Les D-05 Cryptografie

In deze les staan we stil bij hel versleutelen (**encryptie**) en ontcijferen (**decryptie**) van boodschappen. Aan de orde komt de geschiedenis van het geheimschrift: hoe versleutelde men vroeger boodschappen en hoe doen we dat in de datacommunicatie van tegenwoordig?

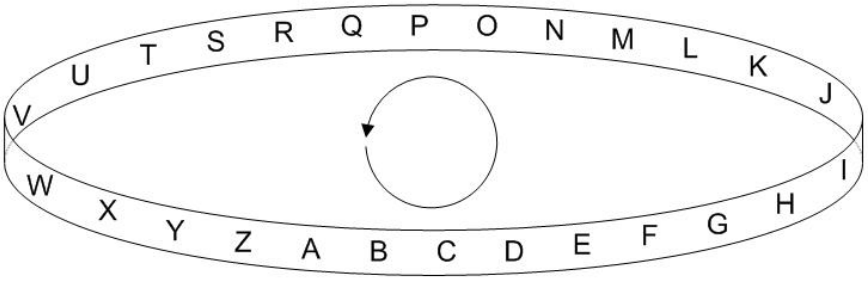
5.1 Vroege geschiedenis van de cryptografie

Het woord **cryptografie** is afgeleid van de Griekse woorden “cryptos” (geheim) en “graphia” (schrijven). Onder cryptografie verstaan we het maken van een geheimschrift (**versleutelen** van een boodschap, **coderen** van een boodschap, **encryptie**) en het ontcijferen van het geheimschrift (**ontsleutelen, decoderen, encryptie**).

Om boodschappen te versleutelen gebruikten de Grieken een **scytale** (stok). De zender van een boodschap wikkelde een strook perkament of leer om de scytale en schreven daar een boodschap op. De ontvanger diende te beschikken over een stok met eenzelfde diameter om de boodschap te kunnen lezen. De scytale was voor de ontvanger dus de **sleutel** waarmee de boodschap kon worden ontcijferd.

scytale

De Romeinen gebruikten een andere methode om boodschappen te versleutelen. Deze methode heet ook wel de **Caesarmethode**, omdat Julius Caesar (100 – 44 B.C) deze methode gebruikte om te communiceren met zijn generaals. In dit geheimschrift wordt iedere letter vervangen door de letter die drie plaatsen verder staat in het alfabet. De letter A wordt dus een D, … de letter X een A, de letter Y een B en de letter Z een C. De ontvanger moet iedere letter dus weer vervangen door de letter die drie plaatsen terug staat in het alfabet.



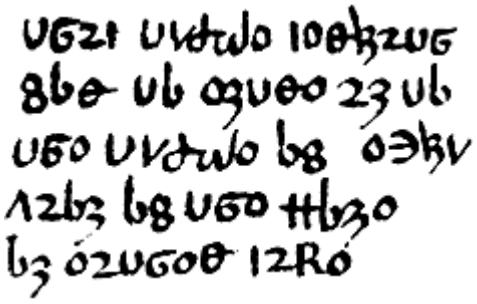
de Caesarmethode

Opdracht 5.1

Hoe wordt de tekst VENI VIDI VICI volgens de Caesarmethode gecodeerd?

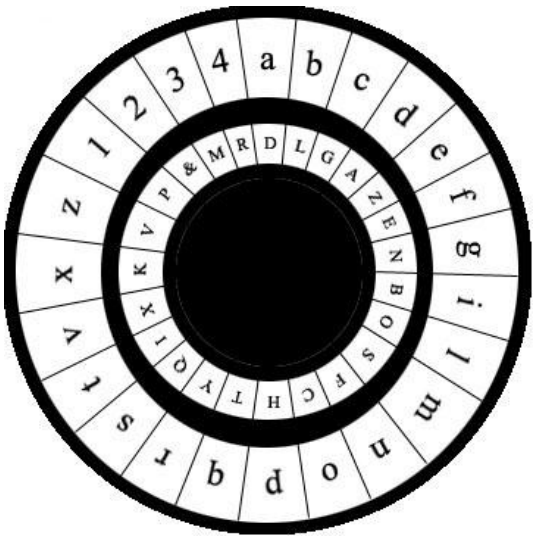
Halverwege de 13e eeuw beschreef de monnik Roger Bacon een aantal verschillende cijfermethoden om boodschappen te versleutelen.

De Engelse dichter Geoffrey Chaucer gebuikte in zijn boek "*The Equatorie of the Planetis"* (1371) zes pagina's vol geheimschrift, waarin iedere letter werd vervangen door een symbool.



symbolentaal van Chaucer

Leon Battista Alberti beschreef in zijn boek *"Tattati in cifra"* (1470) een cijferwiel (cipher diks) waarmee tekst kon worden versleuteld en ontcijferd.



het cijferwiel van Leon Battista Alberti

Een eerste handleiding over cryptografie van de hand van de Gabriele de Lavinde verscheen in 1379. In het vakgebied wordt Johannes Trithemius, abt van Spanheim in Duitsland, beschouwd als de grondlegger van de moderne **cryptologie**. Zijn boek *"Polygraphia"* (1510) was het eerste gedrukte werk op het gebied van de cryptologie.

Cryptologie is de leer van het geheimschrift, dat bestaat uit de vakgebieden:

- **cryptografie:** het ontwerpen en gebruiken van geheimschriften
- **cryptoanalyse:** het analyseren en breken van geheimschriften.
- **steganografie:** de cryptologische methode die tot doel heeft het bestaan van een bericht te verbergen.

