijk 112-bits of 168-bits, waarvan de laatste uiteraard de veiligste vorm is. Het is nu haast onmogelijk om alle sleutels te doorzoeken, de sleutellengte van 3DES is nu zo groot. In tegenstelling tot gewoon DES is 3DES nu een veilige techniek voor versleutelen. Financiële instellingen gebruiken op dit moment alleen 3DES, bij nieuwe implementaties zullen ze voor AES kiezen.

3.6 AES

Middels een wereldwijde openbare wedstrijd in 1997, georganiseerd door het Amerikaans Nationaal Instituut voor Standaardisatie en Technologie (NIST), wordt in 2000 *Rijndael* het winnende algoritme voor een nieuw AES (Advanced Encryption Standard), ook een computer versleutelingstechniek. De sleutels zijn altijd 128-bit. De blokgrootten zijn beperkt tot 128-, 192- of 256-bits. AES is bedoeld als de opvolger van DES en zal gaandeweg ook 3DES gaan vervangen. Een bijkomend groot voordeel van Rijndael ten opzicht van DES is dat het zowel in hardware als in software efficiënt te implementeren is.

3.7 Blokvercijfering[5]

Blokvercijfering wordt ook wel de Heilige Graal van de cryptografie genoemd. De willekeurigheid van de sleutel biedt een zodanige hoge veiligheid dat het voor een cryptoanalist (haast) onmogelijk is een bericht te ontcijferen. Zoals het woord blokcijfer al doet voorspellen, bestaat een blokcijfer uit een blok met cijfers, dat in willekeurige volgorde staan opgesteld. Een blok klaretekst kan in één keer worden vercijferd. De willekeur van de sleutel zorgt ervoor dat er geen structuur, geen patroon, geen enkele houvast in de cijfertekst te vinden is. Het éénmalige blokcijfer, ook wel 'one-time-pad' (van Gilbert Vernam) genoemd, is onbreekbaar en absoluut veilig.

3.8 IDEA

IDEA is de afkorting van International Data Encryption Algorithm ontwikkeld door ETH in Zürich in 1992. Dit symmetrische algoritme maakt gebruik van 64-bits blokvercijfering met een sleutelgrootte van 128-bits. Binnen PGP wordt IDEA gebruikt om RSA sleutels te vercijferen. IDEA staat als 'sterk' bekend. De sleutellengte van 128-bits is te groot om alle mogelijke sleutels te proberen. Voor zover bekend is IDEA nog niet gekraakt.

3.9 PGP

In 1991 ontwikkelt Phil Zimmermann (1954) een RSA-encryptieproduct, gecombineerd met een IDEA-sleutel, voor het versleutelen van het digitale dataverkeer en noemt het *Pretty Good Privacy* (PGP), vernoemd naar Zimmermanns favoriete radioprogramma, Pretty Good Groceries. Tevens heeft Zimmermann een toevalsfactor in PGP gebouwd, om de gebruikers ervan te verzekeren dat ieder zijn eigen priemgetallen gebruikt, en dus zijn eigen unieke privé- en publieke sleutel. De digitale handtekening voor het ondertekenen van een email is ook inbegrepen, gebaseerd op het Diffie-Hellman-systeem.

Zimmermann verspreidt PGP aanvankelijk als freeware. Enerzijds zal het gratis moeten zijn voor particuliere die er geen handel mee willen drijven. Individuen krijgen op deze manier het recht van privacy bij hun digitale communicatie, een weldaad voor de samenleving. Over de hele wereld gebruiken mensenrechtengroepen op een gegeven moment PGP om hun berichten te vercijferen, zodat de informatie niet in handen zal vallen van regimes die worden beschuldigd van het schenden van mensenrechten. Hoewel er een tegenpartij is, die encryptie een bedreiging vinden voor de samenleving, omdat criminelen, pedofielen en terroristen in het geheim met elkaar zullen kunnen communiceren, en beschermd worden tegen telefoontaps van de politie.

Hoewel Zimmermann er niet zijn kwaadste bedoelingen mee heeft om PGP als gratis software te verspreiden, denken de Amerikaanse overheid en de eigenaar van RSA, RSA Data Security Inc., er wel anders over. RSA Data Security Inc. vindt het een vorm van 'roofwaar' en dus patentschending. Volgens de Amerikaanse overheid is de encryptie-software PGP onder haar definitie oorlogsmateriaal, samen met raketten, mortieren en machinegeweren. Zonder vergunning van het ministerie van Buitenlandse Zaken mag PGP niet worden uitgevoerd.

Voor een voorbeeld lees **4.5 Van briefpapier naar email** *in "Alice, Bob en Eve doen hun verhaal".*

Nu is e-mailverkeer niet meer weg te denken uit de samenleving, haast iedereen verzendt en ontvangt e-mails. Hoewel een overgroot deel het overbodig, bovendien te omslachtig en te duur vindt, zijn email te versleutelen, vindt Zimmermann nog steeds dat iedereen het recht heeft op privacy, ook wat e-mails betreft. Dus vindt hij dat ook iedere burger toegang moet hebben tot de gratis software die online wordt aangeboden.

Wat veiligheid betreft. In 1994 reageert William Crowell, vice-directeur van de NSA:

"Als alle personal computers ter wereld – ongeveer 26 miljoen stuks – aan het werk worden gezet aan één met PGP vercijferd bericht, zou het naar schatting zowat 12 miljoen keer de leeftijd van het universum kosten om een enkel bericht te kraken."

Voor een voorbeeld lees **4.6 PGP: Pretty Good Privacy** *in "Alice, Bob en Eve doen hun verhaal".*

Codebrekers hebben als doel het RSA-cijfer te breken, zolang dit niet kan, proberen ze informatie op andere manieren te winnen, zoals:

- Stormaanvallen: het opvangen van aparte elektromagnetische signalen, die worden uitgezonden door een computer als er een letter wordt ingetypt of
- Virussen: via de 'achterdeur' binnenkomen in iemands privé-domein of
- Trojaanse paarden: een net-echt-uitziend-nep-programma die werkt als echt encryptieproduct maar de gebruiker voor de gek houdt doordat er ongezien (geheime) informatie kan worden afgetapt.

Het breken van het RSA-cijfer, ofwel het ontbinden in factoren, is één doel, maar het zoeken naar een mogelijkheid voor sleuteldistributie is een volgend struikelblok. Sleuteldistributie is het grootste probleem binnen de cryptografie. De logistiek en daarmee de veiligheid van de informatie kan nog altijd niet worden gewaarborgd. Sleuteldistributie is het proces dat verzekert dat zowel de

[24] verzender als de ontvanger toegang heeft tot de, voor het vercijferen en ontcijferen van een bericht vereiste, sleutel, en tegelijk verzekert dat de sleutel niet in vijandelijke handen valt.

Vanaf dit punt zullen we de toekomst in duiken, waar de oplossing op voorgaande problemen, op een presenteerblaadje voor ons klaar ligt.

Voor een voorbeeld lees **4.7 Sneller factoriseren** *in "Alice, Bob en Eve doen hun verhaal".*

Steunend op de kwantummechanica en de kwantumtheorie, kan het transporteren van sleutels worden voortgezet en RSA-cijfers in een handomdraai worden gekraakt. Daarom volgt nu een uitleg van de kwantummechanica en de kwantumtheorie.

3.10 De kwantummechanica

Kwantummechanica beschrijft het gedrag van zeer kleine deeltjes, deeltjes die zo klein zijn dat de klassieke mechanica van Isaac Newton (1643-1727) niet meer geldig is. De kwantummechanica is daarom een aanvulling op de Newtoniaanse natuurkunde. De eerste aanwijzingen van deze mechanica komt rond 1900. Te beginnen bij Max Planck (1858-1947). Tijdens het maken van een goede stralingswetformule, moet hij energie verdelen in kleine energiepakketjes, in tegenspraak tot wat de klassieke natuurkunde hierover voorschrijft. Dit is werkelijk zo volstrekt merkwaardig, dat zelfs Planck niet gelooft wat hij zojuist had verdeeld. Planck komt er achter dat energie niet bestaat uit een continu spectrum maar uit een gekwantiseerd (discreet) spectrum. Planck beweert dat de energie die elektronen bezitten, in een stralend voorwerp gekwantiseerd zijn. Een lastig natuurkundig verhaal. Daarom sluit ik me bij Niels Bohr (1885-1962) aan, een der vaders van de kwantummechanica. Hij zegt terecht:

"Wie over de kwantummechanica kan nadenken zonder duizelig te worden, heeft haar niet begrepen."

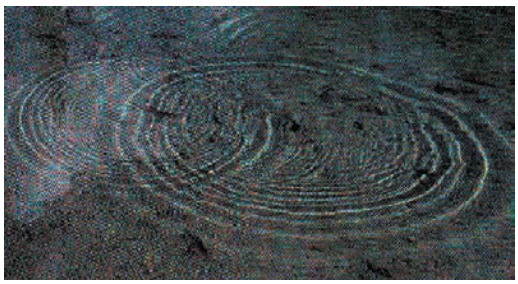
De 'magie' van de kwantummechanica zit hem namelijk in een aantal verschijnselen:

- Interfentie: het feit dat licht plus licht gelijk aan donker kan zijn.
- Superpositie[6]: het op verschillende plaatsen tegelijkertijd zijn;
- Tunnelen: het 'tunnelen' van een elektron door een ondoordringbare muur heen;
- Teleportatie: het 'overstralen'.

3.11 De kwantumtheorie

Uit de kwantummechanica is de kwantumtheorie voort gekomen. De kwantumtheorie verklaart de structuur van atomen, moleculen en in principe alles wat daaruit is opgebouwd. Het beschrijft elk voorwerp, zo geheten een *deeltje* (dit deeltje kan een atoom, foton of elektron zijn) met een golf. Bijvoorbeeld een steentje als deeltje, die als je deze in het water gooit, een golf maakt. Elk deeltje heeft zijn eigen speciale golf. Er kan een voorstelling worden gemaakt van deze golf, maar in de natuur heeft dit deeltje geen waarneembare golf. Deze golf wordt slechts als hulpmiddel gebruikt in de waarschijnlijkheidsberekening om het deeltje te kunnen lokaliseren.

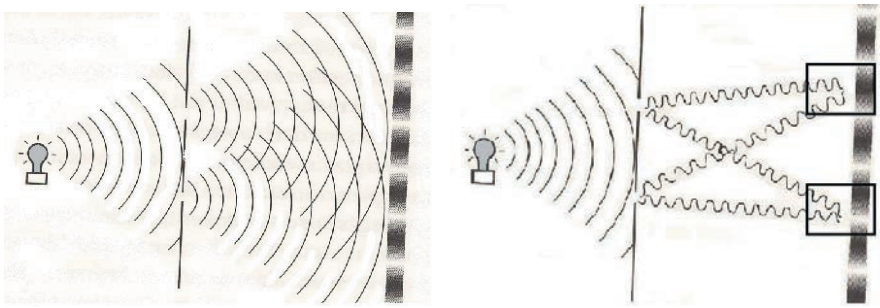
De waarschijnlijkheid kan als volgt worden geïnterpreteerd met als voorbeeld twee steentjes. Als twee steentjes vlak bij elkaar in het water wordt gegooid (zie afbeelding 2), ontstaat een *interfentiepatroon*: op bepaalde plaatsen versterken de golven elkaar en op andere plaatsen doven ze elkaar uit.



Afbeelding 2. Waterkringen

(*NOW-Huygenslezing*, maart 2005, pagina 9)

In de kwantumtheorie wordt ook gebruik gemaakt van golven, zogenoemde kwantumgolven, zoals dat met het licht kan worden gedaan. Een groot verschil echter, is dat deze kwantumgolven geen materie zijn, zoals lichtgolven, maar slechts een middel zijn om de waarschijnlijkheid te meten waar een deeltje zich kan bevinden. Op donkere plaatsen waar golven elkaar hebben uitgedoofd, is de kans klein dat het deeltje zich er bevindt. De kans is dus groot dat het deeltje zich op de lichte plekken bevindt, op plaatsen waar golven elkaar hebben versterkt. Afbeelding 3 toont het experiment, dat Thomas Young (1773-1829) in 1801 uitvoerde, van het interfentiepatroon.



Afbeelding 3. Interfentiepatroon van Thomas Young, 1801

(*Code*, Singh, S., pagina 389)

In het linker figuur, van afbeelding 3, waaiert licht uit door een wand met twee spleten. Door wisselwerking wordt een streeppatroon op het scherm daarachter geworpen. In het rechter figuur is duidelijk de inwerking van de ene golf op de andere te zien:

- piek + dal = donkere streep
- piek + piek = dal + dal = lichte streep

Het interfentiepatroon is aanvankelijk een raadsel voor Thomas Young, het wordt nog maffer als er slechts één deeltje wordt gebruikt voor de metingen, en toch het hele interfentiepatroon te zien is. De kwantumtheorie verklaart, hoe bizar het ook klinkt, dat één enkel deeltje op verschillende

[26] plaatsen tegelijkertijd kan zijn: de kwantumsuperpositie. Toch wordt bij een meting het deeltje op maar één plek waargenomen, maar vóórdat die meting plaatsvindt, bevindt het deeltje zich nog in een superpositie. Om dit wonderlijke verschijnsel echt bizar te maken, is het feit dat het deeltje ook in verschillende snelheden, kleuren en rotatierichtingen tegelijkertijd kan zijn. Licht lijkt zich te gedragen als golf en als deeltje: dit heet golf-deeltjedualiteit. Bohr zegt over golf-deeltjedualiteit:

> *"Of een voorwerp zich als golf of als een deeltje gedraagt, hangt af van de keuze van het apparaat waarmee je ernaar kijkt!"*[7]

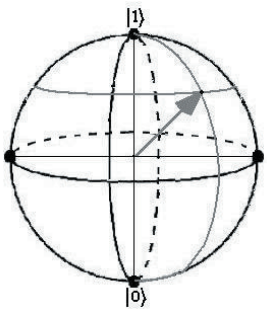
Een lichtbundel bestaat, volgens de moderne fysica, uit talloze individuele deeltjes, fotonen genoemd, die golfachtige eigenschappen vertonen. Verdere verklaringen en bewijzen uit de fysica laat ik buiten beschouwing.

De kwantumtheorie doet zich niet alleen dagelijks voor op het meest elementairste niveau, maar ook op andere niveaus, zoals in een column[8] van Youp van 't Hek:

> *"(...) Heb ook weer genoten van het blik deskundigen dat door de omroepen was opengetrokken. "De groep die de aanslag via de website claimt zou het inderdaad serieus gedaan kunnen hebben, maar misschien ook niet. Je weet het niet!" Dat is informatie waar je wat aan hebt. Het zou kunnen, maar misschien ook weer niet.(...)"*

3.12 De kwantumwereld

Om de kwantumwereld verder te beschrijven wordt gebruik gemaakt van het elektron, het elementair negatief geladen deeltje van een atoom. De spin van het elektron is de interne rotatie om zijn eigen as, vergelijkbaar met het rondtollen van een tennisbal. Deze rotatie kan links om zijn as gaan of rechtsom. De spineigenschap van een elektron kan nu worden meegenomen in de kwantumwereld en gaat dienst doen als kwantumbit, de eenvoudigste eenheid van de kwantuminformatie.



Afbeelding 4. Kwantumbit

(*Natuurwetenschap & Techniek*, juni 2004, pagina 22)

De spin van het elektron kan superposities aannemen, oftewel omlaag (spin = 0) of omhoog (spin = 1) wijzen, maar het kan ook elke waarde tussen 0 en 1 aannemen. Zodra er gemeten wordt, neemt het 0 met kans α of 1 met kans (1-α) aan. Bij deze qubit hoort de zogenaamde golffunctie:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$|0\rangle, |1\rangle$ zijn symbolen voor de golffuncties die de twee uiterste standen van de qubit beschrijven. De coëfficiënten α en β geven aan hoeveel van elke toestanden (horizontaal, vertikaal, diagonaal, etc.) aanwezig is.

Het begrip superpositie kan samen met voorgaande uitleg iets redelijker gemaakt worden aan de hand van de kat van Schödinger. Hiermee de volgende golffunctie in acht genomen:

$$|kat\rangle = |levend\rangle + |dood\rangle$$

De kat is tegelijkertijd levend en dood, pas na de meting is de kans fiftyfifty of de kat volledig levend of volledig dood is. De kat gaat in een doos en de kleppen worden gesloten, onmiddellijk zijn er twee mogelijke toestanden voor de kat, namelijk dood of levend. De kat is levend de doos ingegaan en is dus heel zeker dat de kat zich in de levende toestand verkeert, als de doos opengaat, leeft zij nog. Op dit punt bevindt de kat zich niet in een superpositie van toestanden. Nu wordt een atoomkern, die de doodsoorzaak wordt als de kern uiteenvalt, naast de kat in de doos geplaatst en doen het deksel weer dicht. Vanaf dit moment is een periode van onwetendheid, want de toestand van de kat kan niet gezien of gemeten worden. Leeft ze nog, of is de atoomkern uiteengevallen en is ze nu dood? Volgens de traditie is de kat of dood of levend, alleen is onbekend wat van tweeën. Gelukkig geeft de kwantumtheorie het verlossende antwoord en 'zegt' dat de kat zich bevindt in een superpositie van twee toestanden – zij is zowel dood als levend, zij voldoet aan alle mogelijkheden:

$$\Psi = |\text{levend, niet uiteengevallen}\rangle + |\text{dood, uiteengevallen}\rangle$$

Superpositie treedt alleen op wanneer een voorwerp uit het oog wordt verloren. Tevens is het een manier om een voorwerp te beschrijven in een periode van dubbelzinnigheid. Als ten slotte de doos wordt geopend, kan gezien worden of de kat dood of levend is. Het kijken naar de kat dwingt haar in een bepaalde toestand en op datzelfde moment verdwijnt de superpositie. Deze waargenomen toestand is nu verstrengeld, omdat er een direct verband bestaat tussen de toestanden van *(levend, niet uiteengevallen)* en *(dood, uiteengevallen)*. Als de toestand van één van beide vastligt, is zonder te meten bekend wat de toestand van de andere is. Een meting van het ene deeltje heeft invloed op de toestand van het andere deeltje, hoe ver deze zich ook van elkaar bevinden.