De Italiaan Simeone de Crema, actief op het vakgebied van de cryptoanalyse, bedacht in 1401 dat je door de frequentie te analyseren waarmee letters voorkomen in een cryptografische boodschap enerzijds en in gewone teksten anderzijds, de sleutel vaak eenvoudig kan vinden. Zo kan bijvoorbeeld de codering van de letter "e" in het geheimschrift al snel worden ontdekt omdat deze vaak voorkomt. In zijn publicatie *"Regulae ad extrahendum litteras zifferatas sine exemplo"* (1479) beschreef zijn landgenoot Sicco Simonetta ontcijfermethoden met behulp van taalstatistieken.

Veel klassieke versleutelingsmethoden gebruikten vervanging van letters door bijbehorende letters of symbolen (Caesarmethode, symbolentaal van Chaucer, cijferwiel van Alberti). Deze vorm van versleuteling wordt dan ook **substitutie versleuteling** genoemd. Met frequentieanalysemethoden zijn door substitutie versleuteling verkregen boodschappen makkelijk te kraken.

Een andere vorm van vorm van versleuteling is **transpositie versleuteling**, waarbij de tekst in een andere volgorde wordt herordend.

Een andere reden dat de frequentieanalyse bij de klassieke versleutelingsmethoden veel succes had, was omdat bij deze methoden elke letter werd vervangen door één andere letter of symbool. Bij deze versleutelingsmethoden is sprake van **mono-alfabetische versleuteling**.

De Fransman Blaise de Vigenère publiceerde in zijn boek "*Traicté des chiffres ou secrètes manières d'escrire"* (1585) een methode om tekst meerdere keren alfabetisch te versleutelen. Bij zijn methode vindt **poly-alfabetische versleuteling** plaats. Elke letter wordt met een andere rij uit het onderstaande tableau versleuteld.

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

versleutelingstableau van Vigenère

Het tableau van Vigenère werkt als volgt. Een boodschap, bv VENI VIDI VICI wordt versleuteld met behulp van een codewoord, bv VIGENERE. De letter wordt omgezet in de bijbehorende letter in de rij van de letter van het codewoord:

```
VIGE NERE VIGE      codewoord
VENI VIDI VICI      boodschap
QMTM IMUM QQIM      versleutelde boodschap
```

De letter “V” in rij “V” wordt een Q,
de lette “E” in rij “I” wordt een “M” enz.

Opdracht 5.2

Versleutel de boodschap “IK ZIE JE MORGEN” volgens de methode van Vigenère met als codewoord VRIEND.

Opdracht 5.3

Leg uit waarom poly-alfabetisch versleutelde boodschappen lastiger met behulp van frequentieanalyse te kraken zijn.

Een voorbeeld van steganografie (het verbergen van boodschappen) is de methode die Francis Bacon (1561-1626). Hij codeerde een alfabet op basis van vijftallen letters in een stuk tekst waarbij wordt bijgehouden welke letter vetgedrukt is (* = normaal, B = bold (vet)):

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

alfabetcodering van Francis Bacon

Voorbeeld

T**o** **b**e or n**o**t to b**e** th**a**t i**s** **th**e **q**uest**i**on. Whet**h**er **'t**is no**ble**r **i**n the **mi**n**d** to s**uff**er **th**e s**lin**gs **a**nd ar**ro**w**s** **o**f out**ra**geous fort**un**e **o**r t**o** **t**ak**e** ar**m**s ag**ai**ns**t** a sea **o**f tr**oub**l**es** **a**nd **by** **o**pp**o**s**in**g end them?

T**ob**eo	*BB**	= M
rn**o**tt	**B**	= E
ob**e**th	**B**	= E
ati**st**	B**BB	= T
h**eq**ue	*BB**	= M
st**i**on	**B**	= E
Whet**h**	****B	= B
er**t**is	**B**	= E
no**ble**	**BBB	= H
r**i**nth	*B***	= I

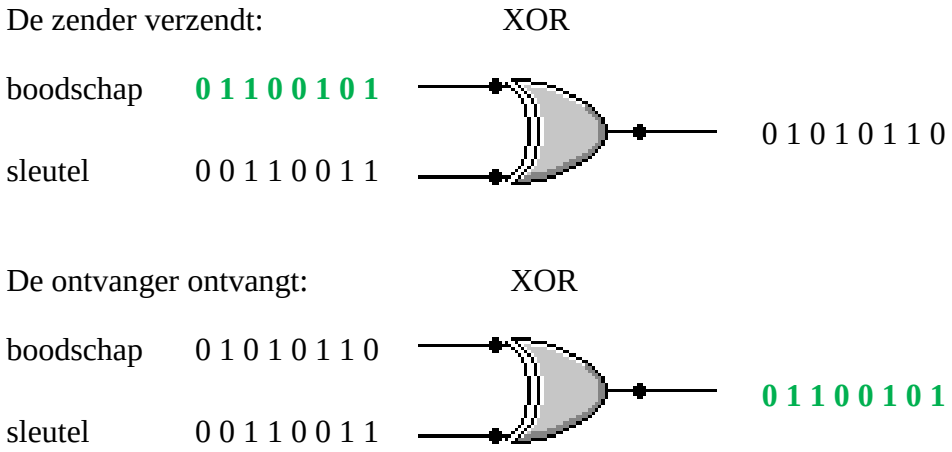
Opdracht 5.4

Maak de ontcijfering van de tekst uit het bovenstaande voorbeeld af.

In de 18e en 19e eeuw hadden de Europese grootmachten eigen geheime diensten waar een team van codebrekers geheime berichten ontcijferden. Cryptografie speelde een belangrijke rol in een aantal slagen in de Spaanse Onafhankelijkheidsoorlog. De Brit George Scovell wist het berichtenverkeer van Napoleons troepen te ontcijferen waardoor de troepen van de Hertog van Wellington voorkennis hadden van op handen zijnde activiteiten.