3.13 De kwantumcomputer

Dit waarschijnlijkheidskarakter kan een bit tegelijkertijd 0 én 1 laten zijn, waarmee het vele rekenmogelijkheden kent. Stel een kwantumbit, de zogeheten qubit, is een spintoestand of foton (lichtdeeltje). Met N traditionele bits zijn er 2^N mogelijke combinaties ná elkaar mogelijk, met twee bits zijn die 00, 01, 10 en 11. Met N qubits kunnen twee qubits zich, met hun eigenschap superpositie, tegelijkertijd in 00, 01, 10 en 11 bevinden. Een kwantumcomputer, opgebouwd uit N qubits, zou dus 2^N berekeningen tegelijkertijd kunnen uitvoeren.

[28] Als wetenschappers een kwantumcomputer op een redelijke schaal kunnen bouwen, zou die de veiligheid van alle huidige encryptie en decryptie cijfers in gevaar brengen, behalve het eenmalige blokcijfer. Een belangrijk element in de ontwikkeling van de kwantumcomputer is het doen overgaan van kwantuminformatie. Als een kwantumvoorwerp met kwantuminformatie opgeslagen verstuurd wordt, wordt de kwantumtoestand en niet het kwantumvoorwerp verplaatst gedurende de kwantumteleportatie. Het is immers de kwantumgolf van het voorwerp die de eigenschappen van het voorwerp beschrijft.

Een journalist vroeg eens aan de fysicus Asher Peres (1934-2005) of enkel alleen het lichaam kon worden geteleporteerd of ook de geest, Peres antwoord:

"Alleen de geest kan geteleporteerd worden."

Met een kwantumcomputer zou je nu ook het factorisatieprobleem van het RSA-cijfer kunnen oplossen. Hoe ontbind je een getal in zijn priemdelers, precies die delers die priemgetallen zijn. Hoewel het tegenwoordig mogelijk is, dit probleem op te lossen, kost het alleen de allersnelste computer vier maanden om een getal van ongeveer 130 cijfers te factoriseren. Als het getal nog eens twee keer zo lang is, is de oplossingstijd dusdanig exponentieel gegroeid, dat wachten compleet zinloos is.

Ook al is er nog helemaal geen kwantumcomputer, de rekenmethode is al bedacht door wiskundige Peter Shor (1959) in 1994. De toekomstige kwantumcomputer zou het factorisatieprobleem in een tel kunnen oplossen, waardoor de tegenwoordige beveiligingen in één klap onveilig zijn.

Zoeken in grote databestanden zal ook veel gemakkelijker worden. Nu moet alle gegevens op zichzelf omstebeurt doorzocht worden. Dankzij de kwantumsuperposities worden alle gegevens tegelijkertijd doorzocht. Lov Grover bedacht er in 1996 alvast een programma voor, waarmee het DES-cijfer gekraakt zou kunnen worden.

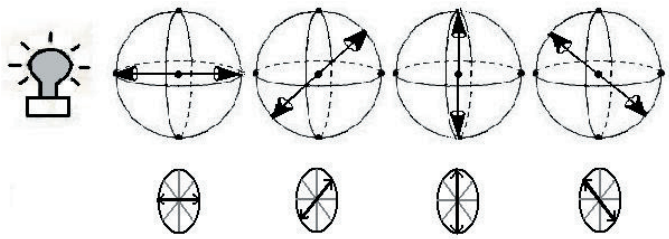
Zoals al eerder is opgemerkt over de superpositie van een qubit, is vóór de meting de qubit nog 'ergens'. Pas op het moment van de meting, komt er een werkelijke waarde uit. Een kwantumsysteem kan zich tegelijkertijd in 2^N toestanden bevinden, maar zodra iemand gaat meten, blijft er maar één uitkomst over. Nu de grote vraag: is dit wel de juiste uitkomst? Met een nog te ontworpen algoritme zouden de gewenste berekeningen elkaar moeten versterken en de niet gewenste elkaar moeten uitdoven. Zodat bij de uiteindelijke metingen, de qubits alleen het correcte antwoord geven.

3.14 De kwantumcryptografie

Als de kwantumcomputer gerealiseerd is, kan het RSA-cijfer (en het DES-cijfer) gebroken worden, en is de tot dan toe veiligste vorm van cryptografie gebroken. Hoewel... de overdachte kwantumtheorie komt als een geschenk uit de hemel, het nu al ouderwetse geheimschrift kan gemoderniseerd worden met de kwantumcryptografie. Kwantumcryptografie wordt de onbreekbare vorm van cryptografie die gebruikmaakt van de kwantumtheorie, maar nog meer speciaal van de onzekerheidsrelatie. De kwantumcryptografie garandeert de veilige uitwisseling van een willekeurige reeks bits. Deze reeks bits wordt dan gebruikt als de basis voor een eenmalig blokcijfer van Vernam, de enige vorm van encryptie, die onbreekbaar is. Het steunt op een willekeurige sleutel die even lang is als het

bericht. Elke sleutel kan eenmaal en niet meer dan eenmaal worden gebruikt. [29]

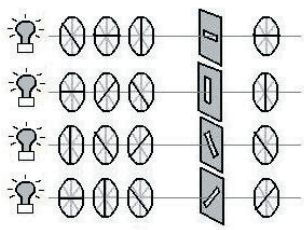
Kwantumcryptografie is net als de kwantumcomputer, gebaseerd op de kwantumtheorie. Het idee was er al eind jaren zestig, uitgewerkt door de toenmalige postdoc aan de Columbia University Stephen Wiesner (1942), toentertijd door niemand serieus genomen. Kwantumcryptografie zal uitstekend gebruikt kunnen worden voor kwantumgeld, met het grote voordeel dat het onmogelijk te vervalsen is. Wiesner neemt hiervoor de fotonenfysica in gedachten. Om kort samen te vatten, fotonen trillen wanneer ze zich verplaatsen. In afbeelding 5 bewegen fotonen zich wel in dezelfde richting, alleen telkens onder een andere hoek. Deze trillingshoek wordt de polarisatie van een foton genoemd.



Afbeelding 5. Mogelijke polarisatierichtingen van een foton

(*Code*, Singh, S., pagina 402)

Voor het gemak beschouwen we alleen bovenstaande polarisatierichtingen, dat zijn dus: ↕↔↘↗. Wanneer er een zogeheten polaroidfilter voor de fotonen wordt gehouden, gaan alleen die fotonen er doorheen die overeenkomen met de gebruikte polaroidfilter, ofwel de fotonen met dezelfde polarisatie. Hierbij kun je nu voor het gemak aan een rooster met lucifers denken. De lucifers gaan alleen door de rooster heen als ze zich onder de juiste hoek bevinden. Zoals te zien is in afbeelding 6.



Afb.6. De vier verschillende polaroidfilters

(*Code*, Singh, S., pagina 402)

In bovenstaande afbeelding komen diagonale (rechtlijnige) gepolariseerde fotonen, zoals in de tweede (eerste) en vierde (derde) rij, bij een rechtlijnige (diagonale) polaroidfilter voor een kwantumdilemma te staan. Ze zullen er voor de helft door heen gaan, waarna ze getransformeerd worden naar een rechtlijnige (diagonale) polarisatie. De andere helft wordt of helemaal geblokkeerd of deels geblokkeerd en deels doorgelaten. Wiesners idee is nu om een aantal lichtvangertjes in het biljet te

[30] maken, gevuld met gepolariseerde fotonen, die niet met het blote oog zichtbaar zijn. Het biljet bevat bovendien een uniek serienummer, deze combinatie identificeert het bankbiljet. Een valsemunter kan de polarisatie in het bankbiljet niet meten, omdat hij niet weet welk type foton zich in elk lichtvangertje bevindt, en dus ook niet kan weten hoe hij een polaroidfilter moet houden. De bank kan het biljet wel controleren, daar zij de ontbrekende informatie van het biljet weet. Kwantumgeld is een groots idee, maar alleen technisch al moeilijk uitvoerbaar.

Charles Bennett (1943), een oude universiteitsvriend van Wiesner, en Gilles Brassard (1955), een computerwetenschapper aan de universiteit van Montreal, vinden Wiesners idee niet eens zo gek, helemaal niet. Hun gedachten brengt het idee naar een toepassing in de cryptografie.

Voor een voorbeeld lees **4.8 Het maken van een kwantumsprong** *in "Alice, Bob en Eve doen hun verhaal".*

De kwantumcryptografie kan een systeem worden dat de veiligheid van een bericht verzekert. Een luistervink kan direct worden opgemerkt. Kwantumcryptografie is dus niet alleen veilig, maar kent ook absolute privacy. De werkwijze is als volgt te omschrijven: Alice stuurt Bob een willekeurige reeks fotonen. Bob meet deze. Bob vertelt Alice welke filters hij telkens heeft gebruikt, Alice geeft aan wanneer hij dit correct heeft gedaan. Alice en Bob verwijderen de incorrecte metingen, nu ontstaat een identiek eenmalig blokcijfer. Dit eenmalige blokcijfer wordt onmiddellijk getest op de deugdelijkheid ervan. Als er geen problemen zijn, kunnen ze het gebruiken bij het vercijferen van een bericht. Wanneer er toch problemen zijn, weten Alice en Bob onmiddellijk dat Eve tussen beiden is gekomen. Voor de veiligheid moeten Alice en Bob weer van voor af aan beginnen.

Kwantumcryptografie hoeft niet te wachten totdat er een kwantumcomputer is. Sterker nog, als de kwantumcomputer is gebouwd en zijn functies kan uitvoeren waarvoor hij gemaakt is, zoals factoriseren van immense getallen, is de kwantumcryptografie de veiligste cryptografie die nog rest. Het gaat er nu om een kwantumcryptografisch systeem te bouwen dat over bruikbare afstanden werkt. Bennet heeft reeds twee computers, genaamd Alice en Bob, gebouwd die fotonen naar elkaar kunnen uitzenden. Op een afstand van dertig centimeter heeft de eerste kwantumcryptografische uitwisseling plaatsgevonden.

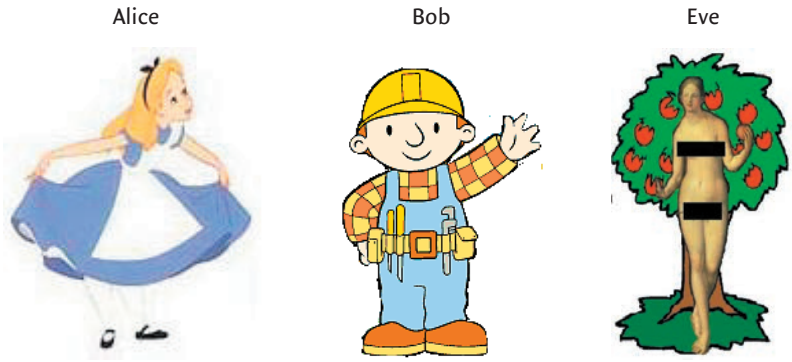
Een grote afstand is lastig, daar fotonen zich erg slecht voortbewegen. Zodra een foton de lucht in gaat, wordt de polarisatie van het foton (sterk) beïnvloedt door luchtmoleculen. In 2002 lukt het een groep onderzoekers aan de universiteit van Genève om kwantumcryptografie toe te passen via een optische vezel van 67 km lang. De Japanners kwamen tot een afstand van 87 km, in 2003 hebben ze zelfs een afstand van 100 km bereikt. Deze oplossing zal gebruikt kunnen worden tussen bedrijven in dezelfde stad onderling om gepolariseerde fotonen naar elkaar toe te zenden. Wetenschappers in de Verenigde Staten, die werken aan een kwantumcryptografisch satellietsysteem, zijn al zover gevorderd dat ze een kwantumsleutel al een kilometer ver, via de lucht kunnen zenden.

De vraag blijft alleen wat zal er eerder zijn: [31]

- de kwantumcomputer, zodat alle tot nu gebuikte cryptografische cijfers, met als belangrijkste het RSA-cijfer, gebroken kunnen worden of
- de kwantumcryptografie, die ons redt voor als de kwantumcomputer ooit zijn doorbraak maakt. of liever gezegd, een systeem waarop de kwantumcryptografie kan draaien.

4 Alice, Bob en Eve doen hun verhaal

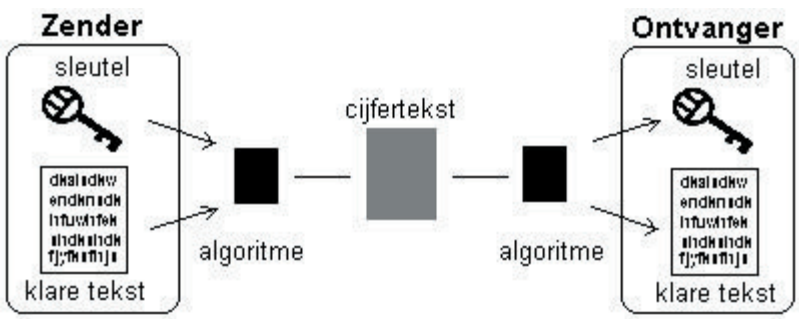
Alice en Bob kennen elkaar alleen als penvrienden. Eve wil graag tussen beiden komen en doet dit op slinkse stiekeme wijze. Bob heeft geen weet van Eve en zou Eve voor Alice kunnen 'aanzien'. Alice, Bob en Eve voorgesteld:



Afbeelding 7. Alice, Bob en Eve stellen zich voor

4.1 Het probleem van sleuteldistributie

Alice wilt een geheime boodschap uitwisselen met Bob, zij zal deze moeten vercijferen. Om dit te kunnen doen, moet zij een sleutel gebruiken die zelf geheim is. Om een klaretekstbericht te vercijferen haalt Alice (zender) het door een encryptie-algoritme. Bob (ontvanger) haalt de cijfertekst wederom door het algoritme als hij weet heeft van de gebruikte sleutel. Maar hoe kan Bob weet hebben van de gebruikte sleutel zonder Alice ontmoet te hebben?

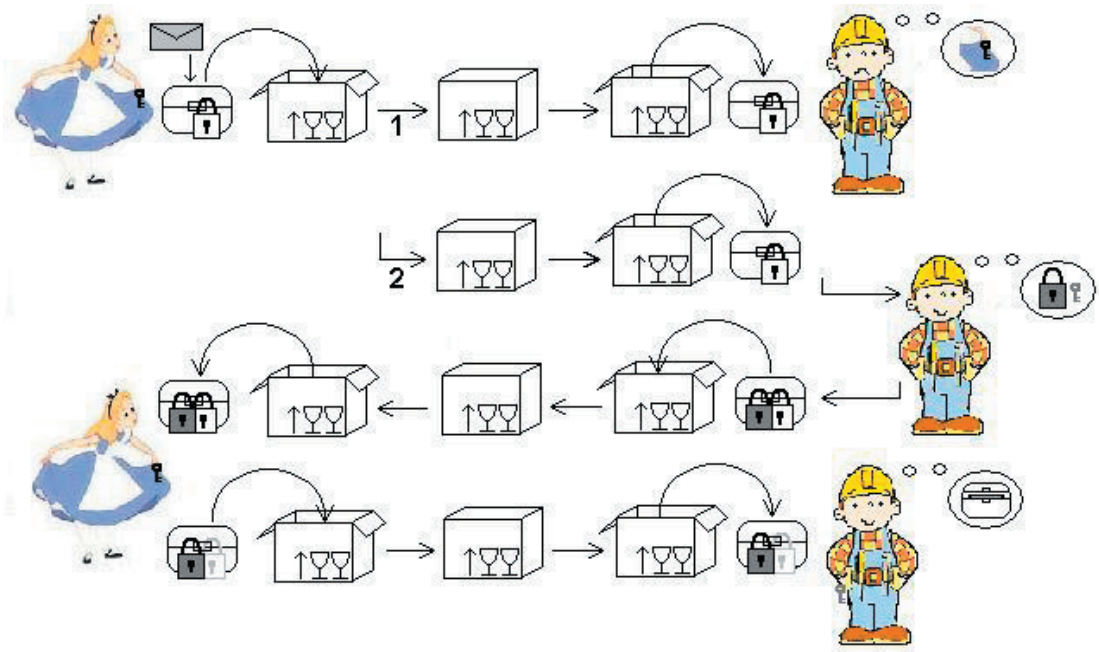


Afbeelding 8. Encryptie-algoritme

(*Code*, Singh, S., pagina 29)

Nu ontstaat het probleem van het overbrengen van de geheime sleutel aan Bob om het geheime bericht weer te ontcijferen. Alice wilt graag een geheim, een vercijferd bericht, delen met Bob, maar ze hebben al een geheim, namelijk de sleutel. Hoe krijgt Bob de sleutel van Alice in handen, zonder met elkaar fysiek af te spreken?

[34] Alice zou een brief in een kistje beveiligd met een slot naar Bob kunnen sturen. Als het kistje bij Bob is, kan hij hem niet openmaken, omdat hij de sleutel niet heeft (1). Bob zou dan opnieuw een slot aan het kistje moeten hangen, vervolgens het kistje terugsturen. Alice kan dan haar slot er afhalen, zij stuurt het kistje weer naar Bob en Bob opent het kistje met daarin de brief (2).



Afbeelding 9. Het principe van Diffie-Hellman. Dit systeem houdt zich bezig met sleutelbeheer. (Roos, L.C.)

Sleuteldistributie hoeft dus geen onvermijdelijk onderdeel te zijn van de cryptografie. Als deze oplossing vertaald wordt naar encryptietermen, komt dit op het volgende neer:

Alice gebruikt haar eigen sleutel om een klaretekst te vercijferen en stuurt dit op naar Bob. Bob vercijfert opnieuw de vercijferde tekst en stuurt de verdubbelde vercijferde tekst terug naar Alice. Alice verwijdert haar eigen encryptie weer en stuurt deze op naar Bob. Bob verwijdert zijn encryptie en kan nu de oorspronkelijke klaretekst lezen.

Helaas kan het dubbele-slotsysteem niet op gaan. Er is een vereiste volgorde waarin de encryptie en decryptie moet plaatsvinden. Als Alice vercijfert, moet eerst dat bericht worden ontcijferd alvorens het opnieuw kan worden vercijferen.

Op een wintermorgen trek je toch ook eerst je sokken aan voordat je schoenen aantrekt, om 's avonds eerst je schoenen en dan pas je sokken uit te kunnen trekken.

4.2 Het hulpstuk eenwegfunctie

Martin Hellman (1945) ontwikkelt een eenwegfunctie $Y^x (mod\ P)$, waarin gebruik wordt gemaakt van modulair rekenen. Alice en Bob kunnen nu een geheim afspreken in een publiekelijk toegankelijk gesprek. Zij hoeven slechts de waarden van Y en P af te spreken, bijvoorbeeld $Y = 7$ en $P = 11$, zoals te zien in afbeelding 10.

	Alice	Bob
	Alice en Bob hebben een eenwegfunctie afgesproken: 7^x(mod 11)	
Fase 1	Alice kiest een getal, zeg *3*, en houdt het geheim. We noemen haar getal A.	Bob kiest een getal, zeg *6*, en houdt het geheim. We noemen zijn getal B.
Fase 2	Alice zet *3* in de eenweg en werkt de uitkomst uit 7^A(mod 11): $7^3(mod\ 11) = 343\ (mod\ 11) = 2$	Bob zet 6 in de eenweg en werkt de uitkomst uit 7^B(mod 11): $7^6(mod\ 11) = 117.649\ (mod\ 11) = 4$
Fase 3	Alice noemt de uitkomst van deze berekening α, en zendt haar uitkomst, 2, aan Bob.	Bob noemt de uitkomst van deze berekening β, en zendt zijn uitkomst, 4, aan Alice.
Omwisseling	Normaal zou dit een cruciaal moment zijn, omdat Alice en Bob informatie uitwisselen en dit dus een kans voor Eve is om hen af te luisteren en achter de bijzonderheden van de informatie te komen. Het blijkt echter dat Eve kan meeluisteren zonder dat het de uiteindelijke veiligheid van het systeem kan beïnvloeden. Alice en Bob kunnen dezelfde telefoonlijn gebruiken die ze namen om de waarden voor Y (=7) en P (=11) af te spreken, en Eve zou de twee getallen kunnen onderscheppen die worden uitgewisseld, 2 en 4. Maar deze getallen zijn niet de sleutel, zodat het niet uitmaakt of Eve ze kent.	
Fase 4	Alice neemt Bobs uitkomst, en rekent de uitkomst uit van β^A (mod 11): $4^3\ (mod\ 11) = 64\ (mod\ 11) = 9$	Bob neemt Alices uitkomst, en rekent de uitkomst uit van α^B (mod 11): $2^6\ (mod\ 11) = 64\ (mod\ 11) = 9$
Sleutel	Het wonder geschiedt: Alice en Bob komen uit op hetzelfde getal: 9. Dit is de sleutel![9]	

Afbeelding 10. Eénwegfunctie (*Code*, Singh, S., pagina 322)

Eve kan dit niet ingrijpen, omdat de waarden van A en B niet zijn uitgewisseld en dus voor haar onbekend zijn. Theoretisch gezien kan ze A uit α afleiden of B uit β, maar de functie is eenwegs, het is haast ondoenlijk om het proces om te keren, vooral als er 'gesleuteld' wordt met grote getallen.

4.3 Het briljante asymmetrische sleutelsysteem

Er rest nog steeds een probleem, hoe komt de afspraak van de Y en de P tot stand? Het is Whitfield Diffie (1944) die met het briljante idee komt van een asymmetrisch sleutelsysteem. De encryptie- en decryptiesleutel zijn niet identiek. Alice heeft van beide een sleutel. Alices decryptiesleutel vertelt ze aan niemand en heet nu voortaan haar privé-sleutel. Haar encryptiesleutel mag ze iedereen vertellen en wordt haar publieke sleutel, deze kan in een soort van telefoonboek worden opgenomen. Bob kan nu aan Alice een bericht sturen, door deze met Alices publieke sleutel te vercijferen en te versturen. Alice ontvangt het vercijferde bericht en ontcijfert het met haar privé-sleutel. Eve kan Bobs boodschappen wel onderscheppen, maar niet ontcijferen. Het algoritme kan nu slechts in een richting worden gebruikt.

Het sluiten (encryptie) van een hangslot kan iedereen, maar het ontsluiten (decryptie) kan alleen diegene die

de sleutel heeft.

Nu alleen nog het vinden van zo'n eenwegfunctie. Diffie, Hellman, Merkle en andere wetenschappers steken de koppen bij elkaar bij het zoeken naar een passende eenwegfunctie. Zonder resultaat. Het zijn Ron Rivest (1947), Leonard Adleman (1945) en Adi Shamir (1952)[10] die met het verlossende asymmetrische RSA-cijfer komen.

4.4 Het verlossende asymmetrische RSA-cijfer

Met behulp van voorgaande uitleg over het RSA-cijfer personaliseert Alice de eenwegfunctie door twee priemgetallen p en q te kiezen; door p en q te vermenigvuldigen, wordt N, de publieke sleutel gevormd. Bob wilt een bericht aan Alice vercijferen. Hij zoekt de N van Alice op en vult deze in de algemene vorm van de eenwegfunctie, die ook bekend zal zijn. Dit vercijferde bericht zendt Bob aan Alice. Bob heeft dus de eenwegfunctie van Alice ingevuld. De functie is nu een kant opgegaan, hoe kan Alice deze omkeerbaar maken? Door het ontwerp van Rivest toe te passen. Zijn proces is omkeerbaar als de waarden van p en q bekend zijn. Als deze waarden niet bekend is, is het vrijwel onmogelijk N te ontbinden in factoren.

Alice hoeft niet langer bang te zijn dat Eve de sleutel onderschept, die voor Bob bestemd is. De overbrenging hiervan is veilig. Alice heeft alleen zorg over het geheim houden van haar privé-sleutel.

4.5 Van briefpapier naar email

Alice en Bob gaan met hun tijd mee en maken gebruik van emails om berichten aan elkaar te verzenden. Eve gooit haar vijgenblad weg en koopt niet alleen de hipste kleren, maar ook de allermodernste computer, bovendien neemt ze direct de snelste internetverbinding. Eve, een echt natuurtalent, hackt bij de server van Alice in en kan alle verzonden emails checken, net zolang totdat zij het emailadres van Alice heeft gevonden. Alle verzonden emails worden doorgestuurd, zonder dat Alice iets in de gaten heeft. RSA-encryptie zou Alices emails kunnen beveiligen.

4.6 PGP: Pretty Good Privacy

RSA-encryptie is toegankelijk gemaakt voor een breed publiek door Phil Zimmermann (1954) met zijn programma PGP, Pretty Good Privacy. Nu wilt Alice met deze nieuwe ontdekking van PGP een bericht sturen aan Bob. Dit bericht versleutelt zij eerst met een symmetrisch cijfer, in PGP het zogeheten IDEA-cijfer. Nu wilt ze het IDEA vercijferen, ze kiest het publieke RSA-cijfer van Bob. Als Alice klaar is met alle vercijferingen, stuurt ze Bob het bericht wat ze met IDEA heeft vercijferd en de IDEA-sleutel zelf. Bob ontcijfert de IDEA-sleutel met zijn prive RSA-sleutel, zodat hij vervolgens het bericht met de IDEA-sleutel kan vercijferen.

Met PGP kan ook de digitale handtekening, gebaseerd op het principe van Diffie en Hellman, worden gezet om auteurschap te kunnen garanderen.

Hoe weet Alice dat zij daadwerkelijk de publieke sleutel van Bob heeft? Stel, Alice en Bob kennen elkaar nog maar net. Alice wilt graag de publieke-sleutel van Bob weten, en vraagt hem deze per email te zenden. Eve onderschept de mail, vernietigt deze en stelt een nieuwe mail op naar Alice die

haar publieke sleutel bevat. Een probleem van publieke-sleutelcryptografie is de zekerheid die Alice wilt hebben dat ze daadwerkelijk over de juiste publieke-sleutel van Bob, en niet van Eve, beschikt. Waarborginstellingen, die Trusted Third Parties of Certification Authorities worden genoemd, kunnen verifiëren of een publieke-sleutel ook echt correspondeert met Bob nadat zij de publieke sleutel hebben gesigneerd (digitaal certificaat). De waarborgautoriteiten laten we in dit werkstuk links liggen.

Zelfs als Alice en Bob RSA-cijfers gebruiken, kan Eve toch nog het een en ander uithalen om informatie af te leiden uit berichten, die zij onderschept heeft. Eve weet de inhoud dan wel niet, maar ze kan wel achterhalen wie het verstuurt heeft en aan wie het wordt verzonden. Met een zogenoemde stormaanval kan zij aparte elektromagnetische signalen opsporen, die worden uitgezonden als een letter wordt ingetypt. Een bericht kan worden onderschept voordat het überhaupt vercijferd is. Op allerlei manieren kan Eve bezig zijn, maar haar uiteindelijk doel lijkt nog onbereikbaar: het kraken van het RSA-cijfer.

4.7 Sneller factoriseren

Eve weet dat het ontbinden in factoren de enige manier is om de twee priemgetallen, die de privé-sleutel vormen, te ontrafelen. Met Eves huidige supersnelle computer duurt het gewoonweg veel te lang om te factoriseren. Ze heeft een methode nodig die miljoenen keren sneller is. De oplossing zou de kwantumcomputer moeten zijn, die berekeningen in een tel kan uitvoeren. Het mooie van een kwantumcomputer is dat deze alle mogelijkheden tegelijkertijd naast elkaar kan uitvoeren. Een traditionele computer leest alleen een 0, of alleen een 1. Een kwantumcomputer leest tegelijkertijd de 1 en de 0.

4.8 Het maken van een kwantumsprong

Met een kwantumsprong in de toekomst van Alice, Bob en Eve, verplaatsen we hun communicatiemogelijkheden door de komst van de kwantumcomputer.

Alice verstuurt een vercijferd binair bericht naar Bob. De enen en nullen vervangt ze door fotonen met bepaalde polarisaties zie onderstaande schema's, die elk een polarisatiefilter voorstellen:

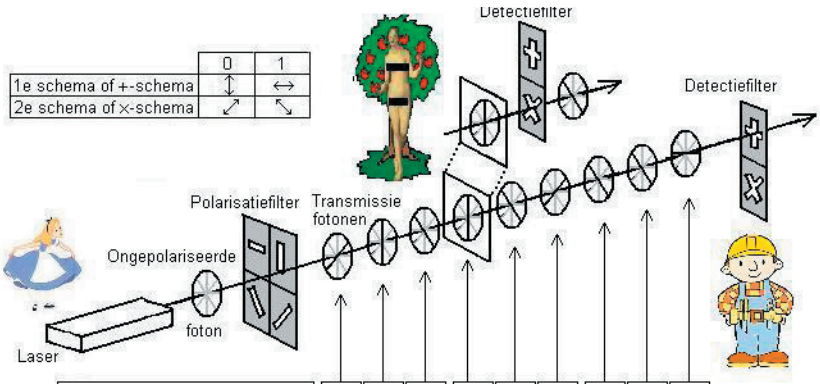
	0	1
1e schema of +-schema	↕	↔
2e schema of ×-schema	⤢	⤡

Alice wisselt, op een niet te voorspellen manier, tussen de twee schema's om dit binaire bericht te verzenden. Zo wordt het voor Eve moeilijk uit te maken hoe ze haar polaroidfilter moet instellen wanneer het foton eraan komt. Ze heeft dan wel weet van de schema's van Alice, maar weet niet wanneer welke worden gebruikt. Gemiddeld de helft van de tijd zal Eve haar filter goed hebben gehouden en de andere keren verkeerd. Een volledige kennis van deze transmissie van Alice kan Eve niet hebben. Bovendien zou ze ook geen gebruik kunnen maken van een dubbele polaroidfilter of een filter die alle polarisaties doorlaat. Een foton is niet deelbaar, dus er kan niet in twee fotonen gesplitst worden.

Waar misschien nog niet over nagedacht is, is het feit hoe Bob moet weten welk polarisatiefilter

[38] hij moet gebruiken. Bob zit nu in hetzelfde schuitje als Eve. Alice zou met Bob kunnen afspreken welk polarisatieschema ze voor welk foton zullen gebruiken. Terug bij af zijn we, als we bedenken hoe de sleuteldistributie gaat plaatsvinden. In een tijd van fotonengebruik is het RSA-cijfer al lang gekraakt door de kwantumcomputer.

Gilles Brassard (1955) en Charles Bennett (1943) helpen Alice en Bob uit de puree, en Eve erin. De allerveiligste vorm van de cryptografie ooit, zal de kwantumcryptografie zijn. Zal een honderd procent veilige sleuteldistributie dan toch zijn gevonden?



	0	1
1e schema of +-schema	↕	↔
2e schema of x-schema	⤢	⤡

Bitreeks van Alice	0	0	1	0	1	0	1	1	1
Filter van Alice	⤢	↕	⤡	↕	⤡	⤢	⤡	⤡	↔
Bobs detectiefilter	+	+	+	+	×	+	+	×	+
Metingen van Bob	1	0	1	0	1	0	0	1	1
Afgesproken bitreeks	–	0	–	0	1	–	–	1	1

Afbeelding 11. Kwantumcryptografie toegepast

(Scientific American, January 2005, pagina 66)

Om een sleutel af te spreken, zendt Alice een reeks nullen en enen (fotonen) met rechtlijnige of diagonale polarisatiefilters naar Bob. Bob kiest willekeurig een detectiefilter voor elke binnenkomende foton. Als hij de juiste heeft, weet hij ook de bitwaarde.

Echter wanneer Bob een verkeerde filter gebruikt, noteert hij met vijftig procent kans de juiste bitwaarde. In afbeelding 12 hieronder staan de verschillende mogelijkheden van de fotonuitwisseling tussen Alice en Bob.

Alices schema	Alices bit	Alice zendt	Bobs detector	Correcte detector?	Bob leest	Bobs bit	Is Bobs bit correct?
Recht-lijnig	1	↔	+	Ja	↔	1	Ja
			x	Nee	↘ ↗	1 0	Ja Nee
	0	↕	+	Ja	↕	0	Ja
			x	Nee	↘ ↗	1 0	Nee Ja
Diago-naal	1	↘	+	Nee	↔ ↕	1 0	Ja Nee
			x	Ja	↘	1	Ja
	0	↗	+	Nee	↔ ↕	1 0	Nee Ja
			x	Ja	↗	0	Nee

Afbeelding 12. Verschillende mogelijkheden van fotonuitwisselingen

(Code, Singh, S., pagina 414)

Als Bob alle fotonen heeft ontvangen, belt hij Alice op en vertelt haar welke filters hij heeft gebruikt in welke volgorde. Bob vertelt niets over de verkregen bitwaarde. Alice controleert de gebruikte detectiefilters van Bob en geeft aan welke correct zijn gekozen. Alice vertelt niet wat de uitslag zou zijn geweest, dus kan het gesprek zonder gevaar worden afgetapt. Alle onjuist gekozen detectiefilters verwijderen Alice en Bob uit de reeks nullen en enen. Er ontstaat nu een gemeenschappelijk cijfer die de sleutel zal vormen tussen Alice en Bob. Alice en Bob kunnen deze sleutel gebruiken bij een absoluut veilig encryptieproces als een eenmalig blokcijfer.