Ook in de Wereldoorlogen aan het begin van de 20^{e} eeuw speelde cryptografie een belangrijke rol. In 1917, tijdens de Eerste Wereldoorlog bedacht de Amerikaan Gilbert Vernam een encryptie methode bedenken, die de Duitsers niet konden kraken. Deze coderingsmethode wordt de **Vernam-codering** genoemd. Bij zijn methode wordt de tekst van een boodschap (vergelijkbaar met ASCII) vertaald in een bitreeks van een bepaalde lengte. Deze bitreeks wordt versleuteld met een sleutel van eenzelfde lengte. De sleutel wordt slechts één keer gebruikt om kraken via cryptoanalyse lastig te maken.

Met een XOR functie wordt de reeks versleuteld en de ontvanger kan de reeks met dezelfde XOR functie ontcijferen.

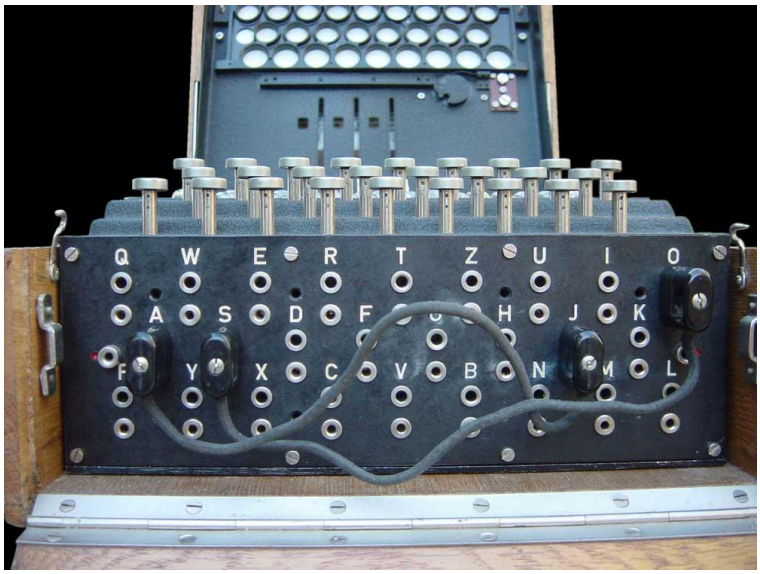


Een nadeel van de Vernam codering is echter … hoe wisselen zender en ontvanger de sleutel uit !?

Na de Eerste Wereldoorlog stond de ontwikkeling van cryptografie natuurlijk niet stil. In 1920 kwam de Amerikaan Edward Hebern met een nieuwe uitvinding. Hij voorzag een typemachine van een draaiend wiel, dat er voor zorgt dat bij het intypen van een bepaalde letter een andere letter wordt afgedrukt.

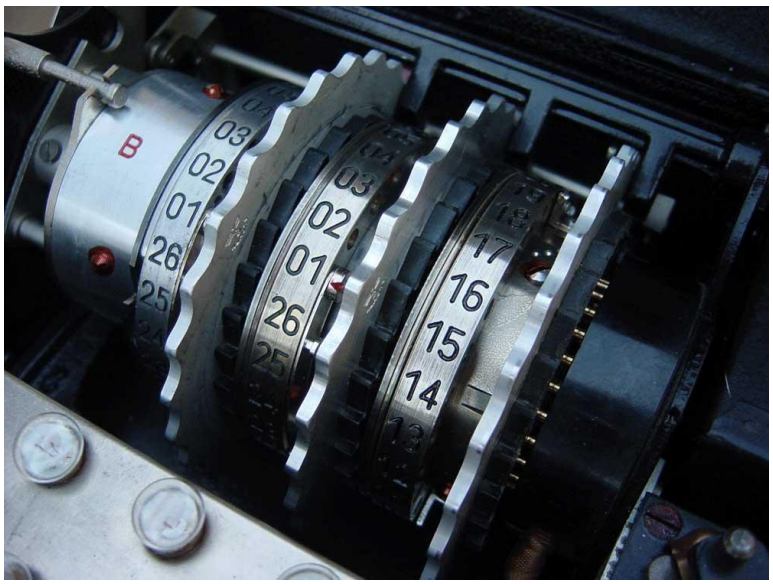
De door Hebern bedachte techniek werd in de Tweede Wereldoorlog toegepast in de **Enigma codeermachine**.

De Enigma bevatte drie **rotors** die er voor zorgden dat de tekst werd gecodeerd. Eerst werd via een geheim codeboek de begininstelling van de Enigma gekozen, per dag een andere.



Die begininstelling zorgde er bijvoorbeeld voor dat een ingetypte W door de eerste rotor veranderde in een P, waarna door de tweede de P in een M en door de derde de M in een A veranderde. Uiteindelijk werd de W dus een A.

Na elke omwenteling draaiden de tweede en derde rotor een plaats door. Zo werd een letter een volgende keer veranderd in een andere letter.



De manier waarop de Enigma boodschappen versleutelde is dus een **poly-alfabetische substitutie versleuteling**.

De drie bewegende rotors kunnen $26^3 = 17576$ mogelijk posities innemen. Doordat er ook nog eens variaties in de bedrading aangebracht waren kon de Enigma in theorie niet gekraakt worden.