Eve heeft met deze nieuwe kwantumcryptografie geen schijn van kans om de sleutel te kunnen onderscheppen. Bij het verzenden van de reeks enen en nullen van Alice, zit Eve in precies dezelfde positie als Bob: ze weet niet welk detectiefilter te gebruiken en ‘doet maar wat’. Alice deelt Bob mee welke schema’s zij heeft gebruikt bij de verplaatsing van de fotonen. Daarbij spreken zij af alleen die fotonen te gebruiken, die werden gemeten bij Bob toen hij de juiste detectiefilter gebruikte. Eve schiet hier dus helemaal niets mee op. Zij kan slechts de helft hebben gemeten met een correcte detector en de helft met een verkeerde, waardoor ze goede bitwaarde uit de sleutel verwijderd.

Een extra faciliteit van de kwantumcryptografie is het ontdekken van spionnen. Alice en Bob merken direct de aanwezigheid van Eve, de spionne. Elke keer dat zij een foton meet, riskeert ze een verandering op de lijn Alice-Bob. Eve kan worden opgemerkt als Alice en Bob hun eenmalig blok testen. Als dit naar wens is, gebruiken ze het eenmalig blokcijfer om een bericht te vercijferen. Als deze test nu fouten opspoort weten ze dat de fotonen zijn afgetapt door Eve.

Namelijk, als Alice ↘ stuurt naar Bob. Eve meet dit met haar +-detector, die dwingt dan de binnenkomende foton als ↕ of als ↔ te voorschijn te komen. Nu meet Bob de getransformeerde foton, die geheel willekeurig een x-detectiefilter voorhoudt, Bob zou nu een ↘ kunnen meten, wat Alice

[40] heeft gezonden, of hij meet ⤢, wat een foutmeting zou zijn. Dit verstoort de communicatie tussen Alice en Bob. Alice heeft met een diagonaal polarisatiefilter de foton gestuurd en Bob heeft een juiste detectiefilter gebruikt, maar heeft het toch bij het verkeerde eind. Eve heeft de foton 'verdraaid' en dat heeft Bob gevoelig gemaakt voor fouten, ook al gebruikt hij de correcte detector.

Met kwantumcryptografie kunnen Alice en Bob absoluut veilig met elkaar digitaal communiceren. Zij worden direct gewaarschuwd als luistervink Eve haar neus in hun zaken steekt.

5 Conclusie

Hoe brengen de rollen van natuurwetenschappen en informatica in de cryptografie, ons naar de toekomst: de kwantumcryptografie?

De kwantumtheorie uit de natuurwetenschappen is de basis van de toekomst, dit blijkt uit deze literatuurstudie voor mijn onderzoek naar de kwantumcryptografie. Als een kwantumcryptografisch bericht ooit ontcijferd wordt, betekent dit dat de kwantumtheorie niet juist is. Dit zou heel ellendig zijn voor de fysici. Hun inzicht, in hoe de wereld op het allerelementairste niveau in elkaar zit, wordt dan verstoord. De ideeën over een kwantumrekenaar, de kwantumcomputer, die het huidige encryptiesysteem kan kraken, zijn dan ook labiel. De theorie van de kwantumcryptografie en kwantumcomputer zijn al uitgedacht, en er zijn al diverse experimenten om deze in praktijk te brengen.

Ook de rol van de informatica blijft een belangrijke rol spelen voor zowel de kwantumcryptografie als de kwantumcomputer. Met optische vezels en satellietsystemen is de wetenschap al heel ver om de benodigde fotonen voor het gebruik van de kwantumcryptografie te kunnen verplaatsen van het ene digitale instrument naar het andere.

Het is voor alsnog onbekend hoe überhaupt een kwantumcomputer eruit zal zien, wat deze wel en niet zal kunnen en wat uiteindelijk de interessantste toepassingen zullen zijn. Hoogleraar Hans Mooij van de onderzoeksgroep Kwantumtransport van de TU Delft denkt dat het nog minstens twintig jaar duurt voor dat de kwantumcomputer er is.

Tevens zit men nog altijd met het probleem als waar men ook mee zat toen de eerste computer werd gemaakt. De eigenschap van een (qu)bit. Een bit neemt een waarde 0 of 1 aan, een qubit neemt deze waarde na zijn meting aan. Beide krijgen een waarde, maar kunnen deze niet meer loslaten, eenmaal een 0 (of 1), altijd een 0 (of 1). Als de (qu)bit niet meer nodig is, kun je deze wel 'weggooien' en niet meer wijzigen in een nieuwe waarde. De pracht van een qubit is dan verdwenen dat het tegelijkertijd 0 of 1 kan zijn.

Roger Penrose (1931) heeft een studie gedaan naar een vergelijking tussen de relativiteitstheorie en de kwantumtheorie om over deze vergelijking duidelijkheid te krijgen hoe ver de wetenschap met de kwantumwereld en het praktische nut ervan is. Penrose poogt in zijn *twistortheorie*[11] om de relativiteitstheorie en de kwantumtheorie samen te brengen. De effecten van de fenomenen in de kwantumtheorie die Penrose op kosmologisch niveau onderzoekt, kan de kwantummechanica weer volledig laten wankelen.

Ook al zijn de grondbeginselen van de kwantumtheorie honderd jaar geleden door Albert Einstein gelegd, de 'vaagheid' als de theorie er nu nog over is, zo 'vaag' is men nog over een succesvolle toekomst er van.

Wat kan het bedrijfsleven met deze "toekomst" ondernemen?

De ontdekking van de kwantumcryptografie en de kwantumcomputer kent voor het bedrijfsleven twee kanten. Veel bedrijven, overheden, krijgsmachten en terroristnetwerken hebben hun data en informatie beveiligd met de alom bekende encryptiesystemen, die niet in korte tijd te kraken zijn,

[42] met de huidige computerkrachten. Met de komst van de kwantumcomputer is de beveiliging zo lek als een zeef. Echter met de komst van de kwantumcryptografie is de privacy van de baan. Overheden en krijgsmachten worden verzekerd van een veilige communicatie door de moderne technologieën. Het is de vraag of de regeringen ook het publiek (en dus ook bedrijven en diverse 'netwerken') toestaat gebruik te maken van deze veilige communicatie. Welke reglementen worden opgesteld om zichzelf hierbuiten te stellen, maar tegelijkertijd zich te beschermen tegen criminelen?

Tot dusver houdt het bedrijfsleven en de overheden zich nog bezig met de algoritmen die nu (nog) een hoogstandje zijn en zéér moeilijk te kraken zijn.

Bronnen

Literatuur

Beenakker, C. 2005. *De magie van quantumtechnologie.* NOW-Huygenslezing, Den Haag.

Bennet, C.H. e.a. 1992. *Quantum Cryptography.* Scientific American.

Bouwmeester, D. 2005. *Quantumgeheimschrift en quantumteleportatie.* NOW-Huygenslezing, Den Haag.

Delicado, e.a. 2005. *The quantum cryptograpy: Communication and computation.* Elsevier Ltd, Acta Astronautica.

El Aoufi, S. 1996. *Cryptografie en informatiebeveiliging.* Vrije Universiteit FEW, Amsterdam.

El Aoufi, S. 2001. *Cryptografie en ICT, theorie en praktijk.* Academic Service, Schoonhoven.

El Aoufi, S. 2004. *Veilig dataverkeer door versleuteling van lichtdeeltjes.* Informatiebeveiliging Jaarboek.

Geerts, G. e.a. 1999. *Van Dale. Groot woordenboek der Nederlandse taal.* Van Dale Lexicografie BV, Utrecht/ Antwerpen.

Mols, B. 2004. *Kwantumbits zijn twijfelaars.* Natuurwetenschap & Techniek, Utrecht.

Polkinghorne, J. 2002. *De kortste introductie: Quantumtheorie.* Het Spectrum BV, Utrecht.

Singh, S. 1999. *Code, de wedloop tussen makers en brekers van geheime codes en cijferschrift.* De Arbeiderspers, Amsterdam.

Stix, B.2005. *Best-kept Secrets.* Scientific American.

Valkhof, A. 2003. *PGP: Pretty Good Privacy.* Vrije Universiteit FEW, Amsterdam.

Vertogen, G.2000. *De herschepping van de natuurkunde.* Natuurwetenschap & Techniek, Utrecht.

Whee Ky Ma. 2005. *Grote getallen gesnoeid.* Natuurwetenschap & Techniek, Utrecht.

Internet

Computerwoordenboek. *http://computerwoorden.nl*

Cryptografie begrippenlijst. *http://proto.thinkquest.nl/ffiklb024/begrippen_listbox.php*

Kennislink. *http://www.kennislink.nl*

Tweakers. *http://www.tweakers.net*

Wat een wetenschap! *http://proto.thinkquest.nl/ffillc220/index.php*

Wikipedia. *http://www.wikipedia.nl*

Voetnoten

1 Uit: VPRO's zomerprogramma Zomergasten

2 Uit: *Code*, Simon Singh

3 Sessiesleutel: een symmetrische geheime sleutel die één keer wordt gebruikt voor berichtenuitwisseling en daarna wordt weggegooid.

4 Ook wel Euler-Totiënt-functie genoemd (zie *http://www.pandd.demon.nl/rsa.htm*) voor nadere uitleg)

5 De andere methode is stroomvercijfering, waarbij de klaretekst bit-voor-bit (of woord-voor-woord) in cijfertekst wordt omgezet. Deze methode wordt verder niet behandeld.

6 Of de theorie dat een voorwerp zich in vele universa tegelijk kan bevinden

7 Dit concept werd bekend onder de naam Copenhagen Interpretation.
Uit: http://users.skynet.be/fa041770/lichtdoos.htm

8 Uit: NRC Handelsblad, *Youp, Osama Bin Londen*, zaterdag 9 juli & zondag 10 juli 2005 (naar aanleiding van de aanslagen op 7 juli in de Londense metro).

9 Dit getal 9 zou kunnen worden gebruikt als de sleutel voor een DES-encryptie, die normaal natuurlijk gebruik maakt van veel grotere getallen.

10 Correctie: Het zijn Rivest, Shamir en Adleman die met de publieke-sleuteldistributie naar buiten komen. De heren James Ellis, Clifford Cocks en Malcolm Williamson van GCHQ zijn de eigenlijke 'ontdekkers' ervan.

11 Rond 1965 ontdekt Roger Penrose de twistortheorie.

Bijlage A - Onmisbare begrippenlijst

Belangrijke synoniemen

encryptie = vercijfering = codering = versluiering = versleuteling

decryptie = ontcijfering = decodering = ontsluiering = ontsleuteling

3des Triple Data Encryption Standard is een encryptiealgoritme dat gebruik maakt van DES, maar op zodanige wijze dat het veel moeilijker te kraken is. DES is kraakbaar omdat de sleutels wat kort zijn, namelijk 56 bits. Hierdoor is het aantal mogelijke sleutels zodanig klein dat het doorzoeken van alle mogelijke sleutels tegenwoordig praktisch haalbaar is (nog afhankelijk hoeveel geld men in de computers en rekentijd wilt pompen). Aangezien niet het DES algoritme, maar de gebruikte sleutellengte wel als kraakbaar geldt, heeft men 3DES kunnen ontwikkelen.

A

AES Advanced Encryption Standard. Een standaard om informatie te versleutelen. Het is een computer versleutelingstechniek. De sleutels zijn altijd 128-bit. De blokgrootten zijn beperkt tot 128, 192 of 256 bytes. In programma's zoals WinZip, PowerArchiver, wordt AES als encryptie aangeboden. AES is bedoeld als de opvolger van DES en zal gaandeweg ook 3DES gaan vervangen. DES voldoet niet meer en is te makkelijk te kraken voor de huidige snelle computers.

Algoritme Geordende, eindige verzameling nauwkeurig geformuleerde wiskundige regels voor de oplossing van een probleem. Het oplossen van een probleem door stap voor stap naar de oplossing toe te werken.

ASCII American Standard Code for Information Interchange, een standaard voor het omzetten van alfabetische en andere tekens in getallen.

Asymmetrisch cryptosysteem Een publieke-sleutelcryptografiesysteem, waarbij er een andere sleutel is voor de encryptie dan voor de decryptiede zogenaamde privé- en publieke sleutel. Het is praktisch onmogelijk, een van de sleutels uit de andere sleutel af te leiden.

Authenticiteit Het vaststellen van de identiteit van een zich als zodanig uitgevende persoon en het vaststellen van de herkomst van gegevens. Met behulp van cryptografie kunnen de identiteit en de echtheid van de bron worden verzekerd. Ten behoeve van authenticiteit wordt asymmetrische cryptosystemen gebruikt. Digitale handtekeningen kunnen worden gegenereerd en geverifieerd.

B

Bigram Zie Digraaf

Bit De kleinste binaire eenheid: 1 of 0. Een bit is één geheugencel van de personal computer. Het woord is een samenvoeging van BInairy digiT. Bij gegevensverwerking en -opslag is een bit de kleinste informatie-eenheid die een computer kan hanteren.
Acht bits vormt een byte. Een groep bits noemen we een binaire code.

Blinde handtekening Een vorm van digitale handtekening, waarbij de anonimiteit van een persoon wordt gewaarborgd.

Blokvercijfering Vercijfering waarbij een blok klaretekst in één keer wordt vercijferd. Geheimschrift wordt vercijferd en ontcijferd op basis van blokken, en werkt niet continue op de gegevensstroom.

Boodschap Een (te versturen) bericht bestaande uit een klaretekst: het ongecodeerde bericht, tekst die gewoon kan worden gelezen, die nog niet is versleuteld.

Byte Een combinatie van acht opeenvolgende bits; een groepje van acht 'enen' en 'nullen', die samen een letter, teken of code voorstellen. Het woord is een samentrekking van 'by eight'. Met één byte kunnen 256 verschillende combinaties van enen en nullen gemaakt worden, wat betekent dat er 256 tekens mogelijk zijn. In een byte past karakter (letter, cijfer of (lees-)teken).

C

Certification Authority (CA) Een vertrouwde instantie, in het Nederlandse een Vertrouwde Derde Partij (VDP) en in het Engels een Third Trust Party (TTP), die publieke sleutels certificeert, certificaten publiceert en certificaten intrekt. Indien gewenst kan een CA tevens sleutels aanmaken. Het afgeven, beheren en intrekken van gekwalificeerde certificaten door certificatiedienstverleners (certificatieautoriteiten), alsmede het verlenen van andere diensten die samenhangen met het gebruik van elektronische handtekeningen. Met de certificaten wordt het verband aangetoond tussen de digitale handtekening en de gebruiker. CA's kunnen daarnaast andere functies vervullen. Een Certificate Authority kan een externe onderneming zijn zoals VeriSign of BelSign of een interne organisatie van een onderneming.

Caesarverschuiving substitutiecijfer Oorspronkelijk een cijfer waarin elke letter in het bericht wordt vervangen door de letter drie plaatsen verder in het alfabet. Meer in het algemeen is het een cijfer waarin elke letter in het bericht wordt vervangen door de letters x plaatsen verder in het alfabet, waarbij x een vast getal is tussen 1 en 25.

Cijfer Een wiskundige formule waarmee een symbool (letter of getal) wordt bepaald ter vervanging van een klaretekst letter. Elk algemeen systeem om de betekenis van een bericht te verbergen door elke letter in het oorspronkelijke bericht te vervangen door een andere letter. Het systeem moet een ingebouwde flexibiliteit hebben, die bekendstaat als de sleutel.

Cijferalfabet De herschikking van het normale (of gewone) alfabet, die dan bepaalt hoe elke letter in het oorspronkelijke bericht wordt vercijferd. Het cijferalfabet kan ook bestaan uit getallen of willekeurige andere tekens, maar in alle gevallen dicteert het de vervangingen voor letters in het oorspronkelijke bericht.

Cijfertekst De uitvoer van een vercijferingsproces; het vercijferde bericht. De versleutelde boodschap of data wordt ciphertext of cijfertekst genoemd.

Code Een systeem om de betekenis van een bericht te verbergen door elk woord of zin in het oorspronkelijke bericht te vervangen door een ander teken of een groep tekens. De lijst van vervangingen staat in een codeboek.

Codeboek Een lijst van vervangingen voor woorden of zinsneden in het oorspronkelijke bericht.

Confusie Een cryptografische techniek die de relatie tussen de statistische gegevens van het vercijferde bericht en de waarde van de encryptiesleutel zo complex mogelijk probeert te maken. Dit wordt bereikt door een ingewikkeld coderingsalgoritme te gebruiken dat van de sleutel en van de invoer afhankelijk is.

Conventionele encryptie Zie Symmetrische encryptie.

Cross-certficering Kruiscertificering. Overeenkomst tussen CA's om elkaars certificaten te accepteren, nadat zij elkaars werkwijze en methoden hebben onderzocht en overeen gekomen zijn hetzelfde beveiligingsniveau te garanderen.

Cryptanalist Iemand die cryptoanalyses in praktijk brengt. De kunst en de wetenschap van het kraken van het vercijferde bericht (door de vermomming heen kijken).

Cryptoanalyse Deel van de cryptologie dat zich bezighoudt met het kraken van geheimschriften om informatie te herstellen, of versleutelde informatie die als authentiek zal worden geaccepteerd, te vervalsen. De cryptoanalist analyseert en decodeert decodeerde berichten zonder kennis van de gebruikte (de)codeersleutel en/of algoritme. Het ontsleutelingsproces heet decryptie. Tegenovergestelde is cryptografie.

Cryptografie Deel van de cryptologie dat zich bezighoudt met het systematisch versleutelen van gegevens of de betekenis van gegevens ten behoeve van beveiliging in een vorm die enkel door de geadresseerde kan worden gelezen. De Cryptografie bestaat uit het bedenken en schrijven van een geheimtaal of cryptosysteem. Het versleutelingsproces heet encryptie, ook wel afgekort tot crypto. De cryptograaf is de beoefenaar van de kunst en de wetenschap van de cryptgrafie. Tegenovergestelde is cryptoanalyse.

Cryptografisch algoritme Een wiskundige functie die gebruikt wordt voor encryptie of decryptie van berichten. Er zijn twee algemene typen van op een sleutel gebaseerde algoritmen: symmetrische algoritmen, ook wel conventionele algoritme genoemd; asymmetrische algoritmen, ook wel publieke sleutel algoritme genoemd.

Cryptologie Cryptologie is de wetenschap van het geheimschrijven in alle vormen en het kraken ervan, zowel geldig voor cryptografie als voor cryptoanalyse. De leer van het verbergen. Het woord is ontleend uit het Grieks: “cruptos“ = verborgen en “logos“ = leer. De cryptologist is de beoefenaar van de kunst en de wetenschap van het kraken van het vercijferde bericht.

Cryptosysteem Een systeem voor encryptie en decryptie. Dit is een combinatie van een algoritme en een sleutel.

Cryptware Software waarmee codering en/of decodering van gegevens mogelijk is. PGP is zo’n software.

D

Data recovery Het toegankelijk maken van versleutelde gegevens voor bevoegden die niet (meer) beschikken over de ontcijfersleutel.

Data Recovery Organisatiion (DRO) Een Data Recovery Organisation garandeert dat versleutelde gegevens toegankelijk blijven voor bevoegden, ook indien de ontcijfersleutel niet (meer) beschikbaar is.

Decryptie Ontcijfering of decodering. Het transformerende proces om de vercijferde boodschap, in de oorspronkelijke, begrijpelijke vorm terug te brengen. Dit gebeurt via een sleutel.

DES Data Encryption Standard. Een symmetrische algoritme, ontwikkeld in 1974 door IBM dat door het Amerikaanse Nationale Standaardisatie-instituut ANSI is gestandaardiseerd.
DES is een blokcodering, gebruikt als privé-sleutel. Dit algoritme versleutelt 64 bit blokken met behulp van een 56-bits sleutel. De sleutel bepaalt hoe de 64 bits onderling verwisseld en gewijzigd worden. 3DES is een verbeterde versie op DES. In 1997 is het systeem gekraakt in 96 dagen.

Differentiële cryptoanalyse Een techniek waarbij gekozen klaretekst wordt versleuteld met bepaalde XOR-differentiepatronen. De differentiepatronen van de resulterende vercijferde bericht leveren informatie op waarmee de encryptiesleutel kan worden bepaald.

Diffie-Hellman-Merkle-sleuteluitwisseling Een proces waarbij een verzender en een ontvanger een geheime sleutel kunnen vaststellen via een openbaar gesprek. Is eenmaal de sleutel afgesproken, dan kan de zender een cijfer zoals DES gebruiken om een bericht te vercijferen.

Diffusie Een cryptografische techniek die de statistische structuur van de klaretekst probeert te verbergen door de invloed van elke afzonderlijke klaretekst waarde over een groot aantal het vercijferde berichtwaarden te spreiden.

Digitale handtekening Een authenticiteitcode die berekend wordt met een persoonlijke privé-sleutel, deze wordt toegevoegd aan een elektronisch bericht als authenticiteitkenmerk. De digitale handtekening kan aan een (on)gecodeerd bericht worden toegevoegd. Tevens kan de ontvanger achterhalen of de data sinds de encryptie inhoudelijk is veranderd indien het bericht door een hash is gehaald of het bericht versleuteld is met de publieke sleutel van de ontvanger.

Digram Een tekenreeks van twee letters. In vele talen kan de relatieve frequentie van verschillende digrammen in de klaretekst worden gebruikt bij de cryptoanalyse van sommige encrypties.

DSA Digital Signature Algorithm, een public-key algoritme, niet gebruikt voor encryptie, maar voor digitale handtekeningen.

DSS Digital Signature Standard is ontwikkeld in 1991 en is in de VS ontwikkeld om een elektronische authenticiteit mogelijk te maken.

E

Ecash Elektronisch geld, dit is de binaire representatie van het traditionele geld. Met een elektronische munt kunnen betalingen worden verricht via internet.

E-commerce Omvat alle zakelijke handelingen die op elektronische wijze worden uitgevoerd ter verbetering van de efficiency en effectiviteit van markt– en bedrijfsprocessen. Gebruikmakend van de mogelijkheden van Internet kunnen zowel zakelijke als particuliere gebruikers producten en diensten bekijken, bestuderen, vergelijken met andere leveranciers en direct bestellen of afnemen (downloaden) als het om elektronische producten of diensten gaat (bijvoorbeeld informatie en steeds vaker muziek en videobeelden).

Eenmalig blokcijfer De enige vorm van encryptie die onbreekbaar is. Het steunt op een willekeurige sleutel die even lang is als het bericht. Elke sleutel kan eenmaal en niet meer dan eenmaal worden gebruikt.

Eenrichtingsfunctie Een eenrichtingsfunctie, of éénwegfunctie, f is een (encryptie) functie die zelf gemakkelijk uit te rekenen is, maar waarvoor het bepalen van de inverse functie f^{-1}, dus de decryptie functie, aanzienlijk moeilijker is.

Eénwegfunctie Zie eenrichtingsfunctie.

Electronic Data Interchange (EDI) Gestructureerd elektronisch berichtenverkeer tussen computers van verscheidene organisaties; dit is een eerste stap naar het papierloze kantoor.

Encoderen Coderen van gegevens voor datacompressie of foutdetectie.

Encryptie Het versleutelen/vercijferen van berichten, oftewel het omzetten van data in de een of andere onleesbare vorm om de vertrouwelijkheid te waarborgen. In geval van asymmetrische encryptie wordt gebruik gemaakt van een sleutelpaar. De ene sleutel wordt bekend gemaakt (publieke sleutel) en de andere wordt strikt geheim gehouden (privé sleutel). In geval van symmetrische encryptie wordt een sleutel gebruikt die bij beide partijen bekend is.

Encyrptiesleutel Zie Master key

End-to-end encryptie Een vorm van encryptie in netwerken waarbij de boodschap vercijferd wordt en de header in klaretekst wordt meegezonden. De boodschap wordt bij de bestemming ontcijferd.

Enigma In de Tweede Wereldoorlog in Duitsland ontwikkelde vercijferingsmachine, waarmee vrij complexe vercijferingen snel en automatisch konden worden uitgevoerd. Het zijn zogenaamde rotorsystemen.

F

Factorisatie Ontbinden van een geheel getal N in priemgetallen.

Frequentieanalyse Het onderzoek naar hoe vaak elke letter van een alfabet in een bepaalde taal voorkomt.

G

Gegevensdecryptie Het omzetten van geheimschrift in leesbare tekst.

Gegevensencryptie Het omzetten van een leesbare tekst in geheimschrift.

Gegevensintegriteit Gegevens zijn integer wanneer deze tijdens de overdracht op geen enkele wijze zijn aangetast, vernietigd of gewijzigd. Het SSL-protocol zorgt ervoor dat de vertrouwelijkheid en integriteit van gegevens behouden blijft tijdens de communicatie tussen cliënten en servers op het web.

Geheime sleutel Een privé- of geheime sleutel voor de codering en/of decodering van een bericht, die enkel gekend is door de partij of partijen die geheime boodschappen uitwisselen. Het gevaar bij dit systeem is dat, indien een van beide partijen de sleutel verliest of als die gestolen wordt, het systeem niet meer werkt.

Golftheorie De golftheorie blijkt niet alleen op watergolven toepasbaar, maar ook op geluid en licht. Thomas Young (1773-1829) heeft bewezen dat als je een bundel licht op een heel smalle opening plaatst, er buiging van licht plaatsvindt. Maar dit is niet alles: er bleken ook versterking en uitdoving plaats te vinden, wanneer je twee afgebogen lichtgolven tot halve cirkels elkaar laten passeren. De lichtstralen tonen dus net als bij watergolven buiging, versterking en uitdoving.

H

Hash functie Een hash functie comprimeert een grote hoeveelheid data tot een afgesproken hoeveelheid. Een hash functie H is een speciale éénrichtingsfunctie die een invoer M van variabele lengte omrekent naar een string van een vaste lengte, de hash waarde h (h = H(M)). Het is rekenkundig zeer moeilijk een andere invoer te bepalen die hetzelfde hash resultaat oplevert.

Hash waarde Het resultaat van een hash functie berekend over een bericht. De hash waarde is het resultaat van het omzetten (met een wiskundig algoritme, hash functie genaamd) van een bericht van willekeurige grootte in een reeks met een vaste, meestal korte, lengte. Als het bericht verandert, wijzigt tevens de hash waarde. Uit de hash waarde kan het bericht niet worden berekend. De hash waarde heet ook wel hash of message digest.

Homofoon Eén van de verschillende klaretekst letters die als substitutie worden gebruikt voor een bepaalde klaretekst letter.

I

Informatiebeveiliging Het treffen van een optimaal samenhangend pakket van maatregelen op procesmatig, organisatorisch en technische gebied, dat er op gericht is de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, en hierdoor de continuïteit van de bedrijfsvoering, te waarborgen.

Integriteit De eigenschap dat gegevens niet zijn gewijzigd, toegevoegd of verwijderd, zekerheid over de ongeschondenheid van gegevens. Cryptografie kan uitstekend worden gebruikt om de integriteit te waarborgen. In de praktijk wordt hiervoor hash functies gebruikt. Door hashing toe te passen kunnen wijzigingen in documenten worden gedetecteerd.

Interceptie De informatie wordt onderschept door een derde; dit is een aanval op de vertrouwelijkheid.

Interfentiepatroon Wanneer twee steentjes vlak bij elkaar in het water worden gegooid, ontstaan twee watergolven, deze watergolven komen elkaar op bepaalde punten tegen. Op bepaalde plaatsen versterken golven elkaar en op andere plaatsen doven ze elkaar uit.

K

Ketenvercijfering Elke gecodeerde letter heeft invloed op de codering van de volgende letter.

Klaretekst De oorspronkelijke, begrijpelijke tekst, zoals die was voor de vercijfering en zoals die onthuld wordt door een succesvolle ontcijfering of cryptoanalyse. In het Engels vaak aangeduid met de letter "M" van message.

Klassieke natuurkunde Deze is ontwikkeld door Isaac Newton. Diverse natuurkundige verschijnselen kunnen tot op oneindige precisie worden benaderd, zoals licht een golf is, materie uit deeltjes bestaat en energie iedere gewenste waarde kan aannemen. Met de komst van de kwantumtheorie valt de theorie van de klassieke natuurkunde in duigen.

Kwantumcomputer Een immens krachtige computer die gebruik maakt van de kwantumtheorie.

Kwantumcryptografie Een onbreekbare vorm van cryptografie die gebruik maakt van de kwantumtheorie. Vooral de onzekerheidsrelatie die zegt dat het onmogelijk is alle aspecten van een voorwerp te meten met absolute zekerheid. De kwantumcryptografie garandeert de veilige uitwisseling van een willekeurige reeks bits, die dan wordt gebruikt als de basis voor een eenmalig blokcijfer.

Kwantummechanica Wetenschap die zich bezighoudt met het gedrag van deeltjes op atomaire schaal, waar de klassieke mechanica van Newton niet geldig is: een belangrijk aspect van de kwantummechanica is het onzekerheidsbeginsel.

Kwantumtheorie Theorie die door Max Planck (1858-1947) in 1900 opgesteld werd ten behoeve van een verklaring van de stralingsverschijnselen en de grondslag heeft gevormd voor de gehele moderne natuurkunde: kenmerkend voor de kwantumtheorie is dat energie zich slechts in bepaalde porties kan worden uitgezonden of geabsorbeerd.

De kwantumtheorie zegt kortweg dat energie wordt uitgestraald in kleine pakketjes, ook wel kwanta genoemd. Energie die uitgestraald wordt bestaat in veel verschillende vormen, zoals röntgenstraling, infrarood licht en ultraviolet licht, maar natuurlijk ook het gewone zichtbare licht. Het verschil tussen de verschillende soorten licht is het verschil in golflengte. Volgens Planck bevat elke golflengte zijn eigen hoeveelheid energie per kwantum. Deze kwanta worden ook wel fotonen genoemd.

L

Link encryptie Een vorm van encryptie in netwerken waarbij zowel de boodschap als de header worden vercijferd. Dit heeft als gevolg dat bij elk netwerkknooppunt de boodschap ontcijferd moet worden, zodat de header gelezen kan worden en bepaald kan worden wat het volgende netwerkknooppunt is waarnaar de informatie gezonden moet worden.

Luistervinken Ook wel tegenstanders, aanvallers, interceptors, opponenten, vijanden. Luistervinken hebben volledig toegang tot de communicatie tussen zender en ontvanger.

M

Master key Ook wel encyrptiesleutel. Een sleutel die lang meegaat en wordt gebruikt tussen een sleuteldistributiecentrum en een principaal om de overdracht van sessie sleutels te coderen. Meestal worden de master keys gedistribueerd met non-cryptografische middelen.

Meervoudige encryptie Herhaald gebruik van een encryptiefunctie met verschillende sleutels, om een ingewikkelder omzetting van klaretekst naar het vercijferde bericht te verkrijgen.

Microfotografie Het door middel van een fotografisch procédé zodanig verkleinen van berichten, dat deze voor het blote oog niet leesbaar zijn.

Monoalfabetische substitutie Elke van de karakters in de klaretekst wordt vervangen door een corresponderend karakter of het vercijferde bericht. Een cryptogram in de krant is een simpele substitutie code.

N

NSA National Security Agency (NSA) Een onderdeel van het Amerikaanse ministerie van Defensie, verantwoordelijk voor het verzekeren van de veiligheid van Amerikaanse communicatie en voor het inbreken in de communicatie van andere landen. De Amerikaanse overheid heeft in 1952 de National Security Agency (NSA) opgericht, wat op dit moment nog steeds de belangrijkste afluister- en (de)codeeerdienst ter wereld is.

Nulls Ingevoegde letters, tekens, cijfers of symbolen die geen betekenis hebben, om de onderschepper te misleiden.

O

One-time-pad Het Engelse woord ‘pad’ staat voor een strook papier, de sleutel op het papier bestaat uit willekeurig gekozen letters of cijfers in een willekeurige volgorde, die gebruikt worden om de boodschap teken voor teken te wijzigen. Zender en ontvanger moeten dus allebei deze sleutel hebben. Elke letter uit het pad wordt maar een keer gebruikt. Elke letter van het pad wijzigt precies een letter in de boodschap. Een *a* in het pad betekent dat de bijbehorende letter in de boodschap gewijzigd moet worden in de volgende letter in alfabetische volgorde, een *b* betekend dat de bijbehorende letter gewijzigd moet worden in de letter daaropvolgend in het alfabet, enzovoort. Omdat de letters in het pad willekeurig zijn, is elk schema bruikbaar.

Ontcijferen Het terugbrengen van een vercijferd bericht tot het oorspronkelijke bericht. Formeel verwijst de term alleen naar de beoogde ontvanger die de vereiste sleutel kent om de klaretekst terug te halen, maar informeel benoemt hij ook het proces van de cryptoanalyse, waarin de ontcijfering wordt gedaan door een vijandelijke onderschepper.

Onzekerheidsrelatie De onzekerheidsrelatie zegt dat het onmogelijk is alle aspecten van een voorwerp te meten met absolute zekerheid.

P

Paard van Troje Een, meestal kwaadwillend, programma dat zich hecht aan een ander programma en zo ongemerkt een computersysteem binnendringt.

PGP Pretty Good Privacy, een programma dat gebruikmaakt van cryptografie om bestanden en email te beveiligen tegen kwaadwillende personen of bedrijven. Pretty Good Privacy is ontwikkeld door Phil Zimmermann (1954) en gebaseerd op RSA.

PKI Public Key Infrastructure biedt gebruikers van een in wezen niet-beveiligd publiek netwerk, zoals Internet, beveiliging voor bijvoorbeeld het veilig privé-gegevens en geld uitwisselen.

Plaintext De te versturen boodschap of data wordt algemeen de plaintext of klaretekst genoemd. Plaintext wordt veelal genoteerd met M = message of met P = plaintext.