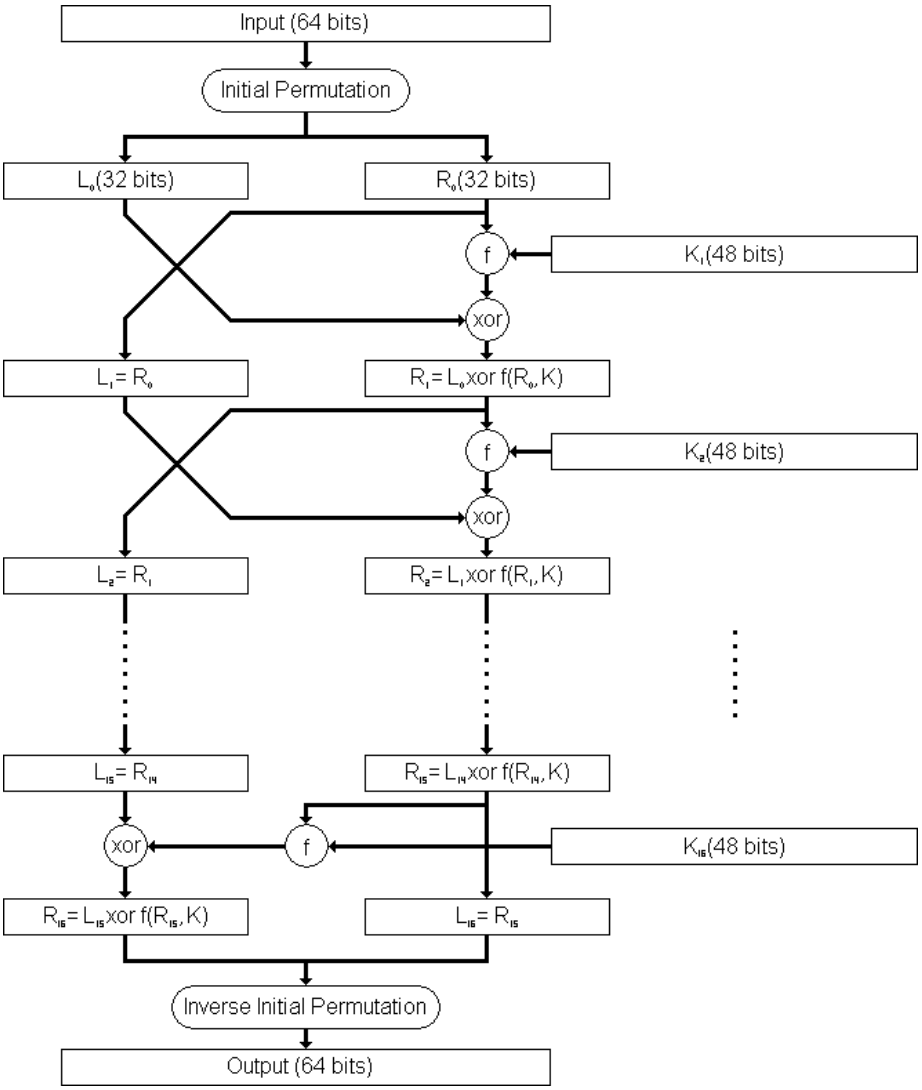
Toch lukte het de Brit **Alan Turing** uiteindelijk alsnog om de Enigma te kraken.

5.2 Cryptografie in het computertijdperk

In de geschiedenis van de cryptografie heeft altijd centraal om informatie te versleutelen zodat deze niet door nieuwsgierige ogen kon worden gelezen, vaak om politieke of militaire redenen. In onze hedendaagse wereld, waar een groot deel van de communicatie via de computer verloopt, zijn er ook voldoende redenen om informatie voor nieuwsgierige ogen te verbergen.

In de jaren ‘70 van de vorige eeuw is door IBM de **Data Encryption Standard** (**DES**) ontwikkeld. Bij deze versleutelingsmethode wordt gebruik gemaakt van een sleutel van 56 bits met 8 controlebits.

Een bericht, dat met DES gecodeerd wordt, wordt eerst in blokken van 64 bits opgesplitst. Ieder blok wordt in twee helften gedeeld die ieder 16 keer worden gehusseld.



Werking van DES-versleuteling

Bij elke husseling worden de linkerhelft L_i en de rechterhelft R_i door een steeds weer andere sleutel K_i met elkaar versleuteld tot een nieuwe linkerhelft L_{i+1} en de rechterhelft R_{i+1}. Ook hierbij wordt weer gebruik gemaakt van de XOR-functie, die (zoals we bij de Vernam-codering hebben gezien) omgekeerd de ontvangen boodschap weer terugvormt.

Bij de 56-bit sleutel die bij DES wordt gebruikt zijn er wel 70.000.000.000.000.000 mogelijkheden. Dat zorgde ervoor dat de methode in de jaren 70 nog erg betrouwbaar was, maar met het sneller worden van computers minder betrouwbaar werd omdat deze sneller gekraakt kon worden.

Vandaar zijn er in de loop der tijd verbeteringen van DES ontstaan:

- **IDEA** (**International Data Encryption Algorithm)** is een verbeterde versie van DES die met een meer complexe manier van husselen en een 128-bits sleutel werkt.
- **Triple DES (3DES)** is een verbetering van DES die het DES-algoritme drie keer uitvoert en daarbij twee verschillende sleutels gebruikt.
- **AES** (**Advanced Encryption Standard)** gebruikt een andere techniek om de bits door elkaar te husselen, en de sleutel kan een lengte van 128, 192 of 256 bits hebben.

Bij de Caesarmethode, bij DES enz gebruik je voor encryptie en decryptie dezelfde sleutel. Dit wordt **symmetrische encryptie** genoemd. Symmetrische encryptiemethoden zijn vaak snel, maar hebben als nadeel dat er een aparte manier moet worden gevonden om de sleutel tussen de communicerende partijen uit te wisselen, omdat de sleutel geheim moet blijven.