Het ongecodeerde bericht is de belangrijke boodschap die niet in verkeerde handen mag komen. Of niet-gecodeerde tekst. Tekst die gewoon kan worden gelezen, die niet is versleuteld (encrypt).

Polyalfabetisch substitutiecijfer Een substitutiecijfer waarin het cijferalfabet verandert tijdens de encryptie, bijvoorbeeld het Vigenère-cijfer. De verandering wordt bepaald door een sleutel. Twee of meer codealfabetten zijn in gebruik om de klaretekst te vervangen door andere letters, cijfers of symbolen. Moderne machines produceren miljoenen codealfabetten.

Polyalfabetische vervanging Methode waarbij voor elk deel van een bericht, of zelfs voor elke letter, een ander cijferalfabet gebruikt wordt om de geheimschriftletters uit te halen. Uitgevonden door Leon Battista in 1568.

Priemgetal Een getal dat alleen deelbaar is door zichzelf en door één.

Principalen De partijen in een transporttransactie.

Principia Voluit Newtons *Philosophiae Naturalis Principia Mathematica* (Wiskundige beginselen van de natuurfilosofie). In dit werk introduceert Newton de basiswetten voor de mechanica, de drie wetten van Newton.

Privé-sleutel Ook wel private sleutel. Eén van de twee sleutels die bij een asymmetrisch encrytiesysteem worden gebruikt, de ander is de publieke of openbare sleutel. Hiermee kan ook een digitale handtekening gemaakt worden. Ook kan de sleutel gebruikt worden om versleutelde berichten leesbaar te maken. Voor veilige communicatie mag de privé-sleutel alleen bij zijn gebruiker bekend zijn. Bij sommige vormen van encryptie, zoals RSA, zijn twee sleutels nodig voor de encryptie van data: een privé-sleutel en een publieke sleutel.

Protocol Een stelsel van voorschriften voor uitwisseling van informatie zodanig dat elke partij zo goed mogelijk is beschermd tegen bedrog door de tegenpartij of indringer.

Pseudorandom getalgenerator Een functie die een reeks getallen produceert die vrijwel willekeurig lijken.

Public Distribution System Publieke sleutel distributie. Twee partijen spreken een gemeenschappelijke sleutel af, zonder elkaar te ontmoeten en zonder de sleutel over het (onveilige) publieke elektronische kanaal te verzenden. In 1977 werd dit geïntroduceerd door Whitfield Diffie (1944) en Martin Hellman (1945).

Publieke sleutel Openbare sleutel van de eigenaar voor de codering van data bij encryptie. Bij sommige vormen van encryptie, zoals RSA, zijn twee sleutels nodig voor de encryptie van data: een privé-sleutel en een publieke sleutel. Bij het versleutelen van een bericht gebruikt de afzender de openbare sleutel van de ontvanger. Hierdoor kan alleen de ontvanger het bericht ontcijferen met behulp van de bijpassende geheime sleutel.
Of omgekeerd een bericht versleutelen met de publieke sleutel; dit is voor het eerst beschreven door Whitfield Diffie (1944) en Martin Hellman (1945) in 1976. De eerste geslaagde toepassing is: RSA.

Publieke sleutel systeem Een openbaar-sleutelsysteem, de vercijfersleutel is in principe openbaar; dat wil zeggen iedereen kan ervan kennis nemen en het gebruiken voor de vercijfering. Iedereen kan een boodschap vercijferen, maar niet ontcijferen; het wordt ondoenlijk gemaakt om de verkregen cijfertekst te ontcijferen. Steeds is er sprake van twee sleutels: één voor het vercijferen en één voor het ontcijferen. Bij dit asymmetrische cryptosysteem wordt één sleutel openbaar bekend gemaakt en de tweede geheim gehouden. Een voorbeeld van Publieke sleutel systemen is de RSA-beveiliging.

Publieke sleutel encryptie Zie asymmetrische encryptie.

Publieke sleutel infrastructuur De infrastructuur waarbij gebruik wordt gemaakt van publieke sleutel cryptografie en waar middels de uitgifte van certificaten veilige communicatie tussen de gebruikers van die certificaten kan worden gewaarborgd.

Publieke sleutelcryptografie Een cryptografisch systeem dat de problemen van de sleuteldistributie overwint. Publieke sleutelcryptografie is asymmetrisch, zodat elke gebruiker een publieke encryptiesleutel en een geheime decryptiesleutel moet vormen.

R

Red and Purple In de Tweede Wereldoorlog in Japan ontwikkelde vercijferingsmachine, waarmee vrij complexe vercijferingen snel en automatisch konden worden uitgevoerd. Purple was de Japanse diplomatieke code. Het zijn zogenaamde rotorsystemen.

Registrerende autoriteit Een vertrouwde instantie die identificatiegegevens van de gebruikers registreert en controleert en deze vervolgens doet toekomen aan de Certification Authority.

Repudiation Een manier van bedrog waarbij een partij ontkent dat hij een bericht gestuurd (of ontvangen) heeft.

Rotorsystemen Machines die een rotor gebruiken bij de versleuteling. Een rotor is een schijf in isolerend materiaal, waar aan beide zijden elektrische contactpunten zitten, één voor elk symbool van het gebruikte alfabet. Elk contactpunt aan de ene kant is binnendoor verbonden met een contactpunt aan de andere kant. De machine had drie of vier rotoren, waarvan de posities bij elk gecodeerde letter wijzigden. De beginpositie van de wielen vormden de sleutel. Het zijn machines die het proces van encryptie automatiseren. De meest bekende rotormachine was de Enigma, met drie rotors gekozen uit een set van vijf.

RSA RSA, genoemd naar zijn uitvinders R.L. Rivest (1947), A. Shamir (1952) en L.M. Adleman (1945). Een populair asymmetrisch systeem uit 1977 voor het aanmaken van paren openbare en geheime sleutels, het gebruikt twee grote priemgetallen om sleutels te generen.
De methodiek kan ook gebruikt worden voor digitale handtekeningen. De lengte van de sleutel in bits bepaalt hoe moeilijk het is om de versleuteling te kraken. RSA is het eerste systeem dat voldeed aan de eisen van de publieke-sleutelcryptografie. De RSA-algoritme is de meest gebruikte algoritme voor codering en validering, en wordt meegeleverd met de browsers Netscape en Microsoft.

S

S/MIME S/MIME (Secure Multi-Purpose Internet Mail Extensions), dat gebruik maakt van het RSA-coderingssysteem, is een veilige methode om emails te versturen. S/MIME is reeds te vinden in de recentste versies van de browsers van Microsoft en Netscape en wordt ook ondersteund door andere verkopers die producten maken waarmee boodschappen kunnen worden verstuurd.

Secure Electronic Transactions (SET) Een protocol dat is ontwikkeld door o.a. Microsoft, IBM en creditcardbedrijven MasterCard Transactions, Visa en American Express voor veilige transacties over internet.

Secure server ID SSL server certificaten waarmee eigenaren van websites zich identificeren en waarmee zij een veilige verbinding opbouwen met hun bezoekers.

Secure Sockets Layer (SSL) Een protocol dat is ontwikkeld door Netscape om berichten veilig over internet te verzenden. SSL biedt beveiliging voor de informatie, met name betalingsverkeer via Internet, die uitgewisseld wordt tussen webbrowsers en webservers. W3-Consortium wil dit protocol combineren met SHTTP.

Sessiesleutel Een symmetrische sleutel die één keer wordt gebruikt voor berichten uitwisseling. Na afloop van die sessie wordt de sleutel weggegooid.

Sigaba In de Tweede Wereldoorlog in USA ontwikkelde vercijferingsmachine, waarmee vrij complexe vercijferingen snel en automatisch konden worden uitgevoerd. Het is een zogenaamd rotorsysteem.

Signatuurmethode Bij dit publieke sleutel-cryptosysteem wordt de privé-sleutel een signatuursleutel, terwijl met de openbare sleutel iedere willekeurige persoon de signatuur op echtheid kan controleren.

Sleutel Een sleutel kan de unieke code zijn die aan een algoritme is te koppelen om versleutelde gegevens te ontcijferen. Deze combinatie vercijfert tekst met behulp van een complexe wiskundige vertaling. In het algemeen gesproken kan de vijand zich bewust zijn van het feit dat de encryptiealgoritme wordt gebruikt door de verzender en de ontvanger, maar de vijand mag de sleutel niet kennen.

Sleutelbeheer Het geheel aan procedures bedoeld voor het genereren, opslaan uitwisselen, archiveren en wissen van sleutels.

Sleutelbewaring Een opzet waarin gebruikers kopieën van hun geheime sleutels in bewaring geven bij een vertrouwde derde partij, de bewaringsagent, die de sleutels alleen zal doorgeven aan wetshandhavers onder bepaalde omstandigheden, bijvoorbeeld in geval van een gerechtelijk bevel.

Sleuteldistributie Het proces dat verzekert dat zowel de verzender als de ontvanger toegang heeft tot de voor het vercijferen en ontcijferen van een bericht vereiste sleutel, en tegelijk verzekert dat de sleutel niet in vijandelijke handen valt. De sleuteldistributie was vóór de uitvinding van de publieke-sleutelcryptografie qua logistiek en veiligheid een groot probleem.

Sleutellengte Computerencryptie vraagt sleutels die getallen zijn. De sleutellengte verwijst naar het aantal cijfers of bits in de sleutel, en geeft zo het grootste getal aan dat als sleutel kan worden gebruikt, waardoor het aantal mogelijke sleutels wordt bepaald. Hoe langer de sleutellengte (of hoe groter het aantal mogelijke sleutels), hoe meer tijd het een cryptoanalist zal kosten om alle sleutels te toetsen.

Sleutelmanagement Houdt zich bezig met het beheren van sleutels vanaf hun ontstaan tot aan hun uiteindelijke vernietiging. Het omvat: generatie, distributie, opslag en uiteindelijk vernietiging van de sleutels.

Sleutelwoord Sleutelwoord of sleutelzin is een woord of zin dat of die bekend is aan zowel de zender als de ontvanger en dat aangeeft hoe het geheimschrift opgelost moet worden.

Smartcard Een chipkaart met een microprocessor en geheugen. Een plastic kaart met een slimme chip, ook wel chipkaart genoemd. Deze bevat een processor, geheugen en een programma die onder andere gebruikt wordt voor machtiging. Er zijn twee uitvoeringen: met contacten en contactloos (radio). Een recente oplossing voor alle problemen, nu en in de toekomst. Worden gebuikt voor bijvoorbeeld toegangscontrole, beveiliging en elektronisch betalen in ondermeer gezondheidzorg, bij openbare diensten en transportsector.

Social engineering In Internettermen betekent het geheime technieken waarmee crackers niet-openbare informatie verzamelen, zoals namen en toegangscodes voor computers en netwerken. Een begrip dat in de sociale wetenschappen diverse betekenissen heeft, maar in internetverband een geheel andere betekenis kent.

Steganografie De wetenschap van het verbergen van het bestaan van een bericht, in tegenstelling tot de cryptografie, de wetenschap van het verbergen van de betekenis van een bericht. Encryptie behelst methoden om een klaretekst door talloze transformaties terug te geven in een voor outsiders onbegrijpelijke vorm, terwijl steganografie het bestaan van het bericht letterlijk verbergt. De methode van steganografie houdt het bestaan van een boodschap geheim, onzichtbare inkt, micropunten en het verstoppen van boodschappen in teksten.

Sterk algoritme Nu of in de nabije toekomst niet met computers te kraken code. De data is te complex, het bewerkingsproces is te complex of de opslag eisen zijn te groot. Veilig omdat het kraken van de code duurder is dan de waarde van de vercijferde informatie of omdat het kraken van de code langer duurt dan dat de periode waarin de informatie nog bruikbaar is.

Strippen Het verwijderen van een vercijfering uit een bericht dat tweemaal vercijferd is om voor een dubbele beveiliging te zorgen.

Stroomvercijfering Een symmetrisch encryptiealgoritme waarin bit-voor-bit of byte-voor-byte het vercijferde berichtuitvoer uit een stroom klaretekst invoer wordt geproduceerd.

Substitutie De letters van de klaretekst worden vervangen door andere letters, nummers of symbolen. Letters behouden hun positie, maar verliezen hun identiteit. Substitutie kan worden gecombineerd met transpositie. Substitutiesystemen zijn meer divers en belangrijker dan transpositiesystemen.

Substitutiecijfer Een encryptiesysteem waarin elke letter van een bericht wordt vervangen door een ander teken, maar haar plaats binnen het bericht behoudt.

Substitutiegeheimschrift Dit geheimschrift laten de volgorde van de symbolen in de klaretekst onveranderd, maar vermommen ze. Elke letter of groep letters worden vervangen door een andere letter of groep letters. Het oudst bekende geheimschrift is de Caesarmethode, toegeschreven aan Julius Caesar (monoalfabetische substitutie of simpel substitutiecode)

Substitutiesystemen Substitutietechnieken houden in dat klaretekst letters worden vervangen door het vercijferde berichtletters of andere symbolen. Deze vervanging verloopt dan volgens een bepaald vervangingsschema.

Substitutievercijferingen Substitutietechnieken houden in dat klaretekst letters worden vervangen door het vercijferde berichtletters of andere symbolen. Deze vervanging verloopt dan volgens een bepaald vervangingsschema.

Symmetrisch algoritme Kan worden verdeeld in twee categorieën: stroomvercijfering en blokvercijfering.

Symmetrisch cryptosysteem Een cryptosysteem, waarbij de sleutels voor cryptosysteem encryptie en decryptie gelijk zijn. Er is hier sprake van één (geheime) sleutel, welke zowel voor vercijferen als ontcijferen worden gebruikt. Het grote nadeel hiervan is dus dat de sleutel van de zender aan de ontvanger moet worden doorgegeven. Hierbij kan onderschepping van de communicatie voorkomen, waardoor de beveiliging steeds minder gebruikt wordt. Voorbeelden zijn o.a. DES en IDEA.

Symmetrische encryptie Een vorm van een cryptosysteem waarin encryptie en decryptie worden uitgevoerd met dezelfde sleutel.

Symmetrische-sleutelcryptografie Een vorm van cryptografie waarin de voor de vercijfering vereiste sleutel dezelfde is als de voor ontcijfering vereiste sleutel. De term beschrijft alle traditionele vormen van encryptie, dat wil zegen die voor de jaren zeventig in gebruik waren.

T

Traffic-analyse Het in de gaten houden door een derde partij wanneer en tussen welke gebruikers informatie-uitwisseling plaatsvindt.

Transpositie De letters van de klaretekst worden gemixt. De posities worden niet gehandhaafd, maar behouden hun identiteit. Transpositie kan worden gecombineerd met substitutie. De letters van de klaretekst worden van plaats gewisseld, en behouden hun identiteit. GEHEIM wordt HEEGIM. Transpositie en substitutie kunnen gecombineerd worden gebruikt. Voorbeeld: “secret“ wordt “ETCRSE” = transpositie

Transpositiecijfer Een encryptiesysteem waarin elke letter van een bericht verandert van positie binnen het bericht, maar haar identiteit behoudt.

Transpositiegeheimschrift Plaatst de letters in een andere volgorde, maar verandert de klaretekst niet. In een eenvoudige transpositie code wordt de klaretekst horizontaal op een papier geschreven.
Frequentieanalyse is voldoende om deze vorm te ontcijferen, omdat de gebruikte letters dezelfde zijn als de oorspronkelijke tekst.

Trusted Third-Party (TTP) Een onafhankelijke en deskundige derde partij in een overeenkomst, die diensten aanbiedt aan partijen die gebruik maken van het elektronische dataverkeer. Een TTP verschaft technisch en juridisch betrouwbare methoden om een elektronische transactie mogelijk te maken en uit te voeren, daaromtrent bewijs te leveren en geschillen te beslechten.

U

Uitputtend sleutelonderzoek Het toepassen van alle mogelijke sleutels op een cijfertekst totdat de juiste is gevonden. Niet heel erg intelligente aanpak, het is gewoon domweg proberen.

V

Vigenère-cijfer Een polyalfabetisch cijfer dat omstreeks 1500 werd ontwikkeld. Het Vigenère-vierkant bevat 26 aparte cijferalfabetten, elk waarvan een alfabet met Caesarverschuiving, en een sleutelwoord bepaalt welk cijferalfabet moet worden gebruikt om elke letter van een bericht te vercijferen.

Bijlage B - Onmisbare introductie

Tijdbalk, slechts ten ingeleide tot de ...

Kwantumcryptografie	Kwantumtheorie	Kwantumcomputer
±500 v.Chr. Ontstaan van *steganografie*, geheime communicatie die wordt bereikt door het verbergen van het bestaan van een boodschap. Herodotus vertelt in *Historiën* de kunst van het geheimschrijven die voorkwam dat Griekenland werd veroverd door de Perzen door de boodschap op het kaalgeschoren hoofd van de boodschapper te schrijven, en hem te laten gaan tot zijn haar weer was aangegroeid.		**±500 v.Chr.** In China en Japan wordt het abacustelraam ontwikkeld, de eerste mechanische 'telmachine' ter wereld.
De allereerste cryptografische militaire methode is de Spartaanse *skutalé*, een staf met een afgesproken diameter, waaromheen een boodschap wordt gewikkeld. Als de ontvanger deze boodschap om net zo'n staf met gelijke diameter wikkelt, kan hij het bericht lezen.		