Bij **asymmetrische encryptie** worden er voor codering en decodering met elkaar samenhangende, verschillende sleutels gebruikt. Het uitwisselen van een cryptografische boodschap gaat bij asymmetrische encryptie als volgt:

1. De ontvanger *O* bedenkt twee sleutels, een codeersleutel *E* (encryptie) en een decodeersleutel *D* (decryptie). De decodeersleutel *D* houdt hij geheim.
2. De ontvanger *O* stuurt de codeersleutel *E* naar de zender *Z*.
3. De zender *Z* gebruikt de codeersleutel van *O* en codeert het bericht m hiermee.
4. *Z* stuurt het gecodeerde bericht *E(m)* naar *O*.
5. De ontvanger *O* gebruikt zijn geheime decodeersleutel *D* om het bericht te decoderen: *D(E(m))=m*.

De codeersleutel kan gewoon worden verzonden. Iemand die deze sleutel onderschept heeft er toch niets aan, want hij beschikt niet over de decodeersleutel. We noemen de codeersleutel dan ook wel een publieke sleutel (**public key**) en deze wijze van asymmetrische encryptie **public key encryptie**.

De meest gebruikte methode van public key encryptie is **RSA**, dat in 1977 werd bedacht en vernoemd is naar de bedenkers Ron **R**ivest, Adi **S**hamir en Len **A**dleman

RSA wordt toegepast bij het leggen van een verbinding bij internetbankieren. Vanwege de complexiteit is RSA traag, dus wordt voor verdere gegevensoverdracht gebruik gemaakt van symmetrische encryptie zoals AES.

Bij RSA versleuteling komt veel wiskunde kijken. Om de basis van RSA versleuteling te begrijpen is het voldoende te begrijpen wat priemgetallen en modulo-rekenen inhouden.

Priemgetallen
Een priemgetal is een natuurlijk getal groter dan 1 dat slechts deelbaar is door 1 en door zichzelf. De eerste tien priemgetallen zijn: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Met behulp van grote priemgetallen en hun eigenschappen kunnen boodschappen via public key encryptie worden versleuteld.

Modulo-rekenen
Modulo-rekenen is een manier van geheeltallig rekenen waarbij een getal als bovengrens fungeert. Dit getal noemen we de modulus. Na dit getal begint men weer opnieuw vanaf 0 te tellen. Je zou kunnen zeggen dat onze uurtelling een vorm van modulo-rekenen is. Na 24 uur beginnen we weer opnieuw te tellen.

$51 \equiv 3 \pmod{24}$, want je kunt 2 x 24 van 51 afhalen en de rest is dan 3

Merk op dat we bij modulo-rekenen een bijzonder ≡ ("is identiek aan") teken gebruiken. Bij modulo-rekenen kunnen we met gewone rekenregels optellen, aftrekken, vermenigvuldigen, delen en machtsverheffen.

$13 + 15 \pmod{24}$	$= 28 \pmod{24}$	$\equiv 4 \pmod{24}$
$10 - 12 \pmod{24}$	$= -2 \pmod{24}$	$\equiv 22 \pmod{24}$
$17 \times 5 \pmod{24}$	$= 85 \pmod{24}$	$\equiv 13 \pmod{24}$
$200 / 5 \pmod{24}$	$= 40 \pmod{24}$	$\equiv 16 \pmod{24}$
$21^2 \pmod{24}$	$= (-3)^2 \pmod{24}$	$\equiv 9 \pmod{24}$

Hoe werkt RSA versleuteling?
RSA versleuteling werkt volgens het volgende algoritme:

- Eerst maak je van elk teken een getal door het om te zetten in de bijbehorende ASCII-code. De ASCII-code van WISKUNDE is: 87 73 83 75 85 78 68 69
- Nu kies je twee priemgetallen p en q.
  Normaal gesproken worden daar gigantisch grote getallen voor gekozen, maar dan wordt in dit voorbeeld het rekenwerk erg lastig. Dus wij nemen twee vrij kleine priemgetallen, namelijk $p = 13$ en $q = 23$.
- Vervolgens bereken je het product van p en q: $N = p \cdot q = 13 \cdot 23 = 299$.
  Verder bereken je: $X = (p - 1) \cdot (q - 1) = 12 \cdot 22 = 264$.
- Daarna kies je een getal dat kleiner dan X is (dus kleiner dan 264) en wel zo dat dit getal geen deler heeft die X ook heeft. Dus de grootste gemene deler (ggd) van dit getal en $X = 264$ moet 1 zijn. Daar zijn meestal een heleboel mogelijkheden voor, maar het getal moet niet te klein worden gekozen want hoe kleiner het is hoe gemakkelijker het te kraken is. Dit getal S is de **coderingssleutel**.
  Bijvoorbeeld $S = 259$ voldoet aan de voorwaarden.
  (Die ggd is gemakkelijk met het algoritme van Euclides te berekenen)
- Nu kun je aan het coderen met behulp van de getallen $S = 253$ en $N = 299$.
- Doe elk getal uit de ASCII-gecodeerde tekst tot de macht 259 (mod 299)
- De RSA-code wordt $87^{259 \pmod{299}}\ 73^{259 \pmod{299}}\ 83^{259 \pmod{299}}$ ……$69^{259 \pmod{299}}$
- De berekening van de afzonderlijke getallen gaat als volgt:
  - $87^{259} = 87^{1 + 2 + 256} = 87^1 \times 87^2 \times 87^{256}$
  - $87^2 = 7569$, $7569 : 299 = 25{,}314$, $7569 - 299 \times 25 = 94$, $87^2 \pmod{299} = 94$
  - $94^2 = 8836$, $8836 : 299 = 29{,}552$, $8836 - 299 \times 29 = 165$, $87^4 \pmod{299} = 165$
- Ga na dat: $87^{259} \pmod{299} = 87^1 \times 87^2 \times 87^{256} = 87 \times 94 \times 243 \pmod{299} = 100$
- De letter "W" met ASCII-code 73 krijgt een bijbehorende RSA-code 100

Opdracht 5.5

Wat is de RSA code die hoort bij de letter ‘I’ (ASCII-code 73)

Hoe werkt RSA ontcijfering?
De getallen N en S vormen de **publieke sleutel**. Die mag iedereen weten, dus zo kan iedereen een bericht versleutelen.

Om het gecodeerde woord weer te decoderen heb je de decodeersleutel D nodig.
De decodeersleutel moet voldoen aan de eis: $D \cdot S = 1 \pmod{X}$, dus in dit geval aan

$$D \cdot 259 = 1 \pmod{264}.$$

Volgens de **stelling van Euler** (die we hier verder buiten beschouwing laten) is er altijd zo'n getal te vinden.

Deze D (hier blijkt dat 211 te zijn) is de **geheime sleutel** die alleen bekend is aan degene die moet decoderen. Je decodeert nu door de afzonderlijke cijfers van het geheimschrift tot de macht D (mod 299) te doen. De decodeersleutel hangt echter volgens de bovenstaande eis samen met de codeersleutels N en S.

De letter “W” met ASCII-code 87 had als bijbehorende RSA-code 100.
Met behulp van de decodeersleutel $D = 211$ rekent de ontvanger uit dat $100^{211 \pmod{299}} = 87$

Opdracht 5.6

Ga na dat $100^{211 \pmod{299}} = 87$

Samenvattend kan de ontvanger de getallen N en S bekend maken als publieke sleutels, waarbij $N = p \cdot q$ en ggd($X=(p-1) \cdot (q-1)$, S) = 1 volgen uit de priemgetallen p en q.

De zender kan nu een tekstboodschap coderen volgens het RSA algoritme en verzenden.

De ontvanger kan deze boodschap decoderen met de geheime sleutel D waarvoor geldt:
$D \cdot S = 1 \pmod{X}$.

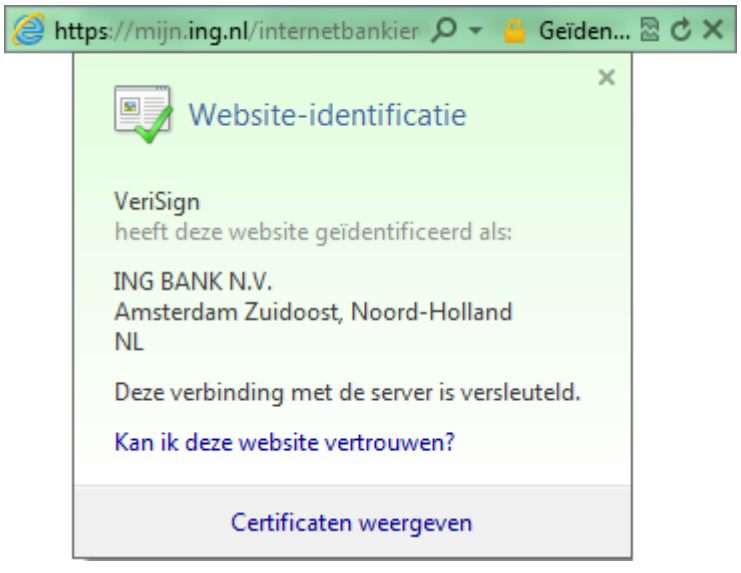
Omdat er in de praktijk gewerkt wordt met grote priemgetallen is de methode nauwelijks te kraken (de geheime sleutel nauwelijks te vinden). De complexe moduloberekeningen maken de RSA versleuteling echter wel traag.