[66]

±70v.Chr. Gebruik van het Ceasar-schrift, een vorm van vervangingsschrift, gebruikt voor militaire doeleinden o.a. in *De Gallische Oorlog* van Julius Ceasar, gebaseerd op een cijferalfabet dat t.o.v. het klare alfabet een bepaald aantal plaatsen opschuift. Het is echter te kraken in maximaal 26 pogingen en dus niet erg veilig.

va300 In de *Kamasutra*, een door de Brahmaanse geleerde Vatsyayana, staat een beschrijving van codering door substitutie. Ook wel vervangingschrift, omdat elke letter in het oorspronkelijke bericht, vóór de encryptie, wordt vervangen door een andere letter.

750 Gouden eeuw der islamitische beschaving, de welgestelde samenleving en de veilige communicatie werd bereikt door het gebruik van het *monoalfabetische substitutiecijfer*, de algemene naam voor elk substitutiecijfer waarin het cijferalfabet kan bestaan uit zowel symbolen als letters.
Arabische geleerden 'vonden' de cryptoanalyse uit, de wetenschap van het ontsleutelen van een bericht zonder een sleutel te kennen. Theologen bestuderen de openbaringen van Mohammed m.b.v. frequentieanalyse.

800-1200 Terwijl Europa nog in de Middeleeuwen zit, beschreef de Arabische geleerde al-Kindi de uitvinding van de cryptoanalyse.

Tot 1000 De kunst van het geheimschrijven wordt gedomineerd door het substitutiecijfer. Agust Kerckhoffs van Nieuwenhof schrijft in zijn boek *La Cryptographie Militaire* dat de veiligheid van de cryptoalgoritme slechts afhangt van het geheimhouden van de sleutel.

±1250 Het eerste bekende Europese boek *Episolae de secretis operibus artis er naturea* (ofwel Epistel over de geheime kunstwerken en de nietigheid van de toverij) wordt door de Engelse franciscaan Roger Bacon. Dit boek bevat zeven methoden voor het geheimhouden van boodschappen.

1400-1500 Europese cryptografie groeit razendsnel. De Renaissance maakt ruimte voor cryptografie en geheime communicatie.

±1435 Leon Battista Alberti 'vindt' het polyalfabetische cijfer, het laten switchen van meerdere cijferalfabetten tijdens het vercijferen, en tevens de cijferschijf uit.

[68]

±1500 Blaise de Viginère 'ontwerpt' het Viginère-cijferschrift, waarin 26 onderscheidenden alfabetten wordt gebruikt om een bericht te ontcijferen. Tevens is het onaantastbaar voor de frequentieanalyse.

1506 De eerste grote Europese cryptoanalist Giovanni Soro wordt aangesteld als codesecretaris in Venetië.

1568 Maria Stuart, koningin der Schotten, die terecht stond wegens verraad tegen het leven van koningin Elizabeth, maakt gebruik van een *nomenclator*. Dit is een versleutelingssysteem dat uitgaat van cijferalfabet voor het vercijferen van het grootste deel van een bericht en een beperkte lijst van codewoorden.

1587 De koningin der Schotten verloor letterlijk haar hoofd doordat haar nicht en aartsrivale koningin Elisabeth I van Engeland de inhoud ontcijferde van een compromitterend bericht dat Maria in code verstuurd had. Maria en haar compagnon Babington hadden vertrouwd op een cijferschrift om hun plannen geheim te houden, maar ze leefden in een periode waarin de cryptografie werd aangetast door vorderingen in de cryptoanalyse.

va1600 Het monoalfabetische cijfer voldoet uitstekend, toch hebben beroepscryptografen behoefte aan iets beters. Men zoekt naar een cijfercode die moeilijker te kraken is dan een monoalfabetisch cijfer, maar makkelijker toepasbaar dan het complexe polyalfabetische cijfer.		**1623** Wilhelm Schickard ontwerpt de eerste mechanische 'rekenklok' voor vermenigvuldigingen.
	±1650 Christiaan Huygens bedacht de verklaring voor de ringen van Saturnus en formuleerde het golfkarakter van het licht.	**1650** Uitvinding van de Pascaline door Blaise Pascal, een mechanische rekenmachine voor het optellen en aftrekken.
±1670 Lodewijk XIV gebruikt het monoalfabetisch cijfer *Grand Chiffre*, uitgevonden door vader en zoon Rossignol, om topgeheimen boodschappen te versleutelen. Het is twee eeuwen ontcijferd gebleven. (eerbewijs: *rossignol* betekent een loper die sloten opent).		
	1686 Eerste opbloei moderne fysische wetenschap bereikte zijn hoogtepunt met de publicatie van Isaac Newtons (1643-1727) *Principia*.	
va1700 De cryptoanalyse raakt geïndustrialiseerd. Elke Europese macht had zijn eigen zogenoemde Zwarte Kamer voor het ontcijferen van berichten en verkrijgen van inlichtingen. De beroemdste is de Geheime Kabinettskanzlei in Wenen.	**1753** Ontwikkeling van de telegraaf.	

va1800 Er ontstaat meer behoefte telegrammen te beschermen tegen onderschepping en ontcijfering.		**1804** Basis voor de ponskaartmachine wordt gelegd door Joseph Jacquard door het besturen van zijn weefgetouwen m.b.v. besturingsnaalden en plankjes met gaatjes.
1810-1830 Thomas J. Beale zet cryptoanalisten voor een raadsel met zijn drie vercijferde vellen, die hen leiden naar een schat van twintig miljoen dollar. Nog altijd zijn de zogenoemde Beale-cijfers niet gekraakt.	**±1810** Thomas Young komt met het zeer overtuigende bewijs dat licht in feite het karakter van een golfbeweging heeft. De doorslaggevende waarnemingen hadden vooral betrekking op, zoals dat nu wordt genoemd, interferentie.	**1822** Cryptoanalist Charles Babbage ontwerpt de blauwdruk voor de moderne computer, de *Differentiemachine No.2*. het bevatte een opslag (geheugen) en een molen (verwerker) die besluiten kan nemen en instructies kan herhalen, de tegenwoordige 'ALS... DAN...'-en de 'LUS'-commando's.
		Helaas kan de machine slechts één programma per keer uitvoeren, daarom gaat Babbage op zoek naar de analytische machine. Een met ponskaarten werkend apparaat dat ieder type berekeningen moet aankunnen.
1835 De Amerikaan Samuel Morse 'vindt' de Morse-code uit door gebruik te maken van een elektromagneet om het signaal van de telegraaflijn te versterken. De morsecode is zelf geen vorm van cryptografie, het is slechts een alternatief alfabet. Een bericht werd eerst versleuteld met gebruik van het Viginère-cijfer voordat het werd getelegrafeerd.		**1833** Augusta Ada, 's werelds *eerste* programmeur en tevens een vriendin van Babbage, werkt zijn ponskaartidee uit door één setje kaarten te gebruiken bij terugkerende bewerkingreeksen (conditionele loop en subroutine).

1839 Het Wheatstine-Cooke-systeem is in gebruik om berichten te verzenden tussen spoorstations m.b.v. detectors.	De aard van de golfbewegingen die met licht samenhing lijkt duidelijk te worden.	
1854 Waarschijnlijk bereikt Babbage de analyse van het Vigenère-cijfer, dit is onzeker omdat dit nooit openbaar is gemaakt.		**1854** De Booleanse algebra, gebaseerd op de operatoren AND, OR en NOT, wordt gepubliceerd door George Boole. Dit wordt de basis van alle logische circuits.
		1855 De *Differentiemachine No.2.* van Babbage wordt gepresenteerd.
1863 Niet Babbage, maar Friedrich Wilhelm Kasiski, bekend van de Kasiski-test, publiceert in *Die Geheumschriften und die Dechiffrirkunst*, zijn analyse van het Viginère-cijfer.		
va1870 Een groter publiek raakte vertrouwd met cryptografie, door bijvoorbeeld vercijferde boodschappen te versturen via de rubriek 'persoonlijke oproepen' of het gebruik van speldenprik-encryptie.	**1873** Eén van de grootste wetenschappelijke publicaties *Treatise on Electricity and Magnetism* door James Clerk Maxwell. De vergelijkingen die hij hierin maakte, bevatte golfachtige oplossingen en de snelheid van deze golven werd bepaald in termen van bekende natuurconstanten. Een van deze constanten bleek later de snelheid van het licht te zijn.	
	Maxwell en tijdgenoten beschouwden de elektromagnetische golven als trillingen in een allesdoordringend, elastisch medium dat 'ether' werd genoemd.	

	De natuurkunde van Newton en Maxwell wordt de *klassieke natuurkunde* genoemd.	
	1885 Eerste teken van de kwantumrevolutie, maar werd nog niet als zodanig onderkend.	**1894** Start van een productie van een telmachine die getallen kunnen nu ook op papier kan afdrukken door William Borough.
1896 Guglielmo Marconi 'vindt' de draadloze telegrafie uit voor het verzenden van een bericht naar de ontvanger. Als door toverkracht verplaatst het zich door de ether.	**1896** Ontdekking radioactiviteit, met zijn waarachtige, maar interessante, willekeurige gedrag voor het creëren van een willekeurige sleutel.	
Marconi gelooft in een begrenzing van de radiocommunicatie, over 3500 km wordt drie uur per dag geseind en Marconi vangt na een aantal dagen de radiogolven op, dit is het eerste transatlantische signaal.	**1897** Joseph John Thompson ontdekt dat de negatieve lading in een atoom afkomstig was van kleine deeltjes die later 'elektronen' zouden worden genoemd.	
De ontdekking van het transatlantische signaal biedt militaire mogelijkheden zoals de directe communicatie tussen twee punten m.b.v. radiogolven, die wel in alle richtingen uitwaaieren zodat het bericht behalve die ontvanger ook de vijand kan bereiken.	**1900** Een eerste aanzet tot de theorie van de kwantummechanica is gegeven door Max Planck in zijn studie gepubliceerd *Zur Theorie des Gesetzes der Energie-Verteilung im Normal-Spektrum* over het probleem van de straling van een zwart lichaam.	**1904** Thomas Watson wordt ontslagen bij het National Cash Register (NCR) als vice-president.
	1905 Albert Einstein doet drie belangrijke ontdekkingen. Eén ervan blijkt de volgende stap in de ontwikkeling van de kwantumtheorie te zijn, naast de relativiteitstheorie en het definitieve bewijs van het bestaan van moleculen.	

	1906 Einstein vindt een eerste toepassing van de kwantum effecten in de fysica van vaste stoffen: gekwantiseerde vibratiegolven.	
	1911 Ernst Rutherford zegt dat atomen een pitvormige, harde kern hebben, en verder leeg zijn.	
	1913 Niels Bohr werkt in Cambridge onder J.J. Thomson, de ontdekker van het elektron. Bohr komt met een atoommodel als miniplanetenstelsel waarin slechts bepaalde elektronen banen zijn toegestaan. Hij gebruikte de kwantumtheorie van Planck en het atoommodel van Rutherford, waar hij later in Manchester mee werkte, om een eigen model van een waterstofatoom te ontwikkelen.	
1914-1918 De Fransen, met de allerbeste codebrekers, onderscheppen zo'n 100.000.000 woorden die slechts bestemd waren voor Duitse oren.	**1914** James Franck en Gustav Hertz hebben een bewijs van het bestaan van stationaire elektrontoestanden in het atoom.	
1917 Het door de Britten ontcijferde Duitse Zimmermantelegram bepaalt dat de Verenigde Staten deel gaat nemen aan de oorlog.	**1917** Albert Einstein voorspelt de theorie van de gestimuleerde emissie.	
One-time-pad wordt ontwikkeld door Gilbert Vernam voor gebruik in telexmachines.		

[74]

1918 Een idee van de Amerikaanse majoor Joseph Mauborgne biedt volmaakte betrouwbaarheid, door het gebruik van een willekeurige sleutel, waardoor de veiligheid van het eenmalige blokcijfer kan worden gewaarborgd, de Heilige Graal der cryptografie.		
Uitvinding van het Enigma, een cryptografisch apparaat en een elektrische versie van de cijferschijf van Alberti, uitgevonden door de Duitse ingenieur Arthur Scherbius.	**In de jaren 1920** Overgang van Newtoniaanse naar Einsteiniaanse fysica voor het grote publiek.	
	1923 Arthur Compton komt met het overtuigende bewijs voor het deeltjeskarakter van elektromagnetische (röntgen) straling.	
	Louis de Broglie oppert het golfkarakter van materie.	
	1924 Fysici ontdekken de ionosfeer, een geïoniseerde laag in de atmosfeer die op 60 km boven de aarde begint, die als een spiegel werkt waartegen radiogolven terugkaatsen.	**1924** De bij NCR ontslagen Thomas Watson wordt, na twintig jaar werknemer bij CTR, chief executive officer en doopt CTR om in International Business Machines (IBM)

	Introductie Bose-Einsteinstatistiek: een nieuwe manier van deeltjes tellen in de statistische fysica. Op deze manier kunnen zij de Bose-Einsteincondensatie voorspellen, waarbij een macroscopische hoeveelheid materie in een enkele kwantumtoestand kan condenseren.
	1925 De onzekerheidsrelatie van Heisenberg, genoemd naar Werner Heisenberg, is een belangrijke relatie in de kwantummechanica die stelt dat het niet mogelijk is om de plaats en de snelheid (of impuls) van een deeltje tegelijkertijd met onbeperkte nauwkeurigheid te weten. Dit komt doordat het proces van de meting altijd het resultaat zal beïnvloeden: op het moment dat er een meting plaatsvindt, verandert deze meteen de plaats, de snelheid of allebei.
	Wolfgang Pauli komt met de verlossende woorden: Geen twee elektronen kunnen zich in dezelfde kwantumtoestand bevinden.

1926 De Britse cryptoanaliseten onderscheppen in Kamer 40 raadselachtige boodschappen. De Duitse Wehrmacht heeft codeermachine Enigma in gebruik genomen.	**1926** Er is enige onzekerheid over het gebruik van het woord *onzekerheid* in verband met het Heisenbergs principe. Micheal Frayn stelt voor dat *onbepaaldheid* een beter voor het principe zou zijn geweest en *onbepaalbaar* nog beter.	
	1927 De Schrödingervergelijking is de basisformule van de kwantumtheorie. In de kwantumtheorie wordt uitgegaan van de tweeledigheid van alle materie. Dat wil zeggen dat deeltjes altijd een golfkarakter met zich meedragen en golven omgekeerd altijd een deeltjeskarakter hebben.	
1930-1938 De Polen kraken de Enigma-codes.	**1930** Eén van de beroemdste wetenschappelijke werken van de 20e eeuw wordt gepubliceerd: *Principles of Quantum Mechanics* van Paul Dirac, waarin het mysterie wordt 'verklaard' door middel van te vertellen hoe de kwantummechanica 'werkt'.	**1936** Konrad Zuse bouwt de elektromechanische buizencomputer Z1 bestuurd door een programma op polsband. Later volgen Z2, Z3 en Z4.
	1935 Einstein spreekt over de kwantumtheorie van een "spookachtige wisselwerking op afstand".	

1938 Gebruik van de microstip in de Tweede Wereldoorlog door de Duitsers, een combinatie van steganografie en cryptografie, door een pagina tekst te verkleinen tot een puntje van 1mm. Dit puntje werd verstopt in een onschuldige brief.	**In de jaren 1930** stonden discussies over de interpretatie en geldigheid van de kwantumtheorie in de belangstelling, er is echter geen vooruitgang geboekt.	**1938** Het eerste product van William Hewlett en Dave Packard wordt een geluidsgenerator voor de film Fantasia van Walt Disney. Het bedrijfje Hewlett-Packard start in een garage.
1939 De Enigma wordt uitgebreid met nieuwe scrambles en extra schakelsnoertjes. Enigma werd opnieuw onkwetsbaar, halverwege 1939 wordt Polen binnegevallen door Duitsland (Blitzkrieg-strategie).		**1939** Een werkend prototype van de elektronische digitale computer wordt gebouwd door John Atanasoff en zijn assistent Clifford Berry, ze noemen hem de Atanasoff Berry Computer (ABC).
1940? Het Britse team van cryptoanalisten, met dank aan de Polen, waarbinnen het grootste brein Alan Turing, kraken Enigma-sleutels met elektromagnetische decodeerapparaten, zogenoemde *bombes*, in minder dan een uur.	**In de jaren 1940** stonden discussies over de interpretatie en geldigheid van de kwantumtheorie nog steeds in de belangstelling, maar nog steeds geen vooruitgang.	**Jaren 1940** De voorzitter van IBM, James Watson, doet de legendarische uitspraak: "*Ik denk dat er een wereldmarkt is voor misschien vijf computers.*"
De Amerikanen kraken tegelijkertijd het Japanse machinecijfer Purple.		
1942 De Amerikaanse ingenieur Philip Johnstons formuleert een nieuw encryptiesysteem, de Navajo-code. Met gebruikmaking van het Navajo stamdialect, een volstrekt onbegrijpelijke taal, worden een Navajo-alfabet en Navajo-codewoorden opgesteld.		**1942** Max Newman ontwerpt een machine, genaamd de Newmanry, die zich kan aanpassen aan diverse problemen, deze is sneller en programmeerbare dan de bombes van Alan Turing.