5.3 RSA in de praktijk

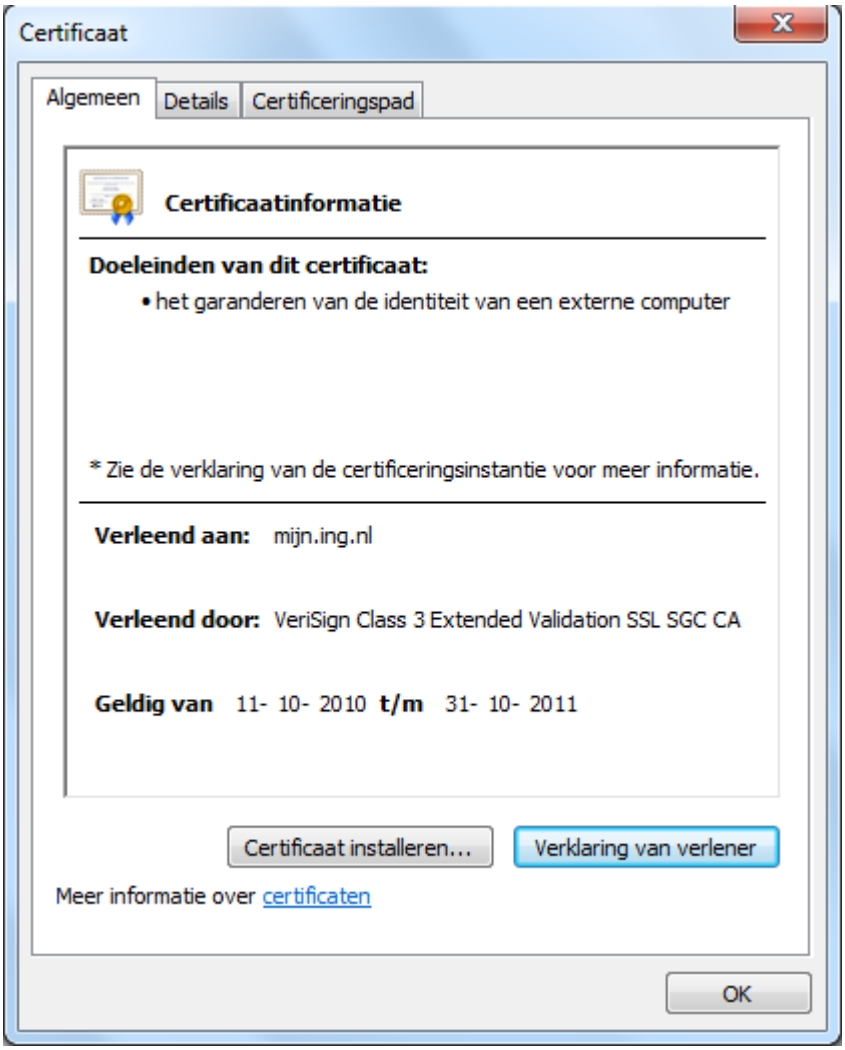
De public keys die bij cryptografietoepassingen worden gebruikt worden uitgegeven door speciale bedrijven. **VeriSign** en **Thawte** zijn voorbeelden van bedrijven die certificaten uitgeven waarin informatie staat over de public key en de eigenaar daarvan. **CACert** is een instelling die gratis werkt. Programma's op je computer die de cryptografie afhandelen kunnen de certificaten opvragen, opslaan en gebruiken.

Als je internetbankiert, bijvoorbeeld bij mijn.ing.nl, kan je de certificaatgegevens opvragen.

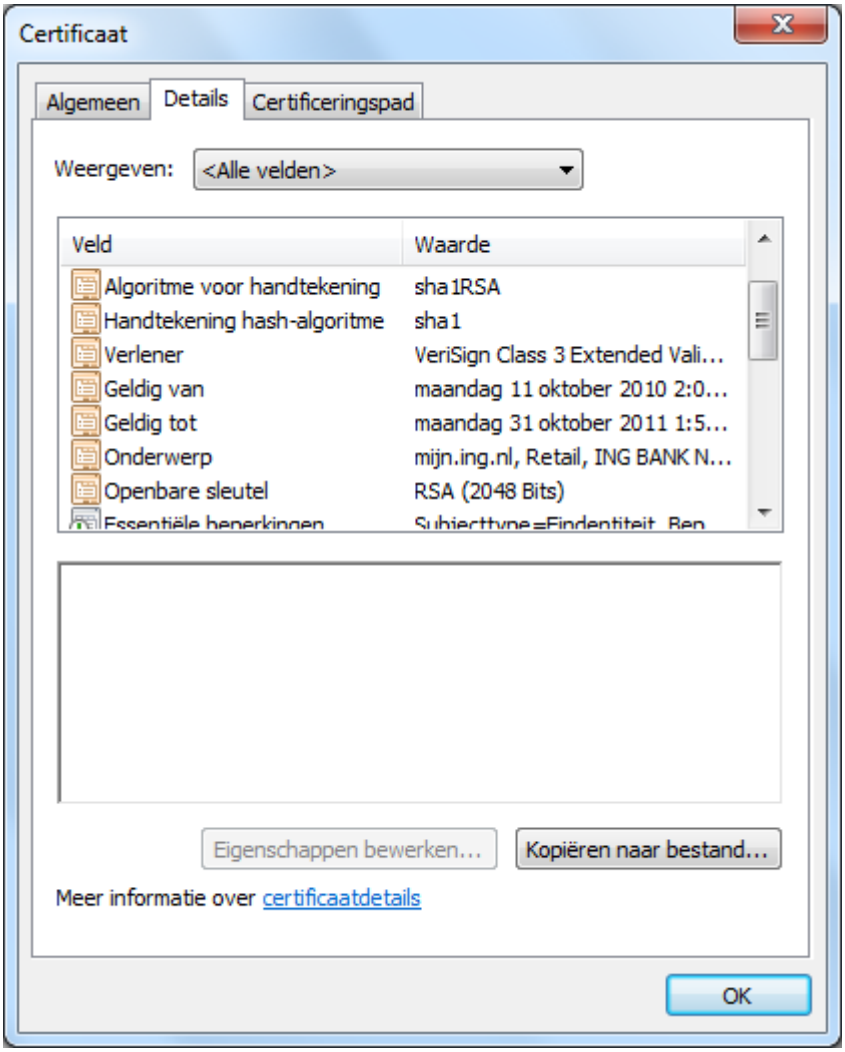
Aan het https:// adres kan je zien dat het protocol **SSL** (**Secure Socket Layer**) of zijn opvolger **TLS** (**Transport Layer Security**) gebruikt wordt om de internetverbinding te beveiligen. Als je op het slotje in het adres klikt, krijg je de certificaatgegevens te zien:



Als je kiest voor “Certificaten weergeven” krijg je onder de algemene gegevens te zien dat VerisSign dit SSL certificaat heeft verleend aan mijn.ing.nl.



Ook kan je de “Details” van het Certificaat opvragen:



Je ziet hier dat er gebruik wordt gemaakt van een 2048 bits RSA sleutel.

Op het moment dat je de verbinding met de “mijn.ing.nl” site maakt stuurt “mijn.ing.nl” een gecodeerd bericht dat er samen met de publieke sleutel van VeriSign voor zorgt dat je op de juiste site terecht komt.