		±1943 Britse uitvinding Colossus moet het gaan opnemen tegen het Duitse Lorenz-cijfer. De machine van Newman wordt omgezet in een Colossus-machine.
		Colussus wordt gezien tot de voorloper van de moderne digitale computer.
		1944 Howard Aiken demonstreert Amerikaans eerste programmabestuurde computer, de Automatic Sequence-Controlled Calculator (ASCC) Mark I.
1946 Het Britse Government Communications Headquarters (GCHQ) wordt opgericht – opvolger van de Government Code and Cipher School (GC&CS). Zij zijn het grootste British Intelligence Service die 'signals intelligence (SIGINT)' bepalen.		**1946** J. Presper Eckert en John W. Mauchley bouwt een nieuwe 'moeder van alle computers', de ENIAC (Electronic Numerical Integrator And Calculator), deze kan tot 5000 berekeningen per seconde uitvoeren. Deze eerste grootschalige elektronische digitale computer bezit 18.000 elektronenbuizen.
		John von Neumann en zijn collega's komen met een concept van een computer met inwendig opgeslagen programma's.
	1947 John Bardeen, William Shockley en Walter Houser Brattain, van At&t Bell Labaroties, vinden de transistor uit. Een elektronische component die de radiobuis vervangt en daarmee de informatie- en communicatiemaatschappij mogelijk maakt.	

	In de jaren 1950 stonden discussies over de interpretatie en geldigheid van de kwantumtheorie nog altijd in de belangstelling, vooruitgang bleef uit.	**1951** Commercieel computergebruik is een realiteit met de eerste inwendige geprogrammeerde elektronische digitale computer van Eckert en Mauchy: de Universal Automatic Computer (Univac).
		1952 Ontstaan van Electronic Discrete Variable Automatic Computer (Edvac) naar een concept van John von Neumann en medewerkers uit 1946.
1952 Oprichting van de Amerikaanse National Security Agency (NSA), de belangrijkste luistervink van de wereld. Zij houden zich, in het geheim, bezig met de beveiliging van de overheidsinformatie, en anderzijds met het afluisteren van communicatie. De NSA houdt zich grotendeels bezig met het ontwikkelen en breken van cryptografische technologie.		
		1953 IBM, maker van tabelleermachines, komt onder leiding van Thomas Watson jr. met zijn eerste computer: de 701.
		Philips maakt voor intern gebruik drie computers, de: 1. PETER (Philips Experimentele Tweetalige Elektronische Rekenmachine); 2. PASCAL (Philips Akelig Snelle Calculator); 3. STEVIN (Snel Tel en Vermenigvuldig Instrument).
		1954 AT&T Bell Labaroties bouwt de eerste algemeen toepasbare transistorcomputer.

1957 IBM maakt voor de 'gewone' mensen Fortan (Formula Translator), een programmeertaal waarmee zij zelf computerprogramma's kunnen schrijven.

1958 De taal Lisp (List Processor) wordt ontwikkeld voor onderzoek naar kunstmatige intelligentie door John McCarthy.

Jack Kilby (van Texas Instruments) demonstreert het eerste werkenden exemplaar van integrated circuit (IC).

1960 Theodore Mainman bouwt de eerste laser op gestimuleerde emissi, een kwantummechanisch verschijnsel bij atomen die spontaan terugvallen naar de grondtoestand. De laser is een *tweede* belangrijk apparaat dat essentieel is voor de moderne communicatiemaatschappijj.

Jaren '60 Bedrijven vertrouwen meer het elektronische vercijferen zoals voor geldtransfers en gevoelige zakelijke onderhandelingen.

1961 *"Elke voldoende geavanceerde technologie is niet te onderscheiden van magie."* Arthur C. Clarke (fysicus en sciencefictiononauteur), Profiles of the future.

1960 De eerste overdraagbare hoger-niveau programmeertaal wordt gepresenteerd: COBOL (Common Business Oriented Language) o.l.v. Grace Hopper.

1963 Ontstaan ASCII (American Standard Code for Information Interchange), die elke letter van het alfabet een bepaald getal toekent.

		Philips gaat commerciële (mini)computers ontwikkelen.
		1964 Presentatie van het eerste programma geschreven in de taal Basic, van de hand van Thomas Kurtz en John Kemeny.
	1965 John Bell schrijft een artikel over een mogelijk experiment om een kwantumverstrengelde toestand te verkrijgen, dat inhoudt dat twee deeltjes onomstotelijk met elkaar verbonden zijn.	**1968** Voor het spel boter-kaas-en-eieren schrijft Bill Gates een softwareprogramma.
		Het Advanced Research Projects Agency, kortweg ARPA, zoekt een oplossing om militaire computers met elkaar te verbinden. Het toenmalige ARPA-net komt tot vier onderling verbonden sites.
1969 James Ellis lijkt het bewijs te hebben voor de mogelijkheden van publieke-sleutelcryptografie, tevens heeft hij een uitwerking van aparte publieke en privé-sleutels.		**1969** K. Thompson en D. Ritchie staan aan de wieg van het besturingssysteem UNIX door de bouw van een ontwikkeltool voor programmeurs.
		1970 ARPA ontwikkelt TCP/IP (Transmission Control Protocol/ Internet Protocol) en daarboven draaiende protocollen TELNET, SMTP en FTP.

		1971 Introductie van eerste microprocessor-chip, gecombineerd met andere chips, ontstaat een complete microcomputer. De chip met 2250 transistoren heeft een gelijke rekenkracht als de ENIAC uit 1946.
		Inmiddels zijn er 37 computers aangesloten op het voormalige Internet (toen heette het nog ArpaNet).
1973 Clifford Cocks heeft een mathematische functie bedacht voor deze publieke-sleutelcryptografie, maar het blijft lastig in praktijk te brengen. Malcolm Williamson buigt er ook zijn hoofd over en ontdekt de Diffie-Hellman-Merkle-sleuteluitwisseling, die pas in 1976 openbaar wordt.		**1973** Het Amerikaanse National Office of Standards voert een standaardencryptiesysteem in voor het geheim communiceren tussen bedrijven onderling.
		1974 Data Encryption Standard (DES) wordt ontwikkeld door IBM, voor het eerste wordt een uniforme standaard voor de versleuteling van vertrouwelijke gegevens gedefinieerd.
		De 56-bits-versie Data Encryptie Standaard (DES) wordt vervangen door het IBM-encryptieproduct Lucifer.

1975 Ellis, Cocks en Williams hebben alledrie een zwijgplicht, daar zij werkzaam zijn bij GCHQ, een dergelijk patent is ook niet aangevraagd.	**1975** De Altair, gebouwd rond de 8-bits 8080 Intel processor, is voor $397 te koop met een werkgeheugen van 256 bytes, geen toetsenbord of beeldscherm, programmeren gaan via schakelaartjes.
1976 Martin Hellman (1945) vindt een strategie voor het oplossen van het probleem van sleuteldistributie. Kort hierop verschijnt het Diffie-Hellman-Merkle-schema voor sleutelwisseling.	Oprichting Micro-Soft door Paul Allen en Bill Gates en ontwikkelen programmeertalen voor microcomputers.
Whitfield Diffie (1944) bedenkt de zogenaamde asymmetrische sleutel, d.w.z. de encryptiesleutel (*publieke sleutel*) en decryptiesleutel (*privé-sleutel*) zijn niet meer identiek.	**1976** Stephen Woxniak en Steve Jobs werken aan de eerste Apple-computer.
1977 RSA is het eerste systeem dat voldoet aan de eisen van de publieke-sleutelcryptografie en wordt uitgevonden door Ron Rivest, Adi Shamir en Leonard Adleman.	**1977** Verschillende 'hobby'-computers komen op de markt waaronder de PET-computer voor $600 en de Apple II.
Honderd miljoen computers zouden meer dan duizend jaar nodig hebben om een RSA-cijfer te kraken, met voldoende grote waarden van p en q (de priemdelers) is RSA onaantastbaar.	

Diffie, Hellman en Ralph Merkle (1952) krijgen wereldwijde erkenning voor hun concept van de publieke-sleutelcryptografie. Rivest, Shamir en Adleman krijgen de eer van het ontwikkelen van RSA.		**1979** Eerste relationeel database management systeem (dbms) gebruikmakend van SQL wordt door Oracle Corporation op de markt gebracht.
	1980 Het experiment dat in Bell's artikel (1965) wordt beschreven, wordt in Parijs uitgevoerd. Bell's voorspellingen komen uit.	**1980** Wereldwijd zijn er 700.000 'huis-, tuin- en keuken' computers. Ashton-Tate zijn de bouwers van het populaire databasepakket voor pc's dBase.
Kwantumverstrengeling is vanaf nu een hot item, het test niet alleen de grondslagen van de natuurwetenschappen, maar blijkt ook interessant te zijn voor geheime informatieoverdracht: het zogenoemde kwantumgeheimschrift. Men was op dreef en deed niet lang hierna voorspellingen van de kwantumteleportatie.		
	1981 Richard Feynman stelt in zijn lezing *Simulating physics with computers* voor om een kwantumsysteem te simuleren met een kwantumsysteem. Ook Charles Bennett (1943) van IBM en Paul Benioff van Argonne National Laboratory speelden een vooraanstaande rol bij de allereerste verkenningen.	
		IBM komt met de IBM-PC, een veel goedkope pc gebaseerd op de Intel 8086-processor Microsoft MS-DOS.
		1982 De enorme groei van ARPA brengt het Internet voort.
		Fundamenten voor Sun Microsystems worden gecreëerd door Scott McNealy, gebaseerd op Unix- en risc-technologie.

1984 Introductie van:
1. IBM met 80286 16-bit PC AT;
2. Apple met Macintosh;
3. Hewlett-Packard met laserjet printer voor pc's.

Ontwikkeling van een apparaatje waarmee Sandy Lerner en Len Bosack elkaar email kunnen versturen: de tegenwoordige router.

1985 David Deutsch van Oxford University beschrijft als eerste een universele kwantumcomputer, zij het als een abstract idee. Deutsch bedenkt ook de kwantumequivalenten voor de klassieke logische poorten AND, OR en NOT. Anders dan bij een klassieken computer moeten deze bij een kwantumcomputer evenveel ingaande bits hebben als uitgaande.

1986 Sleuteldistributie is een probleem. De VS-regeringssleutels worden beheerd door Communication Security (COMSEC).

1988 Toshiba, Tandy en NEC komen met een nieuwe generatie compacte computers: de laptops.

1989 In Cern, het Europese centrum voor deeltjesonderzoek in Genéve, schrijft Time Berners Lee een projectvoorstel, geheten *World Wide Web*, voor een hypertext-achtige systeem waarbij gegevens opgeslagen kunnen worden op geografisch verspreid staande computers. Men vindt het niks.

1990 Het projectvoorstel *World Wide Web* wordt toch onveranderd aangenomen.

Populariteit van geautomatiseerde hulpmiddelen voor de ontwikkeling van software (zogenoemde CASE-tools: computer aided software engineering) groeit.

1991 Phil Zimmermann (1954) ontwikkelt een RSA-encryptie-product voor het versleutelen van het digitale dataverkeer en noemt het *Pretty Good Privacy* (PGP).		
1992 Toepassing van de symmetrische IDEA-sleutel (lijkt op DES), dat binnen PGP gebruikt wordt om RSA-sleutels te vercijferen.		**1992** Het International Data Encryption Algorithm (IDEA) wordt ontwikkeld door het Swiss Federal Institute of Technology ETH in Zurich.
		Intel presenteert de Pentium als opvolger van de 486-processor. DEC komt met de alpha-familie van risc-systemen.
1994 Terwijl de pro-encryptie-lobby pleit voor cryptografische vrijheid en de anti-encryptie-lobby pleit voor cryptografishe beperkingen, is er een derde optie die een compromis zou kunnen bieden: cryptografische sleutelbewaring.	**1994** Wiskundige Peter Shor van AT&T Bell Labs ontdekt een zeer bijzonder algoritme om grote getallen snel te factoriseren met een kwantumcomputer. Deze ontdekking stimuleert het onderzoek naar kwantumcomputers enorm.	
		Er zijn zo'n 26 miljoen personal computers op de wereld.
	1995 Shor doet een voorstel voor methoden van kwantumcorrectie om de fouten te repareren die de omgeving veroorzaakt in een systeem van vele kwantumbits.	
		Sun Microsystems zet de eerste versie van Java op internet in samenwerking met Arthur van Hoff.
		De president van Oracle denkt dat het nieuwe tijdperk *Netwerk Computer* de pc snel gaat verdringen.

1996 Louis J. Freeh, directeur van de FBI, zegt: 'De gemeenschap van wetshandhavers steunt volledig een evenwichtig encryptiebeleid. [...] Sleutelbewaring is niet zomaar de enige oplossing, het is zelfs een uitstekende oplossing, omdat zij daadwerkelijk een evenwicht aanbrengt tussen fundamentele maatschappelijke aangelegenheden als privacy, informatiebeveiliging, elektronische handel en nationale veiligheid.'

	Half miljoen Nederlanders is aangesloten op Internet.
RSA Data Security Inc., het voor RSA-producten verantwoordelijke bedrijf, wordt voor 200 miljoen dollar verkocht.	Lov Grover ontwikkelt bij Bell Labs (inmiddels overgedaan aan Lucent Technologies) het Grover-algoritme. Hiermee kan een kwantumcomputer bepaalde zoekproblemen in grote databestanden kwadratisch sneller oplossen dan een klassieke computer.
Deep Blue, schaakcomputer van IBM, verliest van de wereldschaakmeester Garry Kasparov.	
1997 Ellis, Cocks en Williamsen krijgen de erkenning die hun toekomt, na bijna dertig jaar geheimhouding.	**1997** MIT-onderzoekers publiceren meetresultaten van een enkel kwantumbit: een vloeistof met een miljard maal een miljard identieke moleculen, die gezamenlijk het signaal van een enkele kwantumbit representeren. Met kernspinresonantie (NMR) manipuleren ze het enkele kwantumbit.
Deep Blue verslaat de wereldschaakmeester Garry Kasparov.	
	Het DES-systeem wordt gekraakt in 96 dagen.
	Het Amerikaanse National Institute of Standards (NIST) zoekt naar een vervanger van DES middels een wedstrijd.
	1998 Het eerste twee-kwantumbitsysteem, gerealiseerd met vloeistof- NMR (University of California, Berkely, VS).
	1999 Het eerste drie-kwantumbitsysteem, gerealiseerd met vloeistof- NMR (IBM Almaden Research Center, VS). Dit systeem toont als eerste aan dat het zoekalgoritme van Grover op een kwantumcomputer werkt.

2000 Het eerste vijf-kwantumbitsysteem, gerealiseerd met vloeistof- NMR (IBM). Dit systeem voert een deel van het factorisatie-algoritme van Shor uit. In hetzelfde jaar maken onderzoekers van het NIST in Boulder (VS) een simpele kwantumcomputer van vier ionen in een ionenval.

Hendrik Casimir (1909-2000) omschreef natuurkunde als een *benaderende* beschrijving van een *beperkt* gedeelte der fysische verschijnselen, die op hun beurt slechts een beperkt gedeelte van onze menselijke ervaringen uitmaken.

Het algoritme "Rijndael" van de Belgische cryptografen Joan Daemen en Vincent Rijmen wordt door de NIST verkozen tot veiligste voor het nieuwe AES.

2001 Het eerste zeven-kwantumbitssysteem, gerealiseerd met vloeistof- NMR (IBM). Voor het eerst wordt het algoritme van Shor helemaal uitgevoerd. De zeven kwantumbits factoriseren het getal 15 in zijn priemdelers 3 en 5.

2002 Zwitserse onderzoekers hebben een kwantumsysteem ontwikkeld om kwantumsleutels te distribueren via een optische vezel over een afstand van 67 km.
Het Japanse Mitshubishi Electric lukte het over een afstand van 87 km.

2003 De onderzoekers van Toshiba is het gelukt een afstand van 100 km te overbruggen met behulp van kwantumencryptie.

2004 Bijna alle tot nu toe werkende kwantumrekenaars zijn gebaseerd op vloeistof- NMR. Deze techniek laat zich net als ionenvallen echter niet opschalen naar duizenden kwantumbits. Wereldwijd gebeurt onderzoek naar betere kandidaten als nieuwe ionenvallen, vaste-stof- NMR, supergeleidende lusjes en kwantumdots.

2004 Er zijn zo'n 575 miljoen pc's ter wereld.

2005 De Japanse Groep NEC heeft de industrialisatie van een zender en een ontvanger van verdeelde sleutels via kwantumcryptografie aangekondigd.

2005 Internationaal Jaar van de Natuurkunde. Dit jaar is het precies 100 jaar geleden dat Albert Einstein (1879-1955) zijn 'wonderjaar' had .

2005 Bijna elk huishouden in de westerse wereld heeft al meer dan één computer.