RSA zorgt vervolgens ook voor de overdracht van de sleutel waarmee jij met mijn.ing.nl gaat communiceren. Zodra deze sleutel is uitgewisseld wordt overgeschakeld op AES encryptie, die veel sneller verloopt.

Ook e-mail berichten kunnen met RSA worden versleuteld. Public key encryptiemethoden zoals **PGP** (**Pretty Good Privacy**) en **S/MIME** (**Secure/Multipurpose Internet Mail Extensions**) zijn daar voorbeelden van. PGP en S/MIME maken e-mail berichten en bestanden onleesbaar.

5.4 Samenvatting

Cryptografie is het versleutelen van een boodschap tot geheimschrift om te voorkomen dat de boodschap in verkeerde handen valt.

In de geschiedenis komen we in verschillende culturen voorbeelden tegen:

- de scytale, gebruikt door de Grieken
- de Caesarmethode
- het geheimschrift van Geoffrey Chaucer
- het cijferwiel van Leon Battista Alberti

Het gebruik van deze cryptografische methoden had vaak een militaire of politieke reden.

Bij deze cryptografiemethoden was in het algemeen sprake van **mono-alfabetische substitutie versleuteling**. Iedere letter uit het alfabet wordt in het geheimschrift vervangen door één bijbehorende letter of symbool. Het nadeel van deze methoden is dat via frequentieanalyse de cryptografische sleutel gemakkelijk te vinden is.

Rond 1500 ontstonden de eerste wetenschappelijke werken op het vakgebied van de **cryptologie**, dat bestaat uit de deelgebieden:

- **cryptografie:** het ontwerpen en gebruiken van geheimschriften
- **cryptoanalyse:** het analyseren en breken van geheimschriften.
- **steganografie:** de cryptologische methode die tot doel heeft het bestaan van een bericht te verbergen.

Nieuwe, **poly-alfabetische** versleutelingsmethoden ontstonden, die lastiger te kraken waren.

- de methode van Vigenère
- de Vernam codering
- de Enigma codering

In het moderne tijdperk van datacommunicatie via de computer

- **DES** (**Data Encryption Standard**)
- **IDEA** (**International Data Encryption Algorithm**)
- **3DES**
- **AES** (**Advanced Encryption Standard**)

Bij al deze methoden is sprake van **symmetrische versleuteling**: zender en ontvanger beschikken over dezelfde sleutel. Een voorbeeld van **asymmetrische versleuteling** is **RSA**. Bij RSA, vernoemd naar de bedenkers Ron **R**ivest, Adi **S**hamir en Len **A**dleman stelt de ontvanger een publieke sleutel (**public key**) beschikbaar waarmee de zender zijn boodschap kan versleutelen. Alleen de ontvanger kan de versleutelde boodschap met een geheime sleutel decoderen.

RSA wordt gebruikt door de protocollen **SSL** (**Secure Socket Layer**) of zijn opvolger **TLS** (**Transport Layer Security**) die zorg dragen voor het beveiligen van internetverbindingen en door **PGP** (**Pretty Good Privacy**) en **S/MIME** (**Secure/Multipurpose Internet Mail Extensions**) die zorgen voor het beveiligen van e-mail verkeer.

ANTWOORDEN

Opdracht 5.1
VENI VIDI VICI wordt volgens de Caesarmethode gecodeerd als YHQL YLGL YLFL

Opdracht 5.2

`VR IEN DV RIENDV`	codewoord
`IK ZIE JE MORGEN`	boodschap
`DB HMR MZ DWVTHI`	versleutelde boodschap

Opdracht 5.3
Omdat een letter steeds door een andere letter wordt gecodeerd en de codeletters niet steeds voor dezelfde letter staan, komen deze niet met eenzelfde frequentie voor als in gewone tekst.

Opdracht 5.4
De ontcijfering luidt: MEET ME BEHIND THE GYM AFTER SCHOOL

Opdracht 5.5
Uitgerekend moet worden:

$73^{259} \pmod{299} = 73^1 \times 73^2 \times 73^{256} = 73 \times 246 \times 248 \pmod{299} = 278 \pmod{299}$

Want:

$73^1 \pmod{299} = 73$
$73^2 \pmod{299} = 246$
$73^4 \pmod{299} = 246^2 \pmod{299} = 118$
$73^8 \pmod{299} = 118^2 \pmod{299} = 170$
$73^{16} \pmod{299} = 170^2 \pmod{299} = 196$
$73^{32} \pmod{299} = 196^2 \pmod{299} = 144$
$73^{64} \pmod{299} = 144^2 \pmod{299} = 105$
$73^{128} \pmod{299} = 105^2 \pmod{299} = 261$
$73^{256} \pmod{299} = 261^2 \pmod{299} = 248$

Dus bij een ASCII-code 73 hoort een RSA-code 278.

Opdracht 5.6

$100^{211} \pmod{299} = 100^1 \times 100^2 \times 100^{16} \times 100^{64} \times 100^{128}$
$= 100 \times 133 \times 269 \times 9 \times 81 \pmod{299} = 87$

Want:

$100^1 \pmod{299} = 100$
$100^2 \pmod{299} = 133$
$100^4 \pmod{299} = 133^2 \pmod{299} = 48$
$100^8 \pmod{299} = 48^2 \pmod{299} = 211$
$100^{16} \pmod{299} = 211^2 \pmod{299} = 269$
$100^{32} \pmod{299} = 269^2 \pmod{299} = 3$
$100^{64} \pmod{299} = 3^2 \pmod{299} = 9$
$100^{128} \pmod{299} = 9^2 \pmod{299} = 81